Jiří Matoušek ● Jaroslav Nešetřil

Kapitoly z diskrétní matematiky

Kapitoly z diskrétní matematiky - skvělá, mnohdy i vyžadovaná, přesto špatně sehnatelná knížka.

Tuhle knížku jsem naleznul v útrobách kolejní sítě, kam jí kdosi neznámý dal naskenovanou dvojstránku po dvojstránce - tímto mu moc děkuji, protože mě by se s tím dělat určitě nechtělo. Co mi ale bylo nepříjemné byl formát - přece jenom, v 300 stranách textu, naskenovaných jenom po dvou, se špatně hledá. Takže jsem dvojstránky rozsekal a převedl do mnohem lepšího (a snad i o něco úspornějšího) PDF.

Omlouvám se všem držitelům autorských práv, ale tahle knížka prostě nejde normálně sehnat.

Jen matematikové dovedli ocenit tuto práci ...

Jiří Matoušek • Jaroslav Nešetřil

Kapitoly z diskrétní matematiky

Univerzita Karlova v Praze
Nakladatelství Karolinum
Praha 2002

Recenzenti: doc. RNDr. Jan Kratochvíl, CSc.
prof. RNDr. Zdeněk Ryjáček, CSc.
RNDr. Jiří Sgall, PhD.

ISBN 80-246-0084-6

Obsah

Předmluva

Čtenář, kterého jsme si při psaní této učebnice představovali, byl studentem prvního ročníku matematiky nebo informatiky. Text je ovšem určen i pro posluchače vyšších ročníků, kterým se dostává úvodního kursu diskrétní matematiky později, a může být užitečný i pro jiné zájemce o snadné a rychlé úvodní poučení o kombinatorice, například pro odborníky z četných oblastí, kde se diskrétní matematika využívá. Hlavně jsme však mysleli na našeho studenta prvního ročníku, a tomu jsme podání přizpůsobili. Ne snad vypuštěním všech těžších věcí, nýbrž hlavně důrazem na některé rysy výkladu:

- *Rozvoj matematického myšlení.* Chceme čtenáře seznámit se základy kombinatoriky a teorie grafů. Hlavně mu ale chceme pomoci naučit se matematickému způsobu myšlení, přesnému formulování myšlenek a řešení matematických problémů vyžadujících více rozmyslu než jen dosazení do vzorečku. Volba konkrétního materiálu pro takovou průpravu patrně není klíčová – uchvacuje-li vás algebra, rozhodně vás od ní nebudeme zrazovat! Domníváme se však, že kombinatorika je pro takové první samostatnější ponoření do matematiky zvlášť vhodná, poněvadž problémy a pojmy v ní studované jsou, přinejmenším ze začátku, elementárnější než např. v matematické analýze, která již od úvodního kursu začíná jako dosti hluboká a jednolitá teorie.

- *Radost.* Kniha je psána pro onoho ideálního čtenáře, který aspoň někdy zažil potěšení z důvtipného řešení matematické úlohy či hádanky. Je ovšem též naším smělým přáním, aby tato kniha pomohla podobný pocit vzbudit u těch, u nichž dosud jen dřímal.

Domníváme se, že taková občasná radost z elegantní myšlenky, někdy dokonce smíšená s pocitem dobře vykonané práce, je pro studium matematiky nesmírně důležitá. Ne každý byl obdařen takovým talentem, stejně jako ne každý má rád hudbu. Ale bez podobného pocitu je studium matematiky nejspíš velmi nudné.

- *Karty na stůl.* Látku se snažíme vyložit v úplnosti. Řekneme-li, že něco je jednoduché, myslíme to vážně, a jestliže to čtenáři při pozorném studiu tak nepřipadá, pak je patrně něco v nepořádku: Možná jsme situaci špatně odhadli, ale možná to naznačuje, že čtenář nepochopil něco z předchozí látky.

- *Souvislosti a aplikace.* Probíraná látka dává několik příležitostí ukázat pojmy a výsledky z jiných oblastí matematiky v akci, a tyto souvislosti se snažíme zdůraznit. Takové partie demonstrují vzájemnou provázanost základních matematických oborů, a podle našich zkušeností je studenti mají rádi, pokud se celá aplikace probere důkladně, včetně připomenutí pojmů z příslušného jiného odvětví.

- *A co informatika?* I když dnes mnoho posluchačů kursů diskrétní matematiky studuje informatiku, chtěli jsme text učinit přístupným i pro ty, jež shledávají počítače a programování odpudivými, a proto jsme se informatické terminologii spíše vyhýbali (např. místo „NP-úplná úloha" říkáme vágněji „algoritmicky těžká úloha"). Přesto kniha obsahuje několik pasáží o efektivních algoritmech, a řadu cvičení na sestavení programů, od krátkých až po menší softwarové projekty.

Náplň. Náš text je úvodem do kombinatoriky a teorie grafů. Vychází z koncepce úvodního kursu diskrétní matematiky pro první ročník matematického a informatického studia na Matematicko-fyzikální fakultě University Karlovy v Praze, vypracované druhým z autorů, a pokrývá látku kursu v podobě, v jaké ho autoři řadu let přednášeli. Okruh témat záměrně není příliš široký, protože považujeme za lepší diskutovat v úvodním kursu několik věcí do větší hloubky než se snažit o encyklopedičnost.

Na druhé straně, v jednosemestrálním kursu se neprobírá celý tento text. Připsali jsme hodně rozšiřujícího (a někdy trochu pokročilejšího) materiálu, hlavně v naději, že čtenář si kromě toho, co je zrovna povinné k přednášce, třeba mimoděk přečte i jiné věci; navíc některé kapitoly slouží aspoň jako úvod k specializovanějším kursům (např. o pravděpodobnostní metodě nebo o aplikacích lineární algebry).

Do tohoto vydání jsme vložili i dodatek shrnující základní pojmy a některé výsledky z lineární algebry. Nemůže samozřejmě nahradit řádný kurs, ale kromě připomenutí základních pojmů může být snad užitečný i pro studium lineární algebry jako jistý pohled z ptačí perspektivy, zdůrazňující věci podstatné.

V jednotlivých částech je rozšiřující nebo specializovanější materiál vyznačen takovýmhle menším písmem. Řadu dalších souvisejících informací jsme se snažili propašovat i do cvičení.

O literatuře. V českém jazyce existuje několik knih o teorii grafů, např. [15], i knihy pojednávající o základech kombinatorického počítání (třeba [20]), ale nemusí být snadno dostupné, a značná část zde probrané látky se patrně najde jen v zahraničních učebnicích.

V citacích neuvádíme zdaleka všechny prameny, z nichž jsme čerpali. Chtěli bychom ale vyzdvihnout (a doporučit) jeden z pramenů, totiž velkou sbírku řešených kombinatorických problémů Lovász [14], odkud jsme převzali část materiálu a část těžších cvičení (naše těžší cvičení jsou Lovászovy lehčí problémy). Tato knížka je vynikající pro pokročilejší studium kombinatoriky, i jako soupis spousty kombinatorických výsledků a metod. Dobrá učebnice kombinatoriky, vhodná jako pokračování našeho spisu, je Van Lint a Wilson [13]. Umění kombinatorického počítání a asymptotických odhadů je znamenitě zpracováno v knize Graham, Knuth, Patashnik [8], nebo též v monografii Knuthově [12]. Dobrá moderní učebnice teorie grafů je např. Diestel [7]. Další zmínky o doporučené literatuře jsou roztroušeny po jednotlivých kapitolách. (Učebnic kombinatoriky existuje spousta, zde jsme jen zmínili některé naše oblíbené.)

O cvičeních. Za jednotlivými částmi najde čtenář větší či menší nabídku cvičení (některá souvisí s probraným tématem jen volně, a

jsou zařazena spíš pro oživení a pro všeobecný matematický rozhled). Uspěchanost moderního života a utváření lidské psychologie asi málokomu dovolí, aby si pro vlastní uspokojení a sebevzdělání systematicky vyřešil větší část z uvedených 332 cvičení, i když by to byla asi nakonec časově nejúspornější cesta, jak probírané věci aktivně zvládnout.

Nezařazovali jsme cvičení zcela rutinní (spočívající v aplikaci nějakého probraného „receptu", např. „aplikujte probraný algoritmus na tento konkrétní graf"), věříme, že takovým způsobem si své porozumění látce může ověřit každý sám (apelujeme ale na vedoucí cvičení, aby takové příklady také zařazovali).

Cvičení jsme se pokusili rozdělit na 3 skupiny obtížnosti (bez hvězdičky, s jednou a se dvěma hvězdičkami). Představujeme si, že dobrý student matematiky by měl po pochopení příslušného článku být schopen vyřešit velkou většinu bezhvězdičkových cvičení. Jednohvězdičková cvičení většinou vyžadují nějaký nápad, na nějž člověk přijít může a nemusí, a konečně dvouhvězdičková (kterých je málo) chtějí asi nápad poměrně neotřelý. Skoro všechna cvičení mají krátké řešení — pokud víme, nikde nejsou potřeba dlouhé a úmorné výpočty. Naše rozdělení podle obtížnosti je ovšem subjektivní, a cvičení, které je pro někoho zcela snadné, protože třeba již viděl nějaký matematický obrat použitelný v podobné situaci, může být pro jiného nepřekonatelné. Do tohoto vydání jsme se rozhodli zařadit i krátké návody na řešení některých cvičení. Zatímco přečtením návodu si čtenář může zkazit radost ze samostatného vyřešení problému, zformulovat úplné řešení i za pomoci návodu dá často ještě hodně práce.

O rejstříku. Pokud se pojem, na nějž se v rejstříku odkazuje, vyskytuje v číslovaném odstavci (např. v definici), číslo tohoto odstavce je v závorce za číslem stránky, něco jako 56(3.2.2). Podobně odkazy na cvičení jsou typu 123(cv. 2). U většiny pojmů, zejména všeobecně matematického charakteru (jako např. relace, graf) rejstřík odkazuje pouze na místo jejich definice. Matematické symboly vytvořené z latinských písmen (např. C_n) jsou zařazeny pod příslušným písmenem, před ostatními slovy. Značení zahrnující speciální symboly (jako $X \setminus Y$, $G \cong H$) a řecká písmena je uvedeno na začátku rejstříku.

Historie. Tento text vznikl na katedře aplikované matematiky Matematicko-fyzikální fakulty University Karlovy Praha. Předběžná verze byla vydána katedrou v menším nákladu v prosinci 1995. První vydání vyšlo v nakladatelství Matfyzpress koncem roku 1996; mělo navíc řadu cvičení a několik odstavců textu. Rozšířená anglická verze byla publikována nakladatelstvím Oxford University Press v roce 1998 pod názvem *Invitation to Discrete Mathematics*. Nyní čtete další české vydání z nakladatelství Karolinum, které se liší od edice v Matfyzpressu zejména odstraněním některých chyb, typografickou úpravou, a několika málo rozšířeními, z nichž nejpodstatnější jsou dodatek o algebře a návody ke cvičením. V dotisku z roku 2002 jsou opraveny další chyby, a navíc je zařazena jedna úvodní sekce.

Autorství některých ilustrací. Obrázky na obálce jsou dílem Jiřího Načeradského a Jaroslava Nešetřila. Úvodní ilustrace je rytina G. Rouxe z knihy Julese Verna: Zmatek nad zmatek, vydané nakladatelem J. Vilímkem v Praze roku 1931.

Poděkování. Mnoho našich spolupracovníků z KAM a studentů spoluvytvářelo příjemnou stimulující atmosféru, v níž se nám dobře psalo. Jan Kratochvíl napsal první verze části 3.3 (za chyby, které jsme tam vyrobili dalším jejím přepracováváním, ovšem nenese žádnou zodpovědnost!). Naši kolegové, vedoucí cvičení a někteří studenti přispěli drobnými připomínkami k textu a náměty na cvičení. Velké množství chyb v předchozích vydáních nalezli zejména Pavel Socha, Eva Matoušková, Tomáš Holan, Robert Babilon, a Jana Chlebíková. Martin Klazar a Jiří Otta sestavili sbírku cvičných příkladů, z nichž většinu jsme použili. Aleš Pultr laskavě přispěl k vylepšení dodatku o algebře několika připomínkami, a Martin Klazar nás upozornil na slabosti jednoho z důkazů i na možnosti nápravy. Jana Chlebíková a Karel Horák velmi pomohli prvnímu autorovi radou při amatérském zápolení s typografií knížky. S Jaroslavem Jirsou a Kamilou Schüllerovou z nakladatelství Karolinum byla radost spolupracovat na přípravě druhého vydání. Všem zmíněným (jakož i těm, na které jsme bez zlého úmyslu mohli zapomenout) děkujeme.

Jménem lidstva též děkujeme Otfriedu Cheongovi za napsání grafického editoru Ipe, jímž byla vyrobena většina obrázků. Zmíněný editor je názorným dokladem významu matematického vzdělání pro zdánlivě nematematické činnosti, jako v tomto případě psaní složitého software — stačí tento teoretickým informatikem napsaný program porovnat s chaotičností mnohého komerčního software.

Prosba na závěr. V každém textu jsou nějaké chyby. Už jsme jich spoustu odstranili, ale určitě ne všechny. Zejména se může stát, že některá cvičení jsou nevhodně formulována, nebo že nefunguje řešení, které jsme si představovali. Prosíme čtenáře, který nějaká nedopatření odhalí, aby je sdělil autorům (e-mail `jiri.matousek@mff.cuni.cz` nebo `jaroslav.nesetril@mff.cuni.cz`). Aktuální seznam objevených chyb vystavujeme na internetové stránce přístupné z adresy `http://kam.mff.cuni.cz/~matousek`.

Praha, leden 2000

Jiří Matoušek *Jaroslav Nešetřil*

1

Základní pojmy a označení

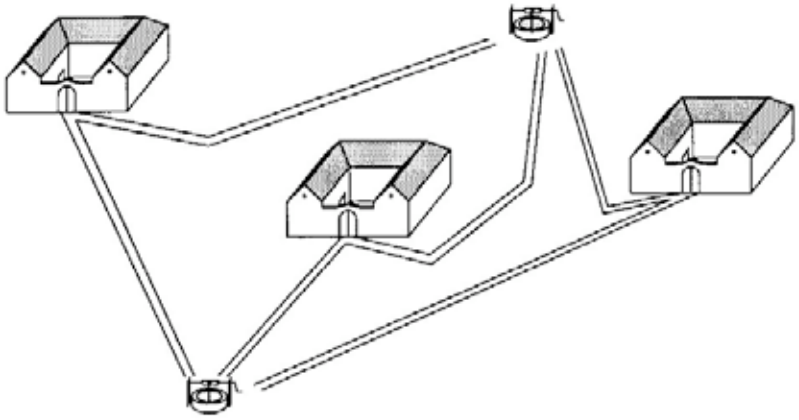
V této úvodní kapitole zavedeme mnoho pojmů. Věříme, že se čtenář jimi nenechá odradit; předpokládáme, že jich většinu dobře zná nebo aspoň již slyšel. Takže vlastně pojmy většinou pouze připomínáme a (hlavně) ukazujeme jejich přirozené souvislosti, různé možné způsoby jejich zavedení a pod. A i když, jakkoliv nepravděpodobně, čtenář nikdy nic podobného neslyšel, jedná se zde o pojmy základní, snadno pochopitelné a názorné.

1.1 Ochutnávka problémů

Nejdříve se podívejme na několik úloh, jimiž se budeme v této knížce zabývat. Zde je zformulujeme jako matematické hádanky, a je dost dobře možné, že se čtenář s některými z nich již setkal v populární literatuře.

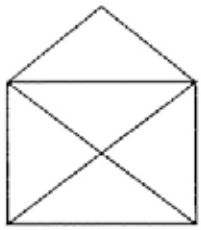
Známý problém pojednává o třech domech a třech studnách. V daleké zemi stály tři pěkné domy, a tři blízké studny jim dávaly čistou chladnou vodu. Všichni tam žili spokojeně, až jednoho dne vypukl spor, a nikdo jej nedokázal rozsoudit. Od každého domu chtěli mít tři cesty, jednu ke každé ze tří studen, a nejen to, s jejich cestami že se nesmí křížit žádná z cest jejich sousedů. Může někdo někdy najít takové cesty?

Kdyby byly studny jenom dvě, řešení by bylo snadné:

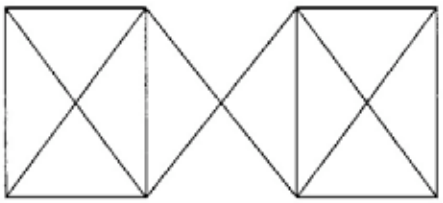


Ale pro tři studny není žádná naděje (pokud by ti zatvrzelci nepřistoupili na chození po mostě nebo tunelem, ale to se asi čekat nedá). Uměli byste úlohu zformulovat jako matematický problém, a třeba dokonce ukázat, proč je neřešitelný?

Tohle byla vpodstatě otázka o kreslení v rovině. Mnoho jiných úloh studovaných v naší knize lze také formulovat pomocí kreslení. Dá se následující obrázek nakreslit jedním tahem, aniž bychom zvedli tužku z papíru, a aniž bychom některou z čar obtáhli vícekrát?



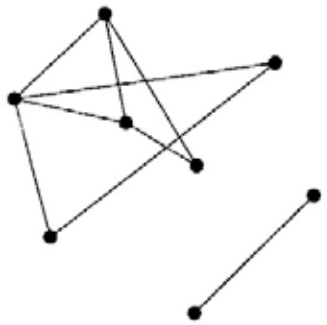
A co tenhle obrázek?



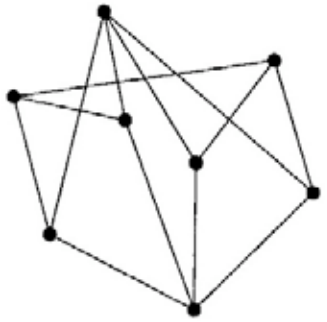
Jestli ne, tak proč? Je nějaký jednoduchý způsob, jak odlišit obrázky, které jdou tak nakreslit, od těch, které nejdou?

K následující sérii problémů si nakreslíme 8 puntíků tak, aby žádné 3 neležely na přímce (číslo 8 je celkem libovolné, obecně bychom mohli

uvažovat n takových puntíků). Spojíme některé dvojice puntíků úsečkami, například takto:

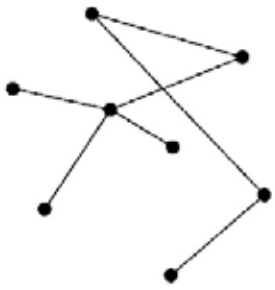


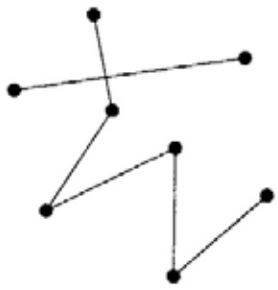
Kolik nanejvýš lze do obrázku s 8 puntíky nakreslit spojnic, když nesmí vzniknout žádný trojúhelník s vrcholy v puntících? Zde je obrázek se 13 spojnicemi:



Dovedete pro 8 puntíků nakreslit větší počet spojnic? Asi ano. Ale uměli byste dokázat, že váš počet už nejde zlepšit?

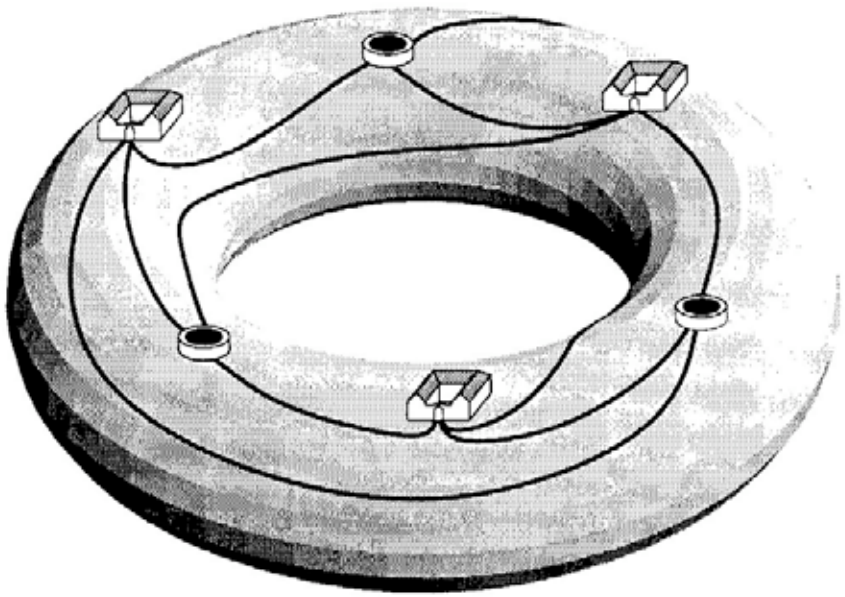
Teď pro změnu chceme nakreslit nějaké spojnice (úsečky) tak, aby se mezi každými dvěma puntíky dalo přejít po cestě, sestávající z nakreslených úseček. Taková cesta nesmí zatáčet mimo puntíky, v místech, kde se úsečky jen kříží. Tedy levý obrázek je správné řešení, zatímco pravý nikoliv:





Jaký je nejmenší počet úseček, které je třeba nakreslit? A kolik existuje různých řešení s tímto minimálním počtem úseček? A jak bychom našli řešení, pro něž je celková délka nakreslených úseček co nejmenší?

Všechny tyhle úlohy jsou populární verze jednoduchých základních otázek *teorie grafů*, což bude jedno z našich hlavních témat (budeme se jí zabývat v kapitolách 3, 4 a 5). Je snadno vidět, že u problémů s 8 puntíky, až na ten poslední, vůbec nesejde na tom, jak jsou puntíky rozmístěny. Záleží jedině na tom, které z dvojic puntíků jsou spojeny a které ne. Většina teorie grafů pojednává o otázkách, které se dají geometricky znázornit, ale v nichž geometrie ve skutečnosti nehraje roli. Naproti tomu úloha o domech a studnách náleží do „opravdu geometrické" části teorie grafů. Je podstatné, že cesty se mají vytýčit v rovině. Kdyby domy a studny byly na maličké planetě tvaru duše z pneumatiky, tak by se požadované cesty daly navrhnout:



Dalším důležitým tématem této knížky je *kombinatorické počítání*, probírané v kapitolách 2 a 10. Úlohy z této oblasti většinou začínají „Kolika způsoby..." nebo nějak podobně. Jednu takovou otázku jsme zmínili v sérii úloh s 8 puntíky (a je to pěkná a nesnadná otázka — je jí zasvěcena celá kapitola 7). Čtenář nepochybně viděl už řadu úloh takového typu. Tady je ještě jedna: Kolika způsoby lze natřít čtyřicetipatrový mrakodrap, když každé ze 40 pater se může natřít buď

zeleně nebo růžově, ale každá dvě růžová patra musejí být oddělena aspoň jedním zeleným?

Ačkoli výše uvedené úlohy mohou vypadat jako pouhé hříčky, každá z nich se dá považovat za výchozí bod zajímavé teorie, s mnoha použitími jak v matematice samé, tak v mnoha jiných odvětvích.

Rozlišit dobré matematické problémy od špatných není snadné. Co je dobrý problém? Je to takový, jehož řešení vede k novým pohledům na známé věci, novým trikům a metodám, či dokonce k celé nové teorii. Mnohé z úloh rekreační matematiky z tohoto hlediska dobré nejsou, i když k jejich vyřešení může být potřeba značný důmysl.

Čtenář může namítnout, že problémy z této sekce jsou pro praxi k ničemu. Proč by se o nich člověk měl učit, když je taková spousta důležitých znalostí, které budou určitě potřeba v budoucím zaměstnání?

Jedna možná odpověď na takové námitky je, že ke každé z uvedených úloh-hříček lze uvést důležitý praktický problém, jehož řešení je založeno na podobných principech. Řekněme, že pošťák má doručit poštu do všech domů v nějaké čtrvti, což znamená aspoň jednou projít každou z ulic. Jaká je nejkratší možná trasa obchůzky? Dá se v rozumném čase najít pomocí stolního počítače? Aby člověk porozuměl tomuto pošťáckému problému, měl by se napřed seznámit s poměrně jednoduchými výsledky o kreslení obrázků jedním tahem.

Podobně úloha o domech a studnách je úvodem například k problémům rozmístění a propojení prvků integrovaného obvodu, a když ji člověk pochopí, je pak mnohem snadnější proniknout do algoritmů pro návrh integrovaných obvodů.

V naší knize se takovými „praktickými" problémy přímo zabývat nebudeme, ale aby člověk porozuměl řešením, popsaným v jiných knihách, nebo dokonce nějaké dobré řešení sám vymyslel, je potřeba se nejdřív seznámit se základními pojmy a myšlenkovými obraty.

Zdůrazněme také, že ačkoliv má matematika odjakživa působivé aplikace, nejkvalitnější matematický výzkum byl zřídkakdy přímo motivován praktickými problémy. Aplikace matematických objevů přicházejí často s velkým časovým odstupem a v překvapivých souvislostech.

K tomuto oddílu nejsou potřeba žádná cvičení. Podaří se vám vyřešit nějakou z uvedených úloh, nebo dokonce všechny?

1.2 Přirozená čísla, množiny

Číselné obory. Pro množinu všech přirozených čísel, t.j. množinu $\{1, 2, 3, \ldots\}$, vyhradíme symbol $\mathbf{N}$. Písmena n, m, k, i, j, p (a případná další) budou většinou rezervována pro přirozená čísla.

Pomocí přirozených čísel se konstruují další, větší číselné obory: čísla celá, racionální a reálná (a také čísla komplexní, ale ta téměř potřebovat nebudeme).

Celá čísla vzniknou z přirozených čísel přidáním záporných čísel a nuly. Množinu všech celých čísel označíme $\mathbf{Z}$. *Racionální čísla* jsou zlomky s celočíselným čitatelem a jmenovatelem; zpravidla se značí písmenem $\mathbf{Q}$, ale v tomto textu pro ně žádný symbol zavádět nepotřebujeme. Konstrukce množiny $\mathbf{R}$ všech *reálných* čísel je složitější a probírá se zpravidla v úvodním kursu analýzy. Známými příklady reálných čísel, jež nejsou racionální, jsou čísla jako $\sqrt{2}$, některé důležité konstanty jako π, a obecně čísla mající v dekadickém zápisu za desetinnou čárkou nekonečnou a neperiodickou posloupnost číslic, třeba $0.12112111211112\ldots$. *Uzavřený interval* od a do b na reálné ose budeme značit $[a, b]$, *otevřený interval* s týmiž koncovými body zapisujeme (a, b).

Operace s čísly. Většina označení pro číselné operace, jako například $+$ pro sčítání, $\sqrt{}$ pro odmocninu atd., je všeobecně známa. *Dělení* budeme zapisovat buď zlomkovou čarou, nebo někdy (pro úsporu místa) lomítkem, tedy ve tvaru $\frac{a}{b}$ nebo a/b.

Zavedeme dvě méně běžné funkce. Pro reálné číslo x se symbol $\lfloor x \rfloor$ nazývá[1] *dolní celá část* x a jeho hodnota je největší celé číslo, které je menší nebo rovno x. Podobně $\lceil x \rceil$, *horní celá část* x, označuje nejmenší celé číslo, které je větší nebo rovno x. Tak například: $\lfloor 0.999 \rfloor = 0$, $\lfloor -0.1 \rfloor = -1$, $\lceil 0.01 \rceil = 1$, $\lceil \frac{17}{3} \rceil = 6$, $\lfloor \sqrt{2} \rfloor = 1$.

Později zavedeme další číselné funkce a symboly, které budeme pro jejich kombinatorický význam zkoumat podrobněji. Patří sem např. $n!$, $\binom{n}{k}$, $\check{s}(n)$.

Sumy a součiny. Jsou-li $a_1, a_2, \ldots, a_n$ reálná čísla, jejich součet

[1] Zejména ve starší literatuře se někdy ve stejném významu používá symbol $[x]$.

$a_1 + a_2 + \cdots + a_n$ se zapisuje také pomocí *sumačního znaménka* $\sum$, ve tvaru

$$\sum_{i=1}^{n} a_i.$$

Tento zápis je trochu podobný `FOR` cyklu z různých programovacích jazyků. Ještě několik příkladů jeho použití:

$$\sum_{j=2}^{5} \frac{1}{2j} = \frac{1}{4} + \frac{1}{6} + \frac{1}{8} + \frac{1}{10}$$

$$\sum_{i=2}^{5} \frac{1}{2j} = \frac{1}{2j} + \frac{1}{2j} + \frac{1}{2j} + \frac{1}{2j} = \frac{2}{j}$$

$$\sum_{i=1}^{n}\sum_{j=1}^{n}(i+j) = \sum_{i=1}^{n}((i+1)+(i+2)+\cdots+(i+n)) =$$

$$\sum_{i=1}^{n}(ni + (1+2+\cdots+n)) = n\left(\sum_{i=1}^{n} i\right) + n(1+2+\cdots+n)$$

$$= 2n(1+2+\cdots+n).$$

Podobně jako součty se zapisují pomocí $\sum$ (což je velké řecké písmeno „sigma“, od slova *s*uma), součiny se vyjadřují užitím znaménka $\prod$ (velké řecké písmeno „pí“, od slova *p*rodukt), kupříkladu

$$\prod_{i=1}^{n} \frac{i+1}{i} = \frac{2}{1} \cdot \frac{3}{2} \cdot \cdots \cdot \frac{n+1}{n} = n+1.$$

Množiny. Jiným základním pojmem, který budeme používat, je pojem množiny. S tímto pojmem jste se patrně setkali již na střední škole (a díky snaživosti pedagogických modernizátorů možná i na základní škole). Množiny budeme označovat zpravidla pomocí písmen velké abecedy:

$$A, B, \ldots, X, Y, \ldots, M, N, \ldots$$

a podobně, a prvky množin budeme značit většinou malými písmeny $a, b, \ldots, x, y, \ldots, m, n, \ldots$.

Skutečnost, že množina X obsahuje prvek x, se označuje tradičně pomocí symbolu $\in$ (což je trochu stylizované řecké písmeno ε — „epsilon"); $x \in X$ čteme „x (je) prvkem X".

Je třeba si uvědomit, že pojem množiny a symbol „$\in$" nedefinujeme (pomocí jiných, dříve zavedených pojmů). Jsou to tzv. primitivní pojmy. Předpokládáme, že ve všech konkrétních případech bude smysl uvažovaných množin a jejich prvků jasný. Jak se ukázalo začátkem století, používá-li se pojem množiny zcela svobodně a bezuzdně, může to vést k různým podivným situacím, tzv. paradoxům[2]. V tomto textu se však něčeho takového obávat nemusíme, většina námi uvažovaných množin bude mít dokonce konečný počet prvků.

Množina s prvky 1, 37 a 55 se zapíše $\{1, 37, 55\}$. To i zápisy $\{37, 1, 55\}$ a $\{1, 37, 1, 55, 55, 1\}$ znamenají všechny totéž (tedy vícenásobný výskyt téhož prvku se ignoruje, týž prvek se nemůže v jedné množině vyskytovat dvakrát). Tři tečky v zápisu množiny $\{2, 4, 6, 8, \ldots\}$ znamenají ovšem „a dále podobně, podle stejné zákonitosti", t.j. v uvedeném případě množinu všech sudých přirozených čísel (příslušná zákonitost by ovšem měla být na první pohled patrná, tak například $\{2^1, 2^2, 2^3, \ldots\}$ je srozumitelné jako množina všech mocnin dvojky, $\{2, 4, 8, \ldots\}$ je už možná srozumitelné méně).

Složitější a zajímavější množiny se zpravidla tvoří ze známých množin pomocí nějakého pravidla. Množinu všech druhých mocnin přirozených čísel bychom mohli zapsat například

$$\{i^2;\ i \in \mathbf{N}\}$$

nebo taky

$$\{n \in \mathbf{N};\ \text{existuje } k \in \mathbf{N} \text{ tak, že } k^2 = n\}$$

či totéž pomocí symbolu $\exists$ pro „existuje"

$$\{n \in \mathbf{N};\ \exists k \in \mathbf{N} : k^2 = n\}.$$

[2]Nejznámější je asi tzv. paradox holiče: vojenský holič má holit všechny vojáky, kteří se neholí sami — má se, jakožto jeden z vojáků, holit, nebo ne? To se dá přeložit do matematické řeči a ukazuje to spornost pojmů jako „množina všech množin" a podobně.

Důležitá je množina neobsahující žádný prvek. Taková množina existuje pouze jedna a je zvykem ji značit $\emptyset$ a nazývat *prázdná množina*. Poznamenejme, že prázdná množina může být prvkem jiné množiny. Například, $\{\emptyset\}$ je množina, obsahující prázdnou množinu jako prvek, a není to tedy totéž jako $\emptyset$!

Počet prvků, neboli *mohutnost* množiny X budeme značit symbolem $|X|$ (jako absolutní hodnota). Cizím slovem se mohutnosti říká také *kardinalita*. Mohutnost se definuje i pro nekonečné množiny; my ji ale budeme uvažovat jen pro množiny konečné.

V matematice máme dost často co dělat s množinami, jejichž prvky jsou jiné množiny. Můžeme třeba definovat množinu

$$M = \{\{1,2\},\{1,2,3\},\{2,3,4\},\{4\}\},$$

jejímiž prvky jsou 4 množiny přirozených čísel, přesněji řečeno 4 podmnožiny množiny $\{1,2,3,4\}$. V diskrétní matematice se s takovými množinami setkáváme běžně. Aby se nemuselo říkat „množina množin", používá se někdy výraz *množinový systém*[3], řekli bychom tedy, že M je systém množin na množině $\{1,2,3,4\}$. Takové množiny množin neboli množinové systémy se někdy označují ozdobnými typy velkých písmen, třeba $\mathcal{M}$. Je ale vidět, že takové rozlišení pomocí typů písma nemůže být úplně důsledné, co třeba když bychom narazili na množinu množin množin?

Množinu všech možných podmnožin nějaké množiny X budeme značit symbolem 2^X. (Jiné v literatuře běžné označení je $\mathcal{P}(X)$, písmeno $\mathcal{P}$ je od anglického „power set").

Obecnější zápis sum a součinů. Někdy je výhodný obecnější způsob zápisu sumy než podle vzoru $\sum_{i=1}^{n} a_i$. Například

$$\sum_{i\in\{1,3,5,7\}} i^2$$

znamená součet $1^2+3^2+5^2+7^2$; pod sumační znaménko se napíše nejdříve proměnná, podle které se sčítá, a potom se nějakým způsobem zapíše množina hodnot, přes něž se sčítá. Ve způsobu zápisu

[3] V angličtině se někdy používá roztomilejší výraz *family of sets*, tedy rodina množin.

této množiny je značná libovůle, někdy se může i zčásti popsat slovy. Třeba:

$$\sum_{\substack{i;1\le i\le 10\\ i \text{ prvočíslo}}} i = 2+3+5+7.$$

Pokud je množina hodnot, přes kterou se má sčítat, prázdná, definuje se hodnota sumy jako 0, tedy například

$$\sum_{i=1}^{0}(i+10) = 0\,, \qquad \sum_{\substack{i\in\{2,4,6,8\}\\ i \text{ liché}}} i^4 = 0.$$

Podobný „množinový zápis" můžeme uplatnit i pro součiny. Prázdný součin, například $\prod_{j;2\le j<1} 2^j$, se definuje jako 1 (tedy ne 0 jako pro prázdnou sumu).

Operace s množinami. Pomocí primitivního pojmu náležení, $\in$, můžeme definovat další vztahy mezi množinami a operace s nimi. Tak například dvě množiny X a Y budeme pokládat za stejné (totožné), jestliže mají stejné prvky. V tom případě budeme psát $X = Y$.

Vztah $X = Y$ tedy definujeme pomocí platnosti výroku „pro každý prvek x platí: $x \in X$, právě když $x \in Y$". Tento výrok můžeme symbolicky zapsat

$$\forall x : (x \in X \Leftrightarrow x \in Y),$$

ale tímto směrem se nebudeme ubírat. Formální (formalizované) teorii množin jsou věnovány jiné texty (v češtině např. kniha Balcara a Štěpánka [3]).

Podobným způsobem můžeme definovat další množinové vztahy. Jsou-li X, Y množiny, znamená $X \subseteq Y$ (slovy „X je podmnožinou Y") to, že každý prvek X je také prvkem Y.

Pomocí $X \subset Y$ se někdy vyznačuje, že X je podmnožina Y, přičemž ale X není rovno Y. Toto značení nebývá v literatuře zcela jednotné.

Průnik množin X a Y, čili množinu všech prvků náležejících zároveň do X i do Y, píšeme $X \cap Y$. Zápis $X \cup Y$ znamená *sjednocení* X a Y, což je množina všech prvků ležících v X nebo v Y (či v obou zároveň!). Chceme-li vyznačit, že sjednocujeme disjunktní množiny X a Y (t.j.

$X \cap Y = \emptyset$), píšeme $X \dot{\cup} Y$. Výraz $X \setminus Y$ je *rozdíl* množin X a Y, t.j. množina všech prvků ležících v X a nikoliv v Y.

Zvětšené symboly $\cup$ a $\cap$ se používají podobně jako symboly $\sum$ a $\prod$. Jsou-li tedy $X_1, \ldots, X_n$ množiny, můžeme jejich sjednocení napsat

$$\bigcup_{i=1}^{n} X_i \tag{1.1}$$

a podobně pro průnik.

Uvědomte si, že tento zápis je možný (nebo korektní, správný) jen díky tomu, že operace sjednocení a průniku množin jsou *asociativní*. Jinými slovy, že platí (pro každou trojici množin X, Y, Z) vztahy

$$X \cap (Y \cap Z) = (X \cap Y) \cap Z,$$

$$X \cup (Y \cup Z) = (X \cup Y) \cup Z.$$

V důsledku toho nezávisí na způsobu „uzávorkování" sjednocení (libovolných) tří, a obecně n, množin, takže můžeme společnou hodnotu označit symbolem (1.1). Operace $\cup$ a $\cap$ jsou ovšem i *komutativní*, neboli splňují vztahy

$$X \cap Y = Y \cap X,$$

$$X \cup Y = Y \cup X.$$

Komutativita a asociativita operací $\cup$ a $\cap$ je doplněna ještě jejich *distributivitou:*

Jestliže X, Y, Z jsou množiny, potom platí:

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z),$$

$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z).$$

Platnost těchto vztahů můžeme ověřit např. pomocí Vennova diagramu pro příslušné tři množiny. Zmíněné vztahy je možno zobecnit na více množin (dokážou se indukcí, viz oddíl 1.3). Např. takto

$$A \cap \left(\bigcup_{i=1}^{n} X_i \right) = \bigcup_{i=1}^{n} (A \cap X_i) \quad \text{nebo}$$

$$A \cup \left(\bigcap_{i=1}^{n} X_i \right) = \bigcap_{i=1}^{n} (A \cup X_i)$$

Jiné populární vztahy pro množiny jsou

$$X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B) \quad \text{a} \quad X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$$

(tzv. *de Morganovy vzorce*), a jejich zobecnění na více množin

$$X \setminus \left(\bigcup_{i=1}^{n} A_i \right) = \bigcap_{i=1}^{n} (X \setminus A_i)$$

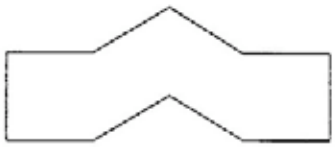
$$X \setminus \left(\bigcap_{i=1}^{n} A_i \right) = \bigcup_{i=1}^{n} (X \setminus A_i).$$

Cvičení

1. Které z následujících vztahů jsou správné?
   (a) $\lfloor \frac{(n+1)^2}{2} \rfloor = \lfloor \frac{n^2}{2} \rfloor + n$,
   (b) $\lfloor \frac{n+k}{2} \rfloor = \lfloor \frac{n}{2} \rfloor + \lfloor \frac{k}{2} \rfloor$,
   (c) $\lceil (\lfloor x \rfloor) \rceil = \lceil x \rceil$ (pro reálné číslo x),
   (d) $\lceil (\lfloor x \rfloor + \lfloor y \rfloor) \rceil = \lfloor x \rfloor + \lfloor y \rfloor$.
2. (a) Pro která přirozená čísla n je pravda, že jejich zápis v desítkové soustavě má $\lceil \log_{10} n \rceil$ číslic?
   (b) Najděte „správnou" formuli pro počet číslic v desítkovém zápisu čísla n.
3.* Dokažte, že pro každé reálné číslo $x > 0$ platí $\lfloor \sqrt{x} \rfloor = \lfloor \sqrt{\lfloor x \rfloor} \rfloor$.
4. Zapište výraz
$$\bigcap_{i=1}^{n} \bigcup_{j=1}^{m} A_{ij}$$
   jako sjednocení průniků.
5. (a) Podejte definici „uzávorkování" sjednocení n množin $\bigcup_{i=1}^{n} X_i$ a „uzávorkování" součtu n čísel $\sum_{i=1}^{n} a_i$.
   (b) Dokažte, že každá dvě uzávorkování výrazu $\bigcap_{i=1}^{n} X_i$ dávají stejný výsledek.
   (c) Kolika způsoby lze uzávorkovat sjednocení 4 množin $A \cup B \cup C \cup D$?
   (d)** Pokuste se odvodit, kolika způsoby lze uzávorkovat sjednocení n množin $\bigcup_{i=1}^{n} X_i$.

6. Je pravda, že pro každé dvě množiny X a Y platí $2^X = 2^Y$ právě když $X = Y$?

7. Na následující úloze si můžete otestovat svou schopnost nacházet jednoduchá leč skrytá řešení. Rozdělte následující obrazec na 7 navzájem shodných částí (všechny ohraničující úsečky mají délku 1 a úhly jsou 90, 120 a 150 stupňů).



1.3 Matematická indukce

Řekněme, že chceme spočítat třeba součet

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^n = \sum_{i=0}^{n} 2^i$$

(a že si nevybavujeme vzorec pro součet geometrické posloupnosti). Výpočtem číselných hodnot pro několik malých hodnot n můžeme odhalit, že uvedený součet bude nejspíš roven $2^{n+1} - 1$. I kdybychom to ale ověřili na počítači pro miliony konkrétních hodnot n, nebude to ještě důkaz. Správnost tohoto vztahu pro všechna n se dá ukázat tzv. *matematickou indukcí* (jiný používaný název je *úplná indukce*). V tomto případě bychom postupovali takto:

1. Vztah $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ je správný pro $n = 1$, jak se přesvědčíme dosazením.

2. Předpokládejme, že uvedený vztah platí pro nějakou hodnotu $n = n_0$. Dokážeme, že platí i pro $n = n_0 + 1$. Skutečně,

$$\sum_{i=0}^{n_0+1} 2^i = \left(\sum_{i=0}^{n_0} 2^i \right) + 2^{n_0+1};$$

suma v závorce je podle předpokladu rovna $2^{n_0+1} - 1$, takže

$$\sum_{i=0}^{n_0+1} 2^i = 2^{n_0+1} - 1 + 2^{n_0+1} = 2 \times 2^{n_0+1} - 1 = 2^{n_0+2} - 1.$$

To je ale požadovaný vztah pro $n = n_0 + 1$.

Tím jsme dokázali platnost vztahu pro libovolné n: Podle kroku 1 totiž vztah platí pro $n = 1$, podle kroku 2 platí i pro $n = 2$ (použijeme krok 2 s $n_0 = 1$), opět podle kroku 2 platí pro $n = 3, \ldots$, a takto můžeme pokračovat libovolně daleko.

Krok 2 v tomto typu důkazu se jmenuje *indukční krok*. Předpoklad, že dokazované tvrzení již platí pro nějaké $n = n_0$, se nazývá *indukční předpoklad*.

Obecně se princip matematické indukce dá formulovat například takto:

1.3.1 Tvrzení. *Nechť X je množina přirozených čísel, pro niž platí:*

(i) Číslo 1 je prvkem X.

(ii) Je-li číslo n prvkem X, potom rovněž číslo $n + 1$ je prvkem X.

Potom X je množina všech přirozených čísel (tedy $X = \mathbf{N}$).

V aplikacích bude X množina všech n, pro něž platí dokazované tvrzení.

Schéma důkazu indukcí má mnoho různých obměn. Například, chceme-li nějaké tvrzení dokazovat pro všechna $n \geq 2$, bude první krok důkazu patrně ověření platnosti tvrzení pro $n = 2$. Jako indukční předpoklad můžeme někdy využívat nejen platnosti tvrzení pro $n = n_0$, ale i pro všechna $n \leq n_0$. A tak dále.

Matematickou indukci můžeme pokládat buď za základní vlastnost přirozených čísel (t.j. axiom, který nedokazujeme), nebo ji můžeme dokázat z jiné základní vlastnosti (axiomu), totiž že každá neprázdná podmnožina přirozených čísel má nejmenší prvek (to se vyjadřuje obratem, že uspořádání přirozených čísel podle velikosti je *dobré uspořádání*).

Důkaz tvrzení 1.3.1 z vlastnosti dobrého uspořádání: Předpokládejme pro spor, že X splňuje (i) a (ii), ale neobsahuje všechna přirozená čísla. Nechť tedy přirozené číslo n nenáleží X. Mezi všemi takovými přirozenými čísly n (nenáležejícími X) zvolme číslo nejmenší a označme ho n_0. Podle podmínky (i) víme, že $n_0 > 1$, a protože n_0 bylo minimální, je číslo $n_0 - 1$ prvkem množiny X. Použitím (ii) však dostaneme, že n_0 je prvkem X, což je spor. □

Poznamenejme, že tento typ úvahy, kde řekneme „Nechť n_0 je nejmenší číslo, pro které dokazované tvrzení neplatí" a odvodíme spor — jmenovitě že musí existovat ještě menší číslo, pro nějž tvrzení neplatí — někdy nahrazuje matematickou indukci. Oba způsoby (právě zmíněný a matematická indukce) vpodstatě dělají totéž, a který z nich použijeme je hlavně věc vkusu.

Matematickou indukci budeme často používat, bude to jeden z našich základních důkazových prostředků. Spoustu příkladů a cvičení na indukci najde tedy čtenář v dalších kapitolách.

Cvičení

1. Dokažte indukcí vztahy
   (a) $1 + 2 + 3 + \cdots + n = n(n+1)/2$
   (b) $\sum_{i=1}^{n} i2^i = (n-1)2^{n+1} + 2$.
2. Čísla $F_0, F_1, F_2, \ldots$ jsou zadána takto: $F_0 = 0$, $F_1 = 1$, $F_{n+2} = F_{n+1} + F_n$ pro $n = 0, 1, 2, \ldots$. Dokažte, že pro každé $n \geq 0$ platí $F_n \leq ((1+\sqrt{5})/2)^{n-1}$ (viz též část 10.3).
3. (a) Nakresleme n přímek v rovině tak, že žádné 2 nejsou rovnoběžné a žádné 3 se neprotínají v jednom bodě. Dokažte, že rovina je tím rozdělena na přesně $n(n+1)/2 + 1$ částí.
   (b)* Podobně uvažte n rovin v trírozměrném prostoru, z nichž každé 3 mají právě jeden společný bod a žádné 4 nemají společný bod. Zjistěte, na kolik oblastí rozdělují prostor.
4. Dokažte indukcí *de Moivreovu větu*: $(\cos\alpha + i\sin\alpha)^n = \cos(n\alpha) + \mathrm{i}\sin(n\alpha)$ (kde i je imaginární jednotka, $\mathrm{i}^2 = -1$).
5.* Nechť $M \subseteq \mathbf{R}$ je množina reálných čísel taková, že každá její neprázdná podmnožina má nejmenší prvek a také největší prvek. Dokažte, že M je nutně konečná.

6. Dokážeme indukcí následující tvrzení: *Nechť $p_1, p_2, \ldots, p_n$ je $n \geq 2$ různých přímek v rovině, žádné 2 nejsou rovnoběžné. Potom všechny tyto přímky mají společný bod.*

   1. Pro $n = 2$ tvrzení platí, protože každé 2 různoběžné přímky se protínají.

   2. Nechť tvrzení platí pro $n = n_0$, mějme $n = n_0 + 1$ přímek $p_1, \ldots, p_n$. Podle indukčního předpokladu mají všechny přímky kromě poslední, t.j. $p_1, p_2, \ldots, p_{n-1}$, společný nějaký bod, označme jej x. Podobně přímky $p_1, p_2, \ldots, p_{n-2}, p_n$ mají společný bod, označíme jej y. Přímka p_1 leží v obou skupinách, proto obsahuje jak x, tak y. Totéž platí pro přímku p_{n-2}. Poněvadž jsou p_1 a p_{n-2} podle předpokladu různoběžné a tedy se protínají jen v jednom bodě, platí $x = y$. Tedy všechny přímky $p_1, \ldots, p_n$ mají společný bod.

   Kde je zádrhel?

7. Obyvatelé staroegyptské říše zapisovali zlomky jako součty zlomků s čitatelem 1, např. $\frac{3}{5} = \frac{1}{2} + \frac{1}{10}$. Uvažte následující algoritmus pro zápis zlomku $\frac{m}{n}$ v tomto tvaru ($1 \leq m < n$): napiš zlomek $\frac{1}{\lceil n/m \rceil}$, vypočítej zlomek $\frac{m}{n} - \frac{1}{\lceil n/m \rceil}$, a je-li nenulový, vyjádři jej v požadovaném tvaru týmž algoritmem. Dokažte, že tento algoritmus vždy skončí.

1.4 Relace

Je pozoruhodné, jak mnoho matematických pojmů je možno vyjádřit pomocí množin a rozličných množinových konstrukcí. Je to nejen pozoruhodné, ale i překvapivé, neboť teorie množin, a dokonce pojem množiny, jsou pojmy zařazené do matematiky vlastně nedávno, a ještě před 100 lety byla teorie odmítána i některými předními vědci. Dnes se však teorie množin stala součástí běžného matematického vyjadřování, stala se jazykem matematiky (a matematiků), jazykem, který napomohl chápat současnou matematiku při vší její různorodosti jako jeden celek se společnými základy.

Ukažme si, jak pomocí nejjednodušších množinových prostředků můžeme definovat další matematické pojmy.

Jestliže x a y jsou prvky (nějaké množiny), potom symbol $\{x, y\}$ označuje množinu obsahující právě prvky x a y, a nazývá se *neuspořádaná dvojice* prvků x a y. Připomeňme, že $\{x, y\}$ je totéž jako $\{y, x\}$, a pokud $x = y$, potom $\{x, y\}$ je jednoprvková množina.

Zavedeme rovněž označení (x, y) pro *uspořádanou dvojici* prvků x a y. Při této konstrukci závisí na pořadí prvků x a y. Předpokládáme tedy, že platí

$$(x, y) = (z, t) \text{ právě když } x = z \text{ a } y = t. \tag{1.2}$$

Je zajímavé, že uspořádanou dvojici lze již vytvořit pomocí pojmu neuspořádané dvojice, následovně:

$$(x, y) = \{\{x\}, \{x, y\}\}.$$

Ověřte, že takto definované uspořádané dvojice splňují podmínku (1.2). V tomto textu však bude pro nás jednodušší považovat (x, y) za další primitivní (tedy známý) pojem.

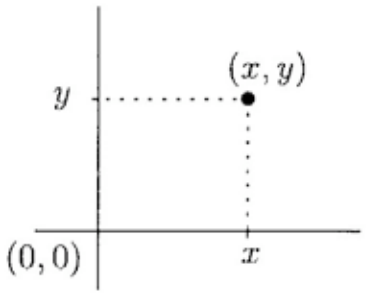
Podobně definujeme *uspořádanou n-tici* prvků $x_1, \ldots, x_n$, již označujeme[4] $(x_1, \ldots, x_n)$.

1.4.1 Definice. *Nechť X a Y jsou množiny. Symbolem $X \times Y$ označíme množinu všech uspořádaných dvojic tvaru (x, y), kde $x \in X$ a $y \in Y$. Formálně zapsáno*

$$X \times Y = \{(x, y);\ x \in X,\ y \in Y\}.$$

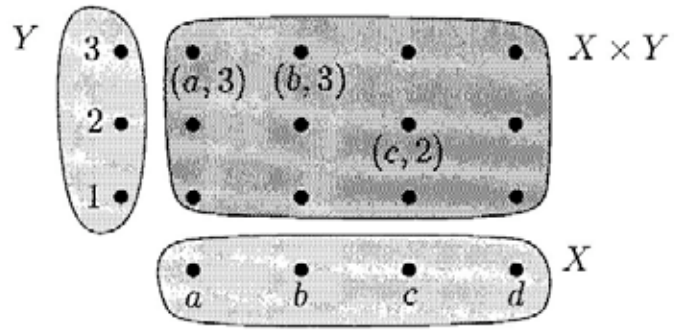
$X \times Y$ se nazývá (kartézský) součin *množin X a Y.*

Název „kartézský součin" pochází z geometrické interpretace (a původně tedy ze jména Descartes): Když např. $X = Y = \mathbf{R}$, potom $X \times Y$ můžeme interpretovat jako všechny body roviny, a v tomto případě x a y jsou (kartézské) souřadnice bodu (x, y) roviny:



[4] Stejný zápis používáme i pro n-rozměrný vektor se složkami $x_1, \ldots, x_n$, jsou-li x_i např. reálná nebo komplexní čísla.

Tohoto názoru používáme nejenom pro číselné množiny, ale například i pro kartézský součin konečných množin:



Kartézský součin $X \times X$ někdy zapisujeme jako mocninu, t.j. X^2, a podobně $X^3 = X \times X \times X$ atd.

Dostáváme se nyní k jednomu z klíčových pojmů celé matematiky. Pojem relace, který nyní zavedeme, zobecňuje tak rozdílné pojmy, jako jsou ekvivalence, funkce a uspořádání.

1.4.2 Definice. Relace[5] *R je množina uspořádaných dvojic. Jsou-li X a Y množiny, nazývá se libovolná podmnožina kartézského součinu* $X \times Y$ relací mezi X a Y. *Zdaleka nejdůležitější případ je $X = Y$, v takovém případě mluvíme o* relaci na X, *což je tedy libovolná podmnožina $R \subseteq X^2$.*

Náleží-li dvojice (x, y) relaci R, t.j., $(x, y) \in R$, říkáme také, že x a y *jsou v relaci* R, a zapisujeme též xRy.

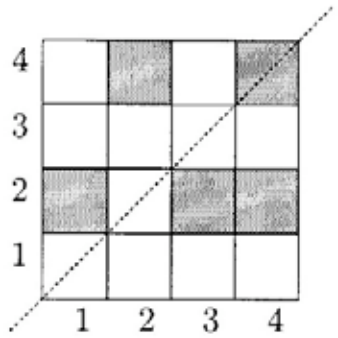
Jako relace v tomto smyslu můžeme interpretovat některé čtenáři dobře známé symboly. Tak například, „=“ (rovnost) i „$\geq$“ (neostrá nerovnost) jsou relace na množině $\mathbf{N}$ všech přirozených čísel. První z nich sestává z dvojic $(1,1), (2,2), (3,3), \ldots$, druhá z dvojic $(1,1), (2,1), (2,2), (3,1), (3,2), (3,3), (4,1), \ldots$. Mohli bychom tedy psát i třeba $(5,2) \in \geq$ místo $5 \geq 2$, což ovšem neděláme. Všimněte si, že jsme museli říci, na jaké množině např. relaci $\geq$ uvažujeme; jako relace třeba na $\mathbf{R}$ by to byla jiná množina dvojic.

Slovo „relace“ pochází z kořene znamenajícího „(příbuzenský) vztah“. Příbuzenské vztahy (např. „býti matkou“, „býti otcem“, „býti sourozen-

[5] Obšírněji *binární relace* (poněvadž dává do vztahu dvojice prvků). Někdy se definují i relace n-ární pro $n > 2$.

cem") skutečně poskytují řadu (netriviálních) příkladů relací na množině všech lidí.

Relaci R na množině X můžeme obrázkově vystihnout dvěma naprosto rozdílnými způsoby. Pro relaci $R = \{(1,2), (2,4), (3,2), (4,2), (4,4)\}$ na množině $\{1,2,3,4\}$ dává první způsob takovýto obrázek:



Čtvercová políčka odpovídají uspořádaným dvojicím v kartézském součinu, a pro dvojice náležející do relace jsme příslušná políčka vybarvili. V tomto obrázku zdůrazňujeme definici relace na X a vystihujeme její „celkový tvar".

Tento obrázek má rovněž velmi blízko k alternativnímu popisu relace na množině X pomocí pojmu matice[6] Jestliže R je relace na nějaké n-prvkové množině $X = \{x_1, \ldots, x_n\}$, potom R je úplně popsána $n \times n$ maticí $A = (a_{ij})$, kde

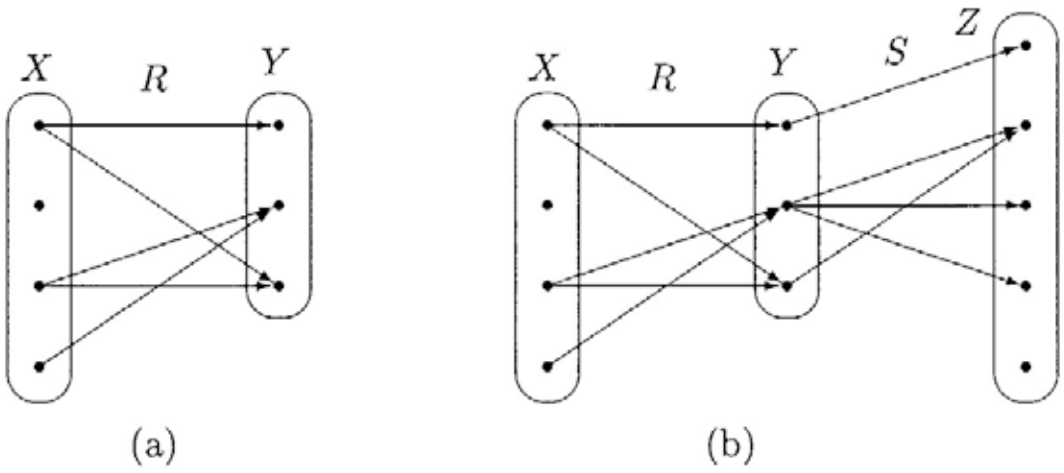
$$\begin{aligned} a_{ij} &= 1 \quad \text{jestliže } (x_i, x_j) \in R \\ a_{ij} &= 0 \quad \text{jestliže } (x_i, x_j) \notin R. \end{aligned}$$

Matici A nazýváme *matice sousednosti* relace R. Například, pro relaci R zobrazenou výše je příslušná matice sousednosti (pro $x_i = i$, $i = 1,2,3,4$)

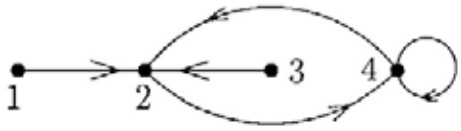
$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Jiný způsob znázornění téže relace je takovýto:

[6] Matice $n \times m$ je obdélníková tabulka čísel s n řádky a m sloupci; viz dodatek o algebře.

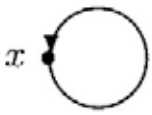


Obrázek 1.1: (a) Znázornění relace mezi X a Y pomocí šipek, (b) skládání relací.



Puntíky odpovídají jednotlivým prvkům množiny X. Skutečnost, že daná uspořádaná dvojice prvků (x, y) náleží relaci R, vyznačíme nakreslením šipky z x do y:

a v případě $x = y$ smyčkou



Oba způsoby znázornění budeme v dalším používat. Podobně můžeme znázorňovat relaci mezi X a Y; znázornění pomocí šipek je na obr. 1.1(a).

Skládání relací. Nechť X, Y, Z jsou množiny, $R \subseteq X \times Y$ nějaká relace mezi X a Y, a $S \subseteq Y \times Z$ relace mezi Y a Z. *Složením relací* R *a* S nazveme relaci $T \subseteq X \times Z$, definovanou následovně: xTz (pro $x \in X$,

$z \in Z$) platí právě tehdy, když existuje nějaké $y \in Y$ takové, že xRy a ySz. Složení relací R a S se značí zpravidla $R \circ S$.

Skládání relací se dá dobře schematicky znázornit pomocí šipek. Na obr. 1.1(b) bude dvojice (x, z) v relaci $R \circ S$, kdykoli lze z x do z projít po šipkách (přes nějaké $y \in Y$).

Všimněme si že složení není definováno pro každé 2 relace: abychom mohli skládat, musí mít relace společnou „prostřední" množinu (již jsme v definici značili Y). Jsou-li však R i S relace na téže množině X, je jejich složení vždy dobře definováno. I v tomto případě výsledek skládání relací záleží na pořadí; $R \circ S$ je obecně něco jiného než $S \circ R$, viz cvičení 2.

Cvičení

1. Popište relaci $R \circ R$, označuje-li R
   (a) relace rovnosti „=" na množině $\mathbf{N}$ všech přirozených čísel,
   (b) relaci „menší nebo rovno" („$\leq$") na $\mathbf{N}$,
   (c) relaci „ostře menší" („$<$") na $\mathbf{N}$,
   (d) relaci „ostře menší" („$<$") na množině $\mathbf{R}$ všech reálných čísel.
2. Najděte relace R a S na nějaké množině X takové, že $R \circ S \neq S \circ R$.
3. Pro relaci R na množině X definujeme indukcí symbol R^n: $R^1 = R$, $R^{n+1} = R \circ R^n$.
   (a) Ukažte, že je-li X konečná množina a R relace na ní, potom existují $r, s \in \mathbf{N}$, $r < s$ taková, že $R^r = R^s$.
   (b) Najděte relaci R na konečné množině takovou, že $R^n \neq R^{n+1}$ pro každé $n \in \mathbf{N}$.
   (c) Ukažte, že je-li X nekonečná, tvrzení (a) platit nemusí (t.j. existuje relace R taková, že všechny relace tvaru R^n jsou navzájem různé).

1.5 Ekvivalence

1.5.1 Definice. *Řekneme, že relace R na množině X je*

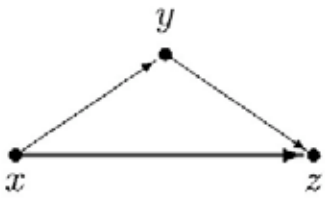
- reflexivní, *jestliže pro každé $x \in X$ platí xRx,*
- symetrická, *jestliže kdykoli xRy, pak i yRx,*
- transitivní, *jestliže ze vztahů xRy a yRz plyne xRz.*

Obrázek 1.2: Schematické znázornění relace ekvivalence na množině.

Ve znázornění jako str. 35 obsahuje reflexivní relace všechny čtverečky na diagonále, a ve znázornění se šipkami má smyčky u všech bodů.

Obrázek jako str. 35 pro symetrickou relaci je symetrický podle diagonály. Ve znázornění pomocí šipek jdou vždy šipky oběma směry:

Podmínka transitivity se dá dobře vyjádřit pomocí šipek: jsou-li v relaci šipky $x \to y$ a $y \to z$, musí tam být i $x \to z$:



1.5.2 Definice. *Řekneme, že relace R na X je* ekvivalence *na X, jestliže je symetrická, reflexivní a transitivní.*

Pojem ekvivalence je střechový pojem pro všechny pojmy vyjadřující stejnost, podobnost, isomorfismus atd. Relace ekvivalence se zpravidla značí symboly jako $=, \equiv, \simeq, \approx, \cong, \pi, \rho$ a podobně.

Přestože ekvivalence R na množině X je speciální relace a můžeme ji tedy znázornit libovolným ze dvou výše uvedených způsobů, je častěji používáno znázornění jako na obr. 1.2.

Klíčem k tomuto znázornění je následující pojem třídy ekvivalence: Nechť R je ekvivalence na množině X, nechť x je libovolný prvek množiny X. Označme symbolem $R[x]$ množinu všech prvků y, které jsou ekvivalentní s x (tedy $R[x]$ označuje množinu $\{y;\, xRy\}$). $R[x]$ se nazývá *třída ekvivalence* R *určená prvkem* x.

1.5.3 Tvrzení. *Pro každou ekvivalenci R na X platí*

(i) $R[x]$ *je neprázdná množina pro každý prvek* $x \in X$.

(ii) Pro každé dva prvky x, y *množiny* X *buď* $R[x] = R[y]$, *nebo* $R[x] \cap R[y] = \emptyset$.

(iii) Třídy ekvivalence jednoznačně určují (popisují) relaci R.

Předtím, než přistoupíme k důkazu, bychom měli vysvětlit smysl bodu (iii). Přesný význam je následující: Jsou-li R a S dvě ekvivalence na množině X a platí-li pro každý prvek x množiny X rovnost $R[x] = S[x]$, potom $R = S$.

Důkaz je jednoduchý použitím všech tří požadavků v definici ekvivalence.

(i) Množina $R[x]$ vždy obsahuje prvek x, protože R je relace reflexivní.

(ii) Nechť x, y jsou dané prvky. Rozlišíme dvě možnosti:

(a) Jestliže xRy, potom dokážeme nejprve $R[x] \subseteq R[y]$. Skutečně, je-li $z \in R[x]$, potom víme rovněž že zRx (použitím symetrie relace R) a tudíž zRy (použitím transitivity R). Proto i $z \in R[y]$. Opětovným použitím symetrie R dostáváme, že z platnosti xRy plyne $R[x] = R[y]$.

(b) Nechť neplatí xRy. Ukážeme, že $R[x] \cap R[y] = \emptyset$. Postupujme sporem: Nechť existuje $z \in R[x] \cap R[y]$. Potom xRz a zRy (použitím symetrie R), a tedy xRy (opětovným použitím transitivity R), což je spor.

(iii) Tato část tvrzení je zřejmá, neboť třídy ekvivalence R určují R vztahem

$$xRy \text{ právě když } \{x, y\} \subseteq R[x].$$

□

Toto tvrzení vysvětluje obrázek 1.2. Podmnožiny dané množiny X, které jsou navzájem disjunktní a které obsahují (dohromady) všechny prvky, tvoří *rozklad množiny* X. Tvrzení 1.5.3 potom zaručuje, že třídy ekvivalence tvoří rozklad množiny a že vztah mezi všemi ekvivalencemi na dané množině X a všemi rozklady X je vzájemně jednoznačný.

Co je to vzájemně jednoznačný vztah? Jak formalizovat tento intuitivně zřejmý pojem? To ukážeme v následující části.

Cvičení

1. Formulujte podmínky pro reflexivitu relace, pro symetrii relace a pro její transitivitu v řeči matice sousednosti relace.

2. Dokažte, že relace R na množině X je transitivní, právě když $R \circ R \subseteq R$.

3. (a) Dokažte, že pro libovolnou relaci R na nějaké množině X je relace $T = R \cup R \circ R \cup R \circ R \circ R \cup \ldots$ (sjednocení všech mnohonásobných složení R) transitivní.

   (b) Dokažte, že každá transitivní relace obsahující R obsahuje i T.

   (c) Dokažte, že je-li $|X| = n$, pak $T = R \cup R \circ R \cup \ldots \cup \underbrace{R \circ R \circ \ldots \circ R}_{(n-1)\times}$.

4. Nechť R a S jsou libovolné ekvivalence na množině X. Rozhodněte, které z následujících relací jsou nutně také ekvivalence.

   (a) $R \cap S$

   (b) $R \cup S$

   (c) $R \setminus S$

   (c) $R \circ S$.

1.6 Funkce

Pojem funkce je jeden ze základních pojmů v matematice. Trvalo dlouho, než se dospělo k dnešnímu chápání funkce (jakožto speciálního typu relace); například v době, kdy byl objeven diferenciální počet, se uvažovaly pouze reálné nebo komplexní funkce, a „poctivá" funkce musela být vyjádřena nějakou formulí nebo součtem nekonečné řady (jako třeba $f(x) = x^2 + 4$, $f(x) = \sqrt{\sin(x/\pi)}$, nebo $f(x) = \int_0^x (\sin t/t)\mathrm{d}t$, $f(x) = \sum_{n=0}^{\infty}(x^n/n!)$). To, že například reálná funkce může přiřazovat každému reálnému číslu nějaké zcela libovolné reálné číslo, je celkem moderní vynález.

1.6.1 Definice. Funkce *z množiny X do množiny Y je relace $f \subseteq X \times Y$, splňující dodatečnou podmínku, že pro každý prvek $x \in X$ existuje právě jediný prvek $y \in Y$ tak, že xfy.*

Při znázornění relace jako na obr. 1.1(a) předchozí definice znamená, že z každého bodu množiny X vychází právě jedna šipka, viz obr. 1.3(a).

To, že f je funkce z množiny X do množiny Y, zapisujeme takhle:

$$f : X \to Y.$$

A to, že funkce f přiřazuje nějakému prvku x jistý prvek y, zapisujeme

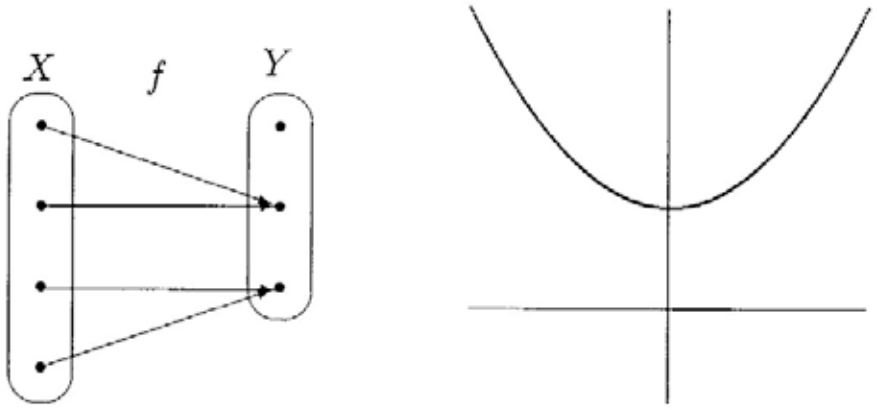
$$f : x \mapsto y.$$

Tento symbol je výhodný, chceme-li mluvit o nějaké funkci aniž bychom ji pojmenovali, například „uvažme funkci $x \mapsto 3a\sin(bx)$" (z tohoto zápisu je vidět, že míníme zkoumat závislost na x a nikoli na a nebo na b — a a b jsou nějaké parametry).

Místo „funkce" se také říká „zobrazení"[7].

Funkce, jakožto podmnožina kartézského součinu $X \times Y$ se také kreslí pomocí *grafu*. To je způsob znázornění, který se nejvíce používá na střední škole i v matematické analýze, viz obr. 1.3(b).

[7] V některých odvětvích matematiky se slovo funkce rezervuje pro funkci do reálných (nebo komplexních) čísel, a slovo zobrazení se používá pro funkce do libovolné množiny. Pro nás budou „funkce" a „zobrazení" synonyma.



(a) (b)

Obrázek 1.3: (a) Znázornění funkce pomocí šipek, (b) graf funkce $f : \mathbf{R} \to \mathbf{R}$, dané předpisem $f(x) = x^2 + 1$.

Pro funkce se ovšem nepoužívá značení, zavedeného pro relace. Je-li $f \subseteq X \times Y$ relace, která je funkcí, $f(x)$ označuje to jediné $y \in Y$, pro něž xfy. Dále, množinu $\{f(x);\, x \in X\}$ označujeme $f(X)$.

Zavádějí se i další termíny (X je *definiční obor*, Y je *obor hodnot*), ale v tomto textu se snažíme používat minimálně formalismu a terminologie.

Skládání funkcí. Funkce se skládají stejně jako relace, ale používá se přitom jiné značení! Definici skládání funkcí můžeme odvodit ze skládání relací, pro jistotu ji zformulujme:

1.6.2 Definice. *Jsou-li $f : X \to Y$ a $g : Y \to Z$ funkce, potom můžeme definovat novou funkci $h : X \to Z$ předpisem*

$$h(x) = g(f(x))$$

pro každé $x \in X$.

Funkce h (přesvědčete se, že h je opravdu funkce) se nazývá složení funkcí g a f *a značí se $g \circ f$. Tedy platí*

$$\big(g \circ f\big)(x) = g(f(x))$$

pro každý prvek $x \in X$.

Tady je zmíněná odlišnost od skládání relací. Pro *relace* je zvykem psát skládání „zleva doprava", pro funkce „zprava doleva". Jsou-li tedy $f : X \to Y$ a $g : Y \to Z$ funkce, jejich složení zapíšeme $g \circ f$, kdybychom je ale chápali jako *relace*, psali bychom pro totéž $f \circ g$! Oba zápisy mají své důvody, takto se značení historicky ustálilo a nemá asi smysl se snažit ho měnit. K nejasnostem by dojít nemělo. V tomto textu budeme téměř výhradně mluvit o skládání funkcí.

Skládání funkcí je asociativní, ale není komutativní. Má-li $g \circ f$ smysl, potom $f \circ g$ nemusí být vůbec definováno.

1.6.3 Definice (Důležité druhy funkcí). *Funkci $f : X \to Y$ nazýváme*

- prostá funkce, *jestliže pro $x \neq y$ je $f(x) \neq f(y)$,*
- funkce na, *jestliže pro každé $y \in Y$ existuje $x \in X$ splňující $f(x) = y$,* a
- vzájemně jednoznačná funkce, *jestliže f je prostá a na.*

Cizími slovy se funkce na nazývá *surjektivní* (z francouzštiny, čte se „syrjektivní"), prostá funkce je *injektivní*, a vzájemně jednoznačná funkce se jmenuje *bijektivní* nebo *bijekce*. „Bijekce" je pro svou krátkost možná vhodnější termín než „vzájemně jednoznačná funkce".

V obrázkovém znázornění funkce pomocí šipek se tyto druhy funkcí poznají takto:

- pro prostou funkci vchází do každého bodu $y \in Y$ *nejvýš jedna* šipka,
- pro funkci na vchází do každého bodu $y \in Y$ *aspoň jedna* šipka, a
- pro bijekci vchází do každého bodu $y \in Y$ *právě jedna* šipka.

Jak již výše uvedeno, funkci f z X do Y značíme $f : X \to Y$. Fakt, že funkce f je prostá, vyznačujeme někdy zápisem

$$f : X \hookrightarrow Y,$$

funkci f, která je *na*, značíme

$$f : X \twoheadrightarrow Y,$$

a konečně funkci vzájemně jednoznačnou značíme

$$f : X \hookrightarrow\!\!\!\!\!\rightarrow Y.$$

(Tohle značení není v literatuře příliš běžné.)

Platí následující:

1.6.4 Tvrzení. *Nechť $f : X \to Y$ a $g : Y \to Z$ jsou funkce.*

(i) Jsou-li f, g prosté funkce, je rovněž $g \circ f$ funkce prostá;

(ii) Jsou-li f, g funkce na, *je rovněž $g \circ f$ funkce* na;

(iii) Jsou-li f, g funkce vzájemně jednoznačné, je rovněž $g \circ f$ funkce vzájemně jednoznačná.

(iv) Pro každou funkci $f : X \to Y$ existuje množina Z, prostá funkce $h : Z \hookrightarrow Y$ a funkce na *$g : X \twoheadrightarrow Z$ tak, že $f = h \circ g$. (Tedy každou funkci lze napsat jako složení funkce prosté a funkce na.)*

Důkaz. Části (i), (ii), (iii) se dostanou přímým ověřením definice. Dokažme např. (ii). Zvolme $z \in Z$, hledáme $x \in X$ splňující $\Big(g \circ f\Big)(x) = z$. Protože g je funkce *na*, existuje nejprve $y \in Y$ tak, že $g(y) = z$. A protože f je funkce *na*, existuje poté $x \in X$ splňující $f(x) = y$. Takový x je hledaný prvek splňující $\Big(g \circ f\Big)(x) = z$.

Nejzajímavější je bod (iv). Buď $Z = f(X) = \{f(x);\, x \in X\}$ (je tedy $Z \subseteq Y$). Definujme zobrazení $g : X \to Z$ a $h : Z \to Y$ předpisem:

$$\begin{aligned} g(x) &= f(x) \quad \text{pro } x \in X \\ h(z) &= z \qquad \text{pro } z \in Z. \end{aligned}$$

Zřejmě g je funkce *na* (čili $g : X \twoheadrightarrow Z$), h je funkce prostá (čili $h : Z \hookrightarrow Y$) a $f = h \circ g$. □

Cvičení

1. Ukažte, že je-li X konečná množina, potom funkce $f : X \to X$ je prostá, právě když je na.

2. Najděte příklad

   (a) prosté funkce $f : \mathbf{N} \hookrightarrow \mathbf{N}$, která není na,

   (b) funkce $f : \mathbf{N} \twoheadrightarrow \mathbf{N}$ (na), která není prostá.

3. Označme $i_X : X \to X$ funkci, která zobrazuje každý prvek množiny X na něj samotný (tato funkce se nazývá *identická* nebo *identita* na X). Nechť $f : X \to Y$ je nějaká funkce. Ukažte, že

   (a) funkce $g : Y \to X$ taková, že $g \circ f = i_X$, existuje právě když f je prostá.

   (b) funkce $g : Y \to X$ taková, že $f \circ g = i_Y$, existuje právě když f je na.

4. (a) Je-li $g \circ f$ funkce na, musí g být na? Musí f být na?

   (b) Je-li $g \circ f$ prostá funkce, musí g být prostá? Musí f být prostá?

5. Nechť R a S jsou relace na nějaké množině X. Řekneme, že R a S jsou *isomorfní*, pokud existuje bijekce $f : X \to X$ taková, že pro každé $x, y \in X$ platí xRy právě když $f(x)Sf(y)$.

   (a) Vypište všechny možné relace na dvouprvkové množině $X = \{a, b\}$. Určete, které jsou navzájem isomorfní.

   (b) Dokažte, pro libovolnou množinu X je vztah „býti isomorfní" ekvivalence na množině všech relací na X.

1.7 Uspořádané množiny

Čtenář jistě zná uspořádání přirozených čísel i dalších číselných oborů podle velikosti. Takové uspořádání se v matematice chápe jako speciální typ relace, t.j. jako vztah dvojic čísel. Tato relace, se ve zmíněném případě zpravidla označuje symbolem „$\leq$" („menší nebo rovno"). I na jiných množinách (třeba na množině všech slov v nějakém jazyku) se zavádějí různá uspořádání, a tutéž množinu lze uspořádat mnoha způsoby.

Než zavedeme obecný pojem uspořádané množiny, definujeme ještě jeden pomocný pojem. Relace R na množině X se nazývá *antisymetrická*[8], pokud pro každé $x, y \in X$ platí, že pokud xRy a zároveň

[8] To, čemu my říkáme antisymetrická relace, se někdy v literatuře nazývá *slabě antisymetrická relace*.

yRx, potom $x = y$. Při znázornění šipkami, v antisymetrické relaci se nevyskytuje situace

1.7.1 Definice. Uspořádání *na nějaké množině X je každá relace na X, která je reflexivní, antisymetrická a transitivní.* Uspořádaná množina *je dvojice (X, R), kde X je množina a R je uspořádání na X.*

Pro relace uspořádání se často používají symboly $\preceq$ nebo $\leq$. První z nich je užitečný, chceme-li např. mluvit ještě o nějakém jiném uspořádání množiny přirozených čísel než je obvyklé uspořádání podle velikosti, nebo uvažujeme-li nějaké obecné uspořádání na libovolné množině.

Máme-li nějaké uspořádání $\preceq$, definujeme odvozenou relaci „ostré nerovnosti" $\prec$: $a \prec b$ právě když $a \preceq b$ a $a \neq b$. Dále můžeme definovat „obrácenou nerovnost", t.j. relaci $\succeq$, vztahem $a \succeq b \Leftrightarrow b \preceq a$.

Příklady. Několik příkladů uspořádaných množin jsme už zmínili — byly to $(\mathbf{N}, \leq)$, $(\mathbf{R}, \leq)$ a podobně, kde $\leq$ ovšem značí obvyklé uspořádání podle velikosti (formálně chápané jako relace).

Jak se snadno ověří, je-li R uspořádání na nějaké množině X, a Y je podmnožina X, je relace $R \cap Y^2$ uspořádání na Y (porovnáváme podle velikosti prvky z Y a na ostatní zapomeneme). Tím máme další příklady uspořádaných množin, totiž všelijakých podmnožin reálných čísel.

Lineární uspořádání. Dosud probrané příklady mají společné to, že každé dva prvky z uvažované uspořádané množiny lze porovnat, jinými slovy, pro libovolné dva různé prvky x a y platí buď $x \leq y$ nebo $y \leq x$. Tato vlastnost z obecné definice uspořádání neplyne, a uspořádání, která ji mají, se nazývají *lineární* (ve stejném významu se také používá termín *úplné uspořádání*).

Příklady částečných uspořádání. Jak mohou vypadat uspořádání, která nejsou úplná? Na libovolné množině X můžeme definovat relaci

Δ, v níž je každý prvek x v relaci jen sám se sebou, t.j. $\Delta = \{(x,x);\ x \in X\}$. Je snadno vidět, že tato relace vyhovuje definici uspořádání.

Aby se zdůraznilo, že se mluví o uspořádání, které nemusí být lineární, říká se někdy obšírněji *částečné uspořádání*. Částečné uspořádání tedy znamená přesně totéž, co uspořádání (bez dalších přívlastků), a podobně místo uspořádaná množina se někdy říká *částečně uspořádaná množina*[9].

Popišme zajímavější příklady částečně uspořádaných množin.

1.7.2 Příklad. *Představme si, že chceme koupit třeba ledničku. Složitou skutečnou situaci si zjednodušíme matematickou abstrakcí, a předpokládáme, že u ledniček hledíme jen na 3 číselné parametry: cenu, spotřebu elektřiny a obsah. Máme-li dva typy ledniček, a první typ je dražší, více spotřebuje a méně se do něj vejde, potom lze považovat druhý typ za lepší — na tom by se shodla asi velká většina kupců ledniček. Na druhé straně, někdo dá přednost menší a levnější ledničce, jiný preferuje větší, i když je dražší, a bohatý ekologický aktivista si možná koupí i drahou ledničku s malou spotřebou. Relace „být jednoznačně horší" (označíme ji $\preceq$) v tomto pojetí je tedy částečné uspořádání na ledničkách, matematicky formulováno na množině všech trojic (a,b,c) reálných čísel, definované takto:*

$$(a_1,b_1,c_1) \preceq (a_2,b_2,c_2) \Leftrightarrow a_1 \geq a_2,\ b_1 \geq b_2 \text{ a } c_1 \leq c_2. \qquad (1.3)$$

1.7.3 Příklad. *Pro přirozená čísla a,b znamená symbol $a|b$ „a dělí b", neboli že existuje přirozené číslo c takové, že $b = ac$. Relace „$|$" (dělitelnost) je částečné uspořádání na $\mathbf{N}$ (ověření přenecháváme čtenáři).*

1.7.4 Příklad. *Nechť X je nějaká množina. Relace „$\subseteq$" (býti podmnožinou) definuje částečné uspořádání na množině 2^X, t.j. na systému všech podmnožin množiny X.*

Znázorňování částečně uspořádaných množin. Konečné částečně uspořádané množiny můžeme znázorňovat pomocí šipek, jako kterékoliv jiné relace. V takových obrázcích bude typicky spousta šipek (například pro 10-prvkovou lineárně uspořádanou množinu bychom museli nakreslit $9+8+\ldots+1 = 45$ šipek a ještě 10 smyček). Řada šipek se ale

[9] Což má i pěknou zkratku. Ostatně v angličtině se plný termín *partially ordered set* také zkracuje na umělé slovo *poset*.

dá zrekonstruovat z transitivity: Víme-li, že $x \preceq y$ a $y \preceq z$, potom už také $x \preceq z$ a šipku z x do z můžeme vynechat. Podobně smyčky není třeba kreslit. Pro konečné uspořádané množiny zachycuje všechnu potřebnou informaci relace „být bezprostředním předchůdcem“, kterou teď definujeme.

Nechť $(X, \preceq)$ je uspořádaná množina. Řekneme, že prvek x je *bezprostředním předchůdcem* prvku y, pokud platí

- $x \prec y$, a
- neexistuje žádné $t \in X$ takové, že $x \prec t \prec y$.

Právě zavedenou relaci bezprostředního předchůdce můžeme označit třeba $\lhd$.

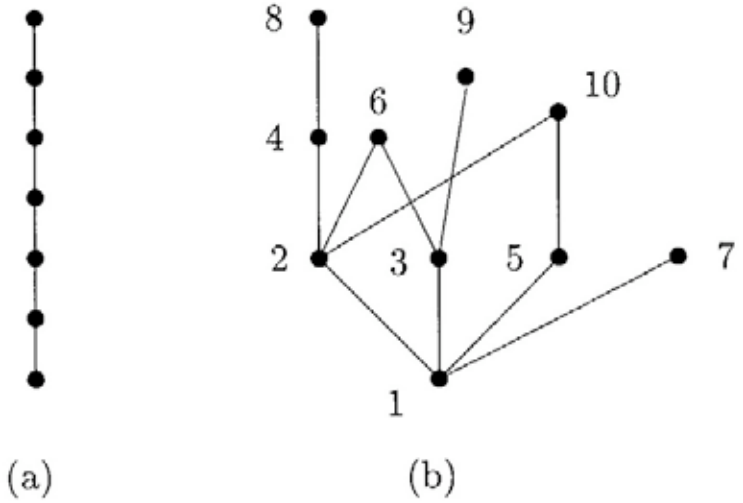
Tvrzení, že uspořádání $\preceq$ lze rekonstruovat z relace $\lhd$, můžeme přesně formulovat takto:

1.7.5 Tvrzení. *Nechť $(X, \preceq)$ je konečná uspořádaná množina, $\lhd$ je příslušná relace bezprostředního předchůdce. Potom pro libovolné dva prvky $x, y \in X$ platí, že $x \prec y$ právě když existují prvky $x_1, x_2, \ldots, x_k \in X$ takové, že $x \lhd x_1 \lhd \ldots \lhd x_k \lhd y$ (případně může být i $k = 0$, t.j. přímo $x \lhd y$).*

Důkaz. Jedna implikace je snadno vidět: Máme-li $x \lhd x_1 \lhd \ldots \lhd x_k \lhd y$, potom podle definice bezprostředního předchůdce je i $x \preceq x_1 \preceq \ldots \preceq x_k \preceq y$, a z transitivity relace $\prec$ plyne $x \prec y$.

Ani opačná implikace není těžká, dokážeme ji indukcí. Budeme dokazovat toto: *Nechť $x, y \in X$, $x \prec y$ jsou takové dva prvky, že existuje nejvýš n prvků $t \in X$ splňujících $x \prec t \prec y$. Potom existují $x_1, x_2, \ldots, x_k \in X$ takové, že $x \lhd x_1 \lhd \ldots \lhd x_k \lhd y$.* Pro $n = 0$ předpoklad tohoto tvrzení říká, že neexistuje žádné t, $x \prec t \prec y$, a proto $x \lhd y$, čili tvrzení platí (volíme $k = 0$).

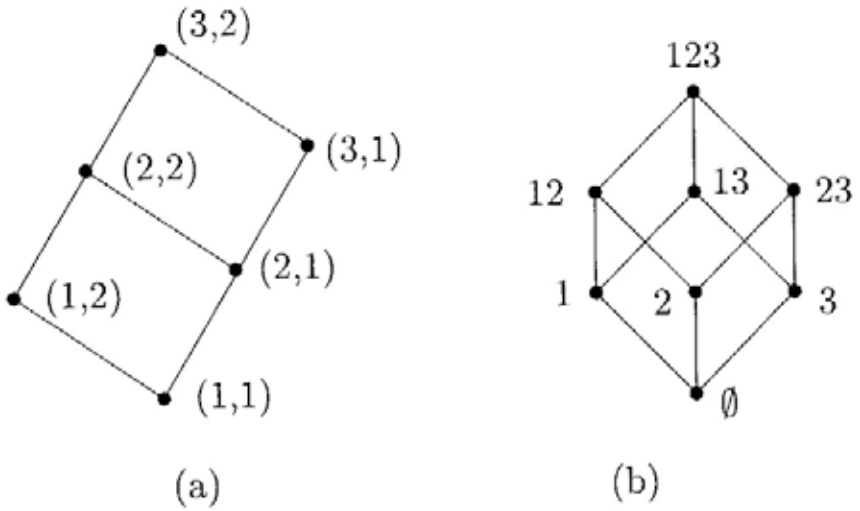
Nechť tvrzení platí pro všechna n až do n_0, a mějme $x \prec y$ takové, že množina $M_{xy} = \{t \in X;\ x \prec t \prec y\}$ má $n = n_0 + 1$ prvků. Vyberme jeden prvek $u \in M_{xy}$, a uvažme množiny $M_{xu} = \{t \in X;\ x \prec t \prec u\}$ a podobně M_{uy}. Z transitivity $\prec$ plyne, že $M_{xu} \subset M_{xy}$, $M_{uy} \subset M_{xy}$. Jak M_{xu}, tak M_{uy} mají aspoň o 1 prvek méně než M_{xy} (protože $u \notin M_{xu}, M_{uy}$), a podle indukčního předpokladu najdeme prvky $x_1, \ldots, x_k$ a $y_1, \ldots, y_\ell$ tak, že $x \lhd x_1 \lhd \ldots \lhd x_k \lhd u$ a $u \lhd y_1 \lhd \ldots \lhd y_\ell \lhd y$. Spojením obou těchto „řetízků“ dostaneme požadovanou posloupnost spojující x a y. □



Obrázek 1.4: Příklady částečně uspořádaných množin: (a) lineární uspořádání, (b) uspořádání dělitelností.

Pro znázornění konečné částečně uspořádané množiny tedy stačí nakreslit šipkami jen relaci bezprostředního předchůdce. Přijmeme-li konvenci, že v obrázku povedou všechny šipky směrem nahoru (t.j., je-li $x \prec y$, bude x nakresleno výš než y), nemusíme ani zakreslovat směr šipek, stačí kreslit spojnice bodů. Takové znázornění částečně uspořádané množiny se nazývá její *Hasseův diagram.* Příklady jsou na obr. 1.4 a 1.5. Obr. 1.4(a) zachycuje sedmiprvkovou lineárně uspořádanou množinu, např. $(\{1,2,\ldots,7\},\leq)$, obr. 1.4(b) ukazuje množinu $\{1,2,\ldots,10\}$ uspořádanou relací dělitelnosti (viz příklad 1.7.3). Obr. 1.5(a) je pro množinu $\{1,2,3\}\times\{1,2\}$ s uspořádáním $\preceq$ daným předpisem $(a_1,b_1)\preceq(a_2,b_2)$ právě když $a_1\leq a_2$ a $b_1\leq b_2$, a konečně obr. 1.5(b) je Hasseův diagram množiny všech podmnožin množiny $\{1,2,3\}$, uspořádaných relací $\subseteq$ (vynecháváme množinové závorky a čárky u popisu bodů, 13 tedy znamená množinu $\{1,3\}$).

Další pojmy pro uspořádané množiny a příklady ponecháváme do cvičení.



Obrázek 1.5: Příklady částečně uspořádaných množin: (a) uspořádání nerovností v obou souřadnicích, (b) uspořádání inkluzí.

Cvičení

1. Popište všechny relace na na množině X, které jsou zároveň ekvivalencí i (částečným) uspořádáním.

2. Nechť R a S jsou libovolná uspořádání na množině X. Rozhodněte, které z následujících relací jsou nutně také uspořádáními.

   (a) $R \cap S$

   (b) $R \cup S$

   (c) $R \setminus S$

   (d) $R \circ S$.

3. Ověřte podrobně, že vztah (1.3) v příkladu 1.7.2 skutečně definuje částečné uspořádání.

4.* Nechť R je relace na množině X taková, že neexistuje konečná posloupnost prvků $x_1, x_2, \ldots, x_k$ splňujících $x_1 R x_2$, $x_2 R x_3, \ldots, x_{k-1} R x_k$, $x_k R x_1$ (říkáme, že taková R *nemá cyklus* nebo že je *acyklická*). Dokažte, že pak existuje uspořádání $\preceq$ na množině X takové, že $R \subseteq \preceq$. (Pomůže-li vám to, předpokládejte, že X je konečná.)

5. (a) Uvažte množinu $\{1, 2, \ldots, n\}$ uspořádanou relací dělitelnosti $|$ (viz příklad 1.7.3). Kolik nejvýše prvků může mít podmnožina $X \subseteq$

$\{1, 2, \ldots, n\}$, která je relací | uspořádána lineárně (takové podmnožině se někdy říká *řetězec*)?

(b) Řešte tutéž otázku pro množinu $2^{\{1,2,\ldots,n\}}$ uspořádanou relací $\subseteq$ (viz příklad 1.7.4).

6. Ukažte, že tvrzení 1.7.5 neplatí pro nekonečné množiny.

7. Buď $(X, \preceq)$ uspořádaná množina. Prvek $a \in X$ nazveme

   - *největším prvkem* X, pokud pro každé $x \in X$ platí $x \preceq a$, a
   - *maximálním prvkem* X, pokud neexistuje žádné $y \in X$ takové, že $a \prec y$.

   Podobně se definuje *nejmenší* a *minimální* prvek.

   (a) Ukažte, že největší prvek je maximální, a ukažte příklad uspořádané množiny, která má maximální prvek, ale nemá největší prvek.

   (b) Najděte uspořádanou množinu, která nemá ani nejmenší, ani minimální prvek, ale má největší prvek.

8.* Nechť $\preceq$ je libovolné (částečné) uspořádání na konečné množině X. Dokažte, že existuje *lineární* uspořádání $\leq$ na X takové, že $x \leq y$ kdykoliv $x \preceq y$ (t.j. $\preceq \subseteq \leq$).

9. Nechť $(X, \leq)$, $(Y, \preceq)$ jsou uspořádané množiny. Říkáme, že tyto uspořádané množiny jsou *isomorfní* (t.j., z hlediska uspořádání „vypadají stejně“), pokud existuje nějaké vzájemně jednoznačné zobrazení $f : X \leftrightarrow\!\!\!\rightarrow Y$ takové, že pro každé $x, y \in X$ platí $x \leq y$ právě když $f(x) \preceq f(y)$.

   (a) Nakreslete všechny navzájem neisomorfní tříprvkové částečně uspořádané množiny.

   (b) Dokažte, že každé dvě n-prvkové *lineárně uspořádané* množiny jsou navzájem isomorfní.

   (c) Najděte dvě navzájem neisomorfní lineární uspořádání množiny všech přirozených čísel.

   (d)* Dokážete najít nekonečně mnoho navzájem neisomorfních lineárních uspořádání $\mathbf{N}$? Nespočetně mnoho?

10.* Dokažte, že pro každou konečnou částečně uspořádanou množinu $(X, \preceq)$ existuje konečná množina A a systém jejích podmnožin $\mathcal{M}$ takový, že $(\mathcal{M}, \subseteq)$ je isomorfní $(X, \preceq)$.

11. Buď $(X, \preceq)$ uspořádaná množina, $A \subseteq X$ její podmnožina. Prvek $s \in X$ nazveme *supremum* množiny A, pokud platí

    (i) $a \preceq s$ pro každé $a \in A$,

    (ii) Pro každé $s' \in X$ platí: jestliže $a \preceq s'$ pro každé $a \in A$, potom $s \preceq s'$.

    Podobně, ale se všemi nerovnostmi v obráceném směru, se definuje *infimum* podmnožiny $A \subseteq X$.

    (a) Jaký prvek je supremem prázdné množiny?

    (b) Najděte příklad uspořádané množiny, jejíž každá neprázdná podmnožina má supremum, ale ne každá neprázdná podmnožina má infimum.

    (c)* Nechť $(X, \preceq)$ je uspořádaná množina, jejíž každá podmnožina (včetně prázdné) má supremum. Dokažte, že každá podmnožina má též infimum.

12. Uvažme částečně uspořádanou množinu $(\mathbf{N}, |)$ (uspořádání dělitelností).

    (a) Rozhodněte, zda každá podmnožina $\mathbf{N}$ má supremum.

    (b) Rozhodněte, zda každá konečná podmnožina $\mathbf{N}$ má supremum.

    (c) Rozhodněte, zda každá neprázdná podmnožina má infimum.

2

Kombinatorické počítání

V této kapitole budeme studovat úlohy „na počet konfigurací“, jako „Kolik je zobrazení dané n-prvkové množiny do m-prvkové?“ a podobně. Začneme jednoduchými příklady, které se dají vyřešit úvahou bez nějakých speciálních znalostí, ale později se dostaneme i k poněkud pokročilejším technikám.

2.1 Funkce a podmnožiny

2.1.1 Tvrzení. *Nechť N je nějaká n-prvková množina (případně i prázdná, t.j. $n = 0, 1, 2, \ldots$), M je m-prvková množina, $m \geq 1$. Potom počet všech zobrazení (neboli funkcí) $f : N \to M$ (zobrazení množiny N do M) je m^n.*

Důkaz. Toto tvrzení asi řada čtenářů zná nebo si jeho pravdivost uvědomí bez velké námahy. Cvičně je nicméně dokážeme indukcí podle n.

Pro $n = 0$ uvažujeme zobrazení prázdné množiny. Podíváme-li se na definici zobrazení, je to relace (tedy podmnožina $N \times M$, čili v našem případě podmnožina prázdné množiny), splňující jistou podmínku — pro každý prvek $a \in N$ existuje v relaci právě jedna dvojice tvaru (a, b), kde $b \in M$. V našem případě N žádný prvek nemá, a proto uvedená podmínka nic nepožaduje, čili jediná možná relace, totiž prázdná, je také zobrazením $N \to M$. Dokazované tvrzení platí pro $n = 0$.

Leckdo by namítl, že zobrazení prázdné množiny nemá žádný smysl

a nebo že není potřeba se jím zabývat (opravdu bychom mohli indukci začít od $n = 1$). V matematických úvahách se většinou vyplatí si podobné „mezní" případy rozmyslet, uvážit, co přesně o nich říká obecná definice. Tím se potom vyhneme různým výjimkám a speciálním případům (nebo chybám) v důkazech.

Předpokládejme, že jsme tvrzení dokázali pro každé $n \leq n_0$ a pro každé m. Máme nyní $n = n_0+1$, n-prvkovou množinu N a m-prvkovou množinu M. Zvolme libovolně jeden prvek $a \in N$. Zadat zobrazení $f : N \to M$ je totéž, jako zadat hodnotu $f(a) \in M$ plus zobrazení $f' : N \setminus \{a\} \to M$ zbývajících prvků. Hodnotu $f(a)$ můžeme zvolit m způsoby, a pro volbu f' máme podle indukčního předpokladu m^{n-1} možností. Každou volbu $f(a)$ můžeme zkombinovat s libovolnou volbou f', takže celkem je počet možností pro f roven $m \cdot m^{n-1} = m^n$. □

2.1.2 Tvrzení. *Libovolná n-prvková množina X má právě 2^n podmnožin.*

Tohle je jiné dobře známé tvrzení. Řekneme si dva důkazy.

První důkaz (indukcí). Pro $X = \emptyset$ existuje jediná podmnožina, totiž prázdná, což souhlasí se vzorečkem, $2^0 = 1$. Máme-li $(n + 1)$-prvkovou množinu X, zvolme jeden její prvek, a, a rozdělme podmnožiny X do dvou typů: ty které neobsahují a, a ty které jej obsahují. První typ jsou právě všechny podmnožiny n-prvkové množiny $X \setminus \{a\}$, a podle indukčního předpokladu jich je 2^n. Pro každou podmnožinu A druhého typu uvažme množinu $A' = A \setminus \{a\}$. To je podmnožina $X \setminus \{a\}$. Zřejmě každá podmnožina $A' \subseteq X \setminus \{a\}$ se takto dostane právě z jedné množiny A, totiž z $A' \cup \{a\}$. Proto podmnožin A druhého typu je také 2^n, a celkem máme $2^n + 2^n = 2^{n+1}$ podmnožin $(n + 1)$-prvkové množiny jak to má být.

Druhý důkaz (převedením na známé tvrzení). Uvažme libovolnou podmnožinu A dané n-prvkové množiny X, a definujme zobrazení $f_A : X \to \{0, 1\}$: pro prvek $x \in X$ položíme

$$f_A(x) = \begin{cases} 1 & \text{pokud } x \in A \\ 0 & \text{pokud } x \notin A. \end{cases}$$

(toto zobrazení se v matematice často objevuje, a nazývá se *charakteristická funkce* množiny A). Různým množinám A přísluší různá zobrazení f_A, a obráceně, pro libovolné zobrazení $f : X \to \{0,1\}$ existuje právě jedna množina $A \subseteq X$ taková, že $f = f_A$. Tudíž podmnožin X je stejný počet jako zobrazení $X \to \{0,1\}$, čili 2^n podle tvrzení 2.1.1. □

Teď trošku těžší tvrzení:

2.1.3 Tvrzení. *Nechť $n \geq 1$. Každá n-prvková množina má právě 2^{n-1} podmnožin liché velikosti a 2^{n-1} podmnožin sudé velikosti.*

Důkaz. Využijeme tvrzení 2.1.2. Zvolme pevně nějaký prvek $a \in X$. Libovolnou podmnožinu $A \subseteq X \setminus \{a\}$ můžeme doplnit na podmnožinu $A' \subseteq X$ s lichým počtem prvků: je-li $|A|$ liché, bude $A' = A$, a pro $|A|$ sudé $A' = A \cup \{a\}$. Je snadné zkontrolovat, že tím jsme našli bijekci mezi množinou všech podmnožin $X \setminus \{a\}$ a množinou všech podmnožin X liché velikosti, a tak posledně jmenovaných je 2^{n-1}. Pro podmnožiny sudé velikosti se postupuje stejně, nebo se řekne, že jich musí být doplněk do počtu všech podmnožin, t.j. $2^n - 2^{n-1} = 2^{n-1}$. □

Vrátíme se k zobrazením.

2.1.4 Tvrzení. *Pro $n, m \geq 0$ existuje právě*

$$m(m-1)\cdots(m-n+1) = \prod_{i=0}^{n-1}(m-i)$$

prostých zobrazení n-prvkové množiny do m-prvkové množiny.

Důkaz. Zase indukcí podle n, budeme postupovat stručněji. Pro $n = 0$, prázdné zobrazení je prosté, tedy existuje jedno zobrazení, což odpovídá tomu, že hodnotu prázdného součinu jsme definovali jako 1. Pro $n > m$ žádné prosté zobrazení neexistuje, což souhlasí s dokazovaným vzorcem (vystupuje v něm totiž jeden činitel rovný 0).

Mějme n-prvkovou množinu N, $n \geq 1$ a m-prvkovou množinu M, $m \geq n$. Vyberme prvek $a \in N$ a zvolme jeho funkční hodnotu $f(a) \in M$ libovolně, jedním z m způsobů. Zbývá prostě zobrazit prvky $N \setminus \{a\}$ do $M \setminus \{f(a)\}$, pro což existuje podle indukčního předpokladu $(m-1)(m-2)\cdots(m-n+1)$ možností. Celkem dostaneme

$$m(m-1)(m-2)\cdots(m-n+1)$$

prostých zobrazení $N \to M$. □

Máme-li množinu M sestávající z m různých předmětů a vyberemeli z nich libovolně uspořádanou n-tici předmětů (t.j. při výběru záleží na pořadí; takové výběry se někdy nazývají *variace*, obšírněji *variace n prvků z m prvků bez opakování*), máme $m(m-1)\ldots(m-n+1)$ možností takového výběru. Každý takový výběr můžeme chápat jako volbu prostého zobrazení $f : \{1, 2, \ldots, n\} \to M$: definujeme $f(1)$ jako první předmět z vybrané n-tice, $f(2)$ jako druhý předmět atd. Obráceně, volbu prostého zobrazení si můžeme představit jako výběr uspořádané n-tice z množiny, do níž zobrazujeme.

Cvičení

1. Určete počet všech uspořádaných dvojic (A, B), kde $A \subseteq B \subseteq \{1, 2, \ldots, n\}$.
2. (a) Kolik existuje $n \times n$ matic s prvky z množiny $\{0, 1, \ldots, q-1\}$?
   (b)* Předpokládejme, že q je prvočíslo. Kolik takových matic má determinant dělitelný q? (Jinými slovy, kolik matic nad tělesem $GF(q)$ je singulárních? Viz algebraický dodatek.)

2.2 Permutace a faktoriály

Prostá zobrazení konečné množiny X do sebe se nazývají *permutace* množiny X. Taková zobrazení jsou ovšem zároveň na.

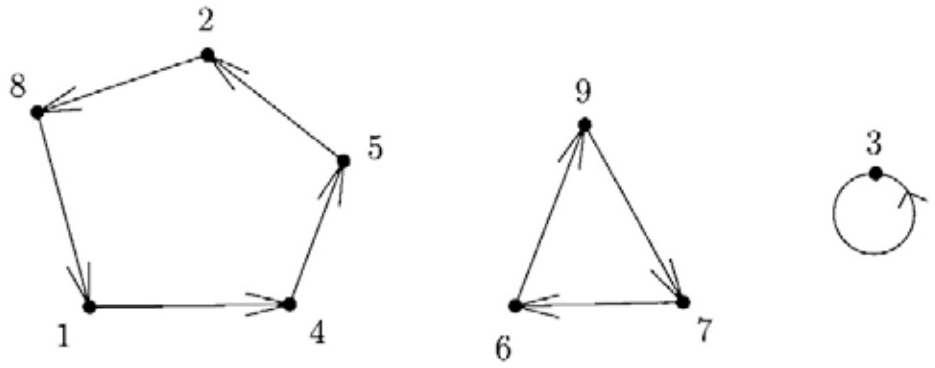
Máme-li prvky X srovnány v nějakém pořadí, můžeme si permutaci představovat jako nějaké jejich přerovnání. Například pro množinu $X = \{a, b, c, d\}$ je jedna možná permutace

$$\begin{pmatrix} a & b & c & d \\ b & d & c & a \end{pmatrix}$$

(v prvním řádku jsme vypsali prvky množiny X, a ve druhém jsme pod každý prvek napsali prvek, na nějž se uvažovanou permutací zobrazí). Nejčastěji se pracuje s permutacemi množiny $\{1, 2, \ldots, n\}$. Předpokládáme-li, že v prvním řádku budou tato čísla vždy zapsána v přirozeném pořadí, stačí uvést pouze druhý řádek; např. (2 4 3 1) by označovalo permutaci p s hodnotami $p(1) = 2$, $p(2) = 4$, $p(3) = 3$ a $p(4) = 1$.

V literatuře se někdy permutace množiny X chápou přímo jako rozložení prvků X v nějakém pořadí, t.j. lineární uspořádání na X. To je někdy také užitečný pohled, my však budeme permutace chápat jako zobrazení, což má některé formální výhody, například že permutace lze přirozeně skládat.

Ještě jiný způsob zápisu permutace je pomocí jejích cyklů. Cykly permutace můžeme asi nejlépe definovat při znázornění permutace pomocí šipek (jako jsme znázorňovali relace v části 1.4, např. na str. 36). V případě permutace $p : X \to X$ znázorníme prvky množiny X body (puntíky), a nakreslíme šipku od každého bodu x k bodu $p(x)$. Například, pro permutaci $p = (4\ 8\ 3\ 5\ 2\ 9\ 6\ 1\ 7)$ (použili jsme jednořádkového zápisu pro permutace množiny $\{1, 2, \ldots, n\}$ vysvětleného výše) vypadá takové znázornění takto:



Z každého bodu vychází právě 1 šipka, a do každého bodu také právě 1 šipka vchází. Je snadné si rozmyslet, že za těchto podmínek je takové znázornění permutace vždy tvořeno několika disjunktními skupinami bodů, přičemž v každé ze skupin jsou body propojeny šipkami do cyklu (orientovaného, to znamená, že cyklus lze procházet kolem dokola podél šipek) — jako na uvedeném obrázku. Tyto cykly budeme nazývat *cykly dané permutace*. Pomocí cyklů by se uvedená permutace zapsala $p = ((1, 4, 5, 2, 8)(3)(6, 9, 7))$. V každé vnitřní závorce jsou vypsány prvky jednoho z cyklů v pořadí podle jeho šipek, počínaje prvkem s nejnižším číslem.

K čemu mohou permutace sloužit? Studují se například při návrhu

a analýze všelijakých algoritmů pro třídění. Některé efektivní algoritmy pro výpočty s grafy, s geometrickými objekty a podobně začínají tím, že rozestaví nějaké vstupní objekty do náhodného pořadí, t.j. vlastně s nimi provedou náhodnou permutaci. Překvapivě komplikované vlastnosti permutací se uplatnily při matematické analýze míchání karet. V teorii grup jsou grupy permutací (se skládáním jako grupovou operací) jedním z hlavních předmětů studia. Prapříčina neřešitelnosti obecné algebraické rovnice pátého stupně je ve vlastnostech grupy všech permutací na 5-prvkové množině.

Podle tvrzení 2.1.4 je počet permutací n-prvkové množiny roven $n(n-1) \times \cdots \times 1$. Toto číslo jako funkce proměnné n se označuje $n!$ a nazývá se n *faktoriál*. Je tedy

$$n! = 1 \times 2 \times 3 \times \ldots \times n = \prod_{i=1}^{n} i.$$

Speciálně pro $n = 0$ je $0!$, jako prázdný součin, roven 1.

Cvičení

1. Kolik existuje permutací množiny $\{1, 2, \ldots, n\}$ s jediným cyklem?

2. Pro permutaci $p : X \to X$ značí p^k permutaci vzniklou k-násobným složením p, t.j. $p^1 = p$, $p^k = p \circ p^{k-1}$. *Řádem* permutace p se rozumí nejmenší přirozené číslo k takové, že $p^k = id$, kde id označuje identickou permutaci, která každý prvek zobrazí na něj samotný.

   (a) Určete řád permutace (2 3 1 5 4 7 8 9 6).

   (b) Ukažte, jak se v obecnosti najde řád permutace pomocí délek jejích cyklů.

3. Buď π permutace na množině $\{1, 2, \ldots, n\}$, zapišme ji jednořádkovým zápisem, a vyznačme ve vzniklé posloupnosti jednotlivé *rostoucí úseky*, např. (4 5 7 2 6 8 3 1). Označme $f(n, k)$ počet permutací n-prvkové množiny s přesně k rostoucími úseky.

   (a)* Dokažte, že $f(n, k) = f(n, n + 1 - k)$, a odvoďte, že průměrný počet úseků permutace (přes všechny permutace) je $(n + 1)/2$.

   (b)* Odvoďte rekurentní vzorec

$$f(n, k) = k\ f(n-1, k) + (n + 1 - k) f(n-1, k-1).$$

(c) Pomocí (b) určete počet permutací se 2, resp. se 3 úseky, případně * s k rostoucími úseky.

(d)* Pro náhodnou permutaci π určete pravděpodobnost, že počáteční rostoucí úsek má délku k. Ukažte, že pro velká n se průměrná délka počátečního rostoucího úseku blíží číslu $e - 1$.

Poznámka: Podobné otázky se studují při analýze některých algoritmů pro třídění.

4. Buď π nějaká permutace množiny $\{1, 2, \ldots, n\}$. Řekneme, že dvojice $(i, j) \in \{1, 2, \ldots, n\} \times \{1, 2, \ldots, n\}$ je *inverze* π, pokud $i < j$ a zároveň $\pi(i) > \pi(j)$.

   (a) Dokažte, že množina $I(\pi)$ všech inverzí, chápaná jako relace, je transitivní. Ukažte že také její doplněk je transitivní relace.

   (b) Uvažme nějaký třídicí algoritmus, který rovná n daných čísel podle velikosti, a přitom v každém kroku vymění pořadí některých dvou sousedních čísel (v momentálním pořadí). Dokažte, že pro setřídění některých posloupností je potřeba řádově aspoň n^2 kroků.

   (c)* Dokázali byste navrhnout algoritmus, který by spočítal počet inverzí dané permutace $\{1, 2, \ldots, n\}$ v podstatně méně než n^2 krocích? (Řešení viz např. [12].)

5. (a)* Zjistěte, jakou nejvyšší mocninou 5 je dělitelné číslo 50!. Kolik bude mít desítkový zápis 50! na konci nul?

   (b) Najděte obecný vzorec pro nejvyšší mocninu k takovou, že číslo $n!$ je dělitelné p^k, kde p je dané prvočíslo.

6. Ukažte, že pro každé $k, n \geq 1$, $(k!)^n$ dělí $(kn)!$.

2.3 Binomické koeficienty

Nechť $n \geq k$ jsou nezáporná celá čísla. *Binomický koeficient* nebo *kombinační číslo* $\binom{n}{k}$ (čteme „en nad ká“, nikoliv „en nad ká*tou*“!) je funkce proměnných n, k, definovaná vzorcem

$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{1 \times 2 \times \cdots \times k} = \frac{\prod_{i=0}^{k-1}(n-i)}{k!}. \qquad (2.1)$$

Čtenář možná zná i jinou formuli, totiž

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}. \tag{2.2}$$

Ta je v naší situaci ekvivalentní (2.1). Z těchto dvou možných definic má (2.1) některé výhody. Číselná hodnota $\binom{n}{k}$ se z ní snadněji spočítá a při výpočtu vycházejí menší mezivýsledky. Navíc (2.1) má smysl pro libovolné reálné číslo n (o tom více v kapitole 10) a speciálně definuje hodnotu $\binom{n}{k}$ i pro přirozené číslo $n < k$; v takovém případě je hodnota $\binom{n}{k}$ rovna 0.

Základní kombinatorický význam kombinačního čísla $\binom{n}{k}$ je *počet všech k-prvkových podmnožin n-prvkové množiny.* To za chvilku dokážeme, nejdřív jedno označení.

2.3.1 Definice. *Nechť X je množina a k nezáporné celé číslo. Symbolem*

$$\binom{X}{k}$$

budeme značit množinu všech k-prvkových podmnožin množiny X.

Příklad:

$$\binom{\{a,b,c\}}{2} = \{\{a,b\},\{a,c\},\{b,c\}\}.$$

Symbol $\binom{x}{k}$ tedy má nyní dva významy, podle toho, zda x je číslo nebo množina. Následující tvrzení je dává do souvislosti:

2.3.2 Tvrzení. *Pro každou konečnou množinu X je počet všech jejích k-prvkových podmnožin roven $\binom{|X|}{k}$.*

V symbolech můžeme toto tvrzení zapsat

$$\left|\binom{X}{k}\right| = \binom{|X|}{k}.$$

Důkaz. Označme $n = |X|$. Budeme dvěma způsoby počítat všechny *uspořádané* k-tice, které lze utvořit z prvků množiny X (bez opakování). Na jedné straně tento počet je $n(n-1)\cdots(n-k+1)$ podle tvrzení 2.1.4 (viz poznámku za jeho důkazem). Na druhé straně, z jedné k-prvkové podmnožiny $M \in \binom{X}{k}$ můžeme vyrobit $k!$ různých uspořádaných k-tic, a každou uspořádanou k-tici dostaneme z nějaké podmnožiny právě jednou. Proto

$$n(n-1)\cdots(n-k+1) = k!\left|\binom{X}{k}\right|.$$

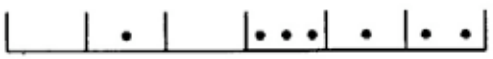
□

Ještě jedna základní úloha vedoucí ke kombinačním číslům. Kolika způsoby můžeme nezáporné celé číslo m zapsat jako součet r nezáporných celých sčítanců (přičemž záleží na pořadí sčítanců)? Jinak řečeno, chceme zjistit, kolik existuje uspořádaných r-tic $(i_1, i_2, \ldots, i_r)$ nezáporných celých čísel, splňujících rovnici

$$i_1 + i_2 + \cdots + i_r = m. \tag{2.3}$$

Odpověď je kombinační číslo $\binom{m+r-1}{r-1}$. To se dá dokázat různými způsoby; zde popíšeme důkaz téměř ve stylu kouzelnického triku.

Představme si, že každé proměnné $i_1, i_2, \ldots, i_r$ odpovídá jedna z r přihrádek. Máme m nerozlišitelných kuliček, a chceme je do těchto přihrádek nějak rozmístit (předpokládáme, že do každé z přihrádek se v případě potřeby vejde i všech m kuliček najednou). Každé možné rozmístění kóduje jedno řešení rovnice (2.3). Zajímá nás tedy, kolika způsoby můžeme rozmístit kuličky do přihrádek. Jedno takové rozmístění, pro $m = 7$ a $r = 6$, vypadá takto:



Odpovídá rozkladu $0 + 1 + 0 + 3 + 1 + 2 = 7$. Necháme nyní zmizet dna přihrádek a dvě krajní stěny, takže zůstane jen m kuliček a $r - 1$ přepážek, oddělujících přihrádky:

| • | | • • • | • | • •

(navíc jsme pro lepší estetický dojem kuličky a přihrádky trochu posunuli). Tato situace stále obsahuje plnou informaci o rozdělení kuliček do přihrádek. Zvolit takové rozdělení tedy znamená vybrat pozice vnitřních přepážek mezi kuličkami. Jinak řečeno, máme $m+r-1$ předmětů, kuliček a vnitřních přepážek, srovnaných v řadě, a určíme, které pozice zaujmou kuličky a které přepážky. To odpovídá výběru $r-1$ pozic z $m+r-1$ možných, takže se to dá udělat $\binom{m+r-1}{r-1}$ způsoby. □

Jednoduché vlastnosti kombinačních čísel. Jedním dobře známým vzorcem je

$$\binom{n}{k} = \binom{n}{n-k}. \tag{2.4}$$

Jeho správnost (pro $n \geq k \geq 0$) je ihned vidět z již zmíněného vztahu $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ Kombinatoricky to znamená, že k-prvkových podmnožin n-prvkové množiny je stejně jako podmnožin s $n-k$ prvky, což můžeme nahlédnout bez odvolávání se na kombinační čísla — stačí každé k-prvkové podmnožině přiřadit její doplněk.

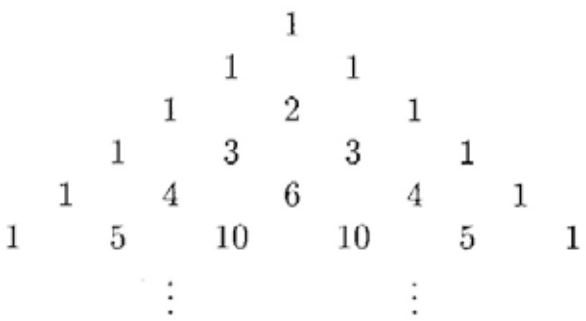
Dosti důležitý je vzorec pro součet kombinačních čísel

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}. \tag{2.5}$$

Jeden elegantní důkaz je založen na kombinatorické interpretaci obou stran (2.5). Pravá strana je počet k-prvkových podmnožin nějaké n-prvkové množiny X. Zvolme jeden prvek $a \in X$ a rozdělme všechny k-prvkové podmnožiny X do dvou skupin podle toho, zda obsahují a. Podmnožiny neobsahující a jsou právě všechny k-prvkové podmnožiny $X \setminus \{a\}$, a je jich tudíž $\binom{n-1}{k}$. Je-li A nějaká k-prvková podmnožina X obsahující prvek a, můžeme jí přiřadit $(k-1)$-prvkovou množinu $A' = A \setminus \{a\}$. Je snadno vidět, že toto přiřazení je bijekce mezi všemi k-prvkovými podmnožinami X obsahujícími prvek a a všemi $(k-1)$-prvkovými podmnožinami množiny $X \setminus \{a\}$. Posledně jmenovaných

je $\binom{n-1}{k-1}$. Dohromady je tedy počet všech k-prvkových podmnožin X roven $\binom{n-1}{k} + \binom{n-1}{k-1}$. □

S identitou (2.5) je spojen tzv. Pascalův trojúhelník:



Každý další řádek v tomto schématu se vyrobí tak, že pod dvojici čísel z předchozího řádku se napíše jejich součet, a na kraje se doplní jedničky. Z (2.5) indukcí vyplývá, že v $(n+1)$-ním řádku jsou právě binomické koeficienty $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$.

Binomická věta. Rovnice (2.5) se také dá využít pro důkaz jiného známého tvrzení zahrnujícího binomické koeficienty — binomické věty (odtud i název „binomické koeficienty"). Tato věta praví, že pro nezáporné celé číslo n

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \tag{2.6}$$

(je to rovnost dvou mnohočlenů v proměnné x, speciálně tedy platí pro každé konkrétní reálné číslo x).

Z binomické věty můžeme dostat všelijaké vztahy pro binomické koeficienty. Nejjednodušší z nich vznikne patrně posazením $x = 1$ a zní

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n. \tag{2.7}$$

Kombinatoricky to ovšem není nic jiného než počítání všech podmnožin n-prvkové množiny; na levé straně jsme je napřed rozdělili podle velikosti.

Druhý důkaz tvrzení 2.1.3 (o počtu podmnožin liché velikosti). Dosazením $x = -1$ do binomické věty vyjde

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \cdots = \sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0. \qquad (2.8)$$

Sečteme-li tuto rovnost s (2.7), budou na levé straně jen binomické koeficienty se sudým k, a každý z nich bude vynásoben 2, t.j.

$$2\left[\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \ldots\right] = 2^n.$$

V hranaté závorce na levé straně stojí právě počet všech podmnožin n-prvkové množiny se sudým počtem prvků. Proto má n-prvková množina právě 2^{n-1} podmnožin sudé velikosti. □

Další identity s kombinačními čísly. Jsou známy doslova tisíce různých vztahů a identit pro kombinační čísla; jsou jim věnovány celé knihy. Zde si předvedeme ještě jednu formuli, která má pěkný kombinatorický důkaz. Další vzorce zmíníme ve cvičení a v kapitole 10.

2.3.3 Tvrzení.

$$\sum_{i=0}^{n} \binom{n}{i}^2 = \binom{2n}{n}.$$

Důkaz. První trik je přepsat sumu pomocí (2.4) — symetrie kombinačního čísla — na

$$\sum_{i=0}^{n} \binom{n}{i}\binom{n}{n-i}.$$

Teď ukážeme, že tato suma vyjadřuje počet n-prvkových podmnožin $2n$-prvkové množiny (a tedy se rovná pravé straně v dokazovaném vzorci). Vezměme $2n$-prvkovou množinu X, a obarvěme n jejích prvků červeně a zbývajících n prvků modře. Zvolit podmnožinu množiny X znamená totéž, jako zvolit nějakou i-prvkovou podmnožinu červených prvků a nějakou $(n-i)$-prvkovou podmnožinu modrých prvků, kde

$i \in \{0, 1, \ldots, n\}$. Pro dané i máme pro výběr červené podmnožiny $\binom{n}{i}$ možností, a pro výběr modré podmnožiny $\binom{n}{n-i}$ možností, celkem tedy $\sum_{i=0}^{n} \binom{n}{i}\binom{n}{n-i}$ možností volby červené a modré podmnožiny s dohromady n prvky. □

Multinomické koeficienty a multinomická věta. Jeden z oblíbených příkladů v amerických učebnicích je tenhle: Kolik různých slov (včetně nesmyslných) můžeme sestavit s použitím (všech) písmen slova MISSISSIPPI? (Tím doufáme čtenáře, v případě potřeby, i nenásilně poučit o pravopisu.) Nejdřív si představme, že stejná písmena v názvu otce řek odlišíme indexy: $M_1I_1S_1S_2I_2S_3S_4I_3P_1P_2I_4$. Tím máme 11 různých písmen, která lze rozestavit 11! různými způsoby. Uvažme nyní jedno (libovolné) slovo vyrobené z „neoindexované" MISSISSIPPI, např. SIPISMSIPIS. Z kolika „oindexovaných" rozestavení vznikne toto slovo vymazáním indexů? Indexy u čtyř písmen S mohou být rozmístěny 4! způsoby, nezávisle na tom indexy u čtyř I také 4! způsoby, pro dvě P máme 2! možností, a konečně pro jediné M jednu (neboli 1!) možnost. Tím pádem slovo SIPISMSIPIS (i každé jiné utvořené z MISSISSIPPI) lze oindexovat 4!4!2!1! způsoby, a proto počet neoindexovaných slov, t.j. odpověď na úlohu, je 11!/(4!4!2!1!).

Stejnou úvahou se zjistí následující výsledek: máme-li předměty m druhů, k_i předmětů od i-tého druhu (a předměty jednoho druhu jsou nerozlišitelné), přičemž $k_1 + \cdots + k_m = n$, potom počet jejich různých seřazení je dán výrazem

$$\frac{n!}{k_1!k_2!\cdots k_m!}.$$

Tento výraz se někdy zapisuje symbolem

$$\binom{n}{k_1, k_2, \ldots, k_m}$$

a nazývá se *multinomický koeficient*. Speciálně pro $m = 2$ dostáváme binomický koeficient, tedy $\binom{n}{k,n-k}$ je totéž co $\binom{n}{k}$. Proč název multinomický koeficient? Vysvětlení dává následující věta:

2.3.4 Věta (Multinomická věta). *Pro libovolná čísla $x_1, \ldots, x_m \in \mathbf{R}$ a libovolné celé $n \geq 1$ platí rovnost*

$$(x_1 + x_2 + \cdots + x_m)^n = \sum_{\substack{k_1+\cdots+k_m=n \\ k_1,\ldots,k_m \geq 0}} \binom{n}{k_1, k_2, \ldots, k_m} x_1^{k_1} x_2^{k_2} \ldots x_m^{k_m}.$$

Tato věta se dá dokazovat, podobně jako věta binomická, indukcí podle n (viz cvičení 21). Přirozenější důkaz vyplyne z metod části 10.1 (cvičení 3).

Cvičení

1. Dokažte součtový vzorec (2.5) použitím definice (2.1) pro kombinační čísla a početní úpravou.

2. (a) Dokažte vzorec

$$\binom{r}{r} + \binom{r+1}{r} + \binom{r+2}{r} + \cdots + \binom{n}{r} = \binom{n+1}{r+1}. \qquad (2.9)$$

indukcí podle n (při pevném r). Uvědomte si, co říká pro $r = 1$.

(b)* Dokažte týž vzorec kombinatoricky.

3.* Pro přirozená čísla $m \leq n$ spočítejte (=vyjádřete jednoduchým vzorcem bez použití sumy) $\sum_{k=m}^{n} \binom{k}{m}\binom{n}{k}$.

4. Spočítejte (=vyjádřete jednoduchým vzorcem bez použití sumy)

(a) $\sum_{k=1}^{n} \binom{k}{m}\frac{1}{k}$,

(b)* $\sum_{k=0}^{n} \binom{k}{m}k$.

5.** Dokažte

$$\sum_{k=0}^{m} \binom{m}{k}\binom{n+k}{m} = \sum_{k=0}^{m} \binom{m}{k}\binom{n}{k}2^k.$$

6.* Kolik existuje funkcí $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$, které jsou *monotoní*, t.j. pro $i < j$ platí $f(i) \leq f(j)$?

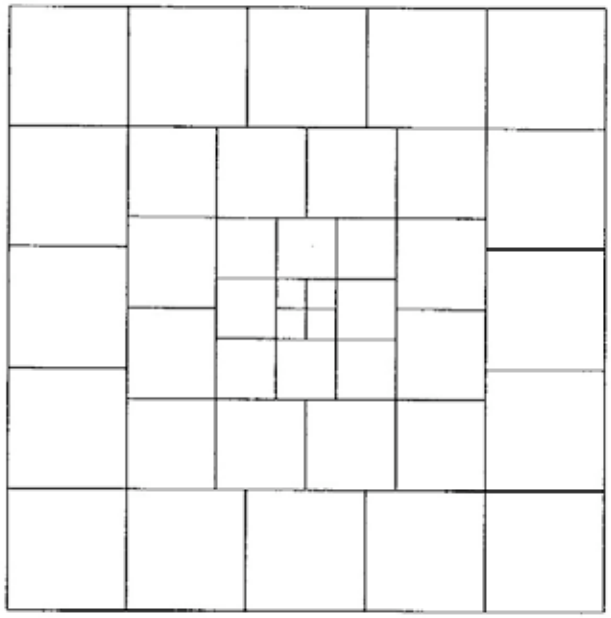
7. Kolik členů má rozvoj výrazu $(x_1 + \cdots + x_m)^n$ podle multinomické věty?

8.* Kolik existuje k-prvkových podmnožin množiny $\{1, 2, \ldots, n\}$, v nichž se nevyskytují žádná 2 po sobě jdoucí čísla?

9. (a) S použitím vzorce (2.9) pro $r = 2$ vyjádřete součty $\sum_{i=2}^{n} i(i-1)$ a $\sum_{i=1}^{n} i^2$.

(b) S pomocí (a) a vzorce (2.9) pro $r = 3$ spočítejte $\sum_{i=1}^{n} i^3$.

(c)* Odvoďte výsledek (b) podle obrázku 2.1.



Obrázek 2.1: Grafické odvození vztahu $1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2 = \binom{n+1}{2}^2$.

10. Dokažte binomickou větu indukcí podle n.

11. Dokažte *Leibnizovu formuli* pro derivování součinu: nechť u, v jsou funkce jedné proměnné, $u^{(k)}$ značí k-tou derivaci funkce u. Potom

$$(uv)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} u^{(k)} v^{(n-k)}$$

(za předpokladu že všechny uvedené derivace existují).

12. Buď p prvočíslo, n, k přirozená čísla.
    (a) Dokažte, že pro $k < p$ je $\binom{p}{k}$ dělitelné p.
    (b) Dokažte, že $\binom{n}{p}$ je dělitelné p právě když $\lfloor n/p \rfloor$ je dělitelné p.

13. (a)* Pomocí binomické věty odvoďte vztah pro počet podmnožin n-prvkové množiny, jejichž velikost je dělitelná 4.
    (b)* Spočítejte počet podmnožin n-prvkové množiny velikosti dělitelné 3.

14. Máme n druhů předmětů, a chceme určit, kolika způsoby můžeme vybrat k-tici předmětů. Uvažujeme varianty jednak podle toho, zda

vybíráme uspořádané nebo neuspořádané k-tice, a jednak podle toho, zda máme k dispozici od každého druhu jen 1 předmět nebo libovolně mnoho předmětů. Vyplňte počty v následující tabulce:

	Jen 1 předmět každého druhu	Libovolně předmětů každého druhu
Uspořádané k-tice		
Neuspořádané k-tice		

15. Máme k kuliček, rozmísťujeme je do n (očíslovaných) přihrádek. Vyplňte počty možných rozmístění ve variantách v následující tabulce:

	≤ 1 kulička do každé přihrádly	Libovolný počet kuliček do přihrádky
Kuličky jsou různobarevné (rozlišitelné)		
Kuličky jsou nerozlišitelné		

16.* Kolika způsoby lze rozestavit 5 vodníků a 7 čarodějnic do řady tak, že žádní 2 vodníci nestojí vedle sebe?

17. Na stole je prostřeno 13 velkých talířů, máme 5 vařených raků (nerozlišitelných) a 8 nadívaných hlemýžďů (též nerozlišitelných). Kolik je způsobů, jak servírovat raky a hlemýždě na talíře (podstatný je postup servírování, t.j. jako bychom se ptali na počet různých filmových scénářů popisujících servírování, např. „nandat hlemýždě na talíř č.5, potom nandat raka na talíř č.7, ...)

(a) má-li se něco nadělit na každý talíř

(b) není-li žádné takové omezení, t.j. např. všechno může přijít na jeden talíř.

18. V senátu zasedá 100 senátorů, po 2 z každého z 50 států. Kolika způsoby lze zvolit 4-členný výbor tak, aby v něm nebyli 2 senátoři z téhož státu?

19.* Uvažme pravidelný n-úhelník. Rozdělíme ho diagonálami na trojúhelníky tak, aby každý z nich měl aspoň jednu stranu společnou s naším n-úhelníkem. Kolik existuje takových rozdělení (triangulací)?

20. Najděte koeficient při x^2y^4z ve výrazu $(2x + y^2 - 5z)^7$.

21. (a) Dokažte rovnost

$$\binom{n}{k_1, k_2, \ldots, k_m} = \binom{n-1}{k_1 - 1, k_2, k_3, \ldots, k_m} + \binom{n-1}{k_1, k_2 - 1, k_3, \ldots, k_m} + \cdots + \binom{n-1}{k_1, k_2, \ldots, k_{m-1}, k_m - 1}$$

$(n \geq 1,\ k_1 + \cdots + k_m = n,\ k_i \geq 1)$.

(b) Dokažte multinomickou větu indukcí podle n.

2.4 Odhady funkcí: faktoriál

V této části budeme odpovídat na otázku „Jak rychle roste funkce $n!$ (faktoriál čísla n)?“.

Na první pohled se může zdát, že sama definice faktoriálu, $n! = 1 \times 2 \times \cdots \times n$, nám o této funkci říká všechno, co můžeme kdy potřebovat: Pro malé n lze $n!$ velmi rychle vyčíslit na počítači, a pro větší n by leckdo mohl prohlásit, že hodnoty faktoriálu již nemají v „reálném“ světě žádný smysl, neboť jsou příliš velké — např. již $70! > 10^{100}$, jak asi ví mnoho majitelů kalkulaček. V různých matematických úvahách však potřebujeme srovnat rychlost růstu funkce $n!$ s jinými funkcemi, a to i pro velmi velké hodnoty n. K tomu samotná definice není zvlášť vhodná, a často ani výpočet hodnot počítačem moc nepomůže. V takových situacích přijdou ke slovu *odhady*, které vyšetřovanou funkci, třeba $n!$, šikovně srovnávají s nějakou „jednodušší“ funkcí, například vhodnou mocninnou funkcí a podobně. V následujícím si několik takových odhadů předvedeme. Ukážeme několik metod a triků, jimiž se dají dělat odhady i pro jiné funkce, sumy, součiny a pod. Nejdříve

ale zavedeme užitečné značení pro porovnávání rychlosti růstu funkcí, hojně používané např. při analýze algoritmů.

Asymptotické porovnávání funkcí. Často je potřeba vyjádřit skutečnosti jako např. že funkce n^2 je „větší" než funkce $10n+5$ a „zhruba stejně velká" jako funkce $n^2 + n\sqrt{n}$ (přitom chceme porovnávat rychlost růstu funkcí pro velká n). K tomu se zavádí následující definice.

Nechť f, g jsou reálné funkce jedné proměnné definované na přirozených číslech, přičemž zpravidla předpokládáme, že hodnoty f i g jsou nezáporné. Zápis

$$f(n) = O(g(n))$$

znamená, že existuje konstanta C taková, že pro všechna $n \in \mathbf{N}$ platí $|f(n)| \leq Cg(n)$. Místo $f(n)$ a $g(n)$ se v tomto zápise objevují i konkrétní formule; například můžeme psát $10n^2 + 5n = O(n^2)$. Zápisu $f(n) = O(g(n))$ tedy můžeme rozumět tak, že funkce f neroste podstatně rychleji než g, neboli že $f(n)/g(n)$ neroste do nekonečna. Zdůrazněme ještě, že ačkoliv se v zavedeném zápisu vyskytuje rovnítko, zápis je nesymetrický (ve své podstatě je to nerovnost); nepíše se $O(f(n)) = g(n)$!

Poznámky. Někdy se podobný zápis používá i pro funkce více proměnných; například $f(m,n) = O(g(m,n))$ znamená, že pro nějakou konstantu C a pro všechny hodnoty m a n platí $|f(n,m)| \leq Cg(m,n)$.

Zdánlivě jiná definice vztahu $f(n) = O(g(n))$ říká, že existují čísla C_0 a n_0 taková, že pro všechna $n \geq n_0$ platí $|f(n)| \leq C_0.g(n)$. Ve skutečnosti je to ale ekvivalentní s naší definicí (ponecháváme jako snadné cvičení).

Pomocí symbolu $O(.)$ můžeme zapsat i přesnější srovnání funkcí. Třeba zápisu $f(n) = g(n) + O(n^3)$ se má rozumět tak, že funkce f roste stejně rychle jako g, až na „chybu" řádu n^3, neboli že $f(n) - g(n) = O(n^3)$. Jednoduchý konkrétní příklad je např.

$$\binom{n}{2} = \frac{n(n-1)}{2} = \frac{n^2}{2} + O(n).$$

V literatuře se běžně vyskytuje ještě několik symbolů pro jiné „nerovnosti" mezi rychlostí růstu funkcí. Pro přehled uvedeme jejich definice ve formě tabulky:

Zápis	Definice	Význam
$f(n) = o(g(n))$	$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$	f roste podstatně pomaleji než g
$f(n) = \Omega(g(n))$	$g(n) = O(f(n))$	f roste aspoň tak rychle jako g
$f(n) = \Theta(g(n))$	$f(n) = O(g(n))$ a $f(n) = \Omega(g(n))$	f a g rostou řádově stejně rychle
$f(n) \sim g(n)$	$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$	$f(n)$ a $g(n)$ rostou asi stejně rychle

Odhady funkce faktoriál. Pro každé $n \geq 1$ je zřejmě pravda

$$n! \leq n^n$$

jak je vidět z definice faktoriálu.

Přesnější odhad ukázal pěkným trikem Gauss (neboli, německy psáno, Gauß):

2.4.1 Věta. *Pro každé $n \geq 1$*

$$n^{n/2} \leq n! \leq \left(\frac{n+1}{2}\right)^n.$$

Důkaz začneme nerovností mezi aritmetickým a geometrickým průměrem. Pro kladná reálná čísla a, b definujeme *aritmetický průměr* a a b výrazem $\frac{a+b}{2}$, a *geometrický průměr* a a b výrazem $\sqrt{ab}$.

2.4.2 Lemma. *Pro každou dvojici kladných reálných čísel a, b, geometrický průměr je nejvýše roven aritmetickému.*

Důkaz. Druhá mocnina reálného čísla je vždy kladná, speciálně tedy $(\sqrt{a} - \sqrt{b})^2 \geq 0$. Po rozepsání levé strany máme $a - 2\sqrt{ab} + b \geq 0$, a

přičtením výrazu $2\sqrt{ab}$ k oběma stranám nerovnosti a dělením 2 vyjde $\sqrt{ab} \leq (a+b)/2$, což je požadovaná nerovnost. □

Důkaz věty 2.4.1. Platí

$$\begin{aligned}(n!)^2 &= 1 \times 2 \times \cdots \times (n-1) \times n \times n \times (n-1) \times \cdots \times 2 \times 1 = \\ &(1 \times n)(2 \times (n-1)) \cdots ((n-1) \times 2)(n \times 1) = \\ &\prod_{i=1}^{n} i(n+1-i)\end{aligned} \tag{2.10}$$

(čísla v součinu jsme jenom přerovnali a sdružili do dvojic). Zvolíme-li v lemmatu 2.4.2 $a = i$, $b = n+1-i$, dostáváme

$$\sqrt{i(n+1-i)} \leq \frac{i+n+1-i}{2} = \frac{n+1}{2},$$

čili podle (2.11)

$$n! = \prod_{i=1}^{n} \sqrt{i(n+1-i)} \leq \prod_{i=1}^{n} \frac{n+1}{2} = \left(\frac{n+1}{2}\right)^n,$$

což dokazuje jednu z nerovností v tvrzení věty 2.4.1. Abychom ukázali druhou nerovnost, uvažme součin $i(n+1-i)$. Pro $i = 1$ a $i = n$ je roven n, a pro $2 \leq i \leq n-1$ máme součin dvou čísel, z nichž větší je aspoň $n/2$ a menší je nejméně 2, tedy součin je také nejméně n. Pokaždé tedy $i(n+1-i) \geq n$, a odtud

$$(n!)^2 = \prod_{i=1}^{n} i(n+1-i) \geq \prod_{i=1}^{n} n = n^n,$$

a proto $n! \geq \sqrt{n^n} = n^{n/2}$, jak jsme chtěli dokázat. □

Příklad. Každý z n lidí si z osudí obsahujícího čísla $1, 2, \ldots, n$ vylosuje jedno číslo, zapamatuje si ho a vrátí do osudí. Jaká je pravděpodobnost, že žádní dva nemají totéž číslo? Řečeno matematicky, jaká je pravděpodobnost, že náhodně zvolené zobrazení množiny $\{1, 2, \ldots, n\}$ do sebe

bude permutace? Všech zobrazení je n^n, permutací je $n!$, hledaná pravděpodobnost je $n!/n^n$. Z horního odhadu z věty 2.4.1 spočítáme

$$\frac{n!}{n^n} \leq \left(\frac{n+1}{n}\right)^n 2^{-n} \leq e\,2^{-n},$$

hledaná pravděpodobnost tedy exponenciálně klesá. Z přesnějších odhadů dokázaných níže se pak dostane, že uvedená pravděpodobnost se chová přibližně jako funkce e^{-n}.

Teď jinými postupy odhad z věty 2.4.1 vylepšíme. V dokonalejším odhadu bude vystupovat *Eulerovo číslo* $e = 2.718281828\ldots$, základ přirozených logaritmů. O této pozoruhodné konstantě se čtenář více dozví v matematické analýze. Zde budeme potřebovat následující užitečný

2.4.3 Fakt. *Pro každé reálné číslo* x,

$$1 + x \leq e^x$$

(viz obrázek 2.2).

S jeho pomocí dokážeme

2.4.4 Věta. *Pro každé* $n \geq 1$,

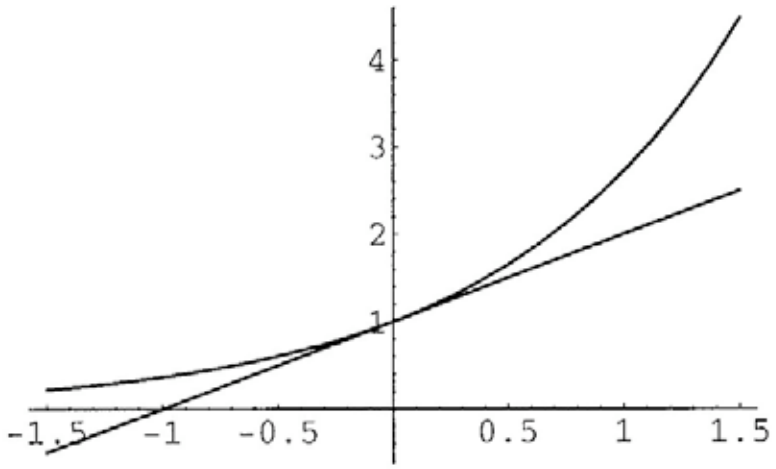
$$e\left(\frac{n}{e}\right)^n \leq n! \leq en\left(\frac{n}{e}\right)^n.$$

První důkaz (matematickou indukcí). Ukážeme pouze horní odhad $n! \leq en(n/e)^n$, dolní odhad ponecháváme jako cvičení 8. Pro $n = 1$ je pravá strana nerovnosti rovna 1, tvrzení tedy platí. Předpokládejme, že jsme je již dokázali pro $n-1$, a odvodíme je pro n. Máme

$$n! = n(n-1)! \leq ne(n-1)\left(\frac{n-1}{e}\right)^{n-1}$$

podle indukčního předpokladu. Pravou stranu dále upravíme na tvar

$$\left[en\left(\frac{n}{e}\right)^n\right] \times \left(\frac{n-1}{n}\right)^n e.$$



Obrázek 2.2: Funkce $y = 1 + x$ a $y = e^x$ v okolí počátku.

V hranaté závorce je výraz, kterým bychom potřebovali shora omezit $n!$, abychom dostali dokazovanou nerovnost pro n. Stačí tedy ukázat, že zbývající část výrazu nepřevyšuje 1. Úpravou a použitím faktu 2.4.3 pro $x = -\frac{1}{n}$ dostáváme

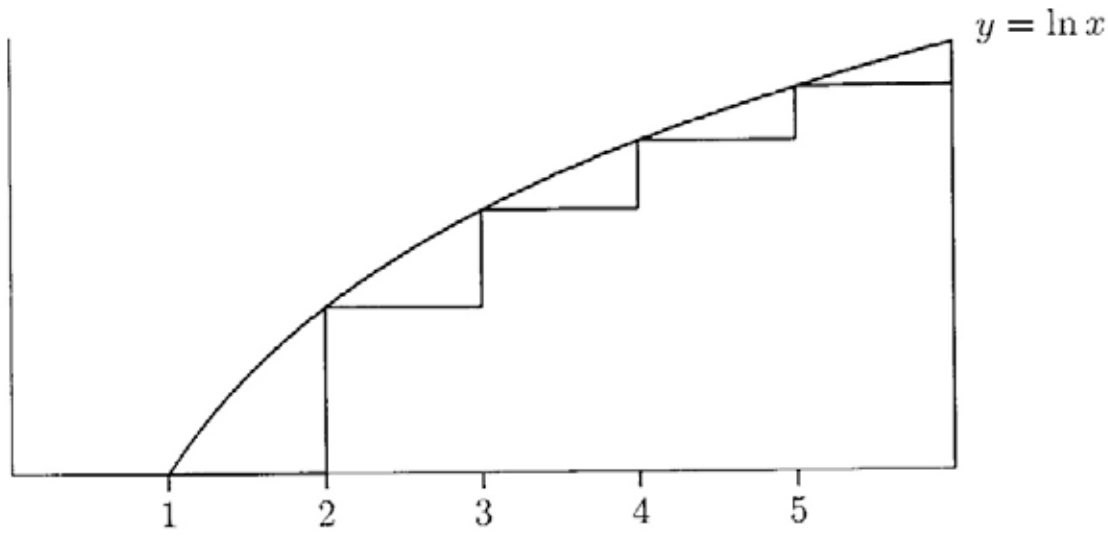
$$e\left(\frac{n-1}{n}\right)^n = e\left(1-\frac{1}{n}\right)^n \leq e\left(e^{-1/n}\right)^n = e \times e^{-1} = 1.$$

□

Druhý důkaz (pomocí integrálu). Zase uděláme jenom horní odhad. Vyjdeme z definice faktoriálu $n! = 1 \times 2 \times \cdots \times n$ a obě strany zlogaritmujeme. Máme tedy

$$\ln n! = \ln 1 + \ln 2 + \cdots + \ln n$$

(funkce ln je logaritmus o základu e). Výraz na pravé straně si můžeme představit jako plochu pod grafem stupňovité funkce na intervalu



Obrázek 2.3: Odhad plochy pod stupňovitou funkcí pomocí integrálu

$[1, n+1]$, jejíž hodnota na intervalu $[i, i+1)$ je rovna $\ln i$, viz obr. 2.3. Uvedená stupňovitá funkce je v každém bodě $x \in [1, n+1)$ nejvýš rovna $\ln x$, čili plocha pod jejím grafem nepřevyšuje plochu pod grafem funkce $\ln x$ na tomto intervalu. Odtud

$$\ln n! \leq \int_1^{n+1} \ln x \, \mathrm{d}x = (n+1)\ln(n+1) - n,$$

jak se spočte jako jednoduché cvičení na integrování. Tento odhad můžeme dále upravit

$$n! \leq e^{(n+1)\ln(n+1)-n} = \frac{(n+1)^{n+1}}{e^n}.$$

To ještě není ten tvar, který chceme. Ale, můžeme použít tento vzorec pro $n-1$, a tím už vyjde tvar, uvedený ve větě:

$$n! = n(n-1)! \leq n\,\frac{n^n}{e^{n-1}} = en\left(\frac{n}{e}\right)^n.$$

□

Pro zajímavost (a pro vzbuzení čtenářovy zvědavosti?) zmiňme ještě přesnější odhad pro $n!$, známý pod jménem *Stirlingova formule*: Definujeme-li funkci

$$f(n) = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$

(kde $\pi = 3.1415926535\ldots$ je Ludolfovo číslo), platí $f(n) \sim n!$, neboli

$$\lim_{n\to\infty} \frac{f(n)}{n!} = 1,$$

to znamená, že odhadneme-li číslo $n!$ hodnotou $f(n)$, pak relativní chyba tohoto odhadu se blíží 0 pro n rostoucí do nekonečna; např. pro $n = 8$ je chyba okolo 1%. Všimněme si, že Stirlingova formule je zhruba „uprostřed" mezi odhady z věty 2.4.4 (viz též cvičení 9).

Cvičení

1. Rozmyslete si, co říkají následující zápisy, a rozhodněte, zda jsou pravdivé.
   (a) $n^2 = O(n^2 \ln n)$
   (b) $n^2 = o(n^2 \ln n)$
   (c) $n^2 + 5n \ln n = n^2\big(1 + o(1)\big) \sim n^2$
   (d) $n^2 + 5n \ln n = n^2 + O(n)$
   (e) $n! \sim ((n+1)/2)^n$
   (f) $\ln(n!) = \Omega(n \ln n)$
   (g) $\sum_{i=1}^{n} i^8 = \Theta(n^9)$
   (h) $\sum_{i=1}^{n} \sqrt{i} = \Theta(n^{3/2})$.

2. Jaký je význam zápisů: $C = O(1)$, $c = \Omega(1)$, $f(n) = n^{O(1)}$? Jak je krátce vyjádřit bez použití symbolu $O(.)$?

3. Srovnejte následující funkce podle rychlosti růstu, a zapište vztahy mezi nimi pomocí značení, zavedeného v této části: $n \ln n$, $(\ln \ln n)^{\ln n}$, $(\ln n)^{\ln \ln n}$, $ne^{\sqrt{\ln n}}$, $(\ln n)^{\ln n}$, $n2^{\ln \ln n}$, $n^{1+1/(\ln \ln n)}$, $n^{1+1/\ln n}$, n^2.

4.* Dokažte fakt 2.4.3.

5. (a) Vyšetřete, pro které dvojice reálných čísel (a, b), $a, b > 0$, platí $\sqrt{ab} = (a+b)/2$.
   (b) *Harmonický průměr* kladných čísel a, b se definuje výrazem $2ab/(a+b)$. Zjistěte, v jakém vztahu (nerovnosti) je harmonický průměr vzhledem k aritmetickému a geometrickému.

6. Nechť $x_1, x_2, \ldots, x_n$ jsou kladná reálná čísla. Jejich *aritmetický průměr* je $(x_1 + x_2 + \cdots + x_n)/n$, a jejich *geometrický průměr* se definuje jako $\sqrt[n]{x_1 x_2 \cdots x_n}$. Nechť $AG(n)$ značí tvrzení „pro každou n-tici kladných reálných čísel $x_1, x_2, \ldots, x_n$ je geometrický průměr nejvýš roven aritmetickému". Dokažte platnost $AG(n)$ pro každé n následující (podivnou) indukcí:

   (a) Dokažte že z $AG(n)$ plyne $AG(2n)$, pro libovolné n.

   (b)* Dokažte že z $AG(n)$ plyne $AG(n-1)$, pro libovolné $n > 1$.

   (c) Vysvětlete, proč z (a) a (b) plyne platnost $AG(n)$ pro všechna n.

7.* Definujme posloupnosti $\{a_n\}$ a $\{b_n\}$ takto: $a_0 = 2$, $b_0 = 4$, $a_{n+1} = \sqrt{a_n b_n}$, $b_{n+1} = 2a_{n+1}b_n/(a_{n+1}+b_n)$. Dokažte, že obě posloupnosti konvergují k číslu π (návod: najděte souvislost s pravidelnými mnohoúhelníky opsanými a vepsanými jednotkové kružnici). *Poznámka:* Tato metoda (Archimedova) výpočtu π není příliš efektivní. Mnohem rychlejší algoritmus je např. tento: $x_1 = 2^{-3/4} + 2^{-5/4}$, $y_1 = \sqrt[4]{2}$, $\pi_0 = 2 + \sqrt{2}$, $\pi_n = \pi_{n-1}(x_n + 1)/(y_n + 1)$, $y_{n+1} = (y_n\sqrt{x_n} + 1/\sqrt{x_n})/(y_n + 1)$, $x_{n+1} = (\sqrt{x_n} + 1/\sqrt{x_n})/2$. Tento i další algoritmy a pozoruhodnou související teorii lze najít např. v [5].

8. Dokažte dolní odhad $n! \geq e(n/e)^n$ ve větě 2.4.4

   (a) indukcí (šikovně využijte faktu 2.4.3),

   (b) pomocí integrálu.

9.* Dokažte následující horní odhad (který je již velmi blízký Stirlingově formuli): $n! \leq e\sqrt{n}\,(n/e)^n$. Vyjděte z důkazu věty 2.4.4 pomocí integrálu, ale od plochy pod křivkou $y = \ln x$ odečtěte ještě plochu vhodných trojúhelníčků.

10. Dokažte *Bernoulliho nerovnost*: Pro každé přirozené n a pro každé reálné $x \geq -1$ platí $(1 + x)^n \geq 1 + nx$.

11. Dokažte, že pro $n = 1, 2, \ldots,$

$$2\sqrt{n+1} - 2 < 1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} \leq 2\sqrt{n} - 1.$$

12. V analýze různých algoritmů se často objevuje součet $H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} = \sum_{i=1}^{n} \frac{1}{i}$ (tzv. *harmonické číslo*).

   (a) Ukažte, že pro každé přirozené m, $1 + \frac{m}{2} \leq H_n < m + 1$, kde $n = 2^m$.

   (b) Dokažte pomocí integrálu, že $\ln n < H_n < \ln n + 1$.

2.5 Odhady: binomické koeficienty

Podobně jako jsme vyšetřovali chování funkce $n!$, budeme se teď zabývat funkcí

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{1\times 2\times\cdots\times k} = \prod_{i=0}^{k-1}\frac{n-i}{k-i}. \tag{2.11}$$

Je hned vidět, že

$$\binom{n}{k} \le n^k,$$

a pro mnoho použití s tímto jednoduchým odhadem vystačíme. Pro $k > n/2$ je ovšem výhodné napřed použít vztahu $\binom{n}{k} = \binom{n}{n-k}$.

Abychom odvodili dolní odhad, podíváme se na definici binomického koeficientu zapsanou jako součin zlomků, tak jako v (2.11). Pro $n \ge k > i \ge 0$ platí $(n-i)/(k-i) \ge n/k$, a proto

$$\binom{n}{k} \ge \left(\frac{n}{k}\right)^k.$$

Následující vylepšený horní odhad je podobného tvaru, a na jeho důkazu předvedeme ještě jednu další metodu.

2.5.1 Věta. *Pro každé $n \ge 1$ a pro každé k, $1 \le k \le n$, platí*

$$\binom{n}{k} \le \left(\frac{en}{k}\right)^k.$$

Důkaz. Ukážeme ve skutečnosti silnější nerovnost

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{k} \le \left(\frac{en}{k}\right)^k.$$

Vyjdeme z binomické věty, která pro libovolné reálné číslo x tvrdí

$$\binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n = (1+x)^n.$$

Předpokládejme nyní, že $0 < x < 1$. Potom vynecháním některých sčítanců na levé straně dostaneme

$$\binom{n}{0} + \binom{n}{1}x + \cdots + \binom{n}{k}x^k \le (1+x)^n,$$

a vydělením obou stran číslem x^k máme

$$\frac{1}{x^k}\binom{n}{0} + \frac{1}{x^{k-1}}\binom{n}{1} + \cdots + \binom{n}{k} \leq \frac{(1+x)^n}{x^k}.$$

Každé z kombinačních čísel na levé straně je vynásobeno číslem větším nebo rovným jedné (poněvadž jsme předpokládali $x < 1$); vynecháme-li tyto koeficienty, levou stranu nezvětšíme. Vyjde

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{k} \leq \frac{(1+x)^n}{x^k}.$$

Číslo x z intervalu $(0,1)$ můžeme zvolit podle potřeby, a uděláme to tak, abychom učinili pravou stranu co nejmenší. Vhodná hodnota je $x = \frac{k}{n}$. Dosazením tohoto výrazu do pravé strany máme

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{k} \leq \left(1 + \frac{k}{n}\right)^n \left(\frac{n}{k}\right)^k.$$

Konečně s využitím faktu 2.4.3 vychází

$$\left(1 + \frac{k}{n}\right)^n \leq \left(e^{k/n}\right)^n = e^k,$$

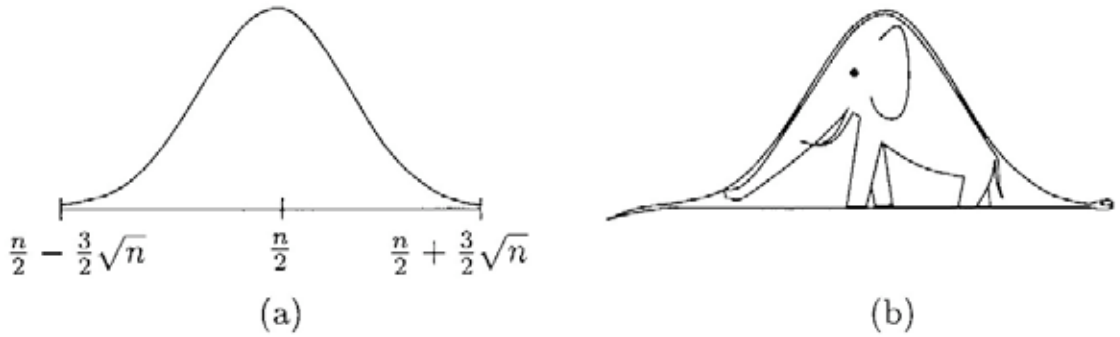
a z toho už máme tvrzení věty 2.5.1. □

Kombinační číslo $\binom{n}{\lfloor n/2 \rfloor}$. Z definice kombinačního čísla snadno plyne následující vzorec:

$$\binom{n}{k} = \frac{n-k+1}{k}\binom{n}{k-1}.$$

Proto pro $k \leq n/2$ máme $\binom{n}{k} > \binom{n}{k-1}$, a naopak pro $k \geq n/2$ dostaneme symetricky $\binom{n}{k} > \binom{n}{k+1}$. Tudíž pro dané n jsou mezi kombinačními čísly $\binom{n}{k}$ největší ta prostřední: pro n sudé je $\binom{n}{n/2}$ větší než všechna ostatní, pro n liché jsou dvě největší kombinační čísla, $\binom{n}{\lfloor n/2 \rfloor}$ a $\binom{n}{\lceil n/2 \rceil}$.

Chování kombinačních čísel $\binom{n}{k}$ pro dané velké n a pro k blízké $n/2$ je znázorněno na obr. 2.4(a). Graf ve skutečnosti není souvislá křivka



Obrázek 2.4: Znázornění relativní velikosti kombinačních čísel $\binom{n}{k}$ pro jedno velké n a k blízké $\frac{n}{2}$ (a); možná též klobouk, případně hroznýš, který sežral slona (b) — viz [18].

(protože $\binom{n}{k}$ je definováno jen pro celá k), ale pro velké n je bodů tolik, že vizuálně splývají v křivku. „Výška" této křivky je právě $\binom{n}{\lfloor n/2 \rfloor}$, a „šířka" zvonovitého tvaru je přibližně $2\sqrt{n}$ (to dokazovat nebudeme); měřítka na svislé a vodorovné ose jsou tedy podstatně odlišná. Křivka takovéhoto tvaru je velmi důležitá např. v teorii pravděpodobnosti (tzv. Gaussova křivka), kde např. dává typické rozložení chyb při měření nějaké veličiny, a vzniká v mnoha nečekaných souvislostech.

Jak je kombinační číslo $\binom{n}{\lfloor n/2 \rfloor}$ velké? Jednoduchý, ale mnohdy dostatečně přesný odhad je

$$\frac{2^n}{n+1} \leq \binom{n}{\lfloor n/2 \rfloor} \leq 2^n.$$

Druhá nerovnost je zřejmá ze vztahu $\sum_{k=0}^{n} \binom{n}{k} = 2^n$, a první vlastně taky — $\binom{n}{\lfloor n/2 \rfloor}$ je největší mezi $n+1$ kombinačními čísly tvaru $\binom{n}{k}$, jejichž součet je 2^n.

Ukážeme podstatně přesnější odhad. Pro pohodlnější zápis budeme pracovat jen se sudými hodnotami n, t.j. $n = 2m$.

2.5.2 Tvrzení. *Pro všechna $m \geq 1$ platí*

$$\frac{2^{2m}}{2\sqrt{m}} \leq \binom{2m}{m} \leq \frac{2^{2m}}{\sqrt{2m}}$$

Důkaz. Obě nerovnosti dokážeme podobně. Uvažme číslo

$$P = \frac{1 \times 3 \times 5 \times \cdots \times (2m-1)}{2 \times 4 \times 6 \times \cdots \times 2m}$$

(v tomto kroku je zakódována skoro celá myšlenka důkazu). Protože

$$P = \frac{1 \times 3 \times 5 \times \cdots \times (2m-1)}{2 \times 4 \times 6 \times \cdots \times 2m} \cdot \frac{2 \times 4 \times \cdots \times (2m)}{2 \times 4 \times \cdots \times (2m)} = \frac{(2m)!}{2^{2m}(m!)^2},$$

dostáváme, že

$$P = \frac{1}{2^{2m}} \binom{2m}{m}.$$

Chceme tedy ukázat

$$\frac{1}{2\sqrt{m}} \leq P \leq \frac{1}{\sqrt{2m}}.$$

Pro horní odhad uvažme součin

$$\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{4^2}\right) \cdots \left(1 - \frac{1}{(2m)^2}\right),$$

který můžeme ekvivalentně přepsat na

$$\left(\frac{1 \times 3}{2^2}\right)\left(\frac{3 \times 5}{4^2}\right) \cdots \left(\frac{(2m-1)(2m+1)}{(2m)^2}\right) = (2m+1)P^2.$$

Protože hodnota součinu je zřejmě < 1, dostáváme $(2m+1)P^2 < 1$, a tedy $P \leq 1/\sqrt{2m}$.

Pro dolní odhad podobně uvážíme součin

$$\left(1 - \frac{1}{3^2}\right)\left(1 - \frac{1}{5^2}\right) \cdots \left(1 - \frac{1}{(2m-1)^2}\right),$$

který přepíšeme na

$$\left(\frac{2 \times 4}{3^2}\right)\left(\frac{4 \times 6}{5^2}\right) \cdots \left(\frac{(2m-2)(2m)}{(2m-1)^2}\right) = \frac{1}{2(2m)P^2},$$

což dává dolní odhad. □

Poznamenejme, že aproximujeme-li $(2m)!$ a $m!$ pomocí Stirlingovy formule (kterou jsme ovšem nedokázali!), dostáváme ještě přesnější výsledek

$$\binom{2m}{m} \sim \frac{2^{2m}}{\sqrt{\pi m}}.$$

Uvažování odhadů čísel $\binom{2m}{m}$ se může zdát jako zbytečná kuriozita. Není tomu tak, a takové odhady mají zajímavé souvislosti např. s teorií čísel. Jedna z nejslavnějších matematických vět je následující tvrzení o hustotě prvočísel:

2.5.3 Věta (Prvočíselná věta). *Označme $\pi(n)$ počet prvočísel nepřevyšujících číslo n. Potom*

$$\pi(n) \sim \frac{n}{\ln n}$$

(čili $\lim_{n\to\infty} \pi(n) \ln n/n = 1$).

Je známo několik důkazů této věty, všechny jsou dost těžké (a hledání různých variací a zjednodušení pokračuje i dnes). Již v minulém století ale našel Čebyšev jednoduchý důkaz takovéhoto slabšího výsledku:

$$\pi(n) = \Theta\left(\frac{n}{\ln n}\right)$$

t.j. $c_1 n/\ln n \leq \pi(n) \leq c_2 n/\ln n$ pro jisté konstanty $c_2 \geq c_1 > 0$. Část důkazu lze založit na odhadech $2^{2m}/(2m+1) \leq \binom{2m}{m} \leq 2^{2m}$ (viz cvičení 2). Čebyšev dokázal rovněž tzv. *Bertrandův postulát: Pro každé $n \geq 1$ existuje prvočíslo p splňující $n < p \leq 2n$.* Dnes asi nejjednodušší známý důkaz je založen (mimo jiné) právě na tvrzení 2.5.2. O těchto velmi pěkných souvislostech se čtenář může poučit např. v knize [6].

Cvičení

1. Dokažte odhad $\binom{n}{k} \leq (en/k)^k$ indukcí podle k.
2. (a) Ukažte, že součin všech prvočísel p, $m < p \leq 2m$, je nejvýš 2^{2m}.

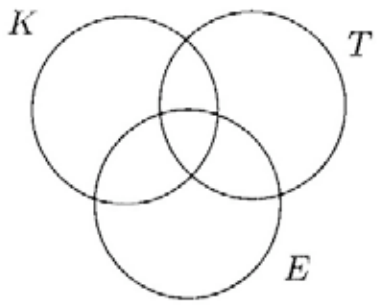
   (b)* Pomocí (a) dokažte odhad $\pi(n) = O(n/\ln n)$, kde $\pi(n)$ je jako ve větě 2.5.3.

   (c)* Buď p prvočíslo, m, k přirozená čísla. Ukažte, že pokud p^k dělí $\binom{2m}{m}$, potom $p^k \leq 2m$.

   (d) Pomocí (c) ukažte odhad $\pi(n) = \Omega(n/\ln n)$.

2.6 Princip inkluze a exkluze

Do češtiny bychom mohli název této části přeložit třeba „princip zahrnutí a vyloučení“. Tím jsme tento pojem asi čtenáři ještě příliš neosvětlili, začněme tedy motivačním příkladem. Jako to již učinili jiní autoři



Obrázek 2.5: Princip inkluze a exkluze pro 3 množiny.

u mnoha jiných příkladů o konečných množinách, uchýlíme se k formulaci s kluby na malém městě, a na znamení úcty k pravlasti klubů to budou kluby tenisový, kriketový a egyptologický.

2.6.1 Příklad. *Ve městě M. fungují 3 kluby. Tenisový klub má 20 členů, kriketový klub 15 členů a egyptologický klub je osmičlenný. Přitom z egyptologů jsou 2 hráči tenisu a 3 hráči kriketu, tenis a kriket zároveň provozuje 6 lidí, a jediná obzvláště agilní osoba je ve všech třech klubech. Kolik osob se celkem účastní klubového života v M.?*

Nejdřív cvičně spočítejme, kolik dohromady čítá členstvo řekněme tenisu a kriketu. Je vidět, že je třeba sečíst počet tenistů a kriketistů a odečíst osoby, které jsou v obou klubech a tedy jsme je počítali dvakrát; symbolicky zapsáno, $|T \cup K| = |T| + |K| - |T \cap K| = 20 + 15 - 6 = 29$. Pokud čtenáře neodradí zjevná přihlouplost celého příkladu z praktického hlediska[1], najde patrně podobnými, ale komplikovanějšími úvahami odpověď pro 3 kluby, která je 33; dobré je si k tomu nakreslit obrázek (obr. 2.5).

Princip inkluze a exkluze je vztah, podle něhož lze řešit úlohy podobného typu obecně. Používá se v situaci, kdy chceme spočítat velikost sjednocení několika množin, a známe přitom velikosti všech možných průniků. Tak pro dvě množiny, K a T, jsme takový vzorec již uvedli, a pro 3 množiny K, T a E zní

$$|K \cup T \cup E| = |K| + |T| + |E| - |K \cap T| - |K \cap E| - |T \cap E| + |K \cap T \cap E|.$$

Slovně vyjádřeno, abychom dostali velikost sjednocení, sečteme na-

[1] Což patrně indikuje jeho matematické sklony.

před velikosti jednotlivých množin, pak odečteme velikosti průniků všech dvojic, a nakonec přičteme velikost průniku všech tří množin. Jak ukážeme za chvíli, takovýto návod funguje i pro obecný počet, n, konečných množin $A_1, A_2, \ldots, A_n$. Velikost jejich sjednocení, t.j. $|A_1 \cup A_2 \cup \ldots \cup A_n|$, dostaneme takto: sečteme velikosti všech množin, odečteme velikosti průniků všech dvojic, přičteme velikosti průniků všech trojic, odečteme velikosti průniků čtveřic, atd.; jako poslední krok buď přičteme (pro liché n) nebo odečteme (pro sudé n) velikost průniku všech n množin. Jak to zapsat vzorcem? Jeden způsob by mohl být

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n| -$$
$$-|A_1 \cap A_2| - |A_1 \cap A_3| - \cdots - |A_1 \cap A_n| - |A_2 \cap A_3| - \cdots - |A_{n-1} \cap A_n| +$$
$$|A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + \cdots$$
$$+(-1)^{n-1}|A_1 \cap A_2 \cap \ldots \cap A_n|.$$

To je velmi těžkopádné vyjádření tak jednoduchého pravidla. Trošku lepší je zápis pomocí sum:

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i_1 < i_2 \le n} |A_{i_1} \cap A_{i_2}| +$$
$$\sum_{1 \le i_1 < i_2 < i_3 \le n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| -$$
$$\cdots + (-1)^{n-1}|A_1 \cap A_2 \cap \ldots \cap A_n|.$$

Vzpomeneme-li si na značení množiny všech k-prvkových podmnožin množiny X symbolem $\binom{X}{k}$ a použijeme-li i pro vícenásobné průniky a sjednocení zápis podobný sumám, můžeme ještě elegantněji zapsat totéž:

2.6.2 Věta (Princip inkluze a exkluze). *Pro každý soubor $A_1, A_2, \ldots, A_n$ konečných množin platí*

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{I \in \binom{\{1,2,\ldots,n\}}{k}} \left|\bigcap_{i \in I} A_i\right|. \qquad (2.12)$$

Konečně nejkratší a takřka ďábelský zápis principu inkluze a exkluze je

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{\emptyset \neq I \subseteq \{1,2,\ldots,n\}} (-1)^{|I|-1} \left|\bigcap_{i \in I} A_i\right|. \tag{2.13}$$

První důkaz principu inkluze a exkluze — indukcí. Indukce postupuje podle počtu množin. Pro 2 množiny vzorec, jak víme, platí. Předpokládejme jeho platnost pro libovolných $n-1$ množin. Budeme postupně upravovat:

$$\left|\bigcup_{i=1}^{n} A_i\right| = \left|\left(\bigcup_{i=1}^{n-1} A_i\right) \cup A_n\right| = \left|\bigcup_{i=1}^{n-1} A_i\right| + |A_n| - \left|\left(\bigcup_{i=1}^{n-1} A_i\right) \cap A_n\right| =$$

(Použili jsme vztahu $|A \cup B| = |A| + |B| - |A \cap B|$ pro $A = A_1 \cup \ldots \cup A_{n-1}$, $B = A_n$.)

$$= \left|\bigcup_{i=1}^{n-1} A_i\right| + |A_n| - \left|\bigcup_{i=1}^{n-1} (A_i \cap A_n)\right| =$$

(Distributivita průniku. Teď dvakrát použijeme indukční předpoklad, jednak pro $|A_1 \cup \ldots \cup A_{n-1}|$, jednak pro $|A'_1 \cup \ldots \cup A'_{n-1}|$, kde $A'_i = A_i \cap A_n$.)

$$= \left(\sum_{k=1}^{n-1} (-1)^{k-1} \sum_{I \in \binom{\{1,2,\ldots,n-1\}}{k}} \left|\bigcap_{i \in I} A_i\right|\right) + |A_n| -$$

$$\left(\sum_{k=1}^{n-1} (-1)^{k-1} \sum_{I \in \binom{\{1,2,\ldots,n-1\}}{k}} \left|\bigcap_{i \in I \cup \{n\}} A_i\right|\right).$$

Už jsme skoro hotovi. V první sumě sčítáme (se správnými znaménky) všechny velikosti průniků nezahrnujících množinu A_n. Ve druhé sumě se objevují právě všechny velikosti průniků obsahujících množinu A_n, a průnik $k+1$ takových množin (t.j. nějakých k z množin $A_1, \ldots, A_{n-1}$ a množiny A_n) má znaménko $-(-1)^{k-1} = (-1)^k$. V druhé sumě přitom není zahrnut člen $|A_n|$, ten však je zvlášť mezi oběma sumami.

Celkem tedy velikost průniku libovolné k-tice množin z $A_1, \ldots, A_n$ se ve výrazu objevuje právě jednou, a se znaménkem $(-1)^{k-1}$, což souhlasí s (2.12). Tím je důkaz indukcí ukončen (bez rozumného zápisu bychom se v tomto důkaze snadno beznadějně zapletli). □

Druhý důkaz principu inkluze a exkluze — počítáním. Uvažme libovolný prvek $x \in A_1 \cup \ldots \cup A_n$. K velikosti sjednocení na levé straně vzorce (2.12) přispívá x právě 1. Podívejme se, kolik přispívá do jednotlivých průniků na straně pravé. Předpokládejme, že x je obsažen právě v j z množin $A_1, \ldots, A_n$, $1 \leq j \leq n$; můžeme množiny přejmenovat tak, aby x byl obsažen právě v $A_1, \ldots, A_j$. Prvek x se tedy objevuje v průniku každé k-tice množin z $A_1, \ldots, A_j$ (a v žádných jiných průnicích). Protože existuje právě $\binom{j}{k}$ k-prvkových podmnožin j-prvkové množiny, bude se x objevovat v $\binom{j}{k}$ průnicích k-tic. Velikosti k-tic jsou přitom započteny se znaménkem $(-1)^{k-1}$, tudíž x na pravé straně přispívá veličinou

$$j - \binom{j}{2} + \binom{j}{3} - \cdots + (-1)^{j-1}\binom{j}{j}.$$

Podle vzorce (2.8) je toto rovno 1. Příspěvek každého prvku k oběma stranám (2.12) je tedy 1, a tím je tento vzorec dokázán. □

A ještě jeden, velmi krátký důkaz. Když se na věc vhodné pohlíží, je princip inkluze a exkluze důsledkem takovéhoto vzorečku pro roznásobení součinu:

$$(1 + x_1)(1 + x_2) \cdots (1 + x_n) = \sum_{I \subseteq \{1,2,\ldots,n\}} \left(\prod_{i \in I} x_i \right). \tag{2.14}$$

Rozvažte, co ten vzoreček říká (rozepište to pro $n = 1, 2, 3$, řekněme) a proč platí.

Abychom dokázali princip inkluze a exkluze, označme $A = A_1 \cup A_2 \cup \ldots \cup A_n$, a nechť $f_i : A \to \{0, 1\}$ je charakteristická funkce množiny A_i, to znamená $f_i(a) = 1$ pro $a \in A_i$ a $f_i(a) = 0$ jinak. Pro každé $a \in A$ platí $\prod_{i=1}^{n}(1 - f_i(a)) = 0$ (ne?), a použitím (2.14) s $x_i = -f_i(a)$ dostaneme

$$\sum_{I \subseteq \{1,2,\ldots,n\}} (-1)^{|I|} \prod_{i \in I} f_i(a) = 0.$$

Sečtením těchto rovností pro všechna $a \in A$, a potom záměnou pořadí sumace, se dopracujeme k

$$0 = \sum_{a \in A} \left(\sum_{I \subseteq \{1,2,\ldots,n\}} (-1)^{|I|} \prod_{i \in I} f_i(a) \right) =$$

$$\sum_{I \subseteq \{1,2,\ldots,n\}} (-1)^{|I|} \left(\sum_{a \in A} \prod_{i \in I} f_i(a) \right). \tag{2.15}$$

Teď už si stačí uvědomit, že $\prod_{i \in I} f_i(a)$ je charakteristická funkce množiny $\bigcap_{i \in I} A_i$, takže $\sum_{a \in A} \prod_{i \in I} f_i(a) = \left| \bigcap_{i \in I} A_i \right|$. Speciálně pro $I = \emptyset$ je $\prod_{i \in \emptyset} f_i(a)$ prázdný součin, jenž podle definice má hodnotu 1, takže $\sum_{a \in A} \prod_{i \in \emptyset} f_i(a) = \sum_{a \in A} 1 = |A|$. Proto (2.15) znamená

$$|A| + \sum_{\emptyset \neq I \subseteq \{1,2,\ldots,n\}} (-1)^{|I|} \left| \bigcap_{i \in I} A_i \right| = 0,$$

což je přesně princip inkluze a exkluze. Vot tak. Znalec algebry tedy může shlížet na princip inkluze a exkluze s jistým pohrdáním — trivialita, řekl by. □

Bonferroniho nerovnosti. Někdy se můžeme octnout v situaci, kdy známe velikosti všech průniků až do m-násobných, ale neznáme velikosti průniků většího počtu množin než m. Pak ovšem nemůžeme velikost sjednocení spočítat přesně. Takzvané *Bonferroniho nerovnosti* říkají, že vynecháme-li na pravé straně principu inkluze a exkluze (2.12) členy od $(m+1)$-ního počínaje, potom *chyba*, jíž se tím dopustíme při výpočtu velikosti sjednocení, *bude mít stejné znaménko jako první vynechaný člen*. Zapsáno formulí, pro každé $q = 1, 2, \ldots$ a libovolné konečné množiny $A_1, \ldots, A_n$ platí

$$\sum_{k=1}^{2q} (-1)^{k-1} \sum_{I \in \binom{\{1,2,\ldots,n\}}{k}} \left| \bigcap_{i \in I} A_i \right| \leq \left| \bigcup_{i=1}^{n} A_i \right| \leq$$

$$\sum_{k=1}^{2q-1} (-1)^{k-1} \sum_{I \in \binom{\{1,2,\ldots,n\}}{k}} \left| \bigcap_{i \in I} A_i \right|. \tag{2.16}$$

To třeba znamená, že nevíme-li v příkladu 2.6.1, kolik horlivců je ve všech třech klubech zároveň, můžeme odhadnout, že celkový počet členů všech tří klubů dohromady je nejméně 32. Důkaz nerovností (2.16) zde neuvádíme.

Cvičení

1. Rozvažte podrobně, proč formule (2.12) a (2.13) vyjadřují totéž.
2.* Dokažte Bonferroniho nerovnosti (2.16). Nevíte-li si rady s obecným případem, zkuste aspoň případ $q = 1$ a $q = 2$.
3. (Eratosthenovo síto) Kolik čísel zbyde z 1,2,...,1000 po vyškrtání všech násobků čísel 2,3,5 a 7?
4. Spočítejte počet přirozených čísel $n < 100$, která nejsou dělitelná druhou mocninou žádného přirozeného čísla (většího než 1).
5. Kolik existuje pořadí písmen A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P, z nichž vypuštěním některých písmen nelze dostat ani jedno ze slov PONK, DOBA, COP? Co když zakážeme ještě OPICE?
6. Kolika způsoby lze seřadit do fronty 5 Čechů, 4 Maďary a 3 Rusy tak, aby všichni příslušníci žádného národa netvořili jeden souvislý blok?

2.7 Šatnářka a ti druzí

2.7.1 Úloha. (Problém šatnářky) *Ctihodní pánové v počtu n přijdou na shromáždění, všichni v kloboucích, a odloží si své klobouky do šatny. Při odchodu šatnářka, možná ten den velmi roztržitá, možná dokonce z mizerného osvětlení osleplá, vydá každému z pánů náhodně jeden z klobouků. Jaká je pravděpodobnost, že žádný pán nedostane od šatnářky zpět svůj klobouk?*

Tento problém je formulován jako hříčka, ale matematicky je pozoruhodný a svého času zaměstnával matematické génie té doby. Nejprve ho přeformulujeme pomocí permutací. Očíslujeme-li pány (s prominutím) $1, 2, \ldots, n$, a jejich klobouky taktéž, potom činnost šatnářky vede k náhodné permutaci π množiny $\{1, 2, \ldots, n\}$, kdy $\pi(i)$ je číslo

klobouku navráceného i-tému pánovi. Otázka zní, s jakou pravděpodobností platí $\pi(i) \neq i$ pro všechna $i \in \{1, 2, \ldots, n\}$. Nazvěme index i splňující $\pi(i) = i$ *pevným bodem* permutace π. Ptáme se tedy, jaká je pravděpodobnost, že náhodně zvolená permutace nemá žádný pevný bod. Každá z $n!$ možných permutací je, podle popisu práce šatnářky, stejně pravděpodobná, takže označíme-li $š(n)$ počet permutací bez pevného bodu na n-prvkové množině, bude zkoumaná pravděpodobnost rovna $š(n)/n!$.

Pomocí principu inkluze a exkluze se dá odvodit vzorec pro $š(n)$. Budeme hledat počet „špatných" permutací, t.j. permutací aspoň s jedním pevným bodem. Nechť S_n (tradičně) značí množinu všech permutací množiny $\{1, 2, \ldots, n\}$, a pro $i = 1, 2, \ldots, n$ definujme $A_i = \{\pi \in S_n;\ \pi(i) = i\}$. Špatné permutace jsou právě sjednocení všech A_i.

> Zde doporučujeme čtenáři, aby si řádně uvědomil definici množin A_i (jejich prvky jsou permutace, nikoli čísla!) — ta bývá často zdrojem nedorozumění.

Abychom mohli aplikovat princip inkluze a exkluze, musíme vyjádřit velikosti k-násobných průniků množin A_i. Je snadno vidět, že $|A_i| = (n-1)!$ ($\pi(i)$ je fixováno, na zbývajících $n-1$ prvcích volíme libovolnou permutaci). Jaké permutace např. jsou v $A_1 \cap A_2$? Právě ty, které mají 1 a 2 jako pevné body (a zbývající prvky zpermutovány libovolně), takových je $(n-2)!$. Obecně pro libovolná $i_1 < i_2 < \cdots < i_k$ máme $|A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}| = (n-k)!$, a proto dosazením do principu inkluze a exkluze vyjde

$$|A_1 \cup \ldots \cup A_n| = \sum_{k=1}^{n} (-1)^{k-1} \binom{n}{k} (n-k)! = \sum_{k=1}^{n} (-1)^{k-1} \frac{n!}{k!}.$$

Připomeňme, že to jsme spočítali permutace s aspoň jedním pevným bodem, tedy

$$š(n) = n! - |A_1 \cup \ldots \cup A_n| = n! - \frac{n!}{1!} + \frac{n!}{2!} - \cdots + (-1)^n \frac{n!}{n!},$$

což můžeme ještě přepsat na tvar

$$š(n) = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n \frac{1}{n!}\right). \tag{2.17}$$

Jak se vyučuje v kursu matematické analýzy, konverguje součet řady v závorce pro rostoucí n k e^{-1} (kde e je Eulerovo číslo), a to velice rychle. Proto máme přibližný vztah $š(n) \approx n!/e$, a pravděpodobnost v problému šatnářky tedy konverguje ke konstantě e^{-1}.

Eulerova funkce φ. V teorii čísel hraje důležitou roli funkce, označovaná zpravidla φ a pojmenovaná po Leonhardu Eulerovi. Pro přirozené číslo n definujeme hodnotu $\varphi(n)$ jako počet přirozených čísel $m \leq n$ nesoudělných s n; formálně tedy

$$\varphi(n) = |\{m \in \{1, 2, \ldots, n\};\ (n, m) = 1\}|$$

(připomeňme, že (n, m) značí největší společný dělitel čísel m a n). Jako příklad na použití principu inkluze a exkluze najdeme vzorec, který umožňuje efektivně spočítat hodnotu $\varphi(n)$ ze znalosti rozkladu čísla n na prvočinitele.

Nejjednodušší je případ, kdy $n = p$ je prvočíslo. Potom každé $m < p$ je s p nesoudělné, a tedy $\varphi(p) = p - 1$.

Další stupínek k řešení je případ, kdy $n = p^\alpha$ ($\alpha \in \mathbf{N}$) je mocnina prvočísla. Potom čísla soudělná s p^α jsou právě násobky p, t.j. $p, 2p, 3p, \ldots, p^{\alpha-1}p$, a takových násobků je $p^{\alpha-1}$ (obecně, pokud d je libovolný dělitel nějakého čísla n, potom násobků d nepřevyšujících n je právě n/d). Čísel nesoudělných s p^α tedy zbývá $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - 1/p)$.

Obecné n můžeme zapsat ve tvaru

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

kde $p_1, \ldots, p_r$ jsou navzájem různá prvočísla a $\alpha_i \in \mathbf{N}$. „Špatná“ $m \leq n$, t.j. taková, která se nepočítají do $\varphi(n)$, jsou právě násobky některého z prvočísel p_i. Označme $A_i = \{m \in \{1, 2, \ldots, n\};\ p_i | m\}$ množinu násobků p_i. Máme tedy $\varphi(n) = n - |A_1 \cup A_2 \cup \ldots \cup A_r|$. Princip inkluze a exkluze velí, abychom zjistili velikosti průniků množin A_i. Tak např. průnik $A_1 \cap A_2$ obsahuje čísla dělitelná jak p_1, tak p_2, čili právě násobky $p_1 p_2$, a proto $|A_1 \cap A_2| = n/(p_1 p_2)$. Obecně máme stejnou úvahou

$$|A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}| = \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_k}}.$$

Podívejme se nejprve na konkrétní případy $r = 2$ a $r = 3$. Pro $n = p_1^{\alpha_1} p_2^{\alpha_2}$ máme

$$\varphi(n) = n - |A_1 \cup A_2| = n - |A_1| - |A_2| + |A_1 \cap A_2| =$$

$$n - \frac{n}{p_1} - \frac{n}{p_2} + \frac{n}{p_1 p_2} == n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right).$$

Podobně pro $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}$ vychází

$$\varphi(n) = n - \frac{n}{p_1} - \frac{n}{p_2} - \frac{n}{p_3} + \frac{n}{p_1 p_2} + \frac{n}{p_1 p_3} + \frac{n}{p_2 p_3} - \frac{n}{p_1 p_2 p_3} =$$

$$n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right).$$

To vzbuzuje podezření na obecný vzorec:

2.7.2 Věta. *Pro $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ platí*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right). \tag{2.18}$$

Dokončení důkazu: Pro obecné r nám princip inkluze a exkluze (s výhodou použijeme tvar (2.13)) dává vyjádření

$$\varphi(n) = n - \sum_{\emptyset \neq I \subseteq \{1,2,\ldots,r\}} (-1)^{|I|-1} \frac{n}{\prod_{i \in I} p_i} = n \cdot \sum_{I \subseteq \{1,2,\ldots,r\}} \frac{(-1)^{|I|}}{\prod_{i \in I} p_i}.$$

Tvrdíme, že tato hrozivě vypadající formule je rovna pravé straně (2.18). Roznásobujeme-li totiž všechny závorky na pravé straně (2.18), dostaneme 2^r součinů, a v každém takovém součinu bereme z každé závorky jeden člen — buď 1 nebo $-1/p_i$. Označíme-li pro takový součin písmenem I množinu indexů i takových, že jsme z i-té závorky použili člen $-1/p_i$, můžeme uvažovaný součin napsat ve tvaru

$$\frac{(-1)^{|I|}}{\prod_{i \in I} p_i},$$

tedy po roznásobení pravé strany vzorce (2.18) vyjde stejná formule jako ta, již jsme odvodili pomocí inkluze a exkluze. □

Cvičení

1. Dokažte vztah

$$\check{s}(n) = n! - n\check{s}(n-1) - \binom{n}{2}\check{s}(n-2) - \cdots - \binom{n}{n-1}\check{s}(1) - 1.$$

2. (a)* Dokažte rekurentní vztah $š(n) = (n-1)[š(n-1) + š(n-2)]$. Dokažte s jeho pomocí vzorec (2.17).

   (b)* Vypočítejte vzorec pro $š(n)$ přímo ze vztahu odvozeného v (a). Použijte pomocnou posloupnost danou vztahem $a_n = š(n) - n\,š(n-1)$.

3. Na plese je n manželských párů. Kolika způsoby lze utvořit n tanečních párů, jestliže žádná manželská dvojice netancuje spolu?

4. Určete počet permutací s právě jedním pevným bodem, resp. * s právě k pevnými body.

5. Kolik existuje permutací čísel 1,2,...,10, v nichž se žádné sudé číslo nezobrazí na sebe?

6. Spočítejte, kolik existuje zobrazení n-prvkové množiny *na* m-prvkovou množinu (t.j. každý prvek musí mít aspoň jeden vzor)

   (a) pro $m = 2$

   (b) pro $m = 3$

   (c)* napište vzorec pro obecné m; zkontrolujte výsledek např. pro $m = n = 10$ (co musí vyjít?).

   (d)* Ukažte, nejlépe bez použití výsledku části (c), že počet zobrazení na m-prvkovou množinu je dělitelný číslem $m!$.

7. (a)* Kolika způsoby lze rozdělit n lidí do k skupin, t.j. kolik existuje ekvivalencí na n-prvkové množině s právě k třídami? Zkuste řešit nejprve pro $k = 2, 3$ a $k = n-1, n-2$.

   (b) Kolik je celkem ekvivalencí na n-prvkové množině?

   (c)* Označíme-li výsledek (b) jako B_n (*n-té Bellovo číslo*) , dokažte následující (překvapivý) vzorec

$$B_n = \frac{1}{e} \sum_{i=0}^{\infty} \frac{i^n}{i!}.$$

8.* Dokažte vzorec (2.18) pro Eulerovu funkci jiným způsobem. Předpokládejte, že platí pro $n = p^\alpha$ (mocninu jediného prvočísla). Dokažte následující *pomocné tvrzení:* Pokud m, n jsou nesoudělná, potom $\varphi(mn) = \varphi(m)\varphi(n)$.

9.* Pro libovolné přirozené n, dokažte vztah $\sum_{d|n} \varphi(d) = n$ (suma je přes všechny přirozené dělitele d čísla n).

10. (a) Kolik je všech dělitelů čísla $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$?

(b) Ukažte, že *součet* všech dělitelů takového čísla n je roven

$$\prod_{i=1}^{r} \frac{p^{\alpha_i+1} - 1}{p_i - 1}.$$

(c)** Nazvěme číslo n *dokonalé*, pokud je rovno součtu svých dělitelů (kromě sebe sama), tak např. $6 = 1 + 2 + 3$ je dokonalé. Dokažte, že každé sudé dokonalé číslo má tvar $2^q(2^{q+1}-1)$, kde $2^{q+1}-1$ je prvočíslo. *Poznámka:* žádná lichá dokonalá čísla známa nejsou, ale nikdo neumí dokázat, že by neexistovala.

11. (a)* Pro dané číslo N určete pravděpodobnost, že zvolíme-li náhodně 2 čísla $m, n \in \{1, 2, \ldots, N\}$, budou nesoudělná.

(b)* Ukažte, že limita pravděpodobnosti v (a) pro $N \to \infty$ je rovna nekonečnému součinu $\prod_p (1 - 1/p^2)$, kde p probíhá všechna prvočísla. *Poznámka:* Hodnota tohoto součinu je $6/\pi^2$.

12. (a) Určete počet grafů na dané n-prvkové množině V bez izolovaných vrcholů. (Definici grafu viz část 3.1.)

(b)* Určete počet grafů na V s aspoň 2 izolovanými vrcholy, resp. s právě 2 izolovanými vrcholy.

13.* Kolika způsoby lze rozesadit n manželských párů kolem kulatého stolu s $2n$ židlemi tak, aby manželé nikdy neseděli vedle sebe?

3

Grafy: úvod

3.1 Pojem grafu; isomorfismus

Mnoho situací v matematice, v informatice i v rozličných prakticky motivovaných úlohách lze vystihnout pomocí schématu sestávajícího hlavně ze dvou věcí:

- (konečné) množiny bodů, a
- spojnic mezi některými dvojicemi bodů.

Například body mohou reprezentovat účastníky nějakého večírku a spojnice ty dvojice účastníků, kteří se navzájem znají. Nebo body mohou odpovídat křižovatkám ve městě a spojnice ulicím mezi nimi. Rovněž elektrotechnická schémata mají často podobný charakter. Body v takovém typu schémat je zvykem nazývat *vrcholy* (nebo též *uzly*) a příslušné spojnice *hrany* (o původu tohoto názvosloví viz část 5.3).

Matematickou abstrakcí podobných schémat je pojem grafu. Čtenář se s ním asi již setkal. Je to jeden ze základních pojmů diskrétní matematiky. To uvidíme i dále v našem textu.

3.1.1 Definice. *Graf*[1] *G je uspořádaná dvojice (V, E), kde V je nějaká neprázdná množina a E je množina dvoubodových podmnožin*

[1] To, čemu zde říkáme prostě graf, se někdy obšírněji nazývá *obyčejný neorientovaný graf*, aby se to odlišilo od dalších příbuzných pojmů — ty zmíníme později.

množiny V. Prvky množiny V se jmenují vrcholy *grafu G a prvky množiny E* hrany[2] *grafu G.*

V našem textu budeme uvažovat grafy s konečnou množinou vrcholů (v několika málo případech, kdy pojednáváme i o nekonečných grafech, to zvlášť zdůrazníme).

Chceme-li vyznačit, že graf G má množinu vrcholů V a množinu hran E, píšeme $G = (V, E)$. Mluvíme-li o nějakém známém grafu G a chceme-li odkázat na jeho množinu vrcholů, značíme ji $V(G)$; podobně množinu hran grafu G zapisujeme $E(G)$. Užitečné je také označení $\binom{V}{2}$ pro množinu všech dvouprvkových podmnožin množiny V (o motivaci tohoto značení viz definici 2.3.1). Můžeme pak krátce říci, že graf je dvojice (V, E), kde $E \subseteq \binom{V}{2}$.

Grafy se znázorňují kreslením do roviny. Vrcholům grafu se přiřadí body roviny (vyznačené zpravidla puntíky) a hrany se vyjádří spojením příslušných dvojic bodů rovnými nebo všelijak zakřivenými čarami (jimž se v této souvislosti říká *oblouky*). Vzniknou tak například obrázky:

Sám název graf pochází snad od možnosti takového znázornění.

Obrázek grafu má však pomocnou úlohu (graf může být koneckonců zadán i mnoha jinými způsoby, a např. v paměti počítače se samozřejmě obrázkem nereprezentuje), a jeden graf lze nakreslit mnoha různými způsoby. Tak např. první dva z právě uvedených obrázků znázorňují týž graf s vrcholy $\{1, 2, 3, 4, 5\}$ a hranami $\{1, 2\}$, $\{2, 3\}$, $\{3, 4\}$, $\{4, 5\}$, $\{5, 1\}$.

Pro přehlednost znázornění je dobré, aby se oblouky přiřazené hranám co nejméně „křížily". V některých schématech elektrických

[2] Písmena V a E pocházejí od anglických termínů pro vrchol a hranu — *vertex* a *edge*.

obvodů i v řadě jiných aplikací je dokonce křížení oblouků zcela nepřípustné. To vede ke studiu důležité třídy tzv. rovinných grafů, viz kapitolu 5.

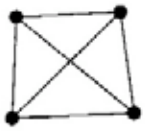
Kreslení grafů je důležitou pomůckou při studiu grafů. Kreslete si obrázky, kdykoliv je to možné. Mnoho pojmů má „obrázkovou" motivaci a tedy kreslení pojem ozřejmí. Na druhé straně je třeba zdůraznit, že pojem grafu (a jeho obrázku) je zde užíván v jiném smyslu než „graf funkce".

Důležité grafy. Zavedeme několik typů konkrétních grafů, které se v teorii grafů vyskytují velmi často a pro něž se ujalo standardní názvosloví a označení.

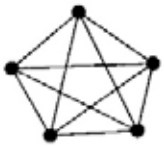
Úplný graf K_n (kde $n \geq 1$):

$$V = \{1, 2, \ldots, n\}, \quad E = \binom{V}{2}.$$

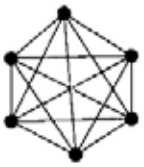
K_3



K_4



K_5



K_6

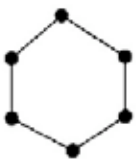
Kružnice C_n (kde $n \geq 3$):

$$V = \{1, 2, \ldots, n\}, \quad E = \{\{i, i+1\};\, i = 1, \ldots, n-1\} \cup \{\{1, n\}\}.$$

C_3

C_4

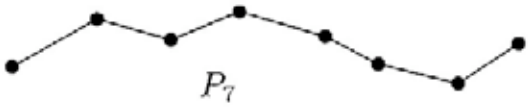
C_5



C_6

Cesta P_n (kde $n \geq 0$):

$$V = \{0, 1, \ldots, n\}, \quad E = \{\{i-1, i\};\, i = 1, \ldots, n\}.$$



P_7

Úplný bipartitní graf $K_{n,m}$ (kde $n, m \geq 1$):

$$V = \{u_1, \ldots, u_n\} \cup \{v_1, \ldots, v_m\},$$

$$E = \{\{u_i, v_j\};\ i = 1, 2, \ldots, n,\ j = 1, 2, \ldots, m\}.$$

$K_{1,1}$ $K_{1,2}$ $K_{1,3}$ $K_{2,3}$ $K_{3,3}$

Tady je asi na místě malé vysvětlení. Slovo „bipartitní" bychom mohli přeložit jako „dvoučásťový". Obecně, graf G se nazývá *bipartitní*, pokud množinu $V(G)$ můžeme rozdělit na dvě disjunktní podmnožiny V_1 a V_2 takové, že každá hrana z $E(G)$ spojuje vrchol z V_1 s vrcholem z V_2; v symbolech $E(G) \subseteq \{\{v, v'\};\ v \in V_1, v' \in V_2\}$.

Isomorfismus grafů. Dva grafy G a G' pokládáme za stejné, jestliže mají totožné množiny vrcholů a hran; tedy $G = G'$ znamená $V(G) = V(G')$ a $E(G) = E(G')$. Mnoho grafů se však liší „pouze" označením svých vrcholů a hran. To vystihuje pojem isomorfismu.

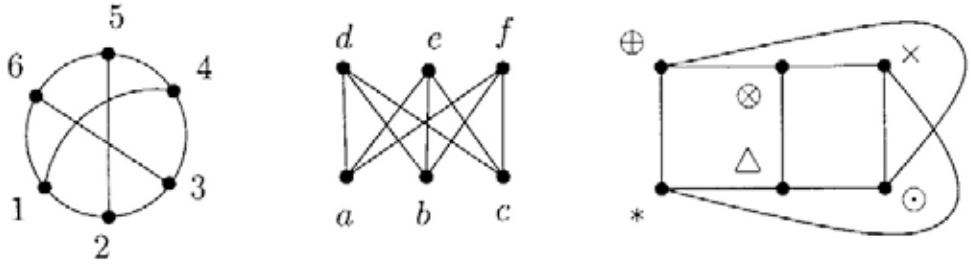
3.1.2 Definice. *Dva grafy* $G = (V, E)$ a $G' = (V', E')$ *nazveme* isomorfní, *jestliže existuje vzájemně jednoznačné zobrazení* $f : V \hookrightarrow\!\!\!\rightarrow V'$ *tak, že platí*

$$\{x, y\} \in E \quad \textit{právě když} \quad \{f(x), f(y)\} \in E'.$$

Zobrazení f *nazýváme* isomorfismus *grafů* G a G'. *Fakt, že grafy* G a G' *jsou isomorfní, vyznačujeme zápisem* $G \cong G'$.

Isomorfismus je tedy vlastně „přejmenování vrcholů" grafu (dejte na definici isomorfismu pozor, je důležitá, ale často se plete!). Relace $\cong$ („býti isomorfní") je ekvivalence — viz cvičení 2.

3.1.3 Úloha. *Následující 3 obrázky znázorňují isomorfní grafy. Nalezněte příslušné isomorfismy.*



Řešení. Všechny tři grafy jsou isomorfní $K_{3,3}$. Isomorfismus (a)→ (b): například $1 \mapsto a$, $2 \mapsto d$, $3 \mapsto b$, $4 \mapsto e$, $5 \mapsto c$, $6 \mapsto f$ (existuje víc možností!). Ostatní přenecháváme čtenáři.

Pro malé obrázky není zpravidla těžké rozhodnout, jestli odpovídají isomorfním grafům nebo ne (i když předchozí úloha naznačuje, že obrázky téhož grafu nemusí zdaleka vypadat na pohled stejně). Nicméně úloha rozhodnout, zda dané dva grafy jsou isomorfní, je obecně obtížná, a není pro ni znám žádný efektivní algoritmus (t.j. fungující efektivně ve všech případech). Dokonce se soudí, že ani žádný efektivní algoritmus neexistuje.

Počet neisomorfních grafů. Na dané n-prvkové množině V je právě $2^{\binom{n}{2}}$ různých grafů (neb tolika způsoby můžeme zvolit množinu E jako podmnožinu množiny $\binom{V}{2}$, a posledně jmenovaná má $\binom{n}{2}$ prvků — viz část 2.1). Grafů, které jsou navzájem neisomorfní, je podstatně méně. Tak např. pro $V = \{1, 2, 3\}$ dostáváme následujících $8 = 2^{\binom{3}{2}}$ grafů

Z těchto 8 možností jen 4 jsou neisomorfní:

Kolik je navzájem neisomorfních grafů na n vrcholech pro obecné n? Určit to přesně je poměrně těžké; jednoduchou úvahou můžeme ale dostat aspoň dobré odhady. Navzájem neisomorfních grafů určitě není více než všech grafů na dané konkrétní n-prvkové množině, t.j. $2^{\binom{n}{2}}$. Na druhé straně, uvažme jeden graf G na množině $V = \{1, 2, \ldots, n\}$. Kolik různých grafů G' na této množině je s grafem G isomorfních? Podle definice, je-li G' takový isomorfní graf, musí existovat bijekce $f : V \leftrightarrow V$,

které je isomorfismem G a G'. Všech bijekcí $f : V \leftrightarrow\!\!\!\!\rightarrow V$ je ale $n!$ (viz část 2.2), tedy G je isomorfní s nejvýš $n!$ grafy na množině V, a proto existuje minimálně

$$\frac{2^{\binom{n}{2}}}{n!}$$

navzájem neisomorfních grafů na n vrcholech.

Tvrdíme, že tato funkce neroste o mnoho pomaleji než $2^{\binom{n}{2}}$. Abychom to nahlédli, zlogaritmujeme obě funkce a poněkud upravíme (přitom použijeme zřejmý odhad $n! \leq n^n$):

$$\log_2 \left[2^{\binom{n}{2}}\right] = \binom{n}{2} = \frac{n^2}{2}\left(1 - \frac{1}{n}\right),$$

$$\log_2 \frac{2^{\binom{n}{2}}}{n!} = \binom{n}{2} - \log_2 n! \geq n^2/2 - n/2 - n\log_2 n =$$

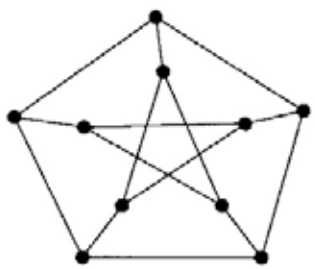
$$\frac{n^2}{2}\left(1 - \frac{1}{n} - \frac{2\log_2 n}{n}\right).$$

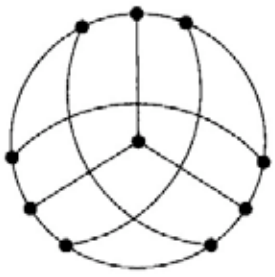
Vidíme, že pro velká n se logaritmy obou funkcí chovají „asi jako“ funkce $n^2/2$: relativní chyba, které bychom se dopustili jejich nahrazením funkcí $n^2/2$, jde v obou případech k nule pro $n \to \infty$. (Více o odhadech funkcí viz část 2.4.) Speciálně, pro dostatečně velké n je mnohem více než např. 2^n navzájem neisomorfních grafů.

Právě uvedená úvaha je pozoruhodná tím, že jsme pouze ukázali existenci velkého množství neisomorfních grafů, ale žádné takové grafy jsme nesestrojili (o podobných úvahách budeme mluvit systematičtěji v kapitole 9). Sestrojit (t.j. explicitně popsat) mnoho neisomorfních grafů není jen tak — viz cvičení 6.

Cvičení

1. Nalezněte isomorfismus mezi grafy





2. Buď $\mathcal{G}$ nějaká množina grafů. Dokažte, že relace „býti isomorfní“ je ekvivalence na $\mathcal{G}$.

3. *Automorfismus* grafu $G = (V, E)$ je každý isomorfismus G s G, t.j. bijekce $f : V \rightarrowtail\!\!\!\!\!\twoheadrightarrow V$ taková, že $\{u, v\} \in E$ právě když $\{f(u), f(v)\} \in E$. Graf se nazývá *asymetrický* (někdy též *strnulý*), je-li jeho jediný automorfismus identické zobrazení (každý vrchol se zobrazí sám na sebe).

   (a) Najděte příklad asymetrického grafu (s aspoň 2 vrcholy).

   (b) Ukažte, že neexistuje žádný asymetrický graf G s $1 < |V(G)| \leq 5$.

4. Dokažte, že graf G s n vrcholy je asymetrický (viz cvičení 3), právě když na množině $V(G)$ existuje $n!$ různých grafů isomorfních G.

5. Graf $G = (V, E)$ se nazývá *vrcholově transitivní*, pokud pro libovolné dva vrcholy $v, v' \in V$ existuje automorfismus $f : V \rightarrowtail\!\!\!\!\!\twoheadrightarrow V$ grafu G (viz cvičení 3) takový, že $f(v) = v'$. Podobně G je *hranově transitivní*, pokud pro libovolné dvě hrany $e, e' \in E$ existuje automorfismus $f : V \rightarrowtail\!\!\!\!\!\twoheadrightarrow V$ takový, že $f(e) = e'$ (označíme-li $e = \{u, v\}$, potom zápis $f(e)$ značí množinu $\{f(u), f(v)\}$).

   (a) Rozhodněte, zda každý vrcholově transitivní graf je také hranově transitivní.

   (b) Najděte příklad grafu, který je hranově transitivní a není vrcholově transitivní.

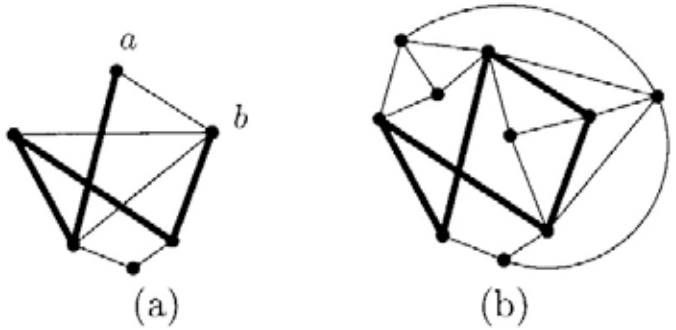
   (c)* Dokažte, že graf jako v (b) je nutně bipartitní.

6. Sestrojte co nejvíce navzájem neisomorfních grafů na množině $\{1, 2, \ldots, n\}$ (předpokládejte, že n je hodně velké číslo). Podaří se vám sestrojit více než n^2 jich? Aspoň $2^{n/10}$, nebo ještě podstatně více?

3.2 Podgrafy, souvislost, metrika a matice sousednosti

3.2.1 Definice. *Řekněme, že graf H je* podgrafem *grafu G, jestliže* $V(H) \subseteq V(G)$ a $E(H) \subseteq E(G)$.

Řekneme, že graf H je indukovaným podgrafem *grafu G, jestliže* $V(H) \subseteq V(G)$ a $E(H) = E(G) \cap \binom{V(H)}{2}$.



Obrázek 3.1: Příklad podgrafu (a), indukovaného podgrafu (b).

Tuto definici můžeme jinak vyjádřit takto: indukovaný podgraf grafu G vznikne vymazáním některých vrcholů G a všech hran vymazané vrcholy obsahujících. Pro podgraf můžeme ještě navíc vymazat některé další hrany, i když nevymažeme žádný z jejich koncových vrcholů. Na obr. 3.1(a) je nakreslen graf, a v něm je silně vytažen podgraf isomorfní cestě P_4. Tento podgraf není indukovaný (kvůli hraně $\{a, b\}$). Obrázek 3.1(b) ukazuje indukovaný podgraf (isomorfní kružnici C_5); ten je ovšem zároveň podgrafem.

Cesty a kružnice. Podgraf grafu G isomorfní nějaké cestě P_t se nazývá *cesta v grafu* G (viz obr. 3.1(a)). Cestu v grafu G můžeme též chápat jako posloupnost

$$(v_0, e_1, v_1, \ldots, e_t, v_t),$$

kde $v_0, v_1, \ldots, v_t$ jsou navzájem různé vrcholy grafu G, a pro každé $i = 1, 2, \ldots, t$ je $e_i = \{v_{i-1}, v_i\} \in E(G)$. Obšírněji se cesta ($v_0$, e_1, v_1,..., e_t, v_t) nazývá *cesta z* v_0 *do* v_t *délky* t. Poznamenejme, že připouštíme $t = 0$, tj. cestu délky 0.

Podobně podgraf grafu G isomorfní nějaké kružnici C_t ($t \geq 3$) se nazývá *kružnice v grafu* G (viz obr. 3.1(b)). Kružnici v grafu G můžeme též chápat jako posloupnost

$$(v_0, e_1, v_1, e_2, \ldots, e_{t-1}, v_{t-1}, e_t, v_0)$$

(počáteční a koncový vrchol jsou tedy shodné), kde $v_0, v_1, \ldots, v_{t-1}$ jsou navzájem různé vrcholy grafu G, a $e_i = \{v_{i-1}, v_i\} \in E(G)$ pro

$i = 1, 2, \ldots, t-1$, a také $e_t = \{v_{t-1}, v_0\} \in E(G)$. Číslo t je délka kružnice.

Souvislost, komponenty. Řekněme, že graf G je *souvislý*, jestliže pro každé dva jeho vrcholy x a y v něm existuje cesta z x do y.

Pojem souvislosti lze definovat také jinak. Nejdříve definujme relaci $\sim$ na množině $V(G)$ vztahem $x \sim y$ právě když v grafu G existuje cesta z x do y.

3.2.2 Tvrzení. *Relace $\sim$ je ekvivalence.*

Důkaz. Ověříme axiomy ekvivalence:

(a) $x \sim x$,

(b) $x \sim y \Rightarrow y \sim x$,

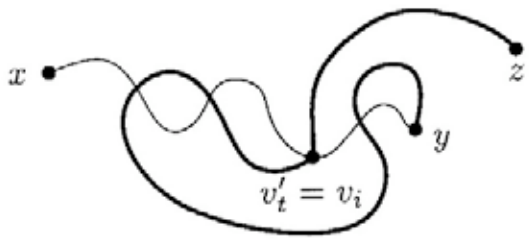
(c) $x \sim y$ a $y \sim z \Rightarrow x \sim z$.

Přitom (a) a (b) plynou bezprostředně z definice relace $\sim$ a zbývá dokázat (c).

Nechť tedy posloupnost $(x = v_0, e_1, v_1, \ldots, e_r, v_r = y)$ je cesta z x do y a posloupnost $(y = v'_0, e'_1, v'_1, \ldots, e'_s, v'_s = z)$ je cesta z y do z. Nechť t je maximální index, pro nějž $v'_t \in \{v_0, \ldots, v_r\}$ (to je korektní definice, protože přinejmenším $v'_0 \in \{v_0, \ldots, v_r\}$). Nechť $v'_t = v_i$. Potom však posloupnost

$$(x = v_0, e_1, v_1, \ldots, e_i, v_i = v'_t, e'_{t+1}, v'_{t+1}, \ldots, e'_s, v'_s = z)$$

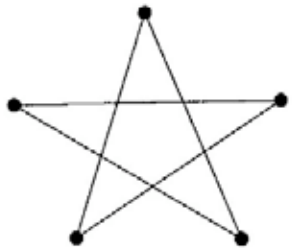
je hledaná cesta z x do z, viz obrázek:



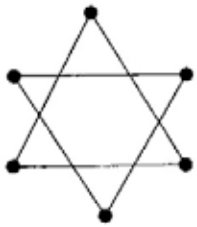
□

Nechť $V = V_1 \dot\cup V_2 \dot\cup \ldots \dot\cup V_k$ je rozklad množiny V na třídy ekvivalence $\sim$. Zřejmě graf G je souvislý právě když $k = 1$. Množiny V_i

se nazývají *komponenty* grafu G. Graf G je tedy sjednocením svých komponent. Na obr. (a) je příklad souvislého grafu,



(a)



(b)

zatímco na obrázku (b) je příklad grafu nesouvislého.

Rozhodnout, zda graf G je souvislý, popřípadě najít všechny jeho komponenty není obtížné. Příslušné algoritmy zde nebudeme popisovat; lze je najít v mnoha učebnicích informatiky (zpravidla jako algoritmy na prohledávání grafu, např. prohledávání do hloubky).

Vzdálenost v grafu. Nechť $G = (V, E)$ je souvislý graf. Pro vrcholy v, v' definujme číslo $d_G(v, v')$ jako délku nejkratší cesty z v do v' v grafu G. Číslo $d_G(v, v')$ se nazývá *vzdálenost vrcholů* v a v' v grafu G.

Funkce $d_G : V \times V \to \mathbf{R}$, kterou nazýváme *metrika grafu* G, má následující vlastnosti

1. $d_G(v, v') \geq 0$, a $d_G(v, v') = 0$ právě když $v = v'$;
2. (symetrie) $d_G(v, v') = d_G(v', v)$ pro každou dvojici vrcholů v, v';
3. (trojúhelníková nerovnost) $d_G(v, v'') \leq d_G(v, v') + d_G(v', v'')$ pro každou trojici v, v', v'' vrcholů z V.

Platnost těchto vztahů plyne bezprostředně z definice čísla $d_G(v, v')$. Každému zobrazení $V \times V$ do $\mathbf{R}$ s vlastnostmi 1–3 se říká *metrika* na množině V. Výše definovaná funkce d_G má navíc ještě následující speciální vlastnosti:

4. $d_G(v, v')$ je nezáporné celé číslo pro každou dvojici v, v';
5. jestliže $d_G(v, v'') > 1$, potom existuje v', $v \neq v' \neq v''$ tak, že $d_G(v, v') + d_G(v', v'') = d_G(v, v'')$.

Podmínku 5 bychom mohli nazvat „obrácení trojúhelníkové nerovnosti“. Podmínky 1–5 již charakterizují funkce odpovídající metrice nějakého grafu G s množinou vrcholů V (viz cvičení 5).

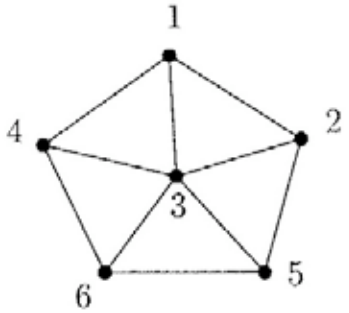
Reprezentace grafů. Kromě geometrických prostředků (kreslení grafů) se při studiu grafů používá i matic a jiných algebraických prostředků. To je důležité např. jestliže chceme zadat graf počítači. Grafy se reprezentují mnoha rozličnými způsoby. Snad nejběžnější a v jistém smyslu základní je pojem matice sousednosti grafu:

3.2.3 Definice. *Nechť $G = (V, E)$ je graf s n vrcholy. Označme vrcholy $v_1, \ldots, v_n$ (v nějakém libovolném pořadí).* Matice sousednosti *grafu G je čtvercová $n \times n$ matice $A_G = (a_{ij})_{i,j=1}^{n}$ definovaná předpisem*

$$a_{ij} = \begin{cases} 1 & \text{pro } \{v_i, v_j\} \in E \\ 0 & \text{jinak.} \end{cases}$$

Tedy matice sousednosti A_G je vždy symetrická čtvercová matice, jejímiž prvky jsou 0 nebo 1, přičemž na hlavní diagonále jsou 0. Každá matice s uvedenými vlastnostmi je maticí sousednosti vhodného grafu.

Příklad. Pro graf G



je matice sousednosti

$$A_G = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Poznamenejme ještě, že matice sousednosti zjevně závisí na zvoleném očíslování vrcholů grafu!

Mezi násobením matice sousednosti a metrikou grafu je jednoduchá souvislost. Nejdříve definujeme pojem sledu v grafu (podobný pojmu cesty):

Nechť $G = (V, E)$ je graf. Posloupnost $(v_0, e_1, v_1, e_2, \ldots, e_n, v_n)$ se nazývá *sled* v grafu G (obšírněji *sled délky* n *z* v_0 *do* v_n), jestliže platí $e_i = \{v_{i-1}, v_i\} \in E$ pro $i = 1, \ldots, n$. Narozdíl od cesty se ve sledu mohou některé vrcholy i hrany opakovat; sled si můžeme představovat jako záznam trasy bloudícího poutníka.

Pišme $v \sim_1 v'$, jestliže existuje sled z v do v'. Z definice sledu plyne, že $\sim_1$ je ekvivalence na množině V. Ve skutečnosti tato ekvivalence splývá ekvivalencí $\sim$ definovanou výše pomocí existence cesty. Plyne to z následujícího:

3.2.4 Lemma. *V grafu G existuje cesta z x do y právě když v G existuje sled z x do y.*

Důkaz. Zřejmě každá cesta tvoří sled. Na druhé straně sled z x do y, který má nejmenší možnou délku, je již nutně cesta. □

3.2.5 Tvrzení. *Nechť $G = (V, E)$ je graf, $V = \{v_1, \ldots, v_n\}$, a nechť $A = A_G$ je jeho matice sousednosti. Označme A^k k-tou mocninu matice sousednosti (při běžném násobení matic, t.j. označíme-li $B = A^2$, platí $b_{ij} = \sum_{k=1}^{n} a_{ik}a_{kj}$). Nechť $a_{ij}^{(k)}$ označuje prvek matice A^k v pozici (i, j). Pak $a_{ij}^{(k)}$ je počet sledů délky k z vrcholu v_i do vrcholu v_j v grafu G.*

Důkaz. Je jednoduchý leč poučný. Pracujeme indukcí podle k. Sled délky 1 mezi dvěma vrcholy znamená přesně že tyto vrcholy jsou spojeny hranou, takže pro $k = 1$ tvrzení je jenom jinak řečená definice matice sousednosti.

Teď předpokládejme, že $k > 1$, a že v_i, v_j jsou nějaké vrcholy (dovolujeme i $v_i = v_j$). Každý sled délky k z v_i do v_j začíná nějakou hranou jdoucí z v_i do nějakého v_ℓ, a zbytek je sled délky $k-1$ z v_ℓ do v_j. Podle indukčního předpokladu je počet sledů délky $k-1$ z v_ℓ do v_j roven $a_{\ell j}^{(k-1)}$. Tím pádem je počet sledů délky k z v_i do v_j

$$\sum_{\{v_i, v_\ell\} \in E(G)} a_{\ell j}^{(k-1)} = \sum_{\ell=1}^{n} a_{i\ell} a_{\ell j}^{(k-1)}.$$

Tohle ale je, podle definice násobení matic, přesně prvek v pozici (i, j) v součinu matic A a A^{k-1}, neboli $a_{ij}^{(k)}$. □

3.2.6 Důsledek. *Pro vzdálenost vrcholů platí*

$$d_G(v_i, v_j) = \min\{k;\, a_{ij}^{(k)} \neq 0\}.$$

Poznamenejme ještě, že matice sousednosti není vždy nejvhodnější způsob reprezentace grafu v paměti počítače. Obzvlášť když má graf málo hran (podstatně méně než $\binom{n}{2}$), bývá výhodnější např. pro každý vrchol zadat seznam jeho sousedů. Pro urychlení některých složitějších algoritmů se používají ještě další, složitější reprezentace.

Cvičení

1.* Kolik nejvíce hran může mít graf s n vrcholy a k komponentami?

2. Zkuste navrhnout algoritmus, který pro zadaný graf G rozhodne, zda je souvislý, a pro nesouvislý graf najde rozklad množiny $V(G)$ na komponenty. (Lze navrhnout algoritmus, který pro graf s n vrcholy a m hranami potřebuje $O(n + m)$ kroků.)

3.* Dokažte, že graf je bipartitní, právě když neobsahuje žádnou kružnici liché délky.

4. (a)* Popište, jak vypadají grafy, neobsahující žádnou cestu délky 3.

   (b)* Popište, jak vypadají grafy, neobsahující žádnou cestu délky 4.

5. Dokažte, že splňuje-li funkce $d : V \times V \to \{0, 1, 2, \ldots\}$ podmínky 1–5, potom existuje graf $G = (V, E)$ tak, že $d_G(v, v') = d(v, v')$ pro každou dvojici prvků množiny V.

6. Definujte průměr a poloměr grafu (v analogii s intuitivním významem těchto pojmů).

7. (a) Najděte souvislý graf na n vrcholech, pro nějž každá mocnina matice sousednosti obsahuje nulové členy.

   (b) Buď G graf na n vrcholech, $A = A_G$ jeho matice sousednosti, a I_n $n \times n$ jednotková matice (mající jedničky na diagonále a nuly všude jinde). Dokažte, že G je souvislý právě když $(I_n + A)^{n-1}$ nemá žádné nulové členy.

   (c) Kde má matice $(I_n + A)^{n-1}$ nulové členy, je-li G nesouvislý?

8. Dokažte, že grafy G a G' jsou isomorfní právě když existuje permutační matice P tak, že

$$A_{G'} = PA_GP^T.$$

Zde A_G je matice sousednosti G a P^T označuje matici transponovanou k matici P. Matice P se nazývá *permutační*, jestliže její prvky jsou 0 a 1 a v každém řádku a sloupci je právě jediná 1.

3.3 Hledání nejkratší cesty

Jednou ze základních algoritmických úloh v teorii grafů je najít nejkratší cestu mezi dvěma danými vrcholy v daném grafu. Takový požadavek vzniká v mnoha praktických aplikacích (třeba při hledání nejkratšího dopravního spojení, vlakem nebo po silnici a pod.). Dosud objevené algoritmy řešící tuto úlohu většinou počítají mnohem více, než se přímo požaduje — zpravidla naleznou nejkratší cesty z výchozího vrcholu do všech (nebo mnoha) vrcholů. Jedna z nejjednodušších a nejdůležitějších takových metod je tzv. *Dijkstrův algoritmus* (čte se, jakožto holandské jméno, „Dajkstrův").

Dijkstrův algoritmus předvedeme v situaci, kdy daný graf G má hrany ohodnocené kladnými reálnými čísly, to znamená, že spolu s každou hranou $e \in E(G)$ je dáno kladné reálné číslo $w(e)$, nebo jinak řečeno, je dána funkce $w : E(G) \to (0, \infty)$. Ohodnocení $w(e)$ hrany e si můžeme představovat jako její délku, nebo cenu, kterou musíme zaplatit za její projití, a pod. Délka nějaké cesty v takto ohodnoceném grafu G je rovna součtu délek jejích hran, a vzdálenost $d_{G,w}(u, v)$ dvou vrcholů $u, v \in V(G)$ je pak rovna nejmenší z délek všech cest, spojujících u a v. „Obyčejná" grafová vzdálenost d_G (definovaná v části 3.2) se dostane jako speciální případ, totiž je-li $w(e) = 1$ pro každou hranu e.

Vstupem Dijkstrova algoritmu je graf $G = (V, E)$, ohodnocení hran $w : E \to (0, \infty)$ a počáteční vrchol s („start"). Algoritmus pro každý vrchol $v \in V(G)$ vypočítá číslo $d_{G,w}(s, v)$, t.j. vzdálenost z s do v. Pro každý vrchol $v \in V$ se zavede jedna číselná proměnná $d(v)$. To je číslo, udávající momentální „odhad" na hledanou hodnotu $d_{G,w}(s, v)$. V každém kroku se pro některé vrcholy v momentální hodnota $d(v)$ prohlásí za definitivní (t.j. je to skutečná vzdálenost v od s), pro ostatní vrcholy

se $d(v)$ přepočítává. Proměnná A je množina „aktivních" vrcholů, což jsou vrcholy, pro něž $d(v)$ dosud nebylo prohlášeno za definitivní. Na začátku volíme $A = V$ a

$$d(v) = \begin{cases} 0 & \text{pro } v = s \\ \infty & \text{pro } v \neq s, \end{cases}$$

což odpovídá tomu, že na začátku známe cestu délky nula z s do s, ale zbytek grafu jsme ještě neprozkoumali.

V obecném kroku algoritmu utvoříme nejdříve množinu N vrcholů, pro něž je $d(v)$ nejmenší možné mezi všemi vrcholy $v \in A$ (množina N bude mít často jen jediný vrchol, aspoň pokud jsou ohodnocení hran např. náhodně vybraná čísla). Všechny vrcholy z N vyjmeme z A a přepočítáme hodnoty $d(x)$ pro jejich sousedy: Pro každou hranu $\{v, y\} \in E$, kde $v \in N$ a $y \in A$, porovnáme hodnoty $d(y)$ a $d(v) + w(\{v, y\})$. Je-li $d(v) + w(\{v, y\}) < d(y)$, znamená to, že přes vrchol v vede do y cesta kratší, než jsme zatím znali. Změníme proto hodnotu $d(y)$ na $d(v)+w(\{v, y\})$. Po takovémto přepočítání přejdeme k dalšímu kroku algoritmu. Algoritmus končí, platí-li $d(x) = \infty$ pro všechna $x \in A$. V takovém případě je buď $A = \emptyset$ (je-li G souvislý), anebo A obsahuje pouze vrcholy nedosažitelné cestou z vrcholu s.

Uvedeme ještě formální popis algoritmu:

3.3.1 Algoritmus (Dijkstrův algoritmus).
Vstup: graf $G = (V, E)$, ohodnocení hran $w(e)$, $e \in E$, startovní vrchol s.
Proměnné: čísla $d(v)$, $v \in V$, číslo δ, množiny $A, N \subseteq V$.
Výstup: po skončení algoritmu udává $d(v)$ vzdálenost v od s, pro každé $v \in V$.

Krok 1. (Inicializace)
$d(s) := 0$; $d(x) := \infty$ pro $x \in V \setminus \{s\}$; $A := V$.

Krok 2. (Test ukončení)
Jestliže pro všechna $x \in A$ platí $d(x) = \infty$, algoritmus končí, jinak se pokračuje krokem 3.

Krok 3. (Volba množiny N)
$\delta := \min\{d(y);\ y \in A\}$
$N := \{v \in A;\ d(v) = \delta\}$
$A := A \setminus N$

Krok 4. (Aktualizace $d(y)$ pro sousedy N)
Pro každou hranu $e = \{v, y\}$, kde $v \in N$ a $y \in A$, proveď příkaz
$d(y) := \min(d(y), d(v) + w(e))$.
Po vyčerpání všech takových hran e pokračuj krokem 2.

Poznámka. Při praktickém programování nahradíme symbol ∞ v inicializaci algoritmu nějakou velkou hodnotou, o které máme zaručeno, že bude větší než délka nejdelší cesty v G, např. $M = 1 + \sum_{e \in E} w(e)$.

Důkaz správnosti algoritmu. Nejprve nahlédneme (indukcí podle počtu opakování kroků 2–4 algoritmu), že v každém okamžiku činnosti algoritmu (a tedy i po jeho skončení) platí pro každý vrchol $v \in V$ nerovnost

$$d(v) \geq d_{G,w}(s, v).$$

To je zajisté pravda na začátku, kdy $0 = d_{G,w}(s, s)$ a $\infty \geq d_{G,w}(s, v)$ pro každé $v \in V$. V okamžiku změny hodnoty $d(y)$ pro nějaké $y \in V$ v kroku 4 ke změně dochází, protože existuje $v \in N$ takové, že $d(v) + w(\{v, y\}) < d(y)$. Pro v však podle indukčního předpokladu platí $d(v) \geq d_{G,w}(s, v)$. Přidáním hrany $\{v, y\}$ za nejkratší cestu z s do v (která má délku $d_{G,w}(s, v)$) získáme cestu z s do y délky $d_{G,w}(s, v) + w(\{v, y\})$, a proto

$$d_{G,w}(s, y) \leq d_{G,w}(s, v) + w(\{v, y\}) \leq d(v) + w(\{v, y\}) = d(y),$$

kde $d(y)$ je hodnota po provedení změny.

Nyní ukážeme, že po skončení činnosti algoritmu bude $d(v) \leq d_{G,w}(s, v)$ pro všechna $v \in V$. Ukážeme dokonce silnější tvrzení: *Jsou-li* $0 = d_1 < d_2 < \ldots < d_k < \infty$ *všechny různé konečné vzdálenosti vrcholů grafu od vrcholu* s, *a označíme-li* $M_i = \{v \in V;\ d_{G,w}(s, v) = d_i\}$

pro $i = 1, 2, \ldots, k$, *pak krok 3 algoritmu se provede přesně* k*-krát, a pro každé* i *po* i*-tém vykonání kroku 3 platí* $N = M_i$, $\delta = d_i$ a $V \setminus A = \bigcup_{j=1}^{i} M_j$.

Toto tvrzení dokážeme indukcí podle i. Pro lepší orientaci v algoritmu přidáme ke jménům proměnných horní index $^{(i)}$ značící hodnotu po i-tém vykonání kroku 2. Pro $i = 1$ tvrzení triviálně platí.

Vezměme nějaké $i > 1$ a $y \in M_i$ a předpokládejme, že tvrzení platí pro každé $j < i$. Jestliže $d_{G_w}(s, y) = d_i < \infty$, pak existuje cesta $(s = v_0, e_1, v_1, \ldots, v_t, e_{t+1}, v_{t+1} = y)$ z s do y délky d_i. Potom $d_{G,w}(s, v_t) \leq d_i - w(\{v_t, y\}) < d_i$, takže $v_t \in M_j$ pro nějaké $j < i$. Podle indukčního předpokladu je $v_t \in N^{(j)}$ a $d^{(j)}(v_t) = d_{G,w}(s, v_t)$. Proto $d^{(j+1)}(y) = d_{G,w}(s, v_t) + w(\{v_t, y\}) = d_{G,w}(s, y) = d_i$ a tím spíše $d^{(i)}(y) = d_i$.

Podle indukčního předpokladu je $d^{(i)}(v) = d_{G,w}(s, v) < d_i$ pro každé $v \in \bigcup_{j=1}^{i-1} M_j = V \setminus A^{(i-1)}$, a podle výše ukázaného je $d^{(i)}(v) \geq d_{G,w}(s, v) > d_i$ pro každé $v \in \bigcup_{i<j\leq k} M_j$. Proto $\delta^{(i)} = d_i$ a $N^{(i)} = M_i$. □

Poznamenejme, že algoritmus můžeme (prakticky beze změny) použít i pro tzv. orientované grafy (ty budou definovány v části 3.7), kde některé hrany se smějí procházet jenom jedním směrem.

Požadavek, že ohodnocení všech hran je kladné, je velmi podstatný. Pro úlohu nalezení nejkratší cesty v grafu, kde některé hrany mohou být ohodnoceny i záporně (za jejich projití dostaneme „prémii"), není známý žádný efektivní algoritmus, a nejspíše ani žádný neexistuje.

Zajímá-li nás pouze nejkratší cesta z vrcholu s do nějakého zadaného vrcholu c (cíl), můžeme použít Dijkstrův algoritmus, ale ukončit jej, jakmile vrchol c opustí množinu A (t.j. jeho vzdálenost se stane definitivní). Přitom však algoritmus stále může prohledávat mnoho vrcholů, z pohledu „zdravého rozumu", zbytečně (hledáme-li nejkratší silniční spojení z Brna do Ostravy, očekáváme, že k tomu není potřeba zjistit nejkratší cestu z Brna do Karlových Varů). K urychlení takového počítání byla vyvinuta zajímavá modifikace Dijkstrova algoritmu, tzv. *Dijkstrův algoritmus s heuristikou.* Slovo heuristika zde znamená (zhruba) něco, o čem si myslíme, že nám to v řešení úlohy pomůže, co „vypadá rozumně", ale zpravidla to neumíme dokázat. Konkrétně, v našem případě pro daný graf G, ohodnocení hran w a cílový vrchol c budeme *heuristi-*

kou rozumět funkci $h : V(G) \to [0, \infty)$, splňující $h(c) = 0$ a následující podmínku:

$$\text{Pro každou hranu } e = \{u, v\} \in E \text{ platí}$$
$$|h(u) - h(v)| \leq w(e).$$

Hodnota $h(v)$ je nějaký dolní odhad vzdálenosti v od c. V problémech dopravního spojení může být $h(v)$ například vzdálenost mezi v a c vzdušnou čarou. Máme-li nějakou takovou funkci h, můžeme Dijkstrův algoritmus modifikovat takto: v kroku 2 položíme $\delta := \min\{h(x) + d(x);\ x \in A\}$, a $N := \{v \in A;\ h(v) + d(v) = \delta\}$. Tento algoritmus zase správně najde vzdálenosti všech vrcholů od s, ale je-li h „kvalitní" (je to dobrý dolní odhad pro vzdálenosti od c), dá se čekat, že algoritmus najde definitivní vzdálenost do c rychleji než Dijkstrův algoritmus samotný. Důkaz správnosti ponecháváme jako cvičení 6.

Cvičení

1. Podle algoritmu napište program v Pascalu nebo C.

2.* Navrhněte podrobně implementaci (způsob naprogramování) Dijkstrova algoritmu tak, aby pracoval vždy v čase $O(n \log n + m)$, kde $n = |V(G)|$, $m = |E(G)|$.

3. Ve kterém místě selže uvedený důkaz správnosti Dijkstrova algoritmu, připustíme-li i záporná ohodnocení hran?

4.* Upravte algoritmus tak, aby nejen našel vzdálenosti $d_{G,w}(s, v)$, ale aby pro každé v též nalezl nějakou nejkratší cestu z s do v.

5. Uvažte následující algoritmus pro graf $G = (V, E)$ a počáteční vrchol s (algoritmus známý pod jménem *prohledávání do šířky*): Položíme $V_0 = \{s\}$, a bylo-li V_i již definováno, položíme $V_{i+1} = \{v \in V \setminus (V_0 \cup V_1 \cup \ldots \cup V_i);$ existuje $u \in V_i$, $\{u, v\} \in E\}$.

   (a) Formulujte přesně podmínku ukončení algoritmu (tak, aby fungoval i pro nesouvislý graf).

   (b) Dokažte, že množina V_i jsou vrcholy v, pro něž $d_G(s, v) = i$.

   (c) Navrhněte implementaci (způsob naprogramování) algoritmu, který vyžaduje nejvýš $O(n + m)$ kroků, kde $n = |V|$, $m = |E|$.

6.* Dokažte správnost Dijkstrova algoritmu s heuristikou, popsaného v závěru této části.

3.4 Skóre grafu

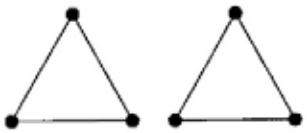
Nechť G je graf, v jeho vrchol. Symbolem $\deg_G(v)$ označme počet hran grafu G obsahujících vrchol v. Číslo $\deg_G(v)$ nazveme *stupněm* vrcholu v v grafu G.

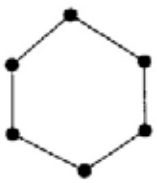
Označme vrcholy grafu G $v_1, v_2, \ldots, v_n$ (v nějakém libovolně zvoleném pořadí). Posloupnost

$$(\deg_G(v_1), \deg_G(v_2), \ldots, \deg_G(v_n))$$

nazýváme *posloupnost stupňů* grafu G, nebo *skóre* grafu G. Dvě skóre přitom považujeme za stejná, pokud jedno můžeme dostat z druhého přerovnáním čísel (to znamená, že skóre nezávisí na zvoleném pořadí vrcholů).

Je snadno vidět, že dva isomorfní grafy mají stejná skóre (v právě zavedeném smyslu); tudíž dva grafy s různým skóre jsou nutně neisomorfní. Na druhé straně, grafy se stejným skóre ještě isomorfní být nemusí. Tak například následující dva grafy

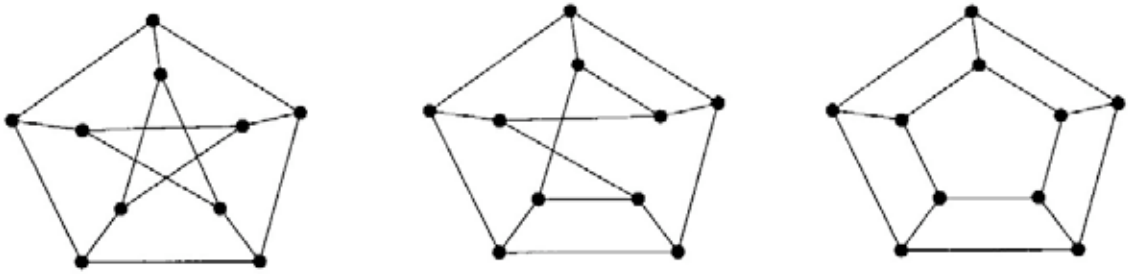




mají oba skóre $(2, 2, 2, 2, 2, 2)$, a přitom jsou zjevně neisomorfní — jeden je totiž souvislý, zatímco druhý není. Všechny tři grafy na obr. 3.2 mají skóre $(3, 3, 3, 3, 3, 3, 3, 3, 3, 3)$ a přitom žádné dva nejsou isomorfní (přesvědčit se o tom je trochu těžší, viz cvičení 1). Přesto však představuje skóre grafu důležitou a snadno zjistitelnou charakteristiku grafu. Budeme nyní hledat vlastnosti, které musí posloupnost čísel mít, aby byla skórem nějakého grafu. Jedna taková významná vlastnost je následující:

3.4.1 Tvrzení (Princip sudosti). *Pro každý graf $G = (V, E)$ platí*

$$\sum_{v \in V} \deg_G(v) = 2|E|.$$



Obrázek 3.2: Tři souvislé neisomorfní grafy s týmž skóre.

Důkaz. Stupeň vrcholu v udává počet hran G obsahujících v. Přitom každá hrana obsahuje dva vrcholy; sečteme-li tedy všechny stupně, dostaneme dvojnásobek počtu hran. □

3.4.2 Důsledek. *Počet vrcholů lichého stupně je sudé číslo pro každý graf.*

(Neboli počet účastníků večírku, kteří si potřásli rukou s lichým počtem jiných účastníků, je sudé číslo — pro každý konečný večírek.)

Poznamenejme, že pro nekonečné večírky věta neplatí: následující graf (jednostranně nekonečná cesta) má jen jediný vrchol lichého stupně.

Důsledek 3.4.2 (ani některé další snadné podmínky) na charakterizaci skóre grafu nestačí. Charakteristika skóre není zrovna jednoduchá a souvisí s problematikou tzv. toků v sítích, jež přesahuje rámec tohoto textu. Ukážeme zde však jednoduchý postup, jak o dané posloupnosti rozhodnout, zda je to skóre nějakého vhodného grafu. Základem je následující:

3.4.3 Věta (Věta o skóre). *Nechť $D = (d_1, d_2, \ldots, d_n)$ je posloupnost přirozených čísel. Předpokládejme, že $d_1 \leq d_2 \leq \ldots \leq d_n$, a*

označme symbolem D' posloupnost $(d'_1, \ldots, d'_{n-1})$, kde

$$d'_i = \begin{cases} d_i & \text{pro } i < n - d_n \\ d_i - 1 & \text{pro } i \geq n - d_n. \end{cases}$$

Potom D je skóre grafu právě když D' je skóre grafu.

Důkaz. Jedním směrem je tvrzení snadné. Předpokládejme, že D' je skóre grafu $G' = (V', E')$, kde $V' = \{v_1, \ldots, v_{n-1}\}$ a $\deg_G(v_i) = d'_i$. Zvolme nový vrchol v_n, různý od $v_1, \ldots, v_{n-1}$, a definujme nový graf $G = (V, E)$, kde

$$V = V' \cup \{v_n\}$$
$$E = E' \cup \{\{v_i, v_n\};\ i = n - d_n, n - d_n + 1, \ldots, n - 1\}$$

(méně formálně řečeno, nový vrchol v_n připojíme k posledním d_n vrcholům grafu G'). Zřejmě skóre grafu G je právě D.

Těžší je dokázat opačnou implikaci. Předpokládejme tedy, že D je skóre nějakého grafu. Uvažme množinu $\mathcal{G}$ všech grafů na množině vrcholů $\{v_1, \ldots, v_n\}$, v nichž je stupeň každého v_i roven d_i (t.j. mají skóre D). Dokážeme následující

> *Pomocné tvrzení:* V množině $\mathcal{G}$ existuje graf G_0, v němž je vrchol v_n spojen právě s vrcholy $v_{n-d_n}, v_{n-d_n+1}, \ldots, v_{n-1}$ (neboli s posledními d_n vrcholy).

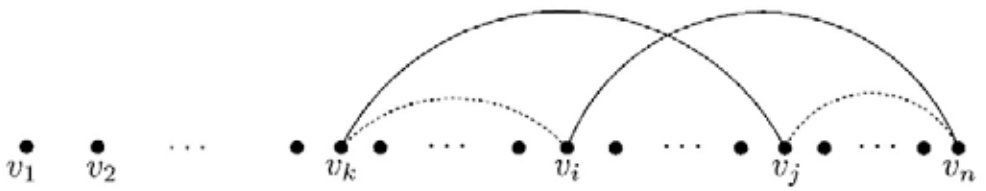
Budeme-li mít graf G_0 jako v pomocném tvrzení, je už jasné, že graf $G' = (\{v_1, \ldots, v_{n-1}\}, E')$, kde $E' = \{e \in E(G_0);\ v_n \notin e\}$, má skóre D', a tím bude věta o skóre dokázána. Zbývá dokázat pomocné tvrzení.

Pokud $d_n = n-1$, t.j. pokud vrchol v_n je spojen s každým z vrcholů $v_1, \ldots, v_{n-1}$, vyhovuje pomocnému tvrzení kterýkoli graf z $\mathcal{G}$ a jsme hotovi. Jinak, t.j. pokud v_n není spojen se všemi ostatními vrcholy, definujme pro každý graf $G \in \mathcal{G}$ číslo $j(G)$, což bude největší index $j \in \{1, 2, \ldots, n-1\}$ takový, že $\{v_j, v_n\} \notin E(G)$. Buď G_0 graf, pro nějž je $j(G)$ nejmenší možné; dokážeme, že $j(G_0) = n - d_n - 1$, z čehož je už patrné, že G_0 vyhovuje pomocnému tvrzení.

Předpokládejme tedy pro spor, že $j = j(G_0) > n - d_n - 1$. Vrchol v_n musí být spojen s d_n vrcholy, a z nich nejvýš $d_n - 1$ může následovat po vrcholu v_j. Proto existuje nějaké $i < j$ takové, že v_i je spojen s vrcholem v_n. Máme tedy $\{v_j, v_n\} \notin E(G_0)$, $\{v_i, v_n\} \in E(G_0)$. Vzhledem k tomu, že $\deg_{G_0}(v_i) \leq \deg_{G_0}(v_j)$, existuje nějaký vrchol v_k, který je spojený hranou s v_j, ale nikoli s v_i. V této situaci uvážíme nový graf $G' = (V(G_0), E')$, kde

$$E' = (E(G_0) \setminus \{\{v_i, v_n\}, \{v_j, v_k\}\}) \cup \{\{v_j, v_n\}, \{v_i, v_k\}\}.$$

Viz obrázek:



Je snadno vidět, že graf G' má rovněž skóre D, a přitom $j(G') \leq j(G_0) - 1$, což je spor s volbou grafu G_0. Tím je dokázáno pomocné tvrzení, a tudíž i věta 3.4.3. □

Z věty 3.4.3 lze odvodit algoritmus, který umožňuje rychle rozhodnout, jestli je daná konečná posloupnost skórem nějakého grafu.

3.4.4 Úloha. *Rozhodněte, zda posloupnost* (1, *1, 1, 2, 2, 3, 4, 5,* 5) *je skóre grafu.*

Řešení. Danou posloupnost redukujeme opakovaným použitím věty 3.4.3. Dostáváme tak posloupnosti

(1, 1, 1, 1, 1, 2, 3, 4)

(1, 1, 1, 0, 0, 1, 2), po přerovnání (0, 0, 1, 1, 1, 1, 2)

(0, 0, 1, 1, 0, 0), po přerovnání (0, 0, 0, 0, 1, 1)

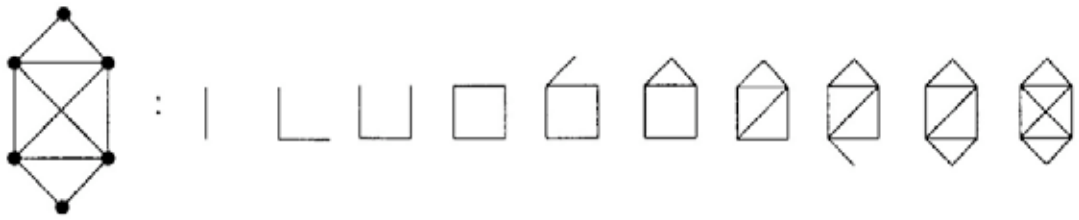
(0, 0, 0, 0, 0).

Protože poslední posloupnost je skóre grafu (grafu s 5 vrcholy a žádnou hranou), dostáváme, že i posloupnost (1, 1, 1, 2, 2, 3, 4, 5, 5) je skóre grafu. Sestrojte sami příklad takového grafu!

Cvičení

1. Dokažte, že tři grafy na obr. 3.2 jsou navzájem neisomorfní.
2. Sestrojte příklad posloupnosti délky n, jejíž každý člen je některé z čísel $1, \ldots, n-1$ a která má sudý počet lichých členů, a přesto není skórem žádného grafu.
3. Najděte nejmenší možný příklad (s co nejméně vrcholy) dvou souvislých neisomorfních grafů se stejným skórem.
4. Nakreslete všechny navzájem neisomorfní grafy se skórem (6, 3, 3, 3, 3, 3, 3) (ukažte, že jste žádný nevynechali!).
5. Uveďte co nejmenší příklad grafu s 6 vrcholy stupně 3, ostatními vrcholy stupně ≤ 2, a s 12 hranami.
6. Buď G graf s 9 vrcholy, každý stupně 5 nebo 6. Dokažte, že má aspoň 5 vrcholů stupně 6 nebo aspoň 6 vrcholů stupně 5.
7. (a) Rozhodněte, zda existuje graf se skórem tvořeným $n \geq 2$ navzájem různými čísly.

   (b)* Pro která n existuje graf na n vrcholech, jehož skóre má všechna čísla navzájem různá až na 2?
8.* Nechť G je graf s maximálním stupněm 3. Dokažte, že jeho vrcholy lze obarvit dvěma barvami tak, že nevznikne jednobarevná cesta se 3 vrcholy.
9.** Nechť G je graf, jehož všechny vrcholy mají stupeň aspoň 3. Dokažte, že potom G obsahuje kružnici, která není indukovaným podgrafem (t.j., má „diagonálu“).
10. Graf G se nazývá *k-regulární* (česky k-pravidelný), jsou-li stupně všech jeho vrcholů přesně k. Určete všechny dvojice (k, n) takové, že existuje k-regulární graf na n vrcholech.
11. Nakreslete všechny 3-regulární grafy na 6 vrcholech.
12. Najděte 3-regulární asymetrický graf (viz cvičení 3 v části 3.1).
13.* Nechť G je souvislý graf, v němž mají každé dva různé vrcholy u, v buď 0 nebo 5 společných sousedů. Dokažte, že G je k-regulární (pro nějaké k).
14.** Dokažte, že v každém grafu se sudým počtem vrcholů existují dva vrcholy, které mají sudý počet společných sousedů.



Obrázek 3.3: Kreslení grafů jedním tahem.

15. Nechť G je graf s n vrcholy, jehož každý vrchol má stupeň větší než $\frac{n}{2}$.

    (a) Dokažte, že G obsahuje aspoň 1 trojúhelník (cyklus délky 3).

    (b)* Dokažte, že existuje hrana $\{x, y\}$ obsažená aspoň v $n/6$ trojúhelnících (t.j. existuje aspoň $n/6$ vrcholů spojených jak s x tak s y). Použijte principu inkluze a exkluze.

3.5 Jednotažky – eulerovské grafy

Jednou ze základních (a nejstarších) úloh týkající se grafu je následující otázka:

> *Nakreslete daný graf $G = (V, E)$ jedním uzavřeným tahem, bez zvednutí tužky z papíru (přičemž žádná hrana se neobtahuje dvakrát).*

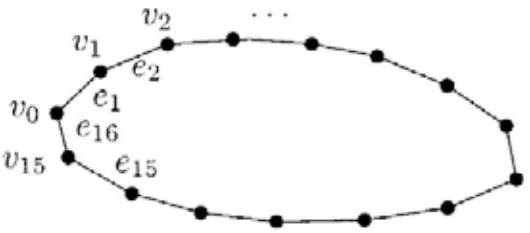
Matematicky lze úlohu formalizovat takto: Najděte uzavřený sled $(v_0, e_1, v_1, \ldots, e_{m-1}, v_{m-1}, e_m, v_0)$, v němž se každá hrana vyskytuje právě jednou a každý vrchol aspoň jednou. Takový sled budeme nazývat *uzavřeným eulerovským tahem.* Graf je eulerovský právě když má aspoň jeden uzavřený eulerovský tah.

Obr. 3.3 ukazuje příklad kreslení grafu jedním tahem.

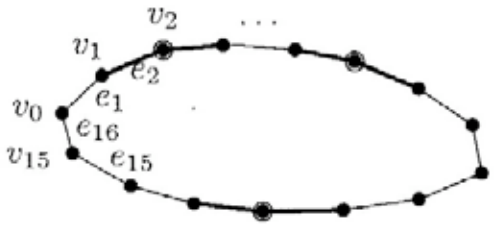
Podáme nyní charakteristiku eulerovských grafů. Pro stručnost definujeme *tah* v grafu G jako sled, v němž se žádná hrana neopakuje (vrcholy se opakovat mohou).

3.5.1 Věta (Charakterizace eulerovských grafů). *Graf G je eulerovský právě když je souvislý a každý vrchol G má sudý stupeň.*

Důkaz. Uvedená podmínka je nutná. Eulerovský graf musí zjevně být souvislý. Stupně vrcholů jsou sudé, protože kdykoli eulerovský tah vstoupí do vrcholu, musí jej také zase opustit. Řekněme to přesněji. Nakresleme si nějaký eulerovský tah schématicky jako kružnici:



V tomto obrázku jsou všechny hrany $e_1, e_2, \ldots$ navzájem různé, ale některé z puntíků $v_0, v_1, \ldots$ mohou ve skutečnosti označovat týž vrchol. Podívejme se na nějaký vrchol $v \in V$, a vyznačme všechny jeho výskyty na předchozím obrázku. Například:



Stupeň v je roven počtu hran zasahujících do vyznačených puntíků na tomto obrázku. Každý vyznačený puntík přispěje dvěma hranami, a žádná hrana nemá oba konce vyznačené (protože vyznačené puntíky odpovádají všechny stejnému vrcholu zatímco hrana má dva různé konce). Proto $\deg_G(v)$ je sudé pro každý vrchol v.

Naopak, nechť souvislý graf G má všechny vrcholy sudého stupně. Uvažme v G tah $T = (v_0, e_1, v_1, \ldots, e_m, v_m)$, který má maximální možnou délku, m.

Nejdříve dokážeme, že $v_0 = v_m$. Kdyby ne, potom do vrcholu v_0 zasahuje lichý počet hran tahu T. Protože ale $\deg_G(v_0)$ je sudý, existuje nějaká hrana $e \in E$, která není v T obsažena, a o tuto hranu bychom mohli tah prodloužit — spor.

Předpokládejme tedy $v_0 = v_m$, a dokazujme že $\{e_1, e, \ldots, e_m\} = E$. Definujme pomocný graf $G' = (V', E')$, kde V' je množina všech vrcholů tahu T a E' je množina všech jeho hran.

Nejdříve předpokládejme $V' \neq V$. Díky souvislosti grafu G existuje hrana tvaru $e = \{v_k, v'\} \in E$, kde $v_k \in V'$ a $v' \notin V'$. V tomto případě tah

$$(v_k, e_{k+1}, v_{k+1}, \ldots, v_{m-1}, e_m, v_0, e_1, v_1, \ldots, e_k, v_k, e, v')$$

má délku $m+1$ a vede tedy ke sporu.

Jestliže $V' = V$ a $E' \neq E$, uvažme hranu $e \in E \setminus E'$, kde $e = \{v_k, v_\ell\}$. Podobně jako v předchozím případě vede tah

$$(v_k, e_{k+1}, v_{k+1}, \ldots, v_{m-1}, e_m, v_0, e_1, v_1, \ldots, e_k, v_k, e, v_\ell)$$

ke sporu. □

Poznámka o hamiltonovských kružnicích. *Hamiltonovská kružnice* v grafu G je kružnice obsahující všechny vrcholy G. Tento pojem je na první pohled podobný uzavřenému eulerovskému tahu: hamiltonovská kružnice má procházet bez opakování všechny vrcholy, a uzavřený eulerovský tah všechny hrany. Přesto je matematická a algoritmická obtížnost obou pojmů úplně rozdílná. Zatímco uzavřené eulerovské tahy jsou snadno zvládnutelné, problém existence hamiltonovské kružnice je matematicky i algoritmicky obtížný a žádnou jednoduchou charakterizaci grafů s hamiltonovskou kružnicí nelze čekat. Některé úvahy o hamiltonovských kružnicích si může čtenář zkusit ve cvičení 6.

Poznámka o násobných hranách. Zatím jsme definovali hrany grafu jako dvoubodové množiny vrcholů (a této definice se budeme zpravidla držet i nadále). To mimo jiné znamená, že dva dané vrcholy mohou být spojeny nejvýš jednou hranou. V některých aplikacích je však přirozené připustit, aby dva vrcholy mohly být spojeny i několika (různými) hranami; dostáváme tak *grafy s násobnými hranami* (zvané též *multigrafy*). Matematicky lze tento pojem vystihnout několika různými (a různě šikovnými) způsoby.

Mohli bychom například každé dvojici vrcholů $\{u, v\}$ přiřadit nezáporné celé číslo $m(u, v)$, *násobnost* hrany $\{u, v\}$. Přitom $m(u, v) = 0$ by znamenalo, že hrana v grafu není přítomna, $m(u, v) = 1$ by znamenalo „obyčejnou“ (jednoduchou) hranu, a $m(u, v) > 1$ by znamenalo,

že graf obsahuje $m(u,v)$ „kopií" hrany $\{u,v\}$. Multigraf by pak byl uspořádaná dvojice (V,m), kde $m : \binom{V}{2} \to \{0,1,\ldots\}$.

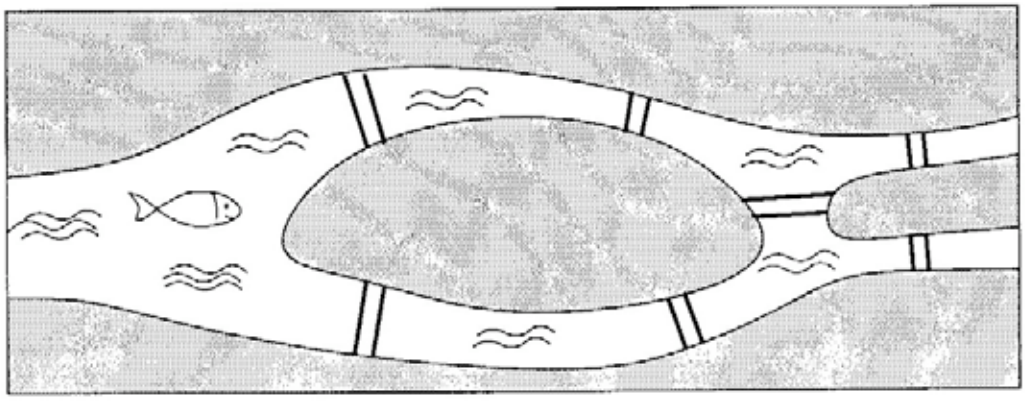
Jiný používaný způsob, z jistého hlediska elegantnější, je prohlásit hrany za „abstraktní" objekty, t.j. vzít E jako nějakou konečnou množinu disjunktní s množinou vrcholů V, a potom pro každou hranu určit dvojici vrcholů, které jsou jejími „konci" (a jedna dvojice vrcholů se může vyskytnout pro více hran). Formálně, graf s násobnými hranami by byl trojice (V,E,ε), kde V a E jsou disjunktní množiny a $\varepsilon : E \to \binom{V}{2}$ je zobrazení, určující konce hran.

Někdy je také výhodné v grafu připouštět *smyčky*, t.j. hrany začínající a končící v témže vrcholu. Formálně je opět možné smyčky zavést řadou způsobů. Nejjednodušeji můžeme smyčku u vrcholu v v množině hran E reprezentovat jako jednoprvkovou množinu $\{v\}$ (zatímco ostatní hrany jsou dvouprvkové). Při zavedení násobných hran pomocí zobrazení ε by se smyčky zavedly tím, že ε bude zobrazení do množiny $\binom{V}{2} \cup V$, a smyčka e se zobrazí na svůj (jediný) koncový vrchol. O ještě další modifikaci pojmu grafu (orientované grafy) budeme mluvit v části 3.7.

U většiny jednodušších aplikací není způsob formálního zavedení grafů s násobnými hranami příliš důležitý, pokud ovšem zvolíme jeden způsob a nadále se jej konzistentně držíme, a pokud to není způsob zbytečně neohrabaný.

Cvičení

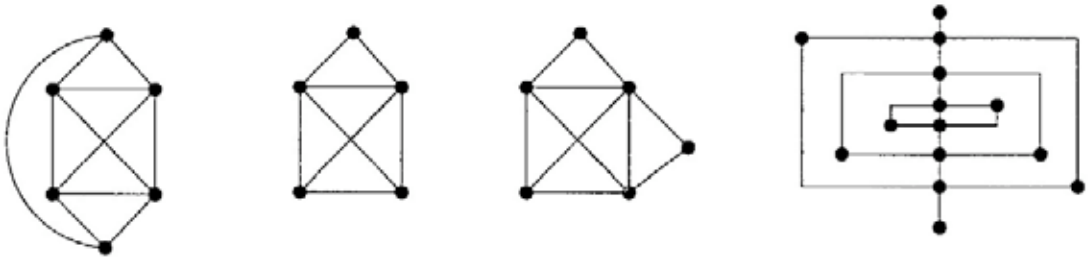
1. Na následujícím plánku města je schématicky znázorněno 7 mostů.



(a) Rozhodněte, zda je možno vyjít z určitého místa, projít všechny mosty, každý z nich však pouze jedenkrát, a vrátit se do výchozího místa. Je možno projít tímto způsobem všechny mosty, aniž bychom požadovali návrat do výchozího místa?
(Toto je historická motivace pojmu eulerovských grafů: plánek odpovídá části města Královce, Königsbergu, či Kaliningradu — jak různě se ve své pohnuté historii nazývalo — a tuto úlohu řešil Euler roku 1736).

(b) Kolik mostů by bylo třeba přistavět (a kde), aby úloha měla kladné řešení?

2. Nakreslete jedním tahem následující grafy



3. Charakterizujte grafy, které lze nakreslit jedním tahem, jenž nemusí být nutně uzavřený.

4. Na základě uvedeného důkazu věty 3.5.1 formulujte algoritmus pro nalezení uzavřeného eulerovského tahu.

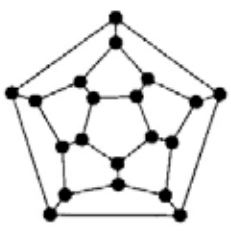
5. Podejte jiný důkaz věty 3.5.1, podle následujícího návodu:

(a) Dokažte, že má-li graf G všechny stupně sudé, lze jeho množinu hran vyjádřit jako disjunktní sjednocení kružnic v grafu G.

(b) Ukažte, že dva uzavřené tahy v grafu, které mají společný aspoň jeden vrchol, lze spojit v jediný uzavřený tah. Dokažte pak větu 3.5.1.

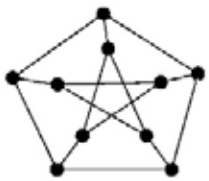
6. (Hamiltonovské kružnice)

(a) Najděte hamiltonovskou kružnici grafu



(to je abstraktní verze hlavolamu, vynalezeného významným matematikem sirem Hamiltonem). Které další z grafů na obr. 5.1 (str. 183) mají hamiltonovskou kružnici?

(b) Pokuste se ukázat, že Petersenův graf



hamiltonovskou kružnici nemá.

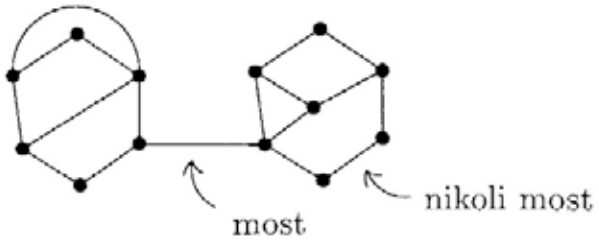
(c) Najděte dva grafy s týmž skóre, z nichž jeden má hamiltonovskou kružnici a druhý ne.

3.6 Algoritmus na kreslení grafu jedním tahem

Věta 3.5.1 poskytuje jednoduchou metodu pro důkaz *neexistence* nakreslení grafu jedním tahem. Jestliže graf splňuje podmínku sudosti stupňů, můžeme z důkazu odvodit algoritmus, který příslušný tah najde (začne se nějakým libovolným tahem a ten se postupně prodlužuje). V této části podáme ještě jeden důkaz, formulovaný přímo jako algoritmus na nalezení příslušného tahu. Tento algoritmus je např. vhodnější pro „ruční" použití (přímo dává jednu po druhé hrany tahu v tom pořadí, jak je máme kreslit, zatímco předchozí důkaz tah mnohokrát měnil), a navíc detailnější analýza (již zde dělat nebudeme) ukazuje, že nový algoritmus je, při vhodném naprogramování všech operací, rychlejší.

Začneme jednoduchým pomocným tvrzením.

Nechť $G = (V, E)$ je graf. Hranu $e \in E$ nazveme *mostem* grafu G, jestliže graf $(V, E \setminus \{e\})$ má větší počet komponent než graf G. Tato definice má intuitivní význam:



3.6.1 Lemma. *Nechť $G = (V, E)$ je graf, jehož všechny stupně jsou sudé. Potom graf G neobsahuje most.*

Důkaz. Postupujme sporem: předpokládejme, že hrana $\{v, v'\} = e$ je most grafu G. Nechť $V_1, \ldots, V_n$ jsou všechny komponenty grafu G, označené tak, že $\{v, v'\} \subseteq V_1$. Uvažme graf $G_1 = (V_1, E_1) = \left(V_1, E \cap \binom{V_1}{2}\right)$. Zřejmě graf G_1 je souvislý, má všechny stupně sudé a navíc hrana e je mostem grafu G_1. Tedy graf $(V_1, E_1 \setminus \{e\}) = (V_1, \bar{E})$ je nesouvislý. Zřejmě však graf $(V_1, \bar{E})$ má právě dvě komponenty: jedna z těchto komponent obsahuje vrchol v a druhá vrchol v'. Navíc však každá z těchto komponent obsahuje právě jediný vrchol lichého stupně: v a v'. To je však spor s principem sudosti. □

Algoritmus pro nakreslení grafu jedním tahem. Nechť $G = (V, E)$ je souvislý graf se všemi stupni sudými, $|E| = m$.

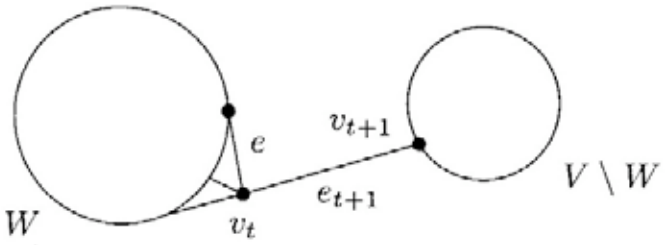
Krok 1. Zvol $v_0 \in V$ libovolně. Polož $T_0 = v_0$.

Krok 2. Opakuj následující krok 3 pro $i = 0, 1, 2, \ldots$, dokud je to možné. Pokud už krok 3 nelze provést, potom $i = m$ a T_m je hledaný tah.

Krok 3. (Prodloužení tahu) Nechť $T_i = (v_0, e_1, v_1, \ldots, e_i, v_i)$ je již definovaný tah. Zvol hranu $e_{i+1} \in E \setminus \{e_1, e_2, \ldots, e_i\}$ obsahující vrchol v_i. Pokud je to možné, zvol e_{i+1} navíc tak, aby grafy $(V, E \setminus \{e_1, \ldots, e_i\})$ a $(V, E \setminus \{e_1, \ldots, e_i, e_{i+1}\})$ měly stejný počet komponent.

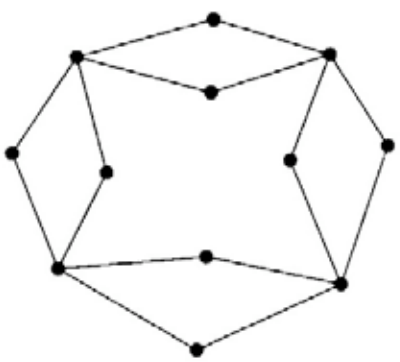
Důkaz správnosti algoritmu. Nechť $T_k = (v_0, e_1, v_1, \ldots, e_k, v_k)$ je výsledek uvedeného algoritmu. Pro $i = 1, \ldots, k$ označme symbolem G_i graf G po odebrání hran $e_1, \ldots, e_i$. Zřejmě $\deg_{G_k}(v_k) = 0$ (jinak bychom mohli tah v kroku 3 prodloužit) a tedy $v_0 = v_k$. Předpokládejme pro spor, že tah T_k neprojde všechny hrany grafu G, t.j. $E(G_k) \neq \emptyset$, a definujme množinu $W = \{v \in V(G);\ \deg_{G_k}(v) > 0\} \neq \emptyset$.

Protože G je souvislý graf, tah T_k množinu W aspoň jednou navštíví. Nechť v_t je vrchol, v němž ji navštíví naposledy. To znamená, že t je maximální index, pro nějž $v_t \in W$; zřejmě $v_{t+1} \notin W$. Jelikož G_k má hrany jenom na množině W a e_{t+1} je poslední hrana tahu T_k, která do W zasahuje, je e_{t+1} jediná hrana v grafu G_t spojující vrchol z W s vrcholem mimo W — jinými slovy e_{t+1} je most v grafu G_t a G_{t+1} má více komponent než G_t.

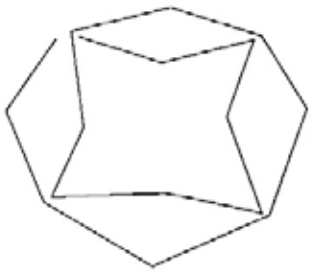


Nechť e je nějaká hrana grafu G_t obsahující vrchol v_t a různá od e_{t+1} (taková existuje, protože $\deg_{G_{t+1}}(v_t) \geq \deg_{G_k}(v_t) > 0$). Podle pravidla v kroku 3 musí být hrana e také most v grafu G_t, jinak bychom ji byli vybrali místo e_{t+1}, a dokonce je e mostem v grafu $G' = (W, E(G_t) \cap \binom{W}{2})$ (podgraf indukovaný množinou W v grafu G_t). Přitom ale podgraf indukovaný množinou W se již odebíráním dalších hran tahu T_k nezmění; zapsáno v symbolech, $E(G') = E(G_k) \cap \binom{W}{2} = E(G_k)$. Stupně všech vrcholů v grafu G_k, a tudíž i v G', jsou sudé, a to je spor s lemmatem 3.6.1 (aplikovaným na graf G'). □

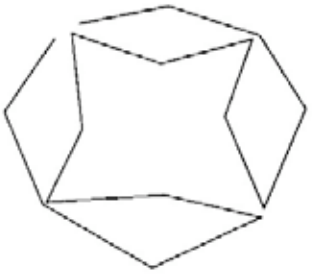
Příklad. Graf G uvedený na obrázku



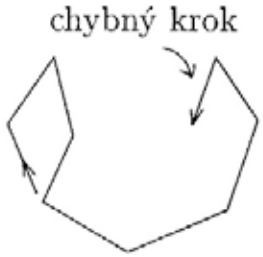
lze nakreslit jedním tahem například takto:



nebo



nikoli však

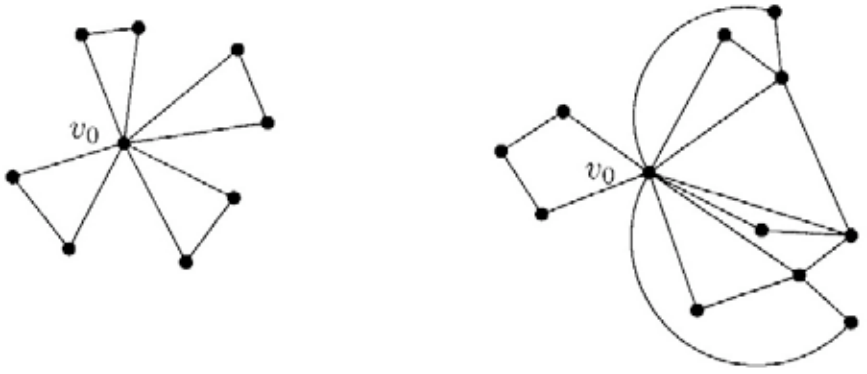


Cvičení

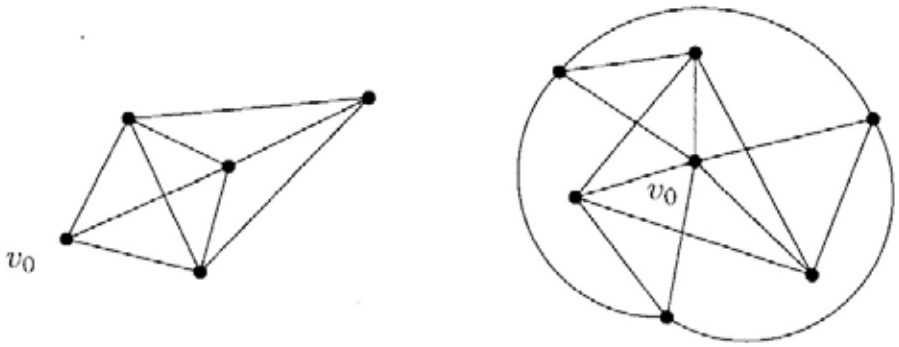
1. Navrhněte podrobně algoritmus, který hledá nakreslení grafu jedním tahem.

2. Řekněme, že graf $G = (V, E)$ je *náhodně eulerovský* z vrcholu v_0 jestliže každý maximální tah z vrcholu v_0 představuje již nakreslení grafu G jedním tahem (ekvivalentně: jestliže libovolný tah počínající ve vrcholu v_0, který již nelze prodloužit, představuje nakreslení grafu G jedním tahem).

   (a) Dokažte, že následující grafy jsou náhodně eulerovské:



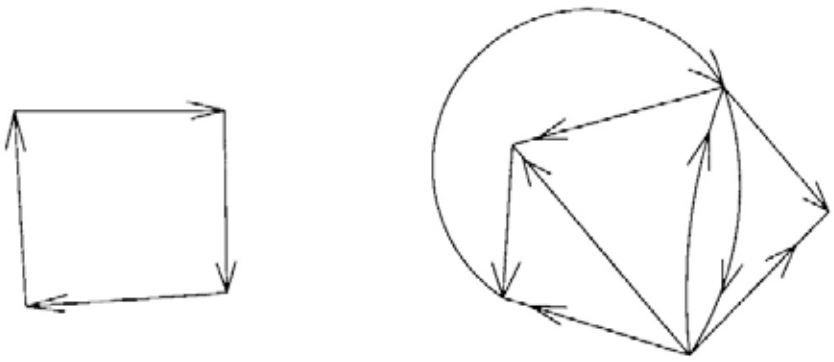
(b) Dokažte, že následující grafy nejsou náhodně eulerovské:



(c)* Dokažte následující charakteristiku náhodně eulerovských grafů: Souvislý graf $G = (V, E)$, jehož všechny vrcholy mají sudý stupeň, je náhodně eulerovský z vrcholu v_0 právě když graf $(V \setminus \{v_0\}, \{e \in E; v_0 \notin e\})$ neobsahuje kružnici (t. j., každá komponenta tohoto grafu je strom; takové grafy se také nazývají *lesy*).

3.7 Eulerovské orientované grafy

Všechny grafy, které jsme dosud uvažovali, byly „neorientované" — jejich hrany byly neuspořádané dvojice. Čtenář se však zajisté setkal se schématy zahrnujícími jednosměrné ulice a schématy podobnými tém na obrázku:



3.7.1 Definice. Orientovaný graf G *je dvojice* (V, E) *kde* E *je podmnožina kartézského součinu* $V \times V$. *Prvky* E *nazýváme* šipky *(nebo* orientované hrany*). Tedy šipka* e *má tvar* (x, y). *Říkáme, že tato šipka* vychází z x a končí v y.

Mnoho úloh a pojmů, které se v tomto textu vyšetřují, je možno snadno modifikovat pro orientované grafy. Často však tato obecnější tvrzení jsou snadným zobecněním a přitom značení a postup by se zkomplikovaly. Proto jsme se rozhodli uvažovat ve většině textu pouze neorientované grafy. Učiňme na tomto místě výjimku a zaveďme eulerovské orientované grafy a popišme jednu jejich aplikaci.

Pozorný čtenář si možná všiml, že orientovaný graf $G = (V, E)$ je vlastně totéž co relace na množině V. Přesto se zavádějí oba tyto pojmy, protože orientované grafy se vyšetřují v jiných souvislostech než relace.

Nyní je přirozené definovat *orientovaný tah* jako posloupnost

$$(v_0, e_1, v_1, e_2, \ldots, e_m, v_m)$$

pro niž platí, že $e_i = (v_{i-1}, v_i) \in E$ pro každé $i = 1, 2, \ldots, m$ a navíc $e_i \neq e_j$ kdykoliv $i \neq j$. (Podobně definujeme pojmy orientovaný sled, orientovaná cesta, orientovaná kružnice — orientované kružnice je zvykem nazývat *cykly*.)

Řekněme, že orientovaný graf (V, E) je *eulerovský*, jestliže v něm existuje uzavřený orientovaný tah, který obsahuje každou hranu právě jednou a každý vrchol aspoň jednou.

Orientované eulerovské grafy lze opět charakterizovat velmi dobře. Před příslušnou větou je však třeba zavést ještě několik pojmů.

Pro daný vrchol v v orientovaném grafu $G = (V, E)$ označme $\deg_G^+(v)$ počet šipek G, které končí ve v. Podobně $\deg_G^-(v)$ označuje počet šipek G, které začínají ve v. Číslo $\deg_G^+(v)$ se nazývá *vstupní stupeň vrcholu* v a $\deg_G^-(v)$ se nazývá *výstupní stupeň* vrcholu v. Orientovaný graf $G = (V, E)$ nazýváme *vyvážený*, jestliže pro každý vrchol $v \in V$ platí $\deg_G^+(v) = \deg_G^-(v)$.

Každému orientovanému grafu $G = (V, E)$ lze přiřadit neorientovaný graf $\operatorname{sym}(G) = (V, \bar{E})$, kde

$$\bar{E} = \{\{x, y\};\ (x, y) \in E \text{ nebo } (y, x) \in E\}.$$

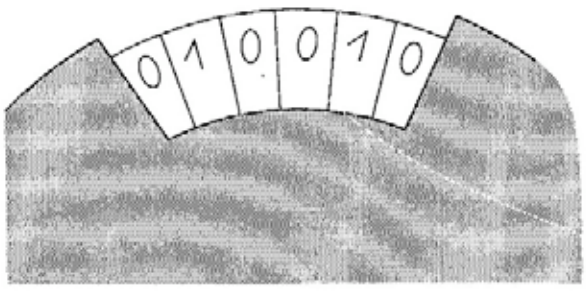
Graf $\operatorname{sym}(G)$ se nazývá *symetrizace* grafu G.

Platí následující charakteristika eulerovských grafů:

3.7.2 Tvrzení. *Orientovaný graf je eulerovský právě když je vyvážený a jeho symetrizace je souvislý graf*[3].

Důkaz tohoto tvrzení je velice podobný důkazu věty 3.5.1, a proto jej ponecháváme jako cvičení.

Aplikace. Představme si, že máme na obvod kotouče rozmístit čísla 0 a 1 takovým způsobem, že v každé poloze kotouče zjistíme tuto polohu jednoznačně z k po sobě jdoucích cifer, které pozorujeme na určitém místě. Při daném k bychom chtěli navrhnout co největší kotouč.



Jiná formulace problému je následující:

[3]Orientovaný graf se souvislou symetrizací se nazývá *slabě souvislý*. Naproti tomu v *silně souvislém* orientovaném grafu lze každé dva vrcholy spojit orientovanou cestou (v obou směrech).

Nalezněte co nejdelší cyklické uspořádání čísel 0 a 1, tak, aby žádné dvě k-tice po sobě jdoucích cifer nebyly stejné (zde cyklickým uspořádáním myslíme rozestavení čísel na obvodu kruhu).

Pro dané k označme délku nejdelšího možného cyklického uspořádání symbolem $u(k)$. Dokážeme následující překvapivé

3.7.3 Tvrzení. *Pro každé $k \geq 1$ platí $u(k) = 2^k$.*

Důkaz. Protože různých posloupností čísel 0 a 1 délky k je 2^k, délka uspořádání nemůže být větší než 2^k. Zbývá sestrojit cyklické uspořádání délky 2^k s požadovanou vlastností.

Definujeme orientovaný graf $G = (V, E)$ následovně:

- V je množina všech posloupností 0 a 1 délky $k-1$ (tedy $|V| = 2^{k-1}$).
- Množina šipek je tvořena množinou všech dvojic tvaru

$$((a_1, \ldots, a_{k-1}), (a_2, \ldots, a_k)).$$

Šipky tedy odpovídají posloupnostem tvaru

$$(a_1, \ldots, a_k),$$

a proto $|E| = 2^k$.

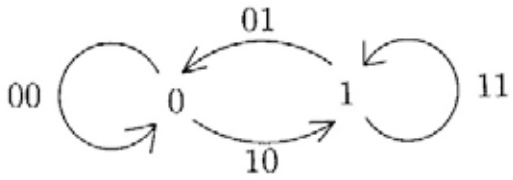
Pro zkrácení budeme rovněž šipku $((a_1, \ldots, a_{k-1}), (a_2, \ldots, a_k))$ označovat symbolem $(a_1, \ldots, a_k)$. Nemůže dojít k mýlce.

Zřejmě $\deg_G^-(v) = \deg_G^+(v) = 2$ pro každý vrchol $v \in V$. Graf $\mathrm{sym}\,(G)$ je rovněž souvislý, neb postupným vynecháváním posledních členů posloupnosti a přidáváním 0 na prvé místo lze každou posloupnost převést na posloupnost $(0, 0, \ldots, 0)$. Tedy G je eulerovský graf.

Položme $|E| = 2^k = K$, a nechť $(e^1, \ldots, e^K)$ je posloupnost hran v nějakém eulerovském tahu v G. Každá hrana e^i je tvaru $e^i = (a_1^i, \ldots, a_k^i)$. Požadované cyklické uspořádání K číslic 0 a 1 definujeme jako $(a_1^1, a_1^2, \ldots, a_1^K)$ (t.j., vzali jsme první prvek z každé

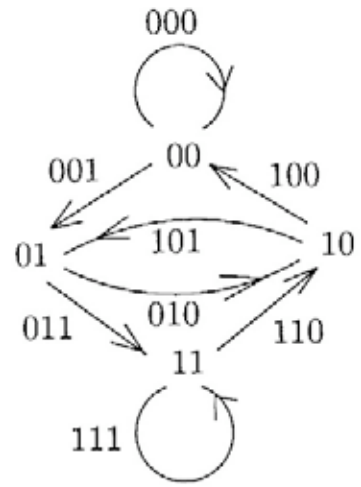
posloupnosti e^i). Vzhledem k volbě vrcholů a hran se každá posloupnost délky k vyskytuje v cyklickém uspořádání $(a_1^1, a_1^2, \ldots, a_1^K)$, a to právě jednou. To dokazuje, že $u(k) = 2^k$. □

Eulerovské orientované grafy, sestrojené v tomto důkaze, se nazývají *De Bruijnovy grafy*. Pro $k = 2$ dostaneme takovouto situaci



tah: 00,01,11,10
cyklická posloupnost: 0011

a pro $k = 3$ tuto:



tah: 000,001,011,111,110,101,010,100
cyklická posloupnost: 00011101.

Cvičení

1. Dokažte tvrzení 3.7.2.
2. Navrhněte algoritmus pro nakreslení orientovaného grafu jedním tahem.
3. Kdy lze nakreslit orientovaný graf jedním tahem, který nemusí být nutně uzavřený?

4. Je-li $G = (V, E)$ graf, *orientace* G je každý orientovaný graf $G' = (V, E')$, který vznikne nahrazením každé hrany $\{u, v\} \in E$ buď šipkou (u, v), nebo šipkou (v, u).

   (a) Dokažte, že má-li graf G všechny stupně sudé, potom existuje jeho vyvážená orientace.

   (b) Dokažte, že vyvážený orientovaný graf je slabě souvislý právě když je silně souvislý.

5.* Buď $G = (V, E)$ orientovaný graf, $w : E \to \mathbf{R}$ nějaké ohodnocení hran reálnými čísly. Funkci $p : V \to \mathbf{R}$ nazveme *potenciálem* pro w, pokud pro každou šipku $e = (u, v)$ platí $w(e) = p(v) - p(u)$. Dokažte, že potenciál pro w existuje právě když součet hodnot w přes hrany každého orientovaného cyklu v G je 0.

6.* Dokažte, že následující 2 podmínky pro silně souvislý orientovaný graf G jsou ekvivalentní:

   (i) G obsahuje orientovaný cyklus sudé délky.

   (ii) Vrcholy G lze obarvit dvěma barvami tak, že z každého vrcholu vychází šipka do vrcholu opačné barvy.

3.8 2-souvislost

Graf G nazveme *vrcholově k-souvislý*, má-li aspoň $k + 1$ vrcholů, a odebráním libovolných nejvýše $k - 1$ vrcholů vždy dostaneme souvislý graf. Graf G nazveme *hranově k-souvislý*, pokud po odebrání libovolných nejvýš $k - 1$ hran zůstane souvislý.

Je-li nějaký graf schématem např. spojů městské dopravy, železniční sítě, elektrického rozvodu a podobně, dává jeho vyšší souvislost naději na rozumné fungování příslušné sítě i za krizových podmínek, kdy jedna nebo několik křižovatek či spojnic selže. Pojem k-souvislosti je v teorii grafů teoreticky i prakticky velmi důležitý a souvisí s problematikou tzv. *toků v sítích*, jíž se v tomto textu zabývat nebudeme. Zde se omezíme na vrcholovou 2-souvislost, již budeme potřebovat v kapitole o rovinných grafech a která nám rovněž poslouží pro ilustraci některých důkazových postupů a konstrukcí.

Vrcholové 2-souvislosti budeme říkat krátce 2-souvislost. Zopakujme tedy ještě pro jistotu definici:

3.8.1 Definice (2-souvislost). *Graf G nazveme* 2-souvislým, *má-li aspoň 3 vrcholy, a vynecháním jeho libovolného vrcholu vznikne souvislý graf.*

Je snadné nahlédnout, že každý 2-souvislý graf je také souvislý (tady se ovšem potřebuje předpoklad, že 2-souvislý graf má aspoň 3 vrcholy — doporučujeme čtenáři rozvážit si to). V tomto článku uvedeme alternativní popisy 2-souvislých grafů. Než začneme, zavedeme označení pro několik grafových operací, které zjednoduší zápis a budou se hodit i v budoucnu.

3.8.2 Definice (Některé grafové operace). *Nechť $G = (V, E)$ je graf. Definujeme*

- *(odebrání hrany)*

$$G - e = (V, E \setminus \{e\}),$$

  kde $e \in E$ je hrana grafu G,

- *(přidání nové hrany)*

$$G + e' = (V, E \cup \{e'\}),$$

  kde $e' \in \binom{V}{2} \setminus E$ je dvojice vrcholů, která není hranou,

- *(odebrání vrcholu)*

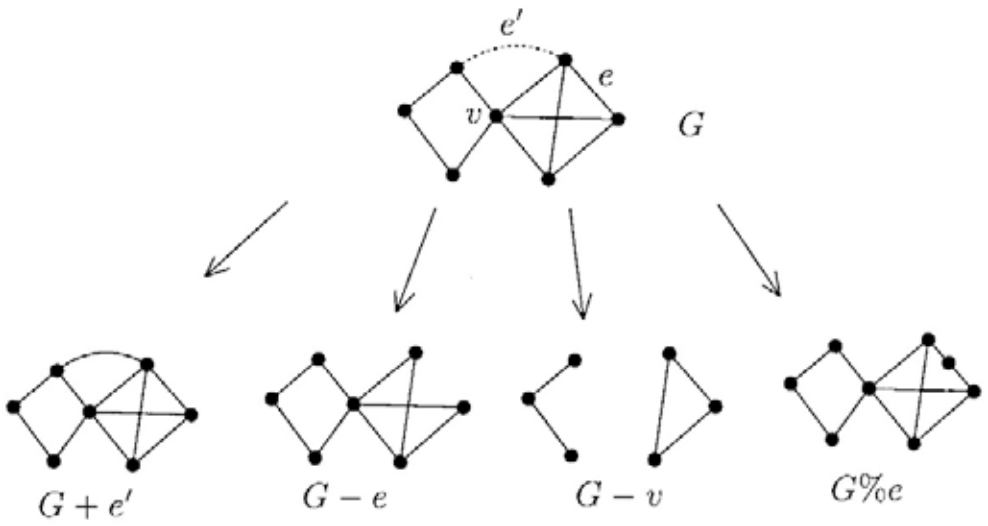
$$G - v = (V \setminus \{v\}, \{e \in E;\, v \notin e\}),$$

  kde $v \in V$ (odebereme vrchol v a všechny hrany do něj zasahující),

- *(dělení hrany)*

$$G\%e = \Big(V \cup \{z\}, (E \setminus \{\{x, y\}\}) \cup \{\{x, z\}, \{z, y\}\}\Big),$$

  kde $\{x, y\} \in E$ je hrana, a $z \notin V$ je nový vrchol (na hranu $\{x, y\}$ „přikreslíme“ nový vrchol z).



Obrázek 3.4: Příklady grafových operací.

Řekneme, že graf G' je dělení *grafu G, pokud G' je isomorfní grafu vytvořenému z grafu G postupným opakováním operace dělení hrany.*

Příklady právě zavedených operací jsou na obr. 3.4.

Vraťme se nyní ke 2-souvislosti. První význačná ekvivalentní charakterizace je následující:

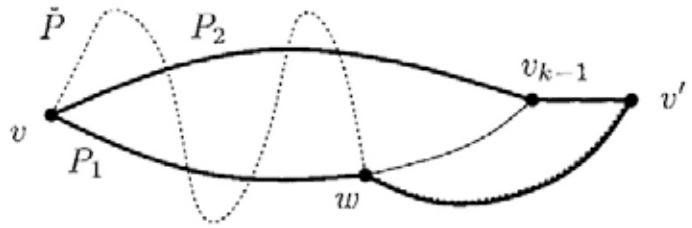
3.8.3 Věta. *Graf G je 2-souvislý, právě když pro každé dva jeho vrcholy existuje kružnice v grafu G, která je obsahuje (t.j., G je 2-souvislý, právě když každé dva vrcholy leží na společné kružnici).*

Důkaz. Uvedená podmínka je zřejmě postačující, neboť leží-li dva vrcholy v, v' na společné kružnici, potom mezi nimi existují dvě cesty, které nemají žádné společné vrcholy mimo koncové, a tedy odebráním jednoho vrcholu se v a v' nemohou nikdy octnout v různých komponentách.

Dokážeme nyní obrácenou implikaci. Existenci společné kružnice pro vrcholy v, v' ukážeme indukcí podle $d_G(v, v')$, vzdálenosti vrcholů v a v'.

Nejdříve nechť $d_G(v, v') = 1$, to znamená, že $\{v, v'\} = e \in E(G)$. Díky 2-souvislosti G je graf $G - e$ také souvislý (kdyby byl $G - e$ nesouvislý, byl by aspoň jeden z grafů $G - v$, $G - v'$ také nesouvislý). Proto existuje v grafu $G - e$ cesta z v do v', a ta spolu s hranou e tvoří kružnici obsahující v i v'.

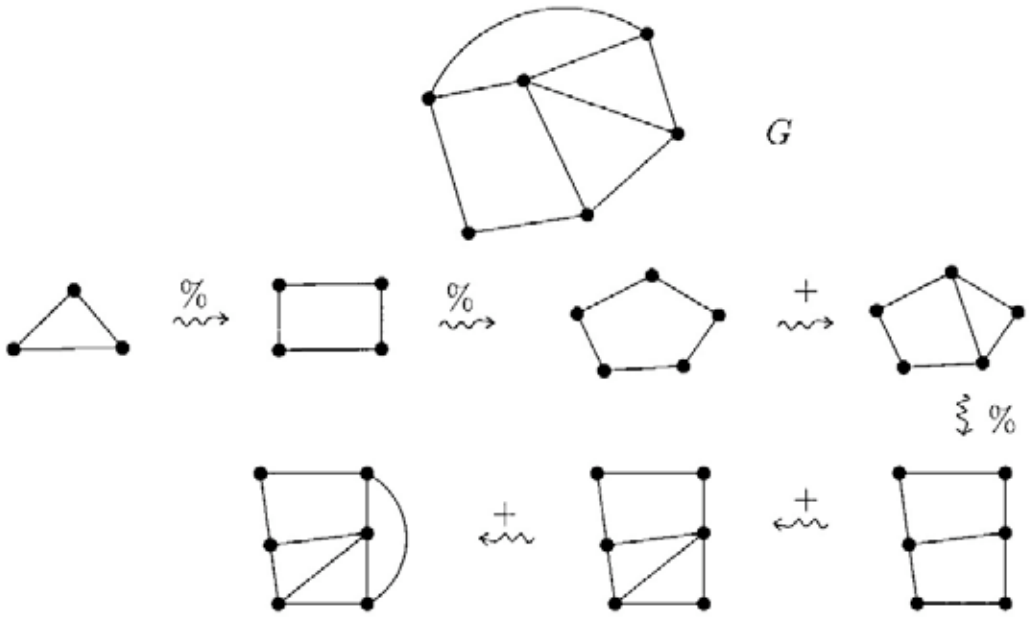
Předpokládejme nyní pro nějaké $k \geq 2$, že každá dvojice vrcholů ve vzdálenosti menší než k leží na společné kružnici, a uvažme dva vrcholy $v, v' \in V$ ve vzdálenosti k. Nechť $P = (v = v_0, e_1, v_1, \ldots, e_k, v_k = v')$ je cesta nejkratší délky z v do v'. Poněvadž $d_G(v, v_{k-1}) = k - 1$, existuje kružnice obsahující v i v_{k-1}. Tato kružnice je tvořena dvěma cestami, P_1 a P_2, z v do v_{k-1}. Uvažme nyní graf $G - v_{k-1}$. Ten je souvislý, a tedy v něm existuje cesta $\check{P}$ z vrcholu v do vrcholu v'. Tato cesta tedy neobsahuje vrchol v_{k-1}. Uvažme poslední vrchol na cestě $\check{P}$ (směrem od vrcholu v) náležející některé z cest P_1, P_2, a označme jej w, viz obrázek:



Předpokládejme (bez újmy na obecnosti), že w je vrcholem cesty P_1. Potom hledaná kružnice obsahující vrcholy v a v' bude tvořena cestou P_2, úsekem cesty P_1 mezi v a w, a úsekem cesty $\check{P}$ mezi w a v' (na obrázku vyznačena silně). □

3.8.4 Tvrzení. *Graf G je 2-souvislý, právě když libovolné jeho dělení je 2-souvislé.*

Důkaz. Stačí dokázat, že G je 2-souvislý právě když $G\%e$ je 2-souvislý (pro libovolnou hranu $e \in E(G)$). Je-li $v \in V(G)$ libovolný vrchol grafu G, je snadno vidět, že $G - v$ je souvislý právě když $(G\%e) - v$ je souvislý. Dále využijeme jednoduchého pozorování, zmíněného v předchozím důkazu: (vrcholově) 2-souvislý graf zůstane souvislý i po odebrání



Obrázek 3.5: Příklad syntézy 2-souvislého grafu.

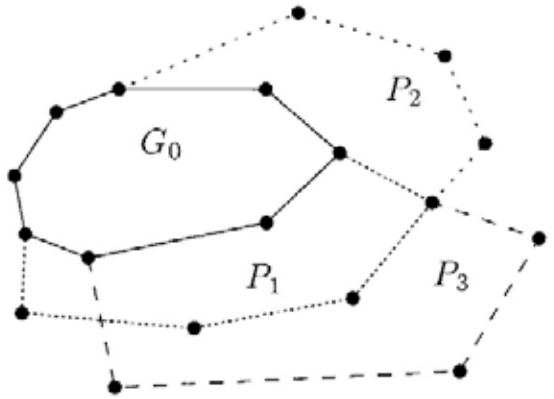
libovolné hrany. Přitom je-li z nově přidaný vrchol v grafu $G\%e$, je $(G\%e) - z$ souvislý právě když $G - e$ je souvislý. Proto je 2-souvislost G a $G\%e$ ekvivalentní. □

Následující charakterizace 2-souvislých grafů je obzvlášť výhodná pro důkazy. Ukážeme totiž, jak lze 2-souvislé grafy konstruovat z grafů jednodušších.

3.8.5 Věta (Syntéza 2-souvislých grafů). *Graf G je 2-souvislý, právě když jej lze vytvořit z trojúhelníku (t.j. z K_3) posloupností dělení hran a přidávání hran (viz obr. 3.5).*

Důkaz. Každý graf, který lze vytvořit z K_3 uvedenými operacemi, je zřejmě 2-souvislý. Chceme tedy ukázat, že můžeme vyrobit libovolný 2-souvislý graf.

Budeme ve skutečnosti dokazovat možnost trochu jiného vytvoření. Začneme s nějakou kružnicí G_0, a byl-li již vytvořen graf G_{i-1}, graf G_i vznikne přidáním nějaké cesty P_i spojující dva vrcholy grafu



Obrázek 3.6: Konstrukce 2-souvislého grafu přilepováním uší.

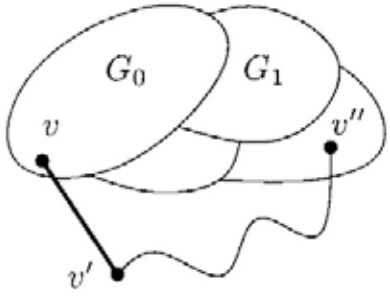
G_{i-1}; přitom cesta P_i má s G_{i-1} společné pouze své koncové vrcholy (tedy žádné hrany ani žádné vnitřní vrcholy). Ke grafu tedy postupně „přilepujeme uši", viz obr 3.6.

Protože přidávání cesty lze zaměnit přidáním hrany a jejím opakovaným dělením[4], stačí zřejmě ukázat, že každý 2-souvislý graf G můžeme dostat opakovaným přidáváním uší.

Zvolme kružnici G_0 v grafu G libovolně. Předpokládejme, že jsme již definovali grafy $G_j = (E_j, V_j)$ pro $j \leq i$ s vlastnostmi jako výše. Pokud $G_i = G$, jsme hotovi; předpokládejme tedy, že $E_i \neq E(G)$. Protože G je souvislý, existuje hrana $e \in E(G) \setminus E_i$ taková, že $e \cap V_i \neq \emptyset$. Jestliže dokonce oba vrcholy hrany e náleží V_i, položme $G_{i+1} = G_i + e$.

V opačném případě nechť $e = \{v, v'\}$, kde $v \in V_i$, $v' \notin V_i$. Uvažme nyní graf $G - v$. Ten je souvislý (neb G je 2-souvislý), takže existuje cesta P spojující vrchol v' s nějakým vrcholem $v'' \in V_i$, přičemž v'' je jediný vrchol cesty P náležející V_i (pro to stačí vzít např. nejkratší cestu mezi v' a V_i v grafu $G - v$). Pak můžeme definovat graf G_{i+1} přidáním hrany e a cesty P ke grafu G_i, t.j. $V_{i+1} = V_i \cup V(P)$, $E_{i+1} = E_i \cup \{e\} \cup E(P)$. Viz obrázek:

[4]Musí se dát malinko pozor: jsou-li $v, v' \in V(G_{i-1})$ již spojeny hranou a spojujeme-li je novou cestou, nemůžeme začít přidáním hrany $\{v, v'\}$ (aspoň nepřipouštíme-li násobné hrany). Musíme nejdříve hranu $\{v, v'\}$ podrozdělit, potom znova přidat hranu $\{v, v'\}$ a pak případně pokračovat v prodlužování cesty dělením.



□

Cvičení

1. Dokažte, že pro každé dvě hrany 2-souvislého grafu existuje kružnice, která je obsahuje.

2. Buď G *kritický 2-souvislý graf*, to znamená, že G je 2-souvislý, ale žádný z grafů tvaru $G - e$ pro $e \in E(G)$ není 2-souvislý.

   (a) Dokažte, že aspoň jeden vrchol G má stupeň 2.

   (b) Pro každé n uveďte příklad kritického 2-souvislého grafu s vrcholem stupně aspoň n.

   (c)* Pro každé n uveďte příklad kritického 2-souvislého grafu s vrcholem stupně aspoň n, jenž je od všech vrcholů stupně 2 vzdálen aspoň n.

3. (a)* Je pravda, že libovolný kritický 2-souvislý graf (viz cvičení 2) lze dostat z nějaké kružnice postupným přilepováním „uší" (cest připojených za koncové vrcholy) délky aspoň 2?

   (b)* Je pravda, že libovolný kritický 2-souvislý graf lze dostat z nějaké kružnice postupným přilepováním „uší" tak, aby všechny mezistupně (po přilepení několika prvních uší) byly kritické 2-souvislé grafy?

4.* Dokažte, že každý 2-souvislý graf má silně souvislou orientaci (pojmy viz část 3.7).

4

Stromy

4.1 Definice a charakteristika stromů

Strom je jeden z nejpřirozenějších útvarů jak v přírodě, tak v matematice. Stromy v přírodě jsou košaté, rozmanité a nesmírně složité. Stromy v teorii grafů jsou téměř nejjednodušší ze všech grafů, ale přesto jejich studium tvoří bohatou a zajímavou oblast. V teorii grafů se stromem rozumí konečný graf, který vypadá podobně jako na následujících obrázcích:

Jak tento pojem vystihnout? Pokuste se o to sami dřív, než budete pokračovat ve čtení.

Z hlediska teorie grafů lze pojem stromu definovat mnoha rozdílnými způsoby. Uvidíme to za okamžik, kdy podáme dokonce pět naprosto rozdílných charakteristik. Snad nejběžnější je však následující definice:

4.1.1 Definice. Strom *je souvislý graf neobsahující kružnici.*

Z mnoha hledisek je tato definice trochu nešikovná. Například není jasné, jak jednoduše zkontrolovat, že daný graf je strom. Souvislost lze ověřit snadno, s neexistencí kružnic je to však horší. Proto jsou důležité alternativní popisy stromů, které budou následovat. Začneme téměř zřejmým pozorováním:

4.1.2 Lemma (O koncovém vrcholu). *Každý strom s alespoň dvěma vrcholy obsahuje alespoň dva vrcholy stupně 1. Vrchol stupně 1 se nazývá* koncový vrchol *nebo* list.

Důkaz. Nechť $P = (v_0, e_1, v_1, \ldots, e_t, v_t)$ je cesta maximální možné délky ve stromu $T = (V, E)$ (strom se v teorii grafů zpravidla označuje písmenem T). Zřejmě délka cesty P je aspoň 1. Tvrdíme, že jak v_0, tak v_t jsou koncové vrcholy T. To můžeme nahlédnout sporem: Není-li např. v_0 koncový vrchol, pak existuje ještě jiná hrana $e \neq e_1$ obsahující vrchol v_0; označme $e = \{v_0, v\}$. Potom buď je v některým z vrcholů cesty P, t.j. $v = v_i$, $i \geq 2$ (v tom případě e spolu s úsekem cesty P od v_0 do v_i tvoří kružnici), anebo $v \notin \{v_0, \ldots, v_t\}$ — tehdy bychom mohli cestu P prodloužit o hranu e. V obou případech dostaneme spor. □

Poznamenejme, že lemma o koncovém vrcholu neplatí pro nekonečné stromy (právě předvedený důkaz selže pro nekonečné stromy na tom, že nejdelší cesta nemusí existovat): například jednostranně nekonečná cesta má jen jeden koncový vrchol

a oboustranně nekonečná cesta nemá dokonce žádný:

My však uvažujeme jen konečné grafy.

Výstavba stromů. Připomeňme značení ze sekce 3.8: je-li $G = (V, E)$ graf a v jeho vrchol, potom $G - v$ označuje graf, který vznikne

z G vynecháním v a všech hran, které vrchol v obsahují. V případě, že v je koncový vrchol stromu T, vznikne $T - v$ odebráním v a jediné hrany jej obsahující.

4.1.3 Tvrzení (Postupná výstavba stromů). *Pro daný graf G a jeho koncový vrchol v jsou následující dvě tvrzení ekvivalentní:*

(i) G je strom

(ii) $G - v$ je strom.

Důkaz je velmi snadný. Dokážeme nejprve implikaci $(i) \Rightarrow (ii)$. Graf G je tedy strom, a chceme dokázat, že i $G - v$ je strom. Jsou-li x, y dva vrcholy grafu G různé od v, uvažme (nějakou) cestu z x do y. Tato cesta nemůže obsahovat vrchol stupně 1 mimo x a y, a tedy neobsahuje v. Proto je celá obsažena také v $G - v$, čili $G - v$ je souvislý. Protože G neobsahuje kružnici, očividně ani $G - v$ neobsahuje kružnici, a je to tudíž strom.

Zbývá dokázat implikaci $(ii) \Rightarrow (i)$. Nechť $G - v$ je strom. Přidáním koncového vrcholu v nemůžeme zjevně vytvořit kružnici. Zbývá nahlédnout souvislost G, ale ta je též zřejmá: mezi libovolnými dvěma vrcholy různými od v vedla cesta už v grafu $G - v$, a cesta z nějakého vrcholu x do vrcholu v se dostane prodloužením cesty spojující x s v' o hranu $\{v', v\}$, kde v' je (jediný) soused vrcholu v v grafu G. □

Toto tvrzení umožňuje postupně převádět daný strom na menší a menší stromy. Ukazuje, že graf G je strom právě když ho lze převést na jeden vrchol postupným odebíráním koncových vrcholů. Přitom v každém kroku můžeme odebrat libovolný koncový vrchol.

Následující věta shrnuje základní poznatky o stromech. Větu formulujeme jako ekvivalenci 5 tvrzení. Jedno z nich např. ukazuje, že strom se mezi souvislými grafy pozná podle počtu vrcholů a hran.

4.1.4 Věta (Charakterizace stromů). *Pro graf $G = (V, E)$ jsou následující podmínky ekvivalentní:*

(i) G je strom

(ii) *(jednoznačnost cesty)*
Pro každé dva vrcholy x, $y \in V$ existuje právě jediná cesta z x do y.

(iii) *(minimální souvislost)*
Graf G je souvislý, a vynecháním libovolné hrany vznikne nesouvislý graf.

(iv) *(maximální graf bez kružnic)*
Graf G neobsahuje kružnici, a každý graf vzniklý z G přidáním hrany (t.j. graf tvaru $G+e$, kde $e \in \binom{V}{2} \setminus E$) již kružnici obsahuje.

(v) *(Eulerův vzorec)*
G je souvislý a $|V| = |E| + 1$.

Toto je pozoruhodná věta, která vlastně popisuje pojem stromu pomocí čtyř dalších způsobů, které jsme se pokusili pojmenovat v záhlaví jednotlivých bodů. Tyto popisy jsou velmi různorodé a zakládají širokou použitelnost pojmu strom.

Důkaz. Důkaz je snadný, jde jen o to jej vhodně zorganizovat. Dokážeme, že každé z tvrzení (ii)–(v) je ekvivalentní (i) (tím je ovšem dokázána i ekvivalence všech tvrzení navzájem). Důkazy povedeme většinou indukcí podle počtu vrcholů grafu G (přitom pro jediný graf s jedním vrcholem všechna tvrzení platí), a budeme využívat postupné výstavby stromu odebíráním koncového vrcholu.

Nejdříve nahlédneme, že z (i) plyne (ii)–(v). Buď tedy G strom na aspoň 2 vrcholech, v jeho koncový vrchol, v' jediný soused vrcholu v, a nechť pro graf $G - v$ už platí (ii)–(v). Platnost (ii), (iii) a (v) pro G je pak téměř zřejmá (přenecháváme detailní rozmyšlení čtenáři). Co se týče (iv), nepotřebujeme ani indukci: poněvadž G je souvislý, mezi libovolnými dvěma vrcholy $x, y \in V(G)$ vede cesta, a pokud $\{x, y\} \notin E(G)$, potom hrana $\{x, y\}$ spolu se zmíněnou cestou tvoří kružnici.

Teď budeme dokazovat, že z každé z podmínek (ii)–(v) plyne (i). U (ii), (iii) již předpokládáme souvislost, a dále graf G splňující (ii)

nebo (iii) nemůže obsahovat kružnici, protože kružnice sama již (ii) ani (iii) nesplňuje. Tím už jsme dokázali ekvivalenci (i)–(iii).

Pro platnost implikace (iv)⇒(i) stačí ověřit, že G je souvislý. Na to se použije argument, jímž jsme dokazovali (i)⇒(iv), obrácený naruby: Jsou-li $x, y \in V(G)$ dva vrcholy, pak buď jsou přímo spojeny hranou, nebo graf $G+\{x,y\}$ obsahuje kružnici, a z té po odebrání hrany $\{x,y\}$ vznikne cesta z x do y v G.

Konečně implikace (v)⇒(i) se dokáže opět indukcí podle počtu vrcholů. Mějme tedy souvislý graf G na aspoň dvou vrcholech splňující $|V| = |E| + 1$. Součet stupňů všech vrcholů je $2|V| - 2$, a protože všechny stupně jsou aspoň 1 (ze souvislosti!), musí existovat vrchol v stupně právě 1, neboli koncový vrchol grafu G. Graf $G' = G-v$ je opět souvislý a splňuje $|V(G')| = |E(G')| + 1$, je to tedy podle indukčního předpokladu strom, a tudíž i G je strom. □

Cvičení

1. Nakreslete všechny stromy na množině $\{1,2,3,4\}$, a všechny navzájem neisomorfní stromy na 6 vrcholech.
2. Dokažte, že graf $G = (V,E)$, který nemá kružnice a pro nějž $|V| = |E| + 1$, je strom.
3. Dokažte, že graf na n vrcholech s c komponentami má aspoň $n - c$ hran.
4. Nechť strom G obsahuje vrchol stupně k. Ukažte, že G obsahuje alespoň k vrcholů stupně 1.
5.* Nechť T je strom s n vrcholy, $n \geq 2$. Pro kladné celé číslo i označme p_i počet vrcholů T, které mají stupeň i. Dokažte, že

$$p_1 - p_3 - 2p_4 - \ldots - (n-3)p_{n-1} = 2.$$

   (To dává jiný důkaz lemmatu o koncovém vrcholu.)

6.* Dokažte, že následující dvě podmínky pro posloupnost $(d_1, \ldots, d_n)$ kladných přirozených čísel jsou navzájem ekvivalentní:

   (i) Existuje strom T se skórem $(d_1, \ldots, d_n)$.

   (ii) Platí $\sum_{i=1}^{n} d_i = 2n - 2$.

4.2 Isomorfismus stromů

Jak jsme se zmínili v části 3.1, není znám žádný rychlý algoritmus, který by pro dva dané grafy rozhodl, zda jsou isomorfní nebo ne. Pro některé speciální třídy grafů však rychlé algoritmy existují. Jedna z takových (jednoduchých) tříd jsou stromy. Ostatně velmi mnoho — asi dokonce většina — algoritmických úloh, které jsou pro obecné grafy obtížné, se dá pro stromy vyřešit poměrně snadno.

V tomto odstavci předvedeme rychlý a snadný postup, který pro dva stromy T a T' rozhodne, zda T a T' jsou isomorfní či nikoliv. Každému stromu T na n vrcholech přiřadíme posloupnost nul a jedniček délky $2n$, zvanou *kód* stromu T, a to tak, že isomorfním stromům se přiřadí týž kód, zatímco neisomorfní stromy budou mít různé kódy. Tím bude isomorfismus stromů převeden na prosté porovnání posloupností.

Následuje řada speciálních pojmů, každý se zvláštním názvem. To je běžné v hraničních oblastech teorie grafů a informatiky, kde mnoho pojmů vzešlo z praxe a kde je terminologie velmi různorodá.

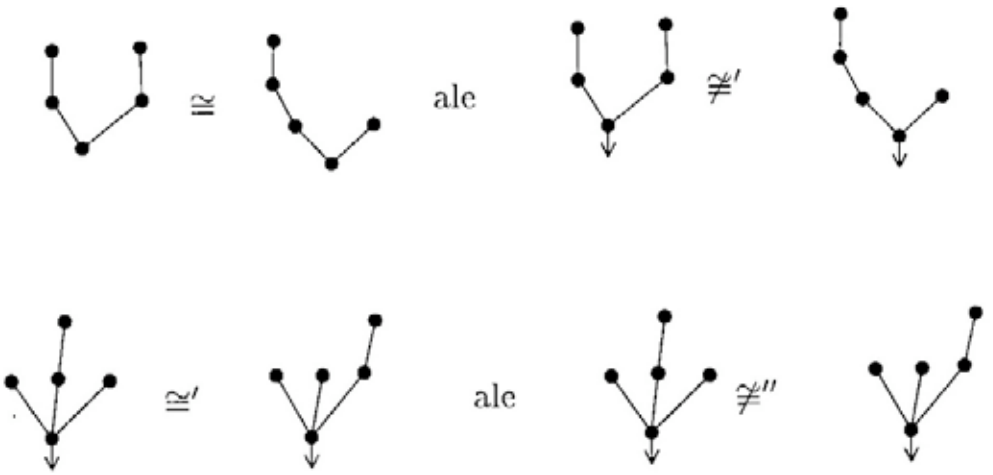
Kořenový strom je dvojice (T, r), kde $r \in V(T)$ je jeden zvolený vrchol T, zvaný *kořen*. Je-li $\{x, y\} \in E(T)$ hrana, a leží-li x na (jediné) cestě z y do kořene, říkáme, že x je *otec* y a y je *syn* x.

Pěstovaný strom je nějaký kořenový strom (T, r), plus jeho pevně zvolené rovinné nakreslení. Přitom kořen se vyznačí šipkou směřující dolů.

Komu se tato definice nelíbí, nechť si uvědomí, že rovinné nakreslení je plně popsáno[1] pořadím synů každého vrcholu. Pěstovaný strom je tedy kořenový strom, kde pro každý vrchol v je dáno pořadí jeho synů. Můžeme proto pěstovaný strom zapisovat jako trojici (T, r, ν), kde ν je soubor lineárních uspořádání, jedno lineární uspořádání pro množinu synů každého vrcholu.

Tyto definice se zavádějí proto, že pro každý pojem se definuje isomorfismus trochu jinak. Připomeňme, že zobrazení $f : V(T) \to V(T')$ je isomorfismus stromů T a T', jestliže f je vzájemně jednoznačné zobrazení (tj. prosté a na) splňující $\{x, y\} \in E(T)$ právě když $\{f(x), f(y)\} \in E(T')$. Existenci takového isomorfismu zapisujeme $T \cong T'$. *Isomor-*

[1] Až na vhodnou spojitou deformaci roviny.



Obrázek 4.1: Isomorfismy stromů.

fismus kořenových stromů (T, r) a (T', r') je takový isomorfismus f stromů T a T', pro nějž navíc $f(r) = r'$. Značíme to $(T, r) \cong' (T', r')$. *Isomorfismus pěstovaných stromů* je takový isomorfismus příslušných kořenových stromů, který zachovává uspořádání synů každého vrcholu. Budeme jej značit $(T, r, \nu) \cong'' (T', r', \nu')$.

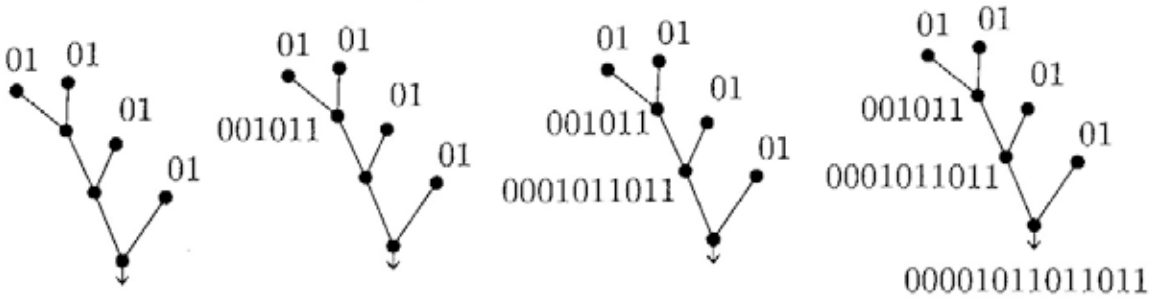
Definice $\cong$, $\cong'$ a $\cong''$ se postupně zesilují. To je nejlépe si uvědomit na malém případě na obr. 4.1.

Definice pěstovaného stromu (a jeho isomorfismus) je nejvíce omezující, a proto je kódování těchto stromů nejsnazší. Následující metoda přiřadí jistý kód každému vrcholu pěstovaného stromu; kód celého stromu bude pak totožný s kódem kořene.

K1. Koncovým vrcholům (různým od kořene) přiřadíme 01.

K2. Buď v nějaký vrchol, $v_1, \ldots, v_t$ jeho synové v pořadí zleva doprava. Má-li syn v_i kód A_i, potom vrcholu v přiřadíme kód $0A_1A_2 \ldots A_t1$.

Proces postupného vytváření kódu je znázorněn na obr. 4.2. Zřejmě jsme isomorfním pěstovaným stromům přiřadili stejný kód, neboť jsme při konstrukci kódu použili jen vlastností, které se zachovávají isomorfismem pěstovaných stromů.



Obrázek 4.2: Kódování pěstovaného stromu.

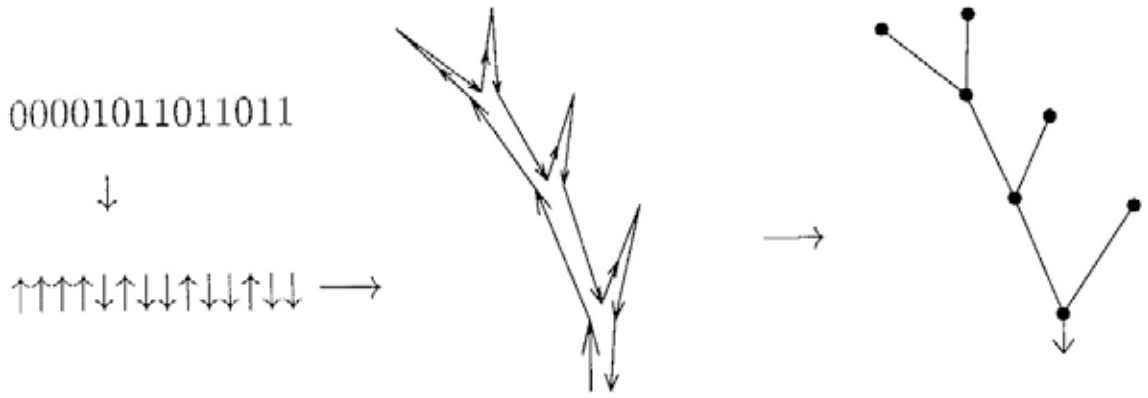
Ukážeme teď, jak ze znalosti kódu jednoznačně rekonstruovat výchozí pěstovaný strom (tím ukážeme, že neisomorfním pěstovaným stromům je přiřazen různý kód). Budeme postupovat indukcí podle délky kódové posloupnosti.

Nejkratší možný kód 01 odpovídá jedinému pěstovanému stromu s jedním vrcholem. V indukčním kroku nechť je dán kód k délky $2(n+1)$. Tento kód je tvaru $0\,A\,1$, přičemž $A = A_1 A_2 \ldots A_t$ je zřetězení kódů několika pěstovaných stromů. Část A_1 identifikujeme jako nejkratší počáteční úsek posloupnosti A, který obsahuje stejný počet nul a jedniček. Podobně A_2 je nejkratší následující úsek posloupnosti obsahující stejně nul a jedniček, atd. Podle indukčního předpokladu každému A_i odpovídá právě jediný pěstovaný strom. Pěstovaný strom kódovaný kódem k bude mít jeden kořen r, a k němu budou v pořadí $r_1, \ldots, r_t$ připojeny hranou kořeny stromů kódovaných A_1, A_2, ... Tedy kód určuje jednoznačně pěstovaný strom.

Dekódování metodou šipek. Ukážeme názorný — obrázkový — postup, jak pěstovaný strom z daného kódu zrekonstruovat.

V daném kódu nahradíme 0 šipkou "↑" a 1 šipkou "↓" a kreslíme graf podle pravidla, že šipka "↑" nikdy nevede po jiné šipce, zatímco šipka "↓" vždy sleduje šipku v protisměru. Celý postup je patrný z obrázku 4.3. (Přitom se nakreslí i kořenová šipka; jednobodový strom má kód 01.)

Věnovali jsme isomorfismu pěstovaných stromů pozornost proto, že isomorfismus jak kořenových tak obecných stromů se již snadno převede na tento případ.



Obrázek 4.3: Dekódování metodou šipek.

Vyšetřeme nejprve kořenové stromy. Je-li (T, r) kořenový strom, budujeme jeho kód podobně jako pro pěstovaný strom, až na to, že pravidlo K2 nahradíme jeho následující modifikací:

K2′ Předpokládejme, že jsme již přiřadili kód $A(w)$ každému synu w vrcholu v. Označme syny $w_1, \ldots, w_t$ tak, že $A(w_1) \leq A(w_2) \leq \ldots \leq A(w_t)$. Vrchol v pak dostane kód $0A_1A_2 \ldots A_t1$, kde $A_i = A(w_i)$.

Zde $A \leq B$ značí, že posloupnost A je menší nebo rovna posloupnosti B v nějakém pevně zvoleném lineárním uspořádání všech konečných posloupností nul a jedniček. Pro určitost můžeme např. použít tzv. *lexikografického uspořádání* (česky „slovníkového"). Dvě (různé) posloupnosti $A = (a_1, a_2, \ldots, a_n)$ a $B = (b_1, \ldots, b_m)$ přitom porovnáváme takto:

- Je-li A počátečním úsekem B, potom $A < B$. Je-li B počátečním úsekem A, potom $B < A$.
- Jinak, buď j nejmenší index takový, že $a_j \neq b_j$. Potom pokud $a_j < b_j$, klademe $A < B$, a pokud $a_j > b_j$, klademe $A > B$.

Podobně, jako jsme se o tom přesvědčili výše pro pěstované stromy, nahlédneme, že dva kořenové stromy jsou isomorfní právě když mají stejné kódy.

Obraťme pozornost ke kódování obecného stromu — stromu bez kořene. Úlohu bychom si zjednodušili, kdybychom nalezli vrchol, který by měl úlohu kořene. Přitom takto nalezený vrchol by se měl zachovávat isomorfismem. Je důležitou skutečností, že v případě stromů lze takový význačný vrchol vždy najít. Příslušné definice mohou být užitečné i jinde, a proto je formulujme poněkud obecněji pro grafy.

Pro vrchol v grafu G označme symbolem $\mathrm{ex}_G(v)$ maximální vzdálenost vrcholu v od jiného vrcholu grafu G. Číslo $\mathrm{ex}_G(v)$ se nazývá *výstřednost* (cizím slovem *excentricita*) vrcholu v grafu G. Vrcholy s velkou výstředností si můžeme představovat "na okraji" grafu G.

Označme nyní $C(G)$ množinu všech vrcholů grafu G, jejichž výstřednost nabývá minimální hodnoty. Množina $C(G)$ se nazývá *střed* [2] (*centrum*) grafu G. Příklad kružnic (a dalších grafů) ukazuje, že střed grafu může splývat s množinou všech vrcholů. Pro stromy však platí:

4.2.1 Tvrzení. *Pro každý strom T má $C(T)$ nejvýše dva vrcholy. Je-li $C(T)$ tvořeno dvěma vrcholy x a y, potom $\{x, y\}$ tvoří hranu.*

Důkaz. Popíšeme postup, jak střed stromu najít. Nechť $T = (V, E)$ je daný strom. Jestliže T má nejvýše dva vrcholy, potom střed T splývá s množinou jeho vrcholů a tvrzení platí. V opačném případě označme $T' = (V', E')$ strom, který vznikne odstraněním všech koncových vrcholů stromu T. Explicitně

$$V' = V \setminus \{x;\ \deg_T(x) = 1\},$$
$$E' = E \setminus \{\{x, y\} \in E;\ \deg_T(x) = 1 \text{ nebo } \deg_T(y) = 1\}.$$

Máme $V(T') \neq \emptyset$. Dále, pro každý vrchol v jsou všechny vrcholy od něj nejvzdálenější nutně koncové, a tím pádem platí pro každý $v \in V'$ vztah

$$\mathrm{ex}_T(v) = \mathrm{ex}_{T'}(v) + 1.$$

Speciálně z toho dostaneme $C(T') = C(T)$. V případě, že T' má alespoň 3 vrcholy, opakujeme uvedenou konstrukci, v opačném případě jsme našli střed stromu T. □

[2] Výstřednost vrcholů středu se jmenuje *poloměr* grafu G.

Popišme nyní vytváření kódu stromu T.

- Jestliže střed stromu T tvoří jediný vrchol, v, potom mu přiřadíme kód jako kořenovému stromu (T, v).

- Jestliže střed stromu T je tvořen hranou $e = \{x_1, x_2\}$, potom uvažme graf $T - e$. Tento graf má právě dvě komponenty T_1 a T_2 (kde $x_i \in V(T_i)$). Označme kód kořenového stromu (T_1, x_1) písmenem A, a kód kořenového stromu (T_2, x_2) písmenem B. Jestliže v lexikografickém uspořádání platí $A \leq B$, kódujeme strom T kódem kořenového stromu (T, x_1), a pro $A \geq B$ kódem kořenového stromu (T, x_2).

Tím je procedura kódování ukončena.

Dekódování se provádí ve všech případech stejně jako pro pěstované stromy. Poněvadž isomorfismus zřejmě převádí střed na střed, a protože jsme již nahlédli, že kódování funguje pro zakořeněné stromy, je už snadno patrné, že dva stromy mají stejný kód právě když jsou isomorfní.

Algoritmy pro isomorfismus stromů uvedené v této části lze implementovat tak, že počet elementárních kroků je omezen lineární funkcí počtu vrcholů vstupních stromů.

Jsou známy i další třídy grafů, pro něž lze problém isomorfismu řešit. Snad nejvýznamnějším takovým příkladem je třída rovinných grafů; zde jsou ale algoritmy na isomorfismus již značně složité.

Cvičení

1. (a) Najděte nějaký *asymetrický* strom s aspoň dvěma vrcholy (t.j. strom jen s jediným automorfismem, viz cvičení 3.1.3).

   (b) Jaký je nejmenší možný počet vrcholů asymetrického stromu (s nejméně 2 vrcholy)?

2. Zakořeněný strom se nazývá *binární*, jestliže každý vrchol kromě koncových má právě dva syny.

   (a) Nakreslete všechny neisomorfní binární stromy s ≤ 9 vrcholy.

   (b) Popište, jak mohou vypadat kódy binárních stromů.

3. Dokažte podrobně, že isomorfní stromy (nezakořeněné) dostanou uvedenou metodou stejný kód, a neisomorfní různé kódy.

4.* Buďte $A_1, \ldots, A_t$ posloupnosti nul a jedniček (mohou být různě dlouhé). Označme součet jejich délek n. Navrhněte algoritmus, který tyto posloupnosti lexikograficky setřídí v $O(n)$ krocích (přičemž jeden krok smí manipulovat jen s jediným členem některého A_i, nikoliv s celou posloupností 0 a 1 najednou).

5. Dokažte, že existuje nejvýš 4^n navzájem neisomorfních stromů na n vrcholech.

6. Buď $T = (V, E)$ strom, v jeho vrchol. Označme $\tau(v)$ číslo $\max(|V(T_1)|, |V(T_2)|, \ldots, |V(T_k)|)$, kde $T_1, \ldots, T_k$ jsou všechny komponenty grafu $T - v$. *Centroid* stromu T je množina všech vrcholů $v \in V$ s minimální hodnotou $\tau(v)$.

   (a)* Dokažte, že centroid každého stromu je buď jeden vrchol, nebo dva vrcholy spojené hranou.

   (b) Musí centroid vždy splývat se středem stromu?

   (c) Dokažte, že je-li v vrchol centroidu, potom $\tau(v) \leq \frac{2}{3}|V(T)|$.

4.3 Kostra grafu

Jednou ze základních grafových konstrukcí je pojem kostry grafu[3]:

4.3.1 Definice. *Nechť $G = (V, E)$ je graf. Libovolný strom tvaru (V, E'), kde $E' \subseteq E$, nazveme* kostra grafu *G. Tedy kostra grafu G je strom, který je podgrafem a obsahuje všechny vrcholy grafu G.*

Je zřejmé, že kostra může existovat pouze tehdy, je-li graf G souvislý. Je snadné ukázat, že každý souvislý graf má kostru. Ukážeme to tak, že popíšeme dva (rychlé) algoritmy, které naleznou kostru pro daný souvislý graf. V dalších článcích uvedeme jejich varianty, a proto jim věnujme pozornost.

[3] Tento morbidní název je zaveden v češtině nebo v němčině — anglicky se kostře grafu říká optimističtěji *spanning tree*.

4.3.2 Algoritmus (Kostra grafu). Buď $G = (V, E)$ graf s n vrcholy a m hranami. Seřaďme hrany grafu G libovolně do posloupnosti $(e_1, e_2, \ldots, e_m)$. V algoritmu budeme postupně konstruovat množiny hran $E_0, E_1, \ldots \subseteq E$.

Položme $E_0 = \emptyset$. Byla-li již nalezena množina E_{i-1}, spočítáme množinu E_i následovně:

$$E_i = \begin{cases} E_{i-1} \cup \{e_i\} & \text{neobsahuje-li graf } (V, E_{i-1} \cup \{e_i\}) \text{ kružnici} \\ E_{i-1} & \text{jinak.} \end{cases}$$

Algoritmus se zastaví, jestliže buď E_i již má $n-1$ hran, nebo $i = m$, t.j. probraly se všechny hrany grafu G. Nechť E_t značí množinu, pro niž se algoritmus zastavil, a nechť T značí graf (V, E_t).

4.3.3 Tvrzení (Správnost algoritmu 4.3.2). *Jestliže algoritmus končí grafem T s $n-1$ hranami, potom T je kostra grafu G. Jestliže T má $k < n-1$ hran, potom G je nesouvislý graf s $n-k$ komponentami.*

Důkaz. Podle pravidla vytváření množin E_i neobsahuje graf T kružnici. Je-li $k = |E(T)| = n-1$, potom T je strom podle věty 4.1.4(v), a tedy je to kostra grafu G. Jestliže $k < n-1$, potom T je nesouvislý graf, jehož každá komponenta je strom. Takový graf se nazývá *les* a snadno nahlédneme, že má $n-k$ komponent.

Dokážeme, že komponenty grafu T splývají s komponentami grafu G. Předpokládejme opak: nechť existují vrcholy x a y ležící v téže komponentě G a v různých komponentách grafu T. Označme C komponentu grafu T obsahující vrchol x, a uvažme nějakou cestu $(x = x_0, x_1, \ldots, x_\ell = y)$ z x do y v grafu G. Nechť i je poslední index, pro nějž je vrchol x_i obsažen v komponentě C. Zřejmě $i < \ell$, a tedy $x_{i+1} \notin C$. Hrana $e = \{x_i, x_{i+1}\}$ tudíž nepatří do grafu T, a musela proto někdy v průběhu algoritmu tvořit spolu s již vybranými hranami kružnici. Proto i graf $T + e$ obsahuje kružnici, to ale není možné, protože e spojuje různé komponenty grafu T. Z toho dostáváme spor. □

Složitost algoritmu. Tím jsme ukázali, že algoritmus 4.3.2 skutečně vždycky spočítá to, co má, t.j. kostru grafu G. Kdybychom ale doopravdy potřebovali nacházet kostry nějakých (velkých) grafů, máme zvolit zrovna tento algoritmus a trávit čas tím, že ho budeme programovat, případně utratit své peníze za program již hotový?

Odpověď není jednoduchá a algoritmy se porovnávají na základě různých (a mnohdy navzájem protichůdných) kritérií. Je např. vhodné si všímat přehlednosti algoritmu (přehlednost vede k lepšímu pochopení a méně chybám), jeho robustnosti (jak se průběh řešení změní při malé změně dat), jeho paměťové náročnosti. Snad nejrozpracovanější mírou je však *časová složitost* algoritmu, to znamená počet operací (jako například sčítání, násobení, porovnání dvou čísel, atd.), které algoritmus potřebuje na vyřešení dané úlohy. Zpravidla se uvažuje časová složitost *v nejhorším případě*, t.j. počet operací potřebných k vyřešení nejhorší možné (nejnaschválnější) úlohy při dané velikosti vstupu. Velikost vstupu by se v našem případě — počítání kostry — mohla měřit jako počet vrcholů plus počet hran grafu G. Místo „časová složitost v nejhorším případě" budeme v dalším říkat krátce „složitost" (poněvadž o jiných typech složitosti hovořit nebudeme).

Složitost algoritmu lze jen velmi zřídka určit přesně. Aby byla vůbec naděje to udělat, museli bychom v první řadě přesně určit, co jsou povolené elementární operace, t.j. vpodstatě se vázat jeden konkrétní počítač, a potom také algoritmus popsat do nejmenších detailů, včetně různých rutinních operací, t.j. vycházet z konkrétního naprogramování. I kdybychom obě tyto věci udělali, určení přesné složitosti je velmi pracné i pro jednoduché algoritmy. Z těchto důvodů se v teoretické analýze algoritmů složitost odhaduje pouze asymptoticky, třeba že nějaký algoritmus má složitost $O(n^{3/2})$, jiný $O(n \log n)$, a podobně (n je přitom míra velikosti vstupu).

Při skutečném posuzování algoritmů je vhodné (a někdy nutné) takovou asymptotickou analýzu doplnit testováním algoritmu pro konkrétní data na konkrétním počítači. Dá-li totiž např. asymptotická analýza pro jeden algoritmus složitost $O(n^2)$ a pro druhý $O(n \log^4 n)$, vypadá druhý podle toho jasně lepší (funkce $n \log^4 n$ roste mnohem pomaleji než n^2). Kdyby však přesná složitost prvního algoritmu byla třeba $n^2 - 5n$ a druhého $20n(\log_2 n)^4$, projeví se převaha druhého algoritmu až od zhruba $n = 5 \times 10^6$, a taková převaha je z praktického hlediska dosti iluzorní.

Pokusme se nějak odhadnout asymptotickou složitost algoritmu 4.3.2. Algoritmus jsme ovšem popsali na „vysoké úrovni", čímž se nemíní spo-

lečenská prestiž, ale to, že jsme při popisu užívali např. test, zda daná množina hran obsahuje kružnici, což ani při liberálním pojetí nelze považovat za elementární operaci. Složitost algoritmu tedy bude záviset na tom, jak efektivně umíme takovou komplikovanou operaci realizovat operacemi elementárními.

U našeho algoritmu 4.3.2 je vidět, že nemusíme uchovávat všechny množiny E_i, a všechny tedy mohou být reprezentovány jednou proměnnou (např. seznamem hran), která postupně nabývá hodnot $E_0, E_1, \ldots$. Jediná složitější otázka je, jak efektivně testovat, jestli přidání nové hrany e_i k již vybraným hranám vytvoří kružnici. Kružnice zřejmě vznikne, právě když koncové vrcholy hrany e_i náleží téže komponentě grafu (V, E_{i-1}). Takže potřebujeme řešit následující úlohu:

4.3.4 Úloha (Udržování ekvivalence). [4] *Je dána množina vrcholů $V = \{1, 2, \ldots, n\}$. Na počátku je rozdělena do jednoprvkových tříd ekvivalence, t.j. žádné dva vrcholy nejsou ekvivalentní. Navrhněte algoritmus, který uchovává ve vhodné datové struktuře ekvivalenci na V (neboli rozdělení V do tříd) tak, aby mohl efektivně vykonávat operace následujících dvou typů:*

(i) (Sjednocení tříd — UNION) Učinit dané dva neekvivalentní vrcholy $i, j \in V$ ekvivalentními, t.j. nahradit třídy obsahující i a j jejich sjednocením.

(ii) (Testování ekvivalence — FIND) Pro dané dva vrcholy $i, j \in V$ rozhodnout, zda jsou momentálně ekvivalentní.

Přitom každá další operace je algoritmu zadána až poté, co vykonal operaci předchozí.

Náš algoritmus 4.3.2 na hledání kostry potřebuje nejvýš $n-1$ operací sjednocení tříd, a nejvýš m operací testování ekvivalence.

Jedno jednoduché řešení úlohy 4.3.4 je následující: Vrcholům z množiny V přiřadíme na počátku různé značky, třeba $1, 2, \ldots, n$. Značky nyní i v budoucnosti budou splňovat podmínku, že dva vrcholy budou mít tutéž značku právě když jsou ekvivalentní. Testování ekvivalence bude pak triviální porovnání značek. Při sjednocení dvou tříd je třeba přeznačit vrcholy jedné ze tříd. Pokud prvky každé třídy zároveň uchováváme např. v seznamu, je čas potřebný na takovou operaci úměrný velikosti přeznačované třídy.

[4] V literatuře čtenář tuto úlohu najde nejspíš pod jménem *UNION-FIND problem.*

Při hrubém odhadu můžeme říci, že každá třída má vždy nejvýš n prvků, tedy jedna operace sjednocení tříd nezabere nikdy více než $O(n)$. Pro $n-1$ operací sjednocení a m operací testování ekvivalence potom vychází odhad $O(n^2+m)$. Jedno nenápadné vylepšení je, že uchováváme také počty prvků tříd a přeznačujeme vždycky menší třídu. Pro takový algoritmus se dá ukázat celkový odhad $O(n \log n + m)$.

Nejlepší známé řešení úlohy 4.3.4 potřebuje na m testů a $n-1$ sjednocení čas nejvýš $O(n\alpha(n)+m)$ (viz např. [1]), kde $\alpha(n)$ je jistá funkce. Definici této funkce zde neuvedeme; poznamenejme jen, že $\alpha(n)$ roste sice do nekonečna pro $n \to \infty$, ale nepředstavitelně pomalu, mnohem pomaleji než např. funkce jako $\log\log n$, $\log\log\log n$, atd. Pro praktické použití je však výše naznačené řešení (s přeznačováním menší třídy) zcela dostačující.

Uveďme ještě jeden (a snad ještě jednodušší) algoritmus pro nalezení kostry.

4.3.5 Algoritmus (Kostra grafu jinak). Je dán graf $G = (V, E)$ s n vrcholy a m hranami. Budeme postupně vytvářet množiny V_0, $V_1, \ldots \subseteq V$ vrcholů a $E_0, E_1, \ldots \subseteq E$ hran, přičemž $E_0 = \emptyset$ a $V_0 = \{v\}$, kde v je libovolně zvolený vrchol.

Jsou-li již V_{i-1} a E_{i-1} vytvořeny, nalezneme nějakou hranu $e_i = \{x_i, y_i\} \in E(G)$ takovou, že $x_i \in V_{i-1}$, $y_i \in V \setminus V_{i-1}$, a položíme $V_i = V_{i-1} \cup \{y_i\}$, $E_i = E_{i-1} \cup \{e_i\}$. Pokud žádná taková hrana neexistuje, algoritmus končí (grafem $(V_t, E_t) = T$).

4.3.6 Tvrzení (Správnost algoritmu 4.3.5). *Jestliže algoritmus končí grafem T s n vrcholy, potom T je kostra. V opačném případě je G nesouvislý graf a vrcholy T tvoří komponentu G obsahující vrchol v.*

Důkaz. Graf T je strom (protože je souvislý a má správný počet vrcholů a hran). Má-li T n vrcholů, potom je to kostra. Předpokládejme tedy, že T má $\bar{n} < n$ vrcholů. Zbývá dokázat, že $V(T)$ tvoří komponentu grafu G.

Předpokládejme opak: nechť existuje $x \in V(T)$ a $y \notin V(T)$, pro něž je v grafu G nějaká cesta z x do y. Podobně jako v důkazu tvrzení 4.3.3 na této cestě najdeme hranu $e = \{x_j, y_j\} \in E(G)$, pro niž $x_j \in V(T)$,

$y_j \in V \setminus V(T)$. Algoritmus tedy mohl ještě přidat hranu e a vrchol y_j a neměl skončit grafem T. To je hledaný spor. □

Poznámka. Detaily právě probraného algoritmu se dají navrhnout tak, že algoritmus pracuje v čase $O(n+m)$.

Cvičení

1. Dokažte, že řešíme-li úlohu 4.3.4 popsaným algoritmem (přeznačujícím vždy menší ze sjednocovaných tříd), je celková složitost $n-1$ operací sjednocení nejvýš $O(n \log n)$.

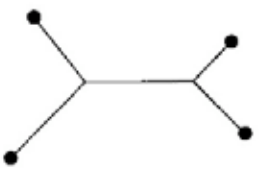
2.* Navrhněte detaily algoritmu 4.3.5 tak, aby měl složitost $O(n+m)$.

4.4 Problém minimální kostry

Představme si mapu jižní Moravy. Máme na ní vyznačeno 30–40 měst a vesniček. Naším úkolem bude tato města navzájem propojit (třeba elektrickým vedením) tak, aby délka spojení nebyla příliš velká. Řekněme dokonce, že bychom chtěli, aby celková délka propojení byla co nejkratší.

Komu tento příklad připadá příliš umělý a dnes už neaktuální (což je pravda), ať si představí návrh letecké sítě nějaké společnosti. Takové úlohy se řeší dosud.

Navíc se rozhodneme, že naše síť se nebude větvit nikde mimo spojované obce, t.j. nebudou v ní situace typu



takže tato 4 místa by se musela propojit takto[5]:

[5]Vynecháme-li právě zavedené omezení, dostaneme problém *minimálního Steinerova stromu*. To je zcela jiná úloha, pro niž nejspíš neexistuje efektivní algoritmus, a která se v praxi zpravidla řeší pouze přibližně.

Tím dostáváme zadání důležité úlohy, známé pod názvem *problém minimální kostry*. Tento oddíl je věnován jejímu řešení.

Úloha vyžaduje malého obohacení pojmu graf: Budeme uvažovat grafy $G = (V, E)$ spolu s *ohodnocenými hranami*. Tím míníme, že pro každou hranu $e \in E$ je dáno číslo $w(e)$, které nazýváme *váha* hrany e — takovou situaci jsme již uvažovali v části 3.3. (Váha je zpravidla kladné číslo.) Graf spolu s ohodnocením w, kde $w : E \to \mathbf{R}$, se nazývá *síť*.

Formulujme tedy problém propojení v grafové formě:

> *Pro souvislý graf $G = (V, E)$ s nezáporným ohodnocením hran w nalezněte souvislý podgraf (V, E') takový, že výraz*
>
> $$w(E') = \sum_{e \in E'} w(e) \tag{4.1}$$
>
> *nabývá minimální hodnoty.*

Je snadno vidět, že mezi řešeními této úlohy je vždy nějaká kostra grafu G (je-li ohodnocení všech hran kladné, může být dokonce řešením *jenom* kostra). Například, jestliže ohodnocení w splňuje $w(e) = 1$ pro každou hranu e, úlohu řeší libovolná kostra a minimální hodnota výrazu (4.1) je $|V| - 1$.

Úlohu můžeme tedy určitěji formulovat následovně:

4.4.1 Úloha (Problém minimální kostry). *Pro souvislý graf $G = (V, E)$ s nezáporným ohodnocením hran w nalezněte kostru $T = (V, E')$ grafu G s nejmenší možnou hodnotou $w(E')$.*

Daný graf může mít velmi mnoho koster (viz kapitolu 7) a nalézt tu nejlepší z nich se může zdát obtížné. Není tomu tak, a řešení je (z dnešního hlediska) snadnou variantou algoritmů z předchozí části. Uvedeme několik postupů. Jeden jednoduchý a oblíbený je následující:

4.4.2 Algoritmus (Kruskalův čili „hladový" algoritmus). Je dán souvislý graf $G = (V, E)$ s ohodnocením w. Předpokládejme, že hrany jsou uspořádány tak, že platí

$$w(e_1) \leq w(e_2) \leq \ldots \leq w(e_m).$$

Pro toto uspořádání proveďme algoritmus 4.3.2.

4.4.3 Tvrzení (Správnost Kruskalova algoritmu). *Kruskalův algoritmus řeší problém minimální kostry.*

Důkaz. Připomeňme si algoritmus 4.3.2 a zachovejme značení tam zavedené. Speciálně, T bude výsledná kostra. Uvažme libovolnou jinou kostru $\check{T}$; potřebujeme dokázat, že $w(E(T)) \leq w(E(\check{T}))$. Přeznačme hrany kostry T jako $e'_1, e'_2, \ldots, e'_{n-1}$ tak, že $w(e'_1) \leq w(e'_2) \leq \ldots \leq w(e'_{n-1})$ (každá hrana kostry T má teď dvě označení, čárkované a nečárkované). Podobně nechť $\check{e}_1, \ldots, \check{e}_{n-1}$ jsou hrany kostry $\check{T}$, uspořádané taky vzestupně podle vah.

Dokážeme, že pro $i = 1, \ldots, n-1$ platí dokonce

$$w(e'_i) \leq w(\check{e}_i). \tag{4.2}$$

Odtud samozřejmě plyne, že T je minimální kostra. Předpokládejme tedy pro spor, že (4.2) neplatí a zvolme nejmenší i takové, že $w(e'_i) > w(\check{e}_i)$. Zřejmě $i > 1$. Uvažme množiny

$$E' = \{e'_1, \ldots, e'_{i-1}\},$$
$$\check{E} = \{\check{e}_1, \ldots, \check{e}_i\}.$$

Grafy (V, E') a $(V, \check{E})$ neobsahují kružnice a navíc $|E'| = i-1$, $|\check{E}| = i$.

K hledanému sporu nám stačí ukázat, že existuje hrana $e \in \check{E}$, pro niž graf $(V, E' \cup \{e\})$ neobsahuje kružnici. Potom totiž $w(e) \leq w(\check{e}_i) < w(e'_i)$ a v tom okamžiku, kdy se v algoritmu rozhodovalo o hraně e, jsme učinili chybu, protože nebylo důvodu ji zamítnout; např. jsme ji měli vybrat místo hrany e'_i.

Stačí tedy ukázat toto: *Jsou-li* $E', \check{E} \subseteq \binom{V}{2}$ *dvě množiny hran, přičemž* $(V, \check{E})$ *neobsahuje kružnici a* $|E'| < |\check{E}|$, *potom nějaká hrana*

$e \in \check{E}$ spojuje vrcholy dvou různých komponent grafu (V, E'). Nechť $V_1, \ldots, V_s$ je rozklad množiny V na komponenty grafu (V, E'). Platí $\left|E' \cap \binom{V_j}{2}\right| \geq |V_j| - 1$, a proto $|E'| \geq n - s$. Na druhé straně, ježto $\check{E}$ neobsahuje kružnice, máme $\left|\check{E} \cap \binom{V_j}{2}\right| \leq |V_j| - 1$, tudíž nanejvýš $n - s$ hran z $\check{E}$ je obsaženo v nějaké z komponent V_j. Protože ale $|\check{E}| > |E'|$, některá hrana $e \in \check{E}$ jde mezi dvěma různými komponentami. □

Pozor, právě dokončený důkaz je velmi snadné poplést (jak vědí oba autoři z vlastní zkušenosti)!

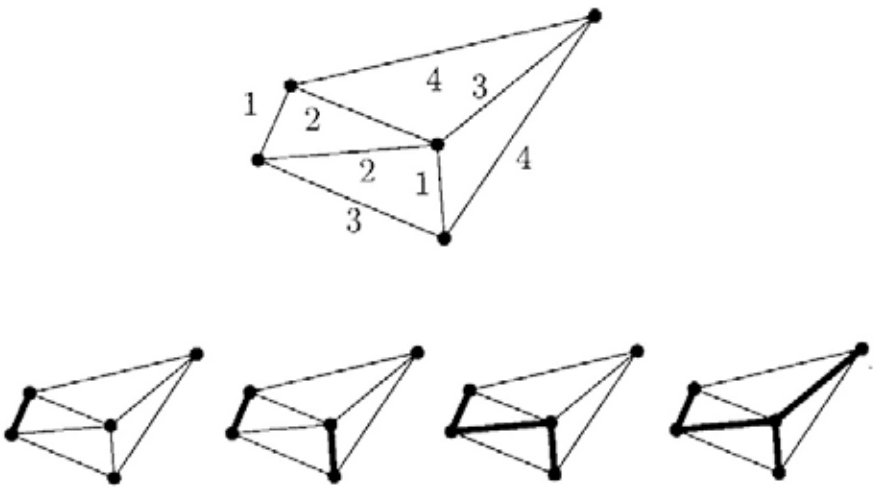
Kruskalův algoritmus je prototypem tzv. *hladového algoritmu*: vzhledem k platným omezením (zde „neobsahovat kružnici") vybereme v každém okamžiku tu nejlacinější hranu. Hladový algoritmus se tedy snaží vždycky „urvat co se dá", a přitom nehledí do budoucnosti.

Pro četné problémy může taková krátkozraká strategie úplně selhat. To není příliš překvapivé: Např. hladový algoritmus aplikován na šachovou hru by odpovídal strategii, kdy by hráč pokud možno bral v každém okamžiku, a to tu nejcennější figuru. A také by snadno při dodržování tak naivního postupu prohrál.

V této souvislosti je spíš překvapivé, že pro problém minimální kostry najde hladový algoritmus optimální řešení. I pro mnoho jiných úloh je hladová strategie užitečná (zejména nevíme-li nic lepšího); mnohdy dává aspoň dobré přibližné řešení. Úlohy, pro něž hladový algoritmus vždy najde optimální řešení, se studují v tzv. *teorii matroidů*.

4.4.4 Příklad. *Aplikujme hladový algoritmus pro problém minimální kostry pro graf na obr. 4.4 s naznačeným ohodnocením hran. Ohodnocení tvoří posloupnost* $1, 1, 2, 2, 3, 3, 4, 4$. *Jeden možný průběh Kruskalova algoritmu je vyznačen na obrázku 4.4.*

Poznámka. Příklad z jižní Moravy (kterým jsme uvedli tento oddíl) si autoři nevymysleli. Ve skutečnosti to je první případ úspěšného řešení problém minimální kostry, které našel v roce 1928 Otakar Borůvka. Značně tak předběhl dobu; mimo Československo na jeho výzkumy navázal až v roce 1956 M. Kruskal. Téma se v té době stalo velmi aktuální v rámci celkového zvýšeného zájmu o algoritmické a výpočetní metody. Od té doby jsou problému minimální kostry věnovány stovky prací. Bo-



Obrázek 4.4: Hledání minimální kostry hladovým algoritmem.

růvkův postup byl složitě napsán (v duchu tehdejšího stylu psaní matematických článků), jeho algoritmus není však složitý a je odlišný od Kruskalova hladového algoritmu. Výstižný popis událostí provázejících Borůvkův objev i celkové ovzduší předválečného brněnského akademického života čtenář najde v práci [4].

Cvičení

1. Podobně jako jsme definovali problém minimální kostry, definujte *problém maximální kostry*. Formulujte hladový algoritmus pro tento problém a ukažte, že najde optimální řešení.

2. Dokažte, že je-li w prosté zobrazení, je minimální kostra souvislého grafu G s ohodnocením w určena jednoznačně.

3. Dokažte, že je-li (V, E') kostra grafu $G = (V, E)$, potom graf $(V, E' \cup \{e\})$, kde e je libovolná hrana z $E \setminus E'$, obsahuje právě jedinou kružnici.

4. Dokažte, že je-li (V, E') kostra grafu $G = (V, E)$, potom pro každé $e \in E \setminus E'$ existuje $e' \in E'$ tak, že $\big(V, (E' \setminus \{e'\}) \cup \{e\}\big)$ je opět kostra grafu G. (Tato vlastnost, tzv. výměnný axiom, je klíčová pro správnost hladového algoritmu.)

5. Nechť w a w' jsou dvě ohodnocení hran grafu $G = (V, E)$. Předpokládejme $w(e_1) < w(e_2)$ právě když $w'(e_1) < w'(e_2)$, pro libovolné

hrany $e_1, e_2 \in E$. Dokažte, že (V, E') je minimální kostra G pro ohodnocení w, právě když (V, E') je minimální kostra G pro ohodnocení w'. (Tedy: řešení problému minimální kostry závisí jen na uspořádání vah na hranách grafu G.)

6. S využitím diskuse algoritmu 4.3.2 navrhněte podrobnosti Kruskalova algoritmu tak, aby měl časovou složitost $O((n+m)\log n)$.

7. Uvažme n-bodovou množinu V v rovině. Definujme ohodnocení hran úplného grafu na V: ohodnocením hrany $\{x, y\}$ bude vzdálenost bodů x a y.

   (a)* Ukažte, že maximální stupeň vrcholu v libovolné minimální kostře je nejvýš 6.

   (b)* Ukažte, že existuje minimální kostra, jejíž hrany se navzájem nekříží.

8.* Nechť V je množina n bodů ve čtverci o straně 1. Dokažte, že existuje kostra na V s celkovou délkou hran nejvýš $10\sqrt{n}$ (uvažujeme všechny kostry úplného grafu na V, a váha hrany $\{x, y\}$ je euklidovská vzdálenost bodů x a y). Konstantu 10 lze podstatně zlepšit, ale nejlepší možná hodnota není známa (jaký nejlepší odhad se podaří najít vám?).

9. Buď $G = (V, E)$ graf, w nezáporné ohodnocení jeho hran.

   (a)* Každá množina $E' \subseteq E$ navzájem disjunktních hran se nazývá *párování* v grafu G. Označme $\nu_w(G)$ maximální možnou hodnotu $w(E')$ pro párování $E' \subseteq E$. Hladový algoritmus pro maximální párování funguje podobně jako algoritmus Kruskalův pro maximální kostru, jenže zamítá hrany protínající některou dříve vybranou hranu. Ukažte, že takový algoritmus vždy najde párování váhy nejméně $\nu_w(G)/2$.

   (b) Ukažte, že odhad v (a) nelze zlepšit, t.j. že pro libovolné $\alpha > \frac{1}{2}$ existuje zadání, pro nějž hladový algoritmus najde párování váhy menší než $\alpha\,\nu_w(G)$.

10. Množinu $C \subseteq E$ v grafu $G = (V, E)$ nazveme *hranovým pokrytím*, pokud každý vrchol $v \in V$ je obsažen aspoň v jedné hraně $e \in C$. Hledejme malé hranové pokrytí hladovým algoritmem (dokud existuje hrana, pokrývající dva dosud nepokryté vrcholy, vybereme libovolnou takovou, jinak libovolnou hranu pokrývající jeden dosud nepokrytý vrchol). Ukažte, že velikost takto nalezeného hranového pokrytí je vždy

   (a) nejvýše dvojnásobek velikosti optimálního pokrytí,

   (b)** dokonce nejvýš $\frac{3}{2}$ velikosti optimálního pokrytí.

* Množinu $D \subseteq V$ v grafu $G = (V, E)$ nazveme *dominující*, pokud $\bigcup_{e \in E;\, e \cap D \neq \emptyset} e = V$. Hledejme malou dominující množinu hladovým algoritmem (vždy vybereme vrchol, který je spojen s největším počtem dosud nepokrytých vrcholů). Ukažte, že pro každé číslo C existuje graf takový, že $|D_H| \geq C|D_M|$, kde D_H je dominující množina vybraná hladovým algoritmem a D_M je nejmenší dominující množina.

Jarníkův algoritmus a Borůvkův algoritmus

Název „Jarníkův algoritmus", ani v poangličtěné podobě, anglickému nebo americkému čtenáři nejspíš mnoho neřekne, a to i když příslušný algoritmus ve skutečnosti zná — zná ho totiž pod jménem *Primův algoritmus*. Protože však Jarník bezprostředně reagoval na průkopnickou Borůvkovu práci již v roce 1930 (Primova práce je z roku 1957) a protože jeho postup je elegantní a precizní (jako veškerá Jarníkova matematická produkce), domníváme se, že je na čase vrátit algoritmu jeho pravé jméno.

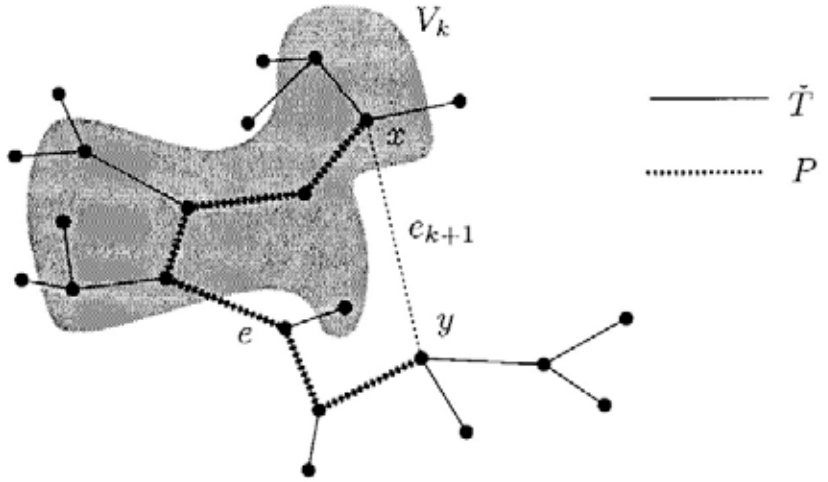
nešního hlediska je Jarníkův algoritmus jednoduchá modifikace al-
tmu 4.3.5. Připomeňte si jej, aby vám byl smysl následujícího po-
ı jasný.

.1 Algoritmus (Jarníkův algoritmus). Postupujme podle algo-
ıu 4.3.5, přičemž hranu e_i volíme jako hranu nejmenší možné váhy
ži hranami množiny $\{\{x, y\} \in E(G);\, x \in V_{i-1}, y \notin V_{i-1}\}$.

.2 Tvrzení (Správnost Jarníkova algoritmu). *Jarníkův algo-
nus nalezne minimální kostru pro každý souvislý graf G s libovol-
n ohodnocením w.*

kaz. Označme $T = (V, E')$ kostru, která je výsledkem Jarní-
a algoritmu, a nechť pořadí, v němž byly hrany E' algoritmem
ɔrány, je $e_1, e_2, \ldots, e_{n-1}$. Předpokládejme pro spor, že T není mini-
lní kostra.

Buď T' nějaká minimální kostra. Symbolem $k(T')$ označme index
akový, že hrany $e_1, e_2, \ldots, e_k$ náležejí do $E(T')$, ale e_{k+1} už nikoliv.
berme mezi všemi minimálními kostrami takovou, pro niž je tento
ex k maximální, a označme ji $\check{T} = (V, \check{E})$.



Obrázek 4.5: K důkazu správnosti Jarníkova algoritmu.

Nyní uvažme ten okamžik algoritmu, kdy byla e_{k+1} vybrána do T. Nechť $T_k = (V_k, E_k)$ je strom tvořený hranami $e_1, \ldots, e_k$. Potom e_{k+1} je tvaru $\{x, y\}$, kde $x \in V(T_k)$ a $y \notin V(T_k)$. Podívejme se na graf $\check{T} + e_{k+1}$. Ten obsahuje nějakou kružnici C (neboť je souvislý a má více než $n-1$ hran), a C musí nutně obsahovat hranu e_{k+1} (viz též cvičení 4.4.3).

Kružnice C sestává z hrany $e_{k+1} = \{x, y\}$ a z cesty P z vrcholu x do y v kostře $\check{T}$. Alespoň jedna hrana cesty P má jeden vrchol v množině V_k a druhý vrchol mimo V_k. Označme e některou takovou hranu. Zřejmě $e \neq e_{k+1}$, a dále víme $e \in \check{E}$, $e_{k+1} \notin \check{E}$, viz obr. 4.5. Jak hrana e, tak hrana e_{k+1} spojují vrchol z V_k s vrcholem mimo V_k, a z pravidla výběru hran v algoritmu tedy plyne $w(e_{k+1}) \leq w(e)$.

Uvažme nyní graf $T' = (\check{T} + e_{k+1}) - e$. Tento graf má $n-1$ hran, a je snadné ověřit, že je souvislý; je to tedy kostra. Přitom $w(E(T')) = w(\check{E}) - w(e) + w(e_{k+1}) \leq w(\check{E})$, čili T' je taky minimální kostra, pro niž ale $k(T') > k(\check{T})$. Vzniklý spor s volbou $\check{T}$ dokazuje tvrzení 4.5.2. □

Na závěr zmiňme ještě algoritmus, který byl historicky prvním postupem pro řešení problému minimální kostry. Jak už to bývá, tento postup je složitější — jak Kruskalův, tak (zvláště) Jarníkův algoritmus jsou koncepčně jednodušší. V poslední době se však právě Borůvkův algoritmus

stal koncepčním základem nejrychlejšího známého algoritmu pro problém minimální kostry ([11]). Tento algoritmus najde minimální kostru v čase $O(n+m)$, kde n je počet vrcholů a m počet hran sítě. Je poměrně složitý a používá ještě řadu dalších myšlenek (do nichž se zde ovšem pouštět nebudeme).

4.5.3 Algoritmus (Borůvkův algoritmus). Je dán graf $G = (V, E)$ s ohodnocením hran w. Předpokládáme navíc, že *různým hranám jsou přiřazena různá čísla*, t.j. že funkce w je prostá. (Tento předpoklad není příliš omezující; každé ohodnocení můžeme libovolně malými změnami některých vah převést na prosté ohodnocení, a váha minimální kostry se přitom změní libovolně málo.)

Algoritmus postupně vytváří množiny hran $E_0, E_1, \ldots \subseteq E$, přičemž $E_0 = \emptyset$.

Předpokládejme, že jsme již spočítali množinu E_{i-1}, a nechť $(V_1, V_2, \ldots, V_t)$ je rozklad množiny V podle komponent souvislosti grafu (V, E_{i-1}) (přísně vzato, měl by tento rozklad mít ještě index i, protože bude v každém kroku jiný, ale pro zjednodušení zápisu index i vynecháme). Pro každou třídu V_j tohoto rozkladu vyhledáme hranu $e_j = \{x_j, y_j\}$ (kde $x_j \in V_j$, $y_j \notin V_j$), jejíž váha je minimální mezi hranami tvaru $\{x, y\}$, $x \in V_j$, $y \in V \setminus V_j$ (přitom se může stát $e_j = e_{j'}$ pro $j \neq j'$). Definujeme $E_i = E_{i-1} \cup \{e_1, \ldots, e_t\}$. Algoritmus končí, má-li graf (V, E_i) jedinou komponentu.

Algoritmus by se také mohl nazývat *bublinkový*. Graf G pokrýváme souborem „bublinek" (kterých je jak borůvek v lese). Nacházíme mezi nimi nejkratší spojení a každé takové spojení vede k tomu, že se bublinky spojí v jednu.

Nebudeme dokazovat správnost algoritmu. Ukážeme pouze, že zkonstruovaný graf $T = (V, E')$ je skutečně strom. Podle definice je tento graf souvislý; stačí tedy ukázat, že nemá kružnici. Předpokládejme pro spor, že v nějakém kroku i kružnice vznikla. To znamená, že existují navzájem různé indexy $j(1), j(2), \ldots, j(k)$, pro něž platí

$$\begin{array}{ll} x_{j(1)} \in V_{j(1)}, & y_{j(1)} \in V_{j(2)} \\ x_{j(2)} \in V_{j(2)}, & y_{j(2)} \in V_{j(3)} \\ & \vdots \\ x_{j(k-1)} \in V_{j(k-1)}, & y_{j(k-1)} \in V_{j(k)} \\ x_{j(k)} \in V_{j(k)}, & y_{j(k)} \in V_{j(1)}. \end{array}$$

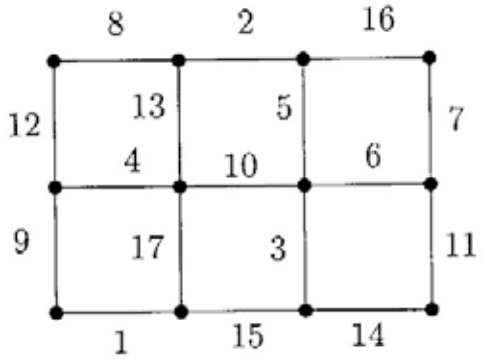
Vzhledem prostotě w a k volbě hran $e_j = \{x_j, y_j\}$ dostáváme násle-

dující nerovnosti:

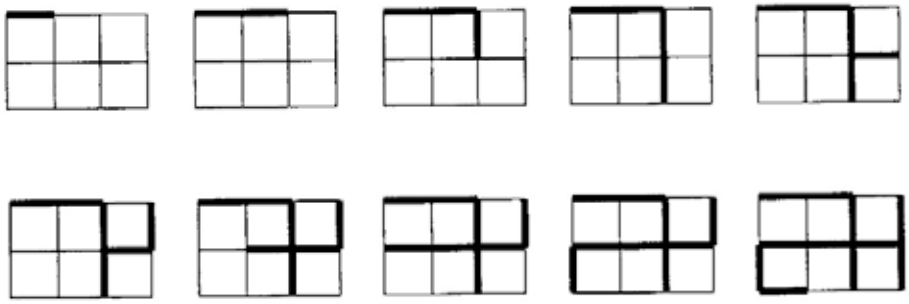
$$w(e_{j(1)}) > w(e_{j(2)}) > \cdots > w(e_{j(k)}) > w(e_{j(1)}).$$

To je však spor, a Borůvkův algoritmus tedy nalezne kostru grafu G (ve skutečnosti nalezne minimální kostru). □

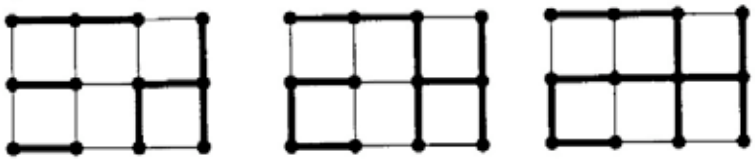
Příklad. Uvažme následující síť (ohodnocení jsou připsána k příslušným hranám):



Jarníkův algoritmus použitý na tuto síť proběhne takto (začínáme v levém horním rohu):



Kruskalův algoritmus by probíhal v 17 krocích (ale jenom v 10 z nich by přibyly hrany kostry). Borůvkův algoritmus je oproti tomu krátký:



Poznamenejme však, že v každém kroku musíme vykonat více práce.

Cvičení

1.* Uvažme takovýto algoritmus pro hledání minimální kostry: Vstupem je souvislý graf $G = (V, E)$ s ohodnocením w. Položíme $E_0 = \emptyset$. Nechť

E_{i-1} bylo již definováno. Zvolme libovolně některou komponentu V_i grafu (V, E_{i-1}), vyberme hranu e_i minimální váhy s jedním vrcholem ve V_i a druhým mimo V_i, a položme $E_i = E_{i-1} \cup \{e_i\}$. Dokažte, že (V, E_{n-1}) je minimální kostra (upravte důkaz správnosti Jarníkova algoritmu).

Ověřte, že tím se naráz dokazuje správnost jak Kruskalova, tak Jarníkova algoritmu.

2.* Uvažme následující algoritmus, jehož vstupem je souvislý graf $G = (V, E)$ s ohodnocením hran w. Seřadíme hrany do pořadí $e_1, \ldots, e_m$ tak, aby $w(e_1) \geq \ldots \geq w(e_m)$. Položíme $E_0 = E$, a

$$E_i = \begin{cases} E_{i-1} \setminus \{e_i\} & \text{je-li } (V, E_{i-1} \setminus \{e_i\}) \text{ souvislý graf} \\ E_i & \text{jinak.} \end{cases}$$

Dokažte, že (V, E_m) je minimální kostra G.

3.* Dokažte správnost Borůvkova algoritmu.

4. Navrhněte podrobnosti Jarníkova algoritmu tak, aby měl časovou složitost $O((m+n)\log n)$ (toto cvičení patrně vyžaduje aspoň základní znalost datových struktur).

5. (a) Ukažte, že Borůvkův algoritmus má nejvýš $O(\log n)$ fází, t.j. že (V, E_i) je souvislý graf již pro nějaké $i = O(\log n)$.

(b) Navrhněte podrobnosti Borůvkova algoritmu tak, aby měl časovou složitost $O((m+n)\log n)$.

TADY NENI NIC

chyba pri skenovani. stane se.

zomg lolz röfl

$\gamma : [0,1] \to \mathbf{R}^2$ je nějaké prosté spojité zobrazení uzavřeného intervalu $[0,1]$ do roviny. Přitom body $\gamma(0)$ a $\gamma(1)$ se jmenují *koncové body* oblouku o.

Tato definice, ačkoli může vypadat nenázorná, má velmi blízko k pojmu kreslení. Interval $[0,1]$ si můžeme představovat jako časový úsek, v němž kreslíme čáru z bodu $\gamma(0)$ do bodu $\gamma(1)$. Potom $\gamma(t)$ vyjadřuje polohu hrotu tužky v čase t. Spojitost zobrazení γ znamená souvislý pohyb po papíře, a prostota vyjadřuje, že čára nikde sama sebe neprotíná.

5.1.1 Definice. Nakreslením grafu $G = (V, E)$ *rozumíme přiřazení, které každému vrcholu v grafu G přiřazuje bod $b(v)$ roviny, a každé hraně $e = \{v, v'\} \in E$ přiřazuje oblouk $o(e)$ v rovině s koncovými body $b(v)$ a $b(v')$. Přitom předpokládáme, že zobrazení b je prosté (různým vrcholům odpovídají různé body), a žádný z bodů tvaru $b(v)$ není nekoncovým bodem žádného z oblouků $o(e)$. Graf spolu s nějakým nakreslením nazýváme* topologický graf.

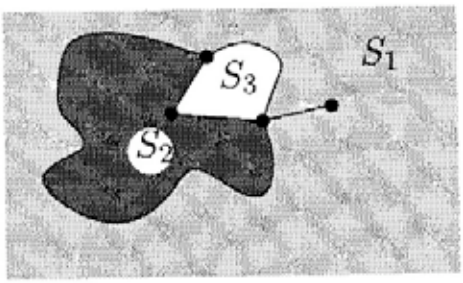
Nakreslení grafu $G = (V, E)$, v němž oblouky odpovídající různým hranám mají společné nanejvýš koncové body, se nazývá rovinné nakreslení. *Graf G je* rovinný, *má-li aspoň jedno rovinné nakreslení.*

Formální definici rovinného nakreslení jsme podali tak trochu „na ukázku", abychom ilustrovali, že i pojem nakreslení lze zahrnout do logické stavby matematiky. Nebudeme však pokračovat v budování příslušné teorie přísně logickým způsobem. Problematika rovinných grafů souvisí s matematickou disciplínou zvanou topologie, která zkoumá např. deformace různých geometrických útvarů (třeba kružnice, sféry, a pod.). V běžných úvodních matematických kursech se z topologie obvykle probere velmi málo, takže bychom museli zavádět poměrně složitý technický aparát. Navíc dokázat některá potřebná „intuitivně zřejmá" tvrzení je překvapivě obtížné. V dalším výkladu tedy budeme poněkud spoléhat na na intuitivní představu čtenáře a předkládat některá (platná!) tvrzení k uvěření. Naštěstí v teorii kreslení grafů intuitivní představa téměř nikdy nezavádí na scestí.

Rovinné nakreslení je výhodné pro znázornění grafu (při nerovinném nakreslení by se průsečíky hran mohly plést s vrcholy, a pod.), a při některých aplikacích, kdy má nakreslení grafu fyzikální význam, může

být křížení oblouků přímo nežádoucí (například při návrhu jednovrstevných integrovaných obvodů).

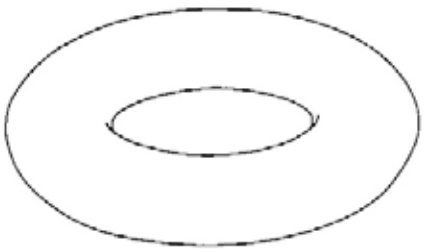
Stěny grafu. Nechť $G = (V, E)$ je topologický rovinný graf, tj. rovinný graf s daným rovinným nakreslením. Uvažme množinu všech bodů roviny, které neleží v žádném z oblouků nakreslení. Tato množina se rozpadne na konečný počet souvislých oblastí (představte si, že rovinu podél nakreslených hran rozstříháme):



Tyto oblasti budeme nazývat *stěny* topologického rovinného grafu. (Množinu $A \subseteq \mathbf{R}^2$ bodů roviny nazveme *souvislou*, jestliže pro libovolné dva body $x, y \in A$ existuje oblouk $o \subseteq A$ s koncovými body x, y. Souvislost[1] je příkladem topologického pojmu.)

Zdůrazněme ještě, že stěny jsou definovány *pro dané rovinné nakreslení*. Pro nerovinné nakreslení se stěny většinou vůbec nedefinují, a také pro graf bez zadaného nakreslení nejsou žádné stěny definovány.

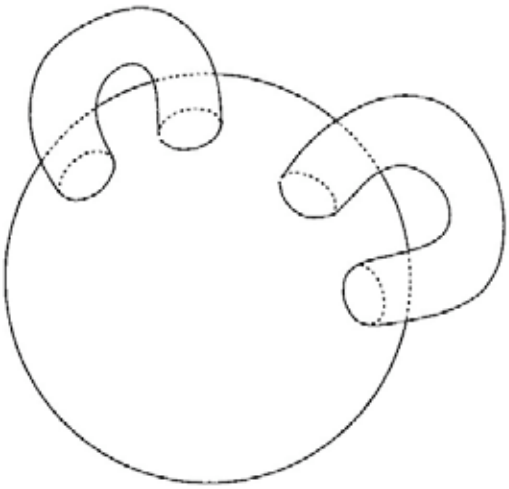
Kreslení na jiných plochách. Graf G můžeme nakreslit i na jiných „plochách" než je rovina, např. na kouli, na anuloidu (někdy zvaném též torus),



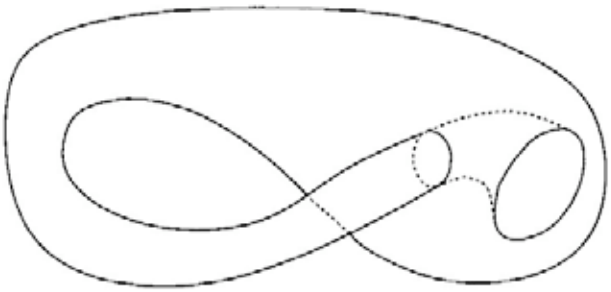
[1] To, co jsme zde definovali jako souvislost, se v topologii většinou jmenuje *oblouková souvislost*, a souvislá množina v rovině se definuje takto: $A \subseteq \mathbf{R}^2$ je souvislá, pokud neexistují dvě disjunktní otevřené množiny $A_1, A_2 \subseteq \mathbf{R}^2$ takové, že $A \subseteq A_1 \cup A_2$ a $A_1 \cap A \neq \emptyset \neq A_2 \cap A$. Pro množiny zde uvažované, např. stěny grafu, oba tyto pojmy souvislosti splývají.

na Möbiově listu,

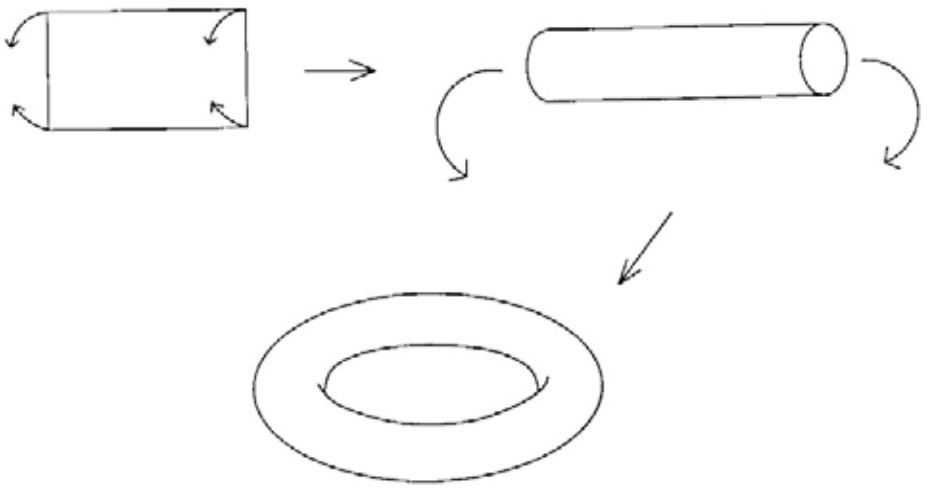
na kouli s „dvěma ušima



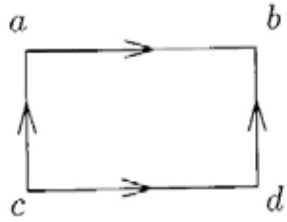
nebo na tzv. Kleinově lahvi.



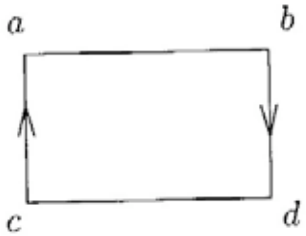
Takové plochy se dají vytvářet „slepováním“ (a vhodnou deformací) z jednodušších ploch; ve výše uvedených příkladech (s výjimkou koule se dvěma ušima) vyjdeme vždy z obdélníka v rovině a vhodně ztotožníme jeho strany. (Takový postup je i základem přesné definice těchto ploch, již zde neuvádíme.) Tak například anuloid lze vytvořit následujícím způsobem:



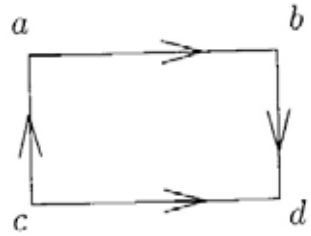
neboli ztotožněním protějších hran obdélníka $abcd$, přičemž strana ab se slepí se stranou cd a strana ca se stranou db (orientace při slepení se vyznačuje šipkami; šipky na následujícím obrázku znamenají, že při slepování stran ca a db přijde bod a k bodu b a bod c k bodu d).



Möbiův list vyrobíme takhle:



(ztotožníme pouze hrany označené šipkou tak, že směr obou šipek souhlasí). Kleinova láhev vznikne následovně:

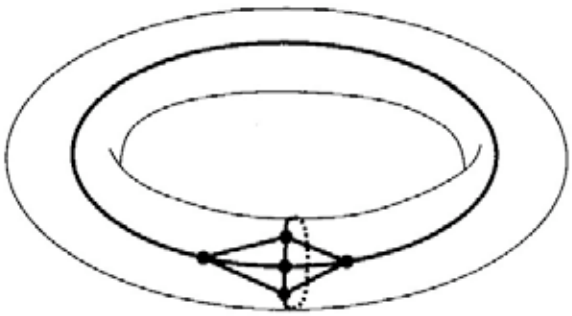


Ve skutečnosti Kleinovu láhev definujeme pomocí tohoto „poslepování“

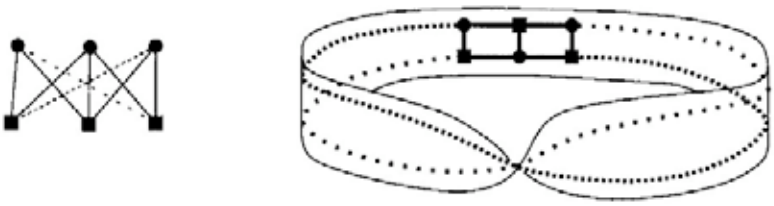
obdélníka; takové poslepování nelze realizovat ve třídimenzionálním prostoru, aniž by obdélník protínal sám sebe. V běžném světě tedy nelze vyrobit model Kleinovy lahve.

Platí obecná věta, která zaručuje, že každá uzavřená plocha (tzv. kompaktní 2-dimenzionální varieta bez okraje) může být vytvořena pomocí podobných poslepování. Navíc, má-li tato plocha dvě strany (Möbiův list i Kleinova láhev mají jenom jednu stranu!), potom takovou plochu lze spojitě deformovat na nějakou kouli s konečně mnoha ušima. Velmi pěkně a názorně jsou základy této teorie a řada souvisejících věcí popsány například v knize [19].

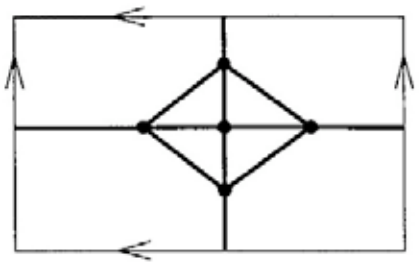
Grafy můžeme rozlišovat podle plochy, na niž je lze nakreslit. Jak ukážeme v následujícím článku, ani graf K_5 (úplný graf na 5 vrcholech), ani graf $K_{3,3}$ (úplný bipartitní graf na $3+3$ vrcholech) nejsou rovinné. Přitom ale například K_5 lze nakreslit na torus:

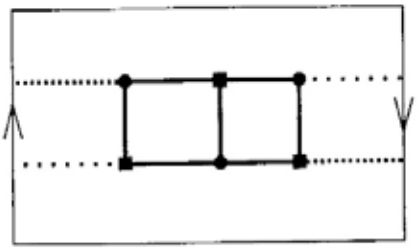


a $K_{3,3}$ na Möbiův list:

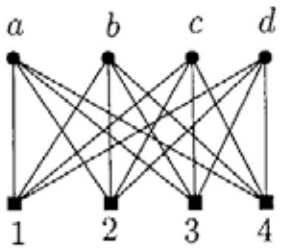


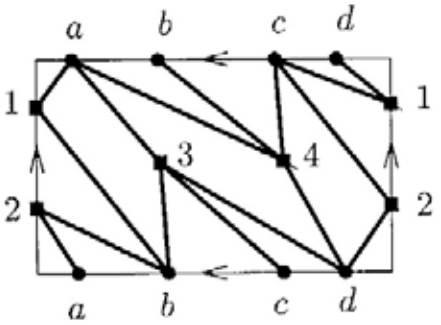
Jak jsme řekli, plochy můžeme vyrábět vhodným slepováním hran obdélníků (a složitějších mnohoúhelníků). Abychom nemuseli přepínat svou prostorovou představivost, můžeme kreslení na plochách převést na modifikované rovinné kreslení, kde hrany mohou „přeskakovat“ mezi slepovanými stranami. Právě uvedená nakreslení lze potom znázornit takto:





Poznamenejme, že na torus lze nakreslit dokonce graf $K_{4,4}$



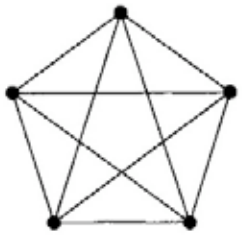


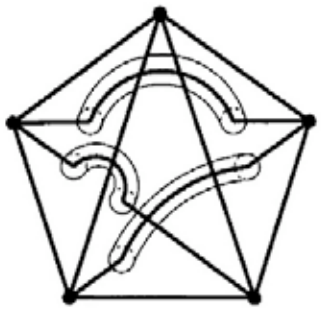
a graf K_7 (cvičení 2). Obecně platí

5.1.2 Tvrzení. *Každý graf lze nakreslit na kouli s dostatečným počtem „uší".*

(Toto tvrzení je třeba chápat intuitivně, neb jsme přesnou definici koule s ušima nepodali.)

Neformální důkaz. Nakresleme graf $G = (V, E)$ v rovině tak, že se některé hrany mohou křížit. Nechť $e_1, \ldots, e_n$ jsou všechny hrany, které se kříží (s nějakou jinou hranou). Pro každou hranu e_i přidejme „ucho" (nebo „přemostění") tak, že přidaná přemostění jsou disjunktní a přitom hrany nakreslené na příslušných přemostěních se již nekříží:





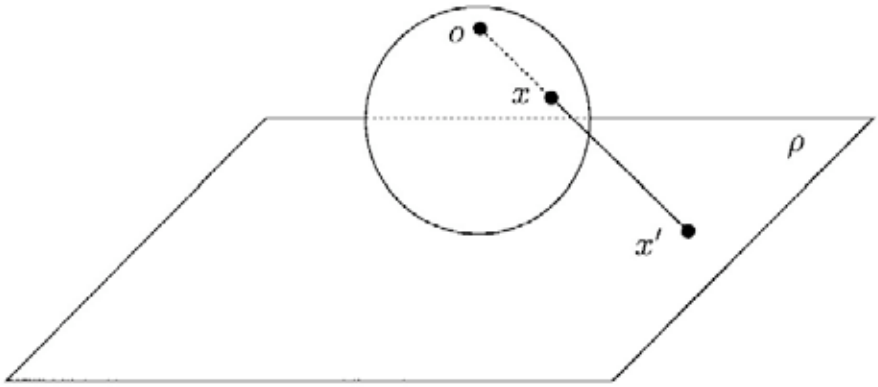
Vzhledem k tomu, že máme co činit pouze s konečným počtem hran, taková přemostění je snadné najít (přesný důkaz však vyžaduje znalost základů topologie roviny). □

Následující definice má tedy smysl:

5.1.3 Definice. *Minimální počet „uší", které je třeba přidat ke kouli tak, aby na vzniklou plochu bylo možno nakreslit graf G bez křížení hran, nazýváme* rod *grafu G.*

Určit rod daného grafu je obecně algoritmicky těžká úloha. Víme-li však, že daný graf má malý rod, např. je-li nakreslen na torus, řada algoritmických problémů se pro něj dá řešit efektivněji než pro obecné grafy (podobně jako rovinné grafy jsou často jednodušší než obecné grafy).

Ukážeme ještě, že rovinné grafy jsou právě grafy rodu 0. To ekvivalentně značí, že graf lze nakreslit v rovině bez křížení hran, právě když jej můžeme nakreslit na kouli bez křížení hran. To je však zřejmé tvrzení, jestliže použijeme *stereografické projekce*. Kouli umístíme v třírozměrném prostoru tak, aby se dotýkala uvažované roviny ρ, a označíme o bod koule nejvzdálenější od roviny ρ („severní pól"):



Potom stereografická projekce přiřazuje každému bodu $x \neq o$ na povrchu koule bod x' v rovině ρ, kde x' je průsečík přímky ox s rovinou ρ. (Pro bod o se projekce nedefinuje.) Toto je bijekce mezi povrchem koule bez bodu o a rovinou ρ. Máme-li nějaké nakreslení grafu G na povrchu koule (bez křížení hran), přičemž bod o neleží na žádném z oblouků nakreslení (což můžeme vždycky předpokládat), potom stereografickou projekcí dostaneme rovinné nakreslení G. Obráceně, z každého rovinného nakreslení dostaneme zpětnou projekcí nakreslení na kouli.

Cvičení

1. Najděte
   (a) rovinný graf, jehož všechny vrcholy mají stupeň 5,
   (b)* nekonečně mnoho neisomorfních souvislých takových grafů.
2. (a) Přesvědčte se, že obrázek v textu skutečně dává nakreslení $K_{4,4}$ na anuloid.

(b) Nalezněte nakreslení grafu K_6 na anuloid.

(c)* Nakreslete K_7 na anuloid.

3.* Buď G rovinný eulerovský graf, a mějme nějaké jeho rovinné nakreslení. Ukažte, že existuje uzavřený eulerovský tah, který v daném nakreslení nikde nekříží sama sebe (může se dotýkat ve vrcholech, ale nikdy nepřejde „na druhou stranu").

5.2 Kružnice v rovinných grafech

Budeme zkoumat kombinatorické vlastnosti rovinných grafů. Mimo jiné se ukáže, že sám pojem rovinného grafu může být definován čistě pomocí kombinatorických prostředků, aniž bychom použili topologických vlastností roviny nebo názoru.

Chceme-li převést topologickou definici rovinného grafu na definici kombinatorickou, musíme použít nějaké vlastnosti roviny, která spojuje geometrii s kombinatorikou. Takovou vlastnost vyjadřuje tzv. Jordanova věta. Nejdříve definice: *Topologická kružnice*[2] je uzavřená křivka v rovině neprotínající sebe sama; formálně se topologická kružnice definuje jako oblouk, jehož koncové body splývají, t.j. spojitý obraz intervalu $[0,1]$ při zobrazení f, které je prosté až na to, že $f(0) = f(1)$. Nebude-li hrozit nedorozumění, budeme místo topologická kružnice říkat jenom kružnice.

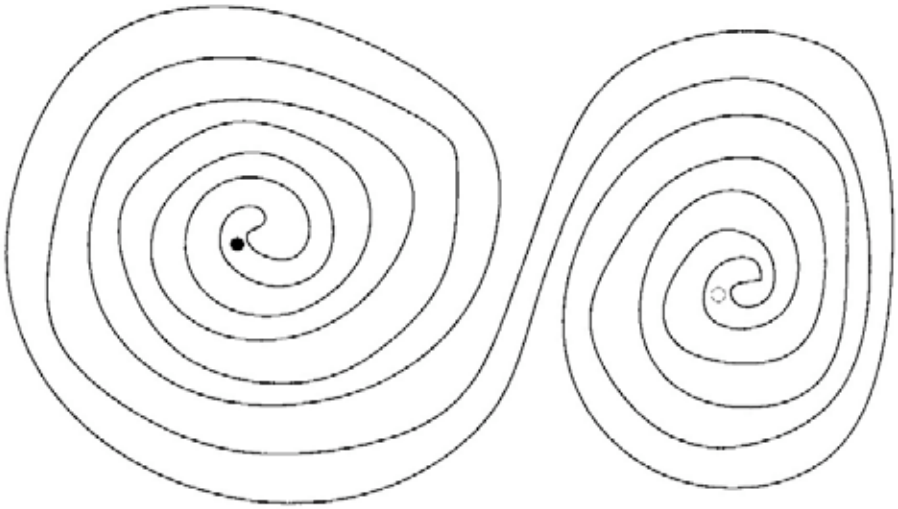
5.2.1 Věta (Jordanova věta o kružnici). *Každá topologická kružnice k rozděluje rovinu na právě dvě souvislé části: „vnitřek" a „vnějšek" kružnice, přičemž k je jejich společnou hranicí (vnitřek a vnějšek budeme společně nazývat* oblasti *kružnice k). To znamená, že definujeme-li na bodech množiny $\mathbf{R}^2 \setminus k$ ekvivalenci $\approx$ předpisem $x \approx y$ právě když x a y lze spojit obloukem neprotínajícím k, potom tato ekvivalence má dvě třídy, z nichž jedna je omezená množina a druhá neomezená množina, a k je hranicí obou těchto množin.*

Tato věta je intuitivně zřejmá, nicméně její důkaz není jednoduchý, i když byla v poslední době nalezena podstatná zjednodušení. Také pro

[2] Jiný používaný název je *jednoduchá uzavřená křivka*, nebo taky *Jordanova křivka*.

některé kružnice v rovině je tvrzení evidentní:

pro jiné už méně evidentní (zkuste najít oblouk mezi body ○ a ●, který neprotíná kružnici):



Abychom ilustrovali, jak se to ve skutečnosti má s takzvanou intuitivní zřejmostí podobných tvrzení, zmiňme jednu související větu. Rozšíření Jordanovy věty, tzv. *Jordanova-Schönfliesova věta* praví, že pro každou kružnici jako v Jordanově větě se vnitřek kružnice dá spojitě deformovat (přesně řečeno, existuje homeomorfismus) na vnitřek (obyčejného) kruhu. Podobně by člověk čekal, že definujeme-li topologickou sféru jako prostý spojitý obraz povrchu obyčejné koule, bude taková věc mít vnitřek, spojitě deformovatelný na vnitřek obyčejné koule. To ale pravda není (protipříklad je znám pod názvem „Alexandrova rohatá sféra").

Poznamenejme ještě, že potíže s důkazem Jordanovy věty pramení hlavně ze značné obecnosti pojmu oblouk (připouštíme libovolné spojité zobrazení, a spojitá zobrazení mohou být velmi „divoká"). Jednodušší způsob, jak vybudovat logicky přesně teorii kreslení grafů, je povolit jen oblouky složené z konečného počtu úseček — lomené čáry (říkejme ji

krátce *lomenice*). Graf můžeme třeba nazývat lomenicově rovinný, dáli se nakreslit oblouky-lomenicemi. Dokázat verzi Jordanovy věty pro lomenicové kružnice, či vlastně mnohoúhelníky, nijak těžké není (viz cvičení 3). A také není obtížné nahlédnout, že každý rovinný graf je také lomenicově rovinný[3] (na to je trochu z topologie potřeba, ale velmi málo), takže vlastně dovolit obecné oblouky nepřináší v kreslení grafů nic nového — jenom komplikace s Jordanovou větou.

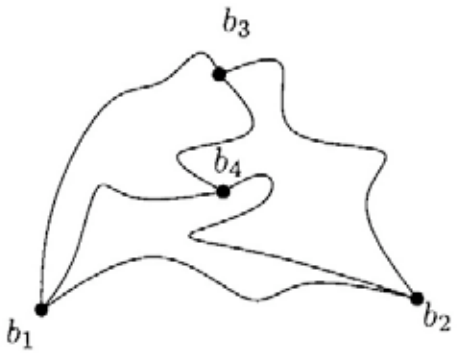
Věty o rovinných grafech, které v dalším dokážeme, nebudeme logicky přesně odvozovat z Jordanovy věty — jak jsme řekli dříve, budeme trochu spoléhat na názor, přičemž většinou na taková místa upozorníme. Za cenu prodloužení a zkomplikování důkazů se ovšem dají všechny takové nedokonalosti odstranit.

Začneme důkazem nerovinnosti grafu K_5 (již později dokážeme ještě jinak).

5.2.2 Tvrzení. *K_5 není rovinný graf.*

Důkaz. Postupujme sporem. Nechť b_1, b_2, b_3, b_4, b_5 jsou body odpovídající vrcholům K_5 při nějakém rovinném nakreslení. Oblouk odpovídající hraně, který spojuje b_i a b_j, označme $o(i,j)$.

Protože b_1, b_2 a b_3 jsou vrcholy kružnice v grafu K_5, tvoří oblouky $o(1,2)$, $o(2,3)$ a $o(3,1)$ (topologickou) kružnici k, a tedy body b_4 a b_5 leží buď oba vně, nebo oba uvnitř kružnice k (jinak by oblouk $o(4,5)$ protnul kružnici k). Předpokládejme nejprve, že b_4 leží uvnitř:



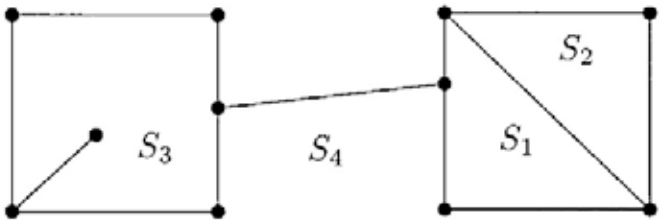
[3] Platí dokonce mnohem silnější věc: každý rovinný graf se dá nakreslit tak, že všechny hrany budou rovné úsečky! To ale není snadná věta.

Potom b_5 musí ležet uvnitř kružnice tvořené buď oblouky $o(1,4)$, $o(4,2)$ a $o(1,2)$, nebo oblouky $o(2,3)$, $o(3,4)$ a $o(2,4)$, nebo oblouky $o(1,3)$, $o(3,4)$ a $o(1,4)$ (odvoláváme se na názor). V prvním z uvedených případů však oblouk $o(3,5)$ musí protnout kružnici tvořenou oblouky $o(1,4)$, $o(4,2)$ a $o(1,2)$ a podobně v ostatních dvou případech.

Jestliže body b_4 a b_5 leží vně kružnice k, postupuje se úplně stejně. □

Stěny a kružnice v 2-souvislých grafech. Jestliže $e_1, \ldots, e_n$ jsou hrany nějaké kružnice v topologickém rovinném grafu G, potom oblouky $o(e_1), \ldots, o(e_n)$ tvoří (topologickou) kružnici (o takové topologické kružnici budeme v dalším hovořit, s jistou formální nepřesností, jako o *kružnici (topologického) grafu* G), a tedy použitím Jordanovy věty dostáváme, že každá stěna topologického rovinného grafu G je buď vně, nebo uvnitř této kružnice.

U některých topologických rovinných grafů je každá stěna vnitřkem nebo vnějškem nějaké kružnice grafu. Vždycky tomu tak ale být nemusí. Tak třeba rovinná nakreslení stromů mají jen jedinou stěnu; jiný příklad vypadá takto:



Platí však následující:

5.2.3 Tvrzení. *Nechť G je 2-souvislý rovinný graf. Potom každá stěna v libovolném nakreslení grafu G je oblastí nějaké kružnice grafu G.*

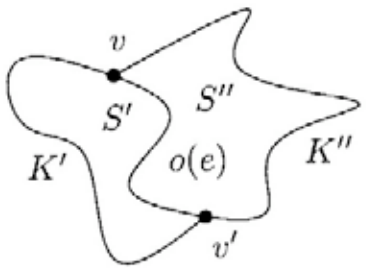
Důkaz. Postupujeme matematickou indukcí, přičemž použijeme tvrzení 3.8.5, které podává charakteristiku 2-souvislých grafů. Je-li graf G trojúhelník, potom tvrzení zřejmě platí.

Nechť $G = (V, E)$ je topologický rovinný graf s aspoň 4 vrcholy, který je 2-souvislý. Podle tvrzení 3.8.5 buď existuje hrana $e \in E$ tak, že

graf $G' = G-e$ je 2-souvislý, nebo existuje 2-souvislý graf $G' = (V', E')$ a hrana $e \in E'$ tak, že $G = G'\%e$, kde $\%$ značí operaci dělení hrany.

Protože graf G je topologický rovinný graf, je graf G' opět topologický rovinný graf. Protože graf G' je 2-souvislý, můžeme použít indukčního předpokladu. Každá stěna topologického rovinného grafu G' je tedy oblastí nějaké kružnice grafu G'.

Uvažme první případ, kdy $G' = G - e$, $e = \{v, v'\}$. Vrcholy v a v' jsou spojeny hranou v grafu G, a tedy leží na hranici společné stěny S v G'. Označme K_S kružnici, ohraničující stěnu S. Oblouk $o(e)$ příslušející hraně e je v oblasti kružnice K_S tvořené stěnou S. Proto stěny topologického rovinného grafu G jsou jednak stěny topologického grafu G' různé od stěny S (a každá taková stěna je oblastí kružnice v G i v G'), a jednak dvě stěny $S', S'' \subset S$. Tyto stěny jsou oblastmi kružnic $o_1 \cup o(e)$ a $o_2 \cup o(e)$, kde o_1 a o_2 jsou dva oblouky mezi v a v' tvořící dohromady kružnici K_S, viz obrázek:



Druhý případ je snazší: Jestliže $G = G'\%e$ a každá stěna G' je oblastí nějaké kružnice, potom G má tutéž vlastnost, jak plyne bezprostředně z definice operace dělení hrany. Tím je důkaz tvrzení ukončen. □

Kombinatorická charakterizace rovinných grafů. Poznamenejme, že platí následující: *Graf je rovinný, právě když libovolné dělení grafu G je rovinný graf.* (Důkaz plyne bezprostředně z definice dělení grafu.) Této vlastnosti lze využít ke kombinatorické charakteristice rovinných grafů — charakteristice, která se neopírá o geometrický názor a používá jen kombinatorických (grafových) prostředků. Je to slavná *Kuratowského věta:*

5.2.4 Věta (Kuratowského věta). *Graf G je rovinný, právě když žádný jeho podgraf není isomorfní dělení grafu $K_{3,3}$ ani dělení grafu K_5.*

Větu je snadno ukázat v jednom směru, opačná implikace je však složitější a v tomto textu ji nebudeme dokazovat.

Z této věty plyne, že nerovinnost libovolného nerovinného grafu můžeme prokázat tím, že v něm najdeme nějaké dělení K_5 nebo $K_{3,3}$. Z algoritmického hlediska, t.j. chceme-li skutečně testovat rovinnost grafu na počítači a případně hledat rovinná nakreslení, takový způsob není příliš vhodný. Jsou sice známy algoritmy pro testování, zda vstupní graf obsahuje dělení nějakého pevně daného grafu, ale ty jsou velmi složité a poměrně nepraktické. Pro testování rovinnosti a hledání „pěkných" rovinných nakreslení byla vynalezena řada efektivních (i když také komplikovaných) metod. Takovými metodami se například dá testovat rovinnost grafu na n vrcholech v čase $O(n)$.

Cvičení

1. Dokažte, že $K_{3,3}$ není rovinný graf.
2. (a) Nalezněte v grafu na obr. 3.2 vlevo buď dělení grafu K_5, nebo dělení grafu $K_{3,3}$.

   (b) Je graf na obr. 3.2 uprostřed rovinný?

   (c) Je graf na obr. 8.1(b) rovinný?
3. V tomto cvičení je cílem podat logicky přesný důkaz, aniž bychom se odvolávali na názor.

   (a) Buď k topologická kružnice, sestávající z konečného počtu úseček. Dokažte, že prohlásíme-li dva body z $\mathbf{R}^2 \setminus k$ za ekvivalentní, pokud je lze spojit lomenicí (viz poznámky za Jordanovou větou), potom tato ekvivalence má nejvýš 2 třídy.

   (b) Ukažte, že v situaci jako v (a), ekvivalence má právě 2 třídy (návod: definujte „vnitřní bod" jako takový, pro nějž polopřímka z něj vycházející má lichý počet průsečíků s k; musíte správně ošetřit případy, kdy tato polopřímka protíná k v úsečkách).

   (c) Buď k kružnice jako v (a), p, q dva její různé body, a ℓ lomenice spojující p a q, která leží celá uvnitř k (až na koncové body). Nechť k_1, k_2 jsou dva oblouky, na něž je k rozdělena body p, q, a nechť $r \in k_1$, $s \in k_2$ jsou body. Dokažte, že každá lomenice spojující r a s a ležící celá uvnitř k protne ℓ.

4. Formalizujte indukci v tvrzení 5.2.3. (Podle čeho se postupuje indukcí?)
5. Dokažte, že pro topologický rovinný graf G jsou následující dvě tvrzení ekvivalentní:
   (a) G je 2-souvislý.
   (b) Každá stěna G je oblastí nějaké kružnice.
6. Dokažte, že graf je rovinný, právě když libovolné jeho dělení je rovinný graf.
7. Dokažte, že $K_{m,n}$ je rovinný graf, právě když $\min\{m,n\} \leq 2$.
8.* Uvažme libovolné nakreslení grafu K_n. Ukažte, že aspoň $\frac{1}{5}\binom{n}{4}$ dvojic hran se protíná (mimo své koncové vrcholy). Využijte nerovinnosti grafu K_5.

5.3 Eulerův vztah

Existuje vpodstatě jediný základní kvantitativní vztah pro rovinné grafy; dá se říci, že všechny ostatní výsledky tento vztah ve větší či menší míře využívají. Je to zároveň vztah nejstarší (Euler jej znal v roce 1752, a někdy se tvrdí, že vztah pochází dokonce od Descarta z r. 1640; původní tvrzení se ovšem týkalo mnohostěnů místo rovinných grafů).

5.3.1 Tvrzení (Eulerův vzorec). *Nechť $G = (V, E)$ je souvislý rovinný graf, a nechť s je počet stěn nějakého rovinného nakreslení G. Potom platí*

$$|V| - |E| + s = 2.$$

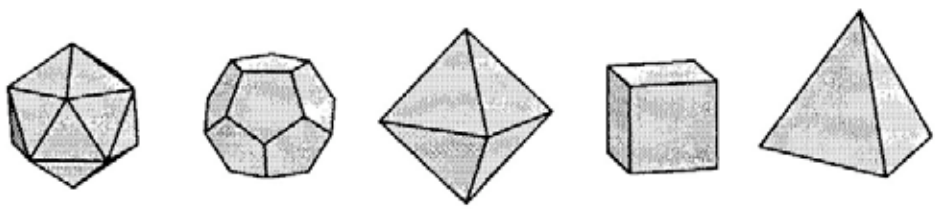
Speciálně počet stěn nezávisí na způsobu rovinného nakreslení.

Důkaz. Postupujme indukcí podle počtu hran grafu G. Je-li $E = \emptyset$, potom $|V| = 1$ a $s = 1$, a vzorec platí. Nechť $|E| \geq 1$; rozlišíme dvě možnosti:

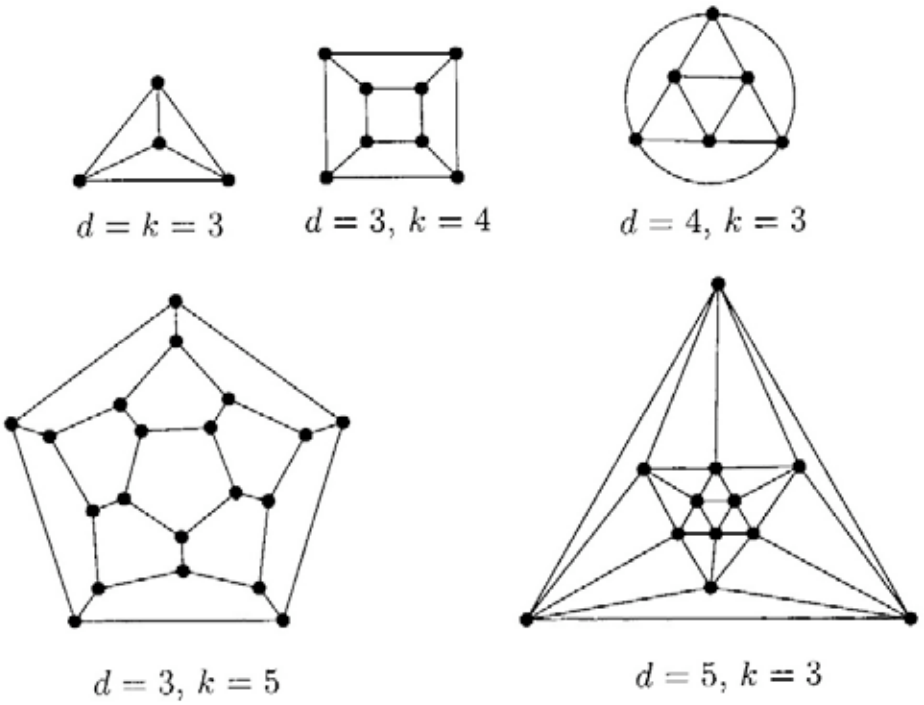
1. Graf G neobsahuje kružnici. Potom G je strom a tedy $|V| = |E| + 1$; přitom $s = 1$ (nakreslení stromu do roviny má jedinou stěnu, což je z názoru jasné a formálně to dokazovat nebudeme).

2. Nějaká hrana $e \in E$ je obsažena v kružnici. V tom případě je graf $G - e$ souvislý. Pro něj podle indukčního předpokladu platí Eulerův vzorec (přitom bereme jeho nakreslení vzniklé z uvažovaného nakreslení G vymazáním hrany e). Hrana e v nakreslení G sousedí se dvěma různými stěnami S a S' (podle Jordanovy věty, neboť e je obsažena v kružnici — přesný formální důkaz opět pomineme), které se v nakreslení $G - e$ stanou stěnou jedinou. Takže počet hran i stěn pro G stoupl ve srovnání s $G - e$ o 1, a počet vrcholů se nezměnil, pročež Eulerův vzorec platí i pro G. □

Aplikace: platónská tělesa. Antická škola myslitelů spojovaná s Platónovým jménem měla v obzvláštní vážnosti vysoce pravidelné geometrické útvary, takzvané *pravidelné mnohostěny*, a hledala je i v základech stavby vesmíru (ostatně i Kepler považoval za jeden ze svých nejdůležitějších objevů teorii — patrně chybnou — podle níž rozestupy mezi drahami planet jsou určeny geometrií pravidelných mnohostěnů). Pravidelný mnohostěn je trojrozměrné konvexní[4] těleso, ohraničené konečným počtem stěn — shodných pravidelných mnohoúhelníků, jichž se v každém vrcholu stýká stejný počet. Jednou z příčin zmíněného zájmu o pravidelné mnohostěny je patrně jejich výlučnost. Už ve starověku se vědělo, že jich je jen 5 typů: pravidelný čtyřstěn, krychle, pravidelný osmistěn, dvanáctistěn a dvacetistěn:



[4]Konvexita znamená, že jsou-li x, y libovolné dva body tělesa, leží i celá úsečka xy uvnitř tělesa, tedy že povrch není nikde „prohnutý dovnitř".



Obrázek 5.1: Grafy platónských těles.

Pomocí Eulerova vzorce ukážeme, že žádné jiné pravidelné mnohostěny existovat nemohou (to, že zmíněné pravidelné mnohostěny skutečně existují, se ovšem musí ověřit jejich geometrickou konstrukcí, čímž se zde zabývat nebudeme). Prvním krokem bude převedení mnohostěnu na graf pomocí stereografické projekce (zavedené v části 5.1). Umístíme zkoumaný mnohostěn dovnitř koule tak, aby její střed ležel uvnitř něj. Promítneme jej ze středu na povrch koule (představte si, že hrany mnohostěnu jsou vyrobeny z drátu), a tím dostaneme nakreslení nějakého rovinného grafu na kouli. Jak již víme, to lze dále stereografickou projekcí proměnit v rovinné nakreslení grafu. Vrcholy mnohostěnu přejdou na vrcholy grafu, hrany mnohostěnu na hrany grafu, a stěny mnohostěnu na stěny tohoto grafu (odtud také termíny vrcholy, hrany a stěny grafu také pocházejí). Pro 5 vyjmenovaných pravidelných mnohostěnů tím obdržíme grafy na obr. 5.1.

Pro každý pravidelný mnohostěn má vzniklý topologický rovinný graf zřejmě stejný stupeň, d, všech vrcholů (přičemž $d \geq 3$) a každá stěna má na hranici stejný počet vrcholů, $k \geq 3$. Neexistence dalších pravidelných mnohostěnů tedy vyplyne z následujícího:

5.3.2 Tvrzení. *Nechť G je topologický rovinný graf, jehož každý vrchol*

má stupeň $d \geq 3$, a jehož každá stěna má $k \geq 3$ vrcholů. Potom G je isomorfní jednomu z grafů na obr. 5.1.

Důkaz. Označme n počet vrcholů, m počet hran, a s počet stěn rovinného grafu $G = (V, E)$. Nejprve využije vztahu $\sum_{v \in V} \deg_G(v) = 2|E|$ (tvrzení 3.4.1), který se v našem případě konkretizuje na

$$dn = 2m.$$

Podobně získáme rovnost

$$2m = ks$$

(dvěma způsoby počítáme počet uspořádaných dvojic (e, S), kde S je stěna grafu G a $e \in E$ je hrana ležící na její hranici: každá hrana přispěje 2 takovými dvojicemi, a každá stěna k dvojicemi). Z právě odvozených vztahů vyjádříme n i s pomocí m, a dosadíme do Eulerova vzorce:

$$2 = n - m + s = \frac{2m}{d} - m + \frac{2m}{k},$$

a odtud po úpravě

$$\frac{1}{d} + \frac{1}{k} = \frac{1}{2} + \frac{1}{m}.$$

Jsou-li tedy d i k známa, jsou ostatní parametry (m, n a s) již určeny jednoznačně. Zjevně $\min(d, k) = 3$. Jestliže $d = 3$, potom máme $\frac{1}{k} - \frac{1}{6} = \frac{1}{m} > 0$, takže $k \in \{3, 4, 5\}$. Podobně pro $k = 3$ dostaneme $d \in \{3, 4, 5\}$. Tedy nastane jedna z následujících možností:

d	k	n	m	s
3	3	4	6	4
3	4	8	12	6
3	5	20	30	12
4	3	6	12	8
5	3	12	30	20

Nyní je snadné se přesvědčit, že v každém z uvedených případů je graf již hodnotami d, k, n, m, s jednoznačně určen, a je isomorfní jednomu z grafů na obr. 5.1. □

Poznamenejme ještě, že souvislost mnohostěnů v trojrozměrném prostoru a rovinných grafů je těsnější, než by se mohlo zdát. Jak jsme viděli, z každého (konvexního) mnohostěnu dostaneme topologický rovinný graf.

Dosti těžká *Steinitzova věta* tvrdí, že pro libovolný vrcholově 3-souvislý rovinný graf G (t.j. graf, který po vymazání libovolných 2 vrcholů zůstává souvislý) existuje konvexní trojrozměrný mnohostěn, jehož grafem je právě G.

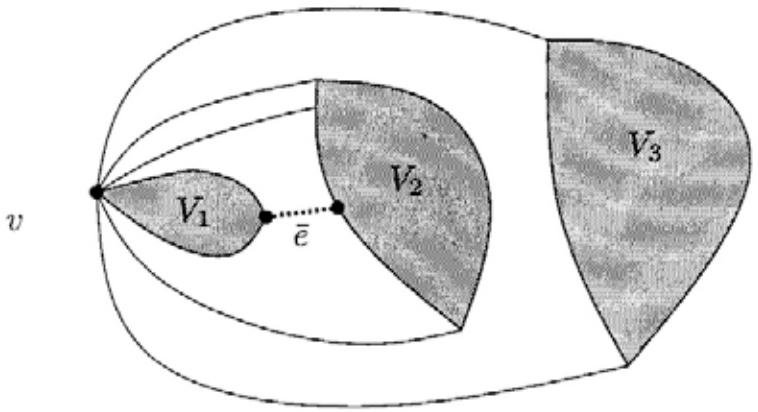
5.3.3 Tvrzení (Maximální počet hran rovinného grafu).
(i) Nechť $G = (V, E)$ je rovinný graf s aspoň 3 vrcholy. Potom $|E| \leq 3|V| - 6$. Navíc rovnost nastává pro každý maximální rovinný graf, *t.j. rovinný graf, k němuž už nejde přidat žádnou hranu (při zachování množiny vrcholů) tak, aby zůstal rovinným.*

(ii) Neobsahuje-li navíc uvažovaný rovinný graf trojúhelník (t.j. K_3 jako podgraf) a má-li aspoň 3 vrcholy, potom $|E| \leq 2|V| - 4$.

(V tomto tvrzení ovšem nepřipouštíme grafy s násobnými hranami!)

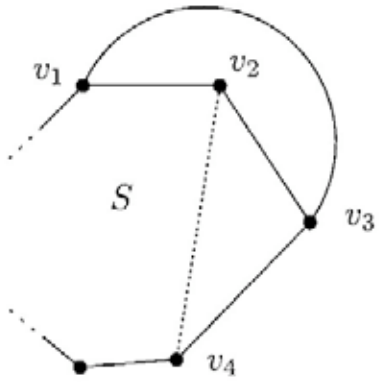
Důkaz (i). Není-li graf G maximální, přidávejme hrany tak dlouho, až se maximálním stane. Tvrdíme, že libovolná stěna (včetně vnější) maximálního rovinného grafu s aspoň 3 vrcholy je trojúhelník, t.j. je ohraničena kružnicí délky 3.

Je-li G nesouvislý, můžeme hranou spojit dvě různé komponenty. Je-li G souvislý, ale nikoliv (vrcholově) 2-souvislý, má nějaký vrchol v, jehož odstranění rozděluje graf G na komponenty $V_1, \ldots, V_k$, $k \geq 2$. Potom můžeme přikreslit nějakou hranu $\bar{e}$ spojující vrcholy z různých komponent:



Maximální rovinný graf s aspoň 3 vrcholy je tedy 2-souvislý, a podle tvrzení 5.2.3 je každá stěna ohraničena kružnicí. Předpoklá-

dejme pro spor, že hraniční kružnice nějaké stěny S má $t \geq 4$ vrcholů $v_1, \ldots, v_t$. Není-li vrchol v_1 spojen hranou s vrcholem v_3, můžeme hranu $\{v_1, v_3\}$ přikreslit dovnitř stěny S. Je-li $\{v_1, v_3\} \in E(G)$, musí jít nakreslení této hrany vnějškem stěny S. Proto již $\{v_2, v_4\} \notin E(G)$, a můžeme přikreslit hranu $\{v_2, v_4\}$ dovnitř stěny S, viz obr.:



Každá stěna maximálního rovinného grafu je tedy trojúhelník jak jsme tvrdili. Z toho už dostaneme podobně jako v důkazu tvrzení 5.3.2 rovnost $3s = 2|E|$, kde s je počet stěn. Dosazením za s do Eulerova vzorce vyjde

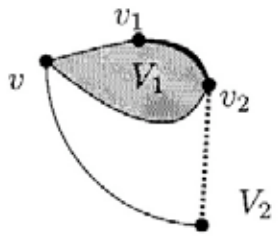
$$|V| - |E| + \frac{2}{3}|E| = 2,$$

z čehož po úpravě máme požadovaný vztah $|E| = 3|V| - 6$ pro maximální rovinné grafy.

Důkaz (ii). Postupujeme obdobně. Po případném přidání hran můžeme uvažovat hranově maximální rovinný graf bez trojúhelníků (t.j. přidáním libovolné hrany buď vznikne trojúhelník, nebo graf přestane být rovinný). Můžeme opět předpokládat, že G je souvislý.

Není-li G (vrcholově) 2-souvislý, má nějaký vrchol v, jehož odstraněním se G rozpadne na komponenty $V_1, \ldots, V_k$, $k \geq 2$. Jistě můžeme přidat nějakou hranu jdoucí mezi různými komponentami tak, aby G zůstal rovinný; pro některé hrany by tím však mohl vzniknout trojúhelník — to v případě, že bychom spojovali vrcholy, které oba sousedí s v. Jsou-li všechny komponenty V_i jednobodové, je G strom, a pro něj vzorec platí. Předpokládejme tedy $|V_1| \geq 2$, a uvažme stěnu S takovou, která má na hranici nějaký vrchol V_1 i vrchol nějaké jiné komponenty

V_i. Když nějaký vrchol z V_1 na hranici stěny S není spojen s v, potom takový vrchol můžeme spojit hranou s vrcholem z V_i, aniž by vznikl trojúhelník. Komponenta V_1 ale musí mít na hranici S aspoň jednu hranu $\{v_1, v_2\}$, a protože G nemá trojúhelník, nemohou oba vrcholy v_1 i v_2 být zároveň spojeny s v. Viz obrázek:



Tudíž můžeme předpokládat, že G je 2-souvislý graf. V takovém případě je každá stěna ohraničena kružnicí. Každá taková kružnice má délku aspoň 4, a počítáním dvěma způsoby tentokrát vyjde $2|E| \geq 4s$. Dosazením do Eulerova vzorce dostaneme $|E| \leq 2|V| - 4$. □

Z části (i) plyne důležitý a často používaný důsledek, totiž že každý rovinný graf má nějaký vrchol stupně nejvýš 5. Podobně (ii) zaručuje, že rovinný graf bez trojúhelníků má vrchol stupně nejvýš 3.

Část (i) ukazuje, že graf K_5 není rovinný (má 10 hran, zatímco rovinný graf na 5 vrcholech má nejvýš 9 hran). Podobně z (ii) plyne nerovinnost $K_{3,3}$ (graf na 6 vrcholech bez trojúhelníků má nejvýše 8 hran).

Dokážeme ještě další tvrzení, poskytující více informací o skóre rovinného grafu.

5.3.4 Tvrzení. *Nechť $G = (V, E)$ je 2-souvislý rovinný graf s nejméně 3 vrcholy. Označme n_i počet vrcholů stupně i, a s_i počet stěn (v nějakém nakreslení) ohraničených kružnicí délky i. Potom platí*

$$\sum_{i \geq 1} (6-)n_i = 12 + 2\sum_{j \geq 3} (j-3)s_j,$$

neboli

$$5n_1 + 4n_2 + 3n_3 + 2n_4 + n_5 - n_7 - 2n_8 - \cdots = 12 + 2s_4 + 4s_5 + 6s_6 + \cdots.$$

Odtud $5n_1 + 4n_2 + 3n_3 + 2n_4 + n_5 \geq 12$, takže každý 2-souvislý rovinný graf s aspoň 3 vrcholy obsahuje aspoň 3 vrcholy stupně ≤ 5.

Důkaz. Zřejmě $|V| = \sum_i n_i$, $s = \sum_i s_i$. Dosazením do Eulerova vzorce získáme

$$2|E| = 2(|V| + s - 2) = \sum_i 2n_i + \sum_j 2s_j - 4. \tag{5.1}$$

Počítáním dvěma způsoby jako v předešlých důkazech dostaneme další vztahy: $\sum_i in_i = 2|E| = \sum_j js_j$. Vyjádřením $2|E|$ pomocí (5.1) tyto rovnosti přejdou na

$$\sum_j (j-2)s_j + 4 = \sum_i 2n_i \qquad \sum_j 2s_j = \sum_i (i-2)n_i + 4.$$

První z těchto rovnic vynásobíme dvěma a odečteme od ní druhou; vyjde

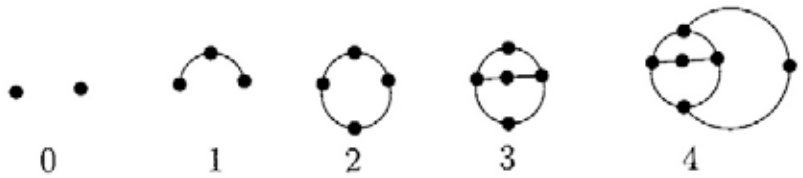
$$\sum_i (6-i)n_i - 4 = 2\sum_j (j-3)s_j + 8.$$

Odtud dostáváme tvrzení. □

Cvičení

1. Ukažte, že odhad $|E| \leq 2|V| - 4$ pro rovinné grafy bez trojúhelníků je nejlepší možný.
2. (a) Ukažte, že rovinný graf s $n \geq 3$ vrcholy má nejvýš $2n - 4$ stěn.
   (b) Ukažte, že rovinný graf bez trojúhelníků má nejvýš $n - 2$ stěn.
3. Dokažte, že rovinný graf, jehož každý vrchol má stupeň aspoň 5, musí mít nejméně 12 vrcholů.
4.* Mějme maximální 2-souvislý rovinný graf $G = (V, E)$ bez trojúhelníků (t.j. libovolný graf tvaru $G + e$, kde $e \in \binom{V}{2} \setminus E$, obsahuje trojúhelník nebo není rovinný). Dokažte, že každá stěna je čtyřúhelník nebo pětiúhelník.
5. (Hra „šprouti“) Následující hru vynalezli J. H. Conway a M. S. Paterson. Anglicky se nazývá *sprouts* („výhonky“). Na papíře je na začátku nakresleno n puntíků (hra je zajímavá už pro malá n, třeba 5). Hráči se střídají v tazích, kdo nemá tah prohraje. V každém tahu hráč spojí dva puntíky obloukem, a někam na tento oblouk se nakreslí nový puntík. Puntík se smí použít jako konec nového oblouku jen pokud z něj vycházejí nanejvýš 2 již nakreslené čáry, a nový oblouk nesmí protnout již nakreslené oblouky (v každém okamžiku máme tedy rovinné

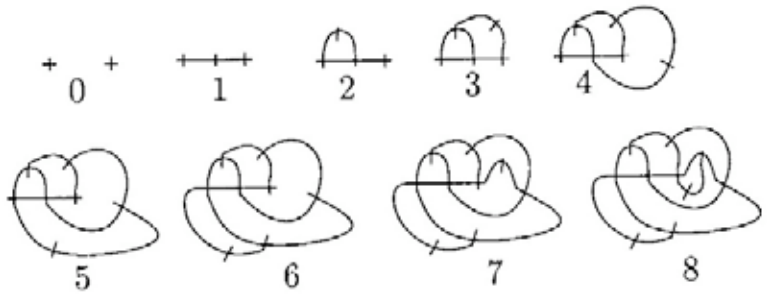
nakreslení grafu s maximálním stupněm 3; puntík na nově přidaném oblouku má už stupeň 2). Například:



(a) Dokažte, že pro n počátečních puntíků má hra nanejvýš $3n - 1$ tahů (při jakékoli strategii hráčů).

(b)* Dokažte, že pro n počátečních puntíků má hra nejméně $2n$ tahů (při jakékoli strategii hráčů).

(c)* („Podvodní šprouti"[5]) Modifikujme hru následovně: Místo puntíků se kreslí křížky, a nové oblouky se připojují k ramenům křížků (vrcholy mohou tentokrát mít maximální stupeň 4). Na nový oblouk se přikresluje křížek přeškrtnutím. Viz obrázek:



Dokažte, že tato hra má vždy přesně $5n - 2$ tahů (takže se dá snadno předem určit kdo vyhraje).

6. Uvažme množinu L sestávající z n přímek v rovině (žádné 2 nejsou rovnoběžné, ale mnoho jich může procházet jedním bodem). Nakreslením těchto přímek vzniknou vrcholy (=průsečíky přímek), hrany (=části přímek mezi průsečíky, včetně nekonečných polopřímek), a stěny (=souvislé části roviny po odebrání přímek).

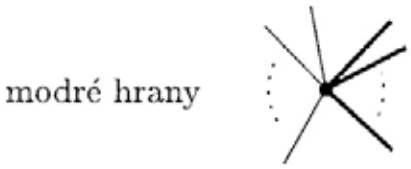
(a) Vyjádřete počet hran pomocí počtu vrcholů a počtu stěn.

(b) Dokažte, že pokud všechny přímky neprocházejí jediným bodem, potom existuje nejvýš n stěn ohraničených jen dvěma hranami.

[5] V originále „Brussels sprouts"; pro čtenáře, který by se chtěl věnovat překladům z angličtiny, může být užitečné vědět, že to znamená růžičková kapusta.

(c)* Dokažte, že pokud všechny přímky neprocházejí jedním bodem, pak existuje aspoň jeden průsečík, jímž procházejí právě 2 přímky (to je takzvaný *Sylvesterův problém*).

7.** Uvažme libovolný topologický rovinný graf. Předpokládejme, že každé hraně je přiřazena jedna ze dvou barev (červená nebo modrá). Ukažte, že existuje vrchol následujícího typu:



(červené hrany tvoří jeden souvislý úsek při obcházení vrcholu, a podobně modré hrany; jedna ze skupin hran může být i prázdná).

5.4 Barevnost mapy — problém 4 barev

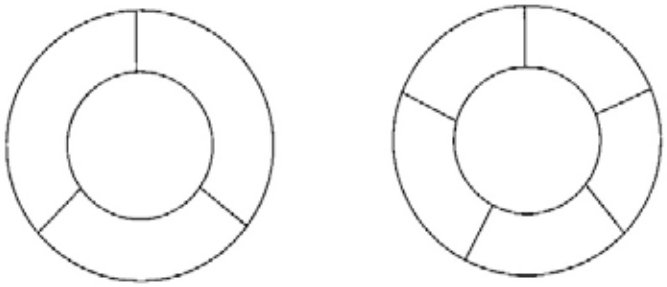
Uvažme politickou mapu, na níž jsou vyznačeny hranice států:

Předpokládejme, že každý stát tvoří souvislou oblast, ohraničenou nějakou topologickou kružnicí (proto jsme na naši schematickou mapu nenakreslili ostrovy jako Británie, Irsko, Sardinie, Sicílie, Korsika atd., a taky jsme vynechali Rusko — L.P. 1995 stát nesouvislý!). Dvě oblasti pokládáme za sousední, jestliže mají společný aspoň kousek hranice (t.j. nestačí, když se hranice dotýkají jen v jenom nebo několika bodech). Každý stát na takové mapě chceme vybarvit nějakou barvou, a to tak, že sousedící státy nikdy nedostanou stejnou barvu (jak je na politických mapách zvykem). Jaký minimální počet barev je potřeba? Pro uvedenou mapu stačí 4 barvy (zkuste takové obarvení najít!).

Jedním z nejznámějších kombinatorických problémů je následující otázka:

Problém čtyř barev: *Je možno každou mapu obarvit 4 barvami?*

Čtyři je určitě minimální počet barev, který připadá obecně v úvahu. To je ilustrováno výše uvedenou mapou (uvažte např. Lucembursko nebo Rakousko) a následujícími příklady:



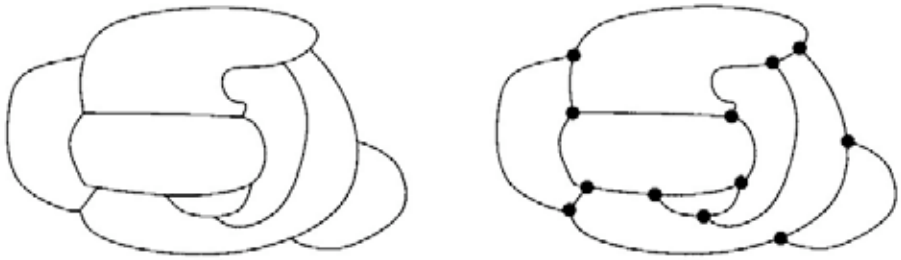
Zde dokážeme, že každou mapu lze obarvit 5 barvami. Přesto, že tento výsledek je znám téměř 100 let, problém čtyř barev byl rozřešen (kladně) teprve koncem 70. let. Moderní důkaz toho, že každou mapu lze obarvit 4 barvami, najde čtenář v práci [17]. Je velmi obtížný a podstatně závisí na probírání mnoha případů počítačem. Některé jeho základní myšlenky se ale objevují i ve (dvou) důkazech „věty o pěti barvách", jež vzápětí popíšeme.

Problém čtyř barev vypadá jako geometrický problém, ale dá se přeformulovat ryze kombinatoricky. Barvení map totiž jednoduše souvisí s barvením grafů. Nejdříve definujeme barevnost pro libovolný graf:

5.4.1 Definice (Barevnost grafu). *Buď $G = (V, E)$ graf, k přirozené číslo. Zobrazení $b : V \to \{1, 2, \ldots, k\}$ nazveme* obarvením grafu G pomocí k barev, *pokud pro každou hranu $\{x, y\} \in E$ platí $b(x) \neq b(y)$.* Barevnost *grafu G, označovaná $\chi(G)$, je minimální počet barev potřebný pro obarvení G.*

Barevnost grafu patří mezi základní kombinatorické pojmy. V našem úvodním textu ji však zmíníme pouze v tomto článku.

Matematicky můžeme mapu chápat jako nakreslení nějakého rovinného grafu, přičemž státy na mapě jsou stěny tohoto grafu (vrcholy grafu budou body, ležící na hranici alespoň 3 států, a hrany jsou odpovídající části oblouků mezi jednotlivými vrcholy):

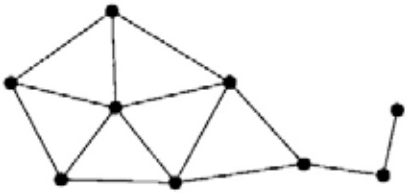


Je vidět, že přitom mohou vzniknout i násobné hrany (viz část 3.5).

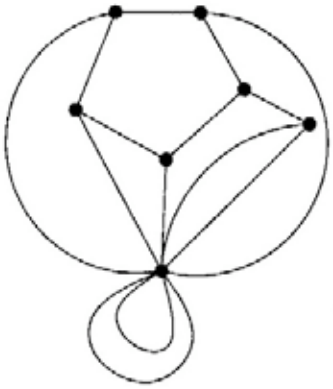
Abychom převedli problém barvení mapy (t.j. barvení stěn topologického rovinného grafu) na barevnost grafu ve smyslu právě uvedené definice, zavedeme tzv. duální graf. Přitom budeme také obecně potřebovat násobné hrany a smyčky; připomeňme si tedy jeden způsob jejich zavedení: graf s násobnými hranami můžeme chápat jako trojici (V, E, ε), kde V, E jsou nějaké (disjunktní) množiny, a $\varepsilon : E \to \binom{V}{2} \cup V$ je zobrazení (přiřazující hraně dvojici jejích konců, příp. smyčce její jediný vrchol), viz též část 3.5.

5.4.2 Definice. *Nechť $G = (V, E)$ je topologický rovinný graf, tj. rovinný graf s pevně zvoleným rovinným nakreslením. Označme S množinu stěn topologického rovinného grafu G. Definujme graf tvaru (S, E, ε), kde ε se definuje předpisem $\varepsilon(e) = \{S_i, S_j\}$, jestliže hrana e je společnou hranicí stěn S_i a S_j (přičemž může být $S_i = S_j$, jestliže z obou stran hrany e je táž stěna). Tento graf (S, E, ε) nazýváme* (geometrickým) duálem *grafu G a značíme jej G^*.*

Příklad:

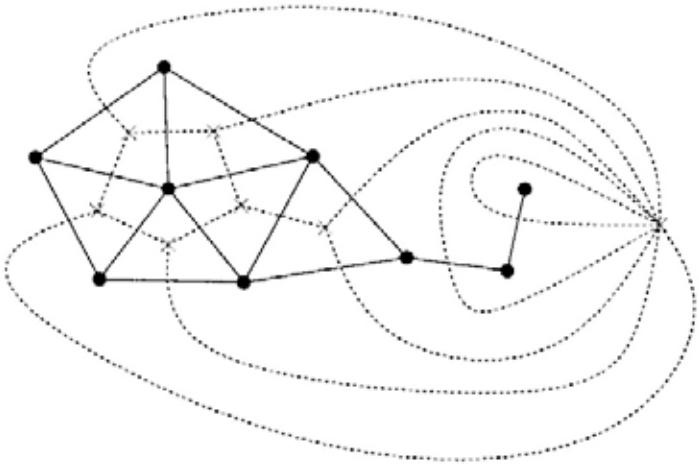


G



G^*

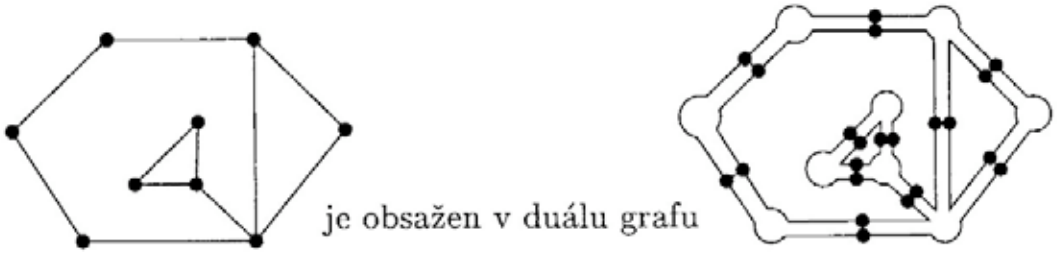
Graf G^* můžeme znázornit společně s nakreslením grafu G. Uvnitř každé stěny S grafu G zvolíme bod b_S, a každé hraně e přiřadíme oblouk, protínající hranu e a spojující body b_S a $b_{S'}$, kde S a S' jsou stěny přiléhající k hraně e. Tím získáme nakreslení grafu G^*:



Z tohoto způsobu kreslení duálního grafu plyne jeho rovinnost (toto je ovšem jedno z míst, kde trochu spoléháme na intuitivní představu a nepodáváme přesný důkaz). Další příklady najde čtenář na obr. 5.1: grafy krychle a pravidelného osmistěnu jsou navzájem duální, podobně grafy dvanáctistěnu a dvacetistěnu, a konečně graf pravidelného čtyřstěnu (čili K_4) je duální sám k sobě.

Máme-li tedy mapu, již chápeme jako nakreslení nějakého grafu G, potom otázka obarvitelnosti mapy pomocí k barev je ekvivalentní s obarvitelností duálního grafu G^* pomocí k barev. Na druhé straně

platí, že každý rovinný graf se vyskytne jako podgraf vhodného duálního grafu. Důkaz naznačíme pouze obrázkem:



Takto lze převést problematiku barvení map na na otázky týkající se barevnosti rovinných grafů. Speciálně můžeme přeformulovat:

Problém čtyř barev: *Platí $\chi(G) \leq 4$ pro každý rovinný graf G?*

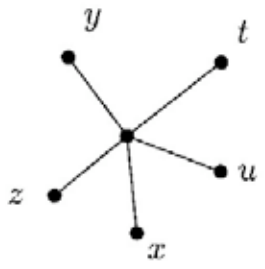
Dokážeme slabší výsledek:

5.4.3 Tvrzení (Věta o 5 barvách). *Pro každý rovinný graf G platí $\chi(G) \leq 5$.*

První důkaz. Postupujeme indukcí dle počtu vrcholů grafu $G = (V, E)$. Pro $|V| \leq 5$ je tvrzení triviální.

Z části 5.3 víme, že v každém rovinném grafu existuje vrchol v stupně ≤ 5. Jestliže $\deg_G(v) < 5$, potom uvažme graf $G - v$ a použijme pro něj indukčního předpokladu: je-li graf $G - v$ obarvený pomocí barev $1, 2, \ldots, 5$, potom v přiřaďme nějakou barvu $i \in \{1, 2, \ldots, 5\}$, jež se nevyskytuje mezi barvami (nejvýš 4) sousedů vrcholu v. Tak dostaneme obarvení grafu G. (Takový argument vlastně již ukazuje, že barevnost rovinného grafu je nejvýš 6.)

Zbývá vyšetřit případ, kdy $\deg_G(v) = 5$. Uvažme graf G s pevně zvoleným rovinným nakreslením, a nechť t, u, x, z, y jsou vrcholy spojené s vrcholem v hranou, vypsané v pořadí, v němž příslušné hrany vycházejí z vrcholu v (např. ve směru hodinových ručiček).



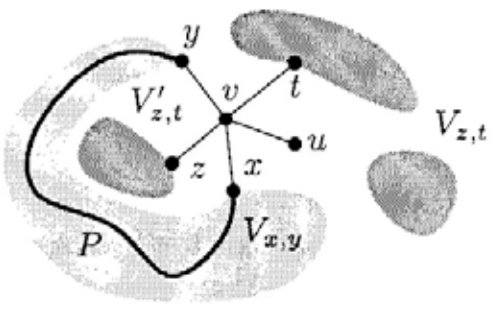
Uvažme opět obarvení b grafu $G' = G - v$ pomocí 5 barev (zaručené indukčním předpokladem). Jestliže $|\{b(u), b(x), b(y), b(z), b(t)\}| < 5$, potom můžeme vrcholu v přiřadit barvu různou od barev jeho sousedů (stejně jako v první části důkazu). Předpokládejme tedy, že sousedi mají 5 různých barev. Uvažme vrcholy x a y, a nechť $V_{x,y}$ je množina všech vrcholů grafu G', které mají buď barvu $b(x)$ nebo barvu $b(y)$. Zřejmě $x, y \in V_{x,y}$. Rozlišíme dva případy podle toho, zda existuje v grafu G cesta z x do y, používající jen vrcholů z množiny $V_{x,y}$.

1. Taková cesta neexistuje. Označme $V'_{x,y}$ množinu těch vrcholů $s \in V(G')$, které jsou v grafu G' spojeny s vrcholem x cestou, používající pouze vrcholů z množiny $V_{x,y}$. Definujme nově obarvení b' předpisem:

$$b'(s) = \begin{cases} b(s) & \text{pokud } s \notin V'_{x,y} \\ b(y) & \text{pokud } s \in V'_{x,y} \text{ a } b(s) = b(x) \\ b(x) & \text{pokud } s \in V'_{x,y} \text{ a } b(s) = b(y) \end{cases}$$

   (t.j., na množině $V'_{x,y}$ zaměníme barvy). Zřejmě b' je opět obarvení, a protože $b'(x) = b'(y) = b(y)$, můžeme položit $b'(v) = b(x)$. Tedy b' je obarvení grafu G 5 barvami.

2. Jestliže existuje cesta P z x do y, jejíž všechny vrcholy jsou prvky množiny $V_{x,y}$, potom uvážíme dvojici vrcholů t a z. Definujme množinu $V_{t,z}$ jako množinu všech těch vrcholů, které jsou obarveny pomocí barev $b(t)$ a $b(z)$. Zřejmě $V_{x,y}$ a $V_{t,z}$ jsou disjunktní množiny. Nakreslení cesty P spolu s hranami $\{v, x\}$ a $\{v, y\}$ tvoří kružnici:



Ta má jeden z bodů z, t uvnitř a druhý vně, a proto každá cesta ze z do t musí používat některého z vrcholů zmíněné kružnice. Tudíž neexistuje cesta ze z do t používající pouze vrcholů množiny $V_{z,t}$, a můžeme tedy zkonstruovat obarvení grafu G 5 barvami podobně jako v případě 1 (jenom místo vrcholů x, y začneme s vrcholy t, z). □

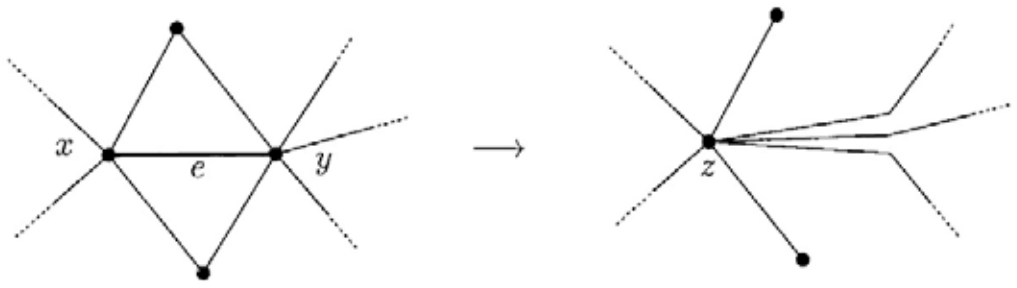
Kontrakce hran. Než začneme s druhým důkazem, zavedeme další důležitou grafovou operaci. Buď $G = (V, E)$ graf a $e \in E$ jeho hrana. Kontrakce hrany e znamená, že oba vrcholy hrany e „slepíme" do jednoho nového vrcholu, a potom odstraníme případné násobné hrany, které by slepením vznikly. Výsledný graf budeme značit $G.e$, a formálně bude definován takto: $G.e = (V', E')$, kde $e = \{x, y\}$ a

$$V' = (V \setminus \{x, y\}) \cup \{z\}$$
$$E' = \{e \in E;\ e \cap \{x, y\} = \emptyset\} \cup$$
$$\{\{z, t\};\ t \in V \setminus \{x, y\},\ \{t, x\} \in E \text{ nebo } \{t, y\} \in E\};$$

přitom $z \notin V$ značí nový vrchol.

5.4.4 Lemma. *Je-li G rovinný graf a $e \in E(G)$, je graf $G.e$ opět rovinný.*

Neformální důkaz. Viz obrázek:



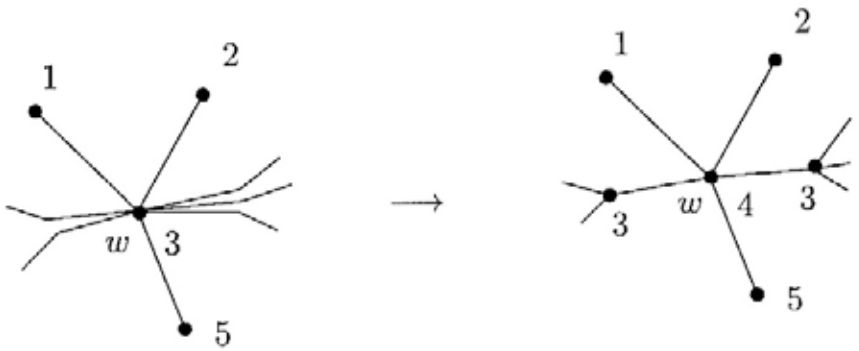
□

Druhý důkaz tvrzení 5.4.3. Postupujeme opět indukcí podle počtu vrcholů grafu $G = (V, E)$. Začneme stejně jako v prvním důkazu.

Můžeme tedy předpokládat, že $G = (V, E)$ je rovinný graf s alespoň 6 vrcholy, v němž každý vrchol má stupeň ≥ 5. Zvolme vrchol v stupně 5. Protože graf G je rovinný, neobsahuje graf K_5, a tedy existuje dvojice sousedů vrcholu v, jež netvoří hranu. Označme tyto sousedy x, y, a zbývající 3 sousedy t, u a z. Uvažme graf G' vzniklý z G kontrakcí hran $\{x, v\}$ a $\{y, v\}$ (t.j. trojice vrcholů x, y, v je nahrazena jediným novým vrcholem w). Tento graf je opět rovinný, a má méně vrcholů než G, neboli podle indukčního předpokladu existuje nějaké jeho obarvení b' pomocí 5 barev. V této situaci definujme obarvení b grafu G takto:

$$b(s) = \begin{cases} b'(s) & s \notin \{x, y, v\} \\ b'(w) & s = x \text{ nebo } s = y \\ i \in \{1, \ldots, 5\} \setminus \{b(x), b(u), b(t), b(z)\} & s = v. \end{cases}$$

Viz obrázek:



situace v G' situace v G

Je snadné nahlédnout, že takto definované zobrazení b je skutečně obarvením grafu G. □

Poznamenejme nakonec, že podobně jako pro rovinné grafy můžeme zkoumat otázku barevnosti grafů na jiných plochách. Tato otázka je dnes beze zbytku vyřešena: maximální barevnost grafu G rodu k je rovna číslu

$$\left\lfloor \frac{7 + \sqrt{1 + 48k}}{2} \right\rfloor$$

(kde $\lfloor x \rfloor$ značí dolní celou část čísla x). Je pozoruhodné, že případ rodu 0 (t.j. rovinných grafů) je zdaleka nejtěžší — pro ostatní rody byl tento výsledek dokázán dávno před řešením problému čtyř barev.

Cvičení

1. Dokažte $\chi(G) \leq 1 + \max\{\deg_G(x); x \in V(G)\}$ pro každý graf G.

2. (a) Na základě každého ze dvou uvedených důkazů formulujte algoritmus pro obarvení daného rovinného grafu 5 barvami. Můžete předpokládat, že je dáno rovinné nakreslení. (Toto cvičení je dobrý test na správné pochopení důkazů.)

   (b)* Rozpracujte některý z algoritmů podrobně, a pokuste se dosáhnout co nejmenší časové složitosti. Podaří se vám dosáhnout složitosti $O(n)$ pro graf s n vrcholy (za předpokladu vhodné vstupní reprezentace rovinného nakreslení)?

3. Pro graf G položte $\delta(G) = \min\{\deg_G(v); v \in V\}$. Dokažte $\chi(G) \leq 1 + \max\{\delta(G'); G' \subseteq G\}$ (kde $G' \subseteq G$ značí, že G' je podgrafem G).

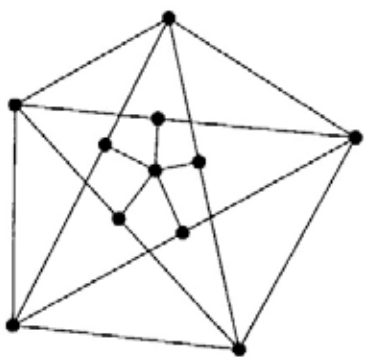
4.* Graf G nazveme *vnějškově rovinným*, existuje-li jeho nakreslení, v němž hranice některé ze stěn obsahuje všechny vrcholy. Dokažte, že každý vnějškově rovinný graf má barevnost nejvýš 3.

5. Buď G rovinný graf neobsahující trojúhelník. Dokažte $\chi(G) \leq 4$.

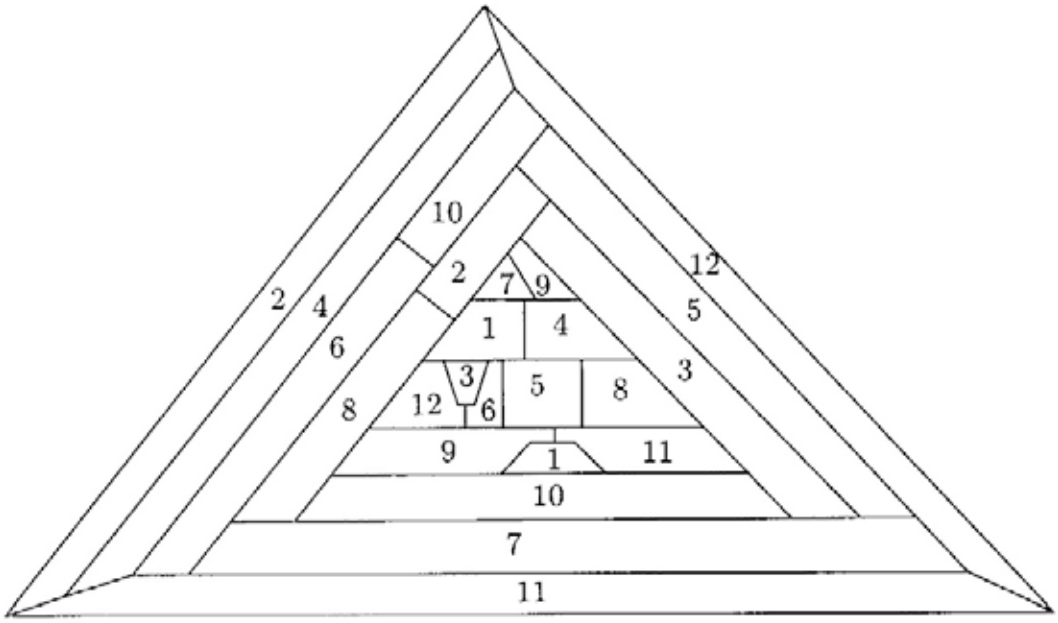
6. (a)* Uvažme rovinný graf, jehož všechny stupně jsou sudé. Ukažte, že mapa vzniklá jeho rovinným nakreslením se dá obarvit dvěma barvami.

   (b)* Pomocí (a) ukažte, že neexistuje žádný topologický rovinný graf, jehož všechny stupně jsou sudé a jehož všechny stěny jsou trojúhelníky, až na jednu, která je pětiúhelník.

7. Dokažte, že graf K_4 lze dostat postupnými kontrakcemi hran z následujícího grafu:



8. Následující obrázek je příklad mapy států, každý se 2 oblastmi. Dokažte, že barevnost této mapy je 12 (pro každý stát jsou obě jeho oblasti obarveny stejnou barvou).



9. Uvažte mapu M, kde každý stát má nejvýše k oblastí. Použitím cvičení 3 ukažte, že barevnost takové mapy je menší nebo rovna číslu $6(k+1)$ (pro každý stát jsou všechny jeho oblasti obarveny stejnou barvou).

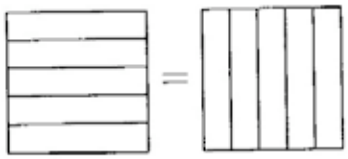
6

Počítání dvěma způsoby

Počítání dvěma způsoby používali například účetní, když ještě neměli počítače. Když chtěli bezchybně sečíst tabulku čísel, sčítali jednou napřed po sloupcích a jednou napřed po řádcích; pokud počítali správně, vyšlo totéž. Matematicky vyjádřeno, je-li A libovolná matice $n \times m$, platí

$$\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij} = \sum_{j=1}^{m}\sum_{i=1}^{n} a_{ij},$$

schematicky



Jinak řečeno, v takovéto dvojité sumě můžeme podle potřeby zaměnit pořadí sumace. Na této prosté myšlence je založeno mnoho matematických triků a důkazů; v těch složitějších jsou pochopitelně navíc další nápady a obraty, hlavně se většinou musí přijít na to, co vlastně počítat dvěma způsoby.

6.1 Princip sudosti

V části 3.4 jsme nahlédli, že *libovolný graf má sudý počet vrcholů lichého stupně*. (To platí i pro grafy s násobnými hranami.) Důkaz byl

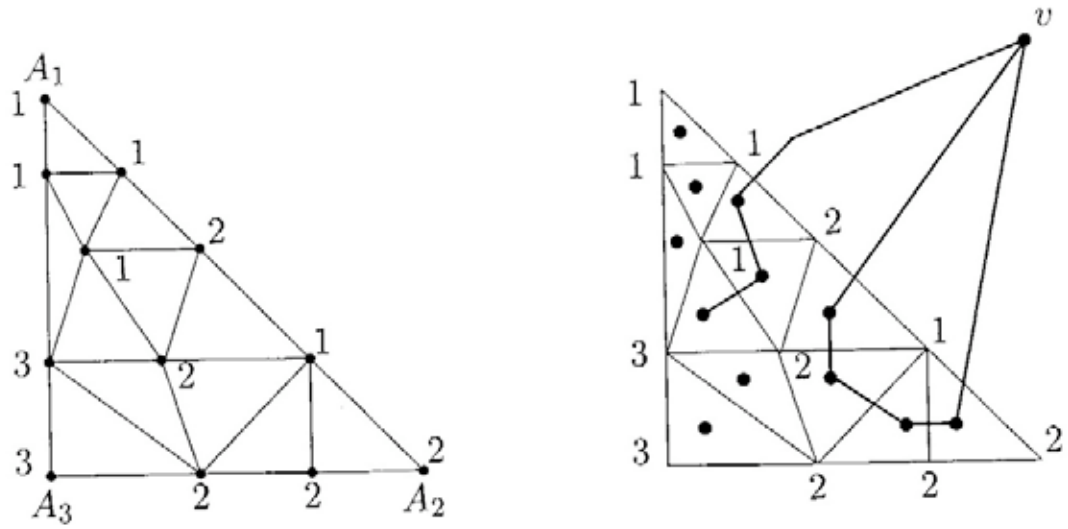
vlastně typické počítání dvěma způsoby (počítali jsme „konce hran"). Pomocí tohoto tvrzení jsme mohli někdy snadno vyloučit některé vektory jako možné skóre grafu, třeba vektor $(3,3,3,3,3)$. Tvrzení lze však použít i mnohem zajímavěji, například na důkaz existence nějakého objektu. K takovému účelu je vyslovíme v takovémto tvaru: *Víme-li, že graf G má aspoň jeden vrchol lichého stupně, potom musí mít aspoň 2 takové vrcholy.* Aplikace následuje.

Nakresleme do roviny velký trojúhelník s vrcholy označenými A_1, A_2, A_3 a rozdělme jej libovolně na konečný počet menších trojúhelníčků (jako na obr. 6.1(a)). Žádný trojúhelníček nesmí mít vrchol uvnitř strany jiného trojúhelníčku, t.j. díváme-li se na obrázek jako na nakreslení rovinného grafu, jsou všechny vnitřní stěny trojúhelníky. Přiřaďme dále každému vrcholu velkého i malých trojúhelníků jedno z čísel 1,2,3: vrchol A_i dostane vždy číslo i, $i = 1,2,3$, a všechny vrcholy ležící na straně A_iA_j velkého trojúhelníka dostanou jen čísla i a j; mimo těchto pravidel je přiřazení je naprosto libovolné.

6.1.1 Tvrzení (Spernerovo lemma — rovinná verze). *V popsané situaci vždy existuje trojúhelníček, jehož vrcholy dostanou čísla 1, 2 a 3.*

Důkaz. Definujeme pomocný graf G, viz obr. 6.1(b). Jeho vrcholy budou stěny nakreslené triangulace, t.j. všechny trojúhelníčky a také vnější stěna. Na obrázku jsme vrcholy znázornili kroužky zakreslenými do příslušných stěn; vrchol vnější stěny je označen v. Dva vrcholy, t.j. stěny, budou spojeny hranou, pokud spolu hraničí přes stranu některého trojúhelníčku, a pokud *koncové vrcholy této strany mají čísla 1 a 2.* To se týká i vnějšího vrcholu v: ten bude spojen se všemi trojúhelníčky přiléhajícími k obvodu velkého trojúhelníka stranou 12.

Stupeň trojúhelníčku v grafu G je nenulový pouze tehdy, je-li jeden z vrcholů očíslován 1 a jeden 2. Má-li zbývající vrchol také číslo 1 nebo 2, je stupeň 2. Pokud zbývající vrchol má číslo 3, je stupeň 1, a *to je jediný případ, kdy je stupeň lichý.* Ukážeme nyní, že vrchol v (vnější stěna) má v grafu G lichý stupeň; tím pádem existuje v G ještě jiný vrchol lichého stupně, a to je hledaný trojúhelníček očíslovaný 1,2,3.



Obrázek 6.1: Situace ve Spernerově lemmatu (a), odpovídající graf stěn (b).

Hrany grafu G mohou zřejmě křižovat pouze stranu A_1A_2 velkého trojúhelníka. Podle pravidel očíslování jsou na této straně povoleny jen vrcholy trojúhelníčků s čísly 1 a 2. Napíšeme-li libovolnou posloupnost jedniček a dvojek začínající 1 a končící 2, potom počet míst, kde končí úsek jedniček a začíná úsek dvojek nebo obráceně je lichý (jdeme-li odleva doprava, po sudém počtu změn mezi jedničkami a dvojkami jsme v jedničce). Proto je stupeň v je lichý. □

Spernerovo lemma není jen samoúčelná hříčka, s jeho pomocí se dá dokázat tzv. Brouwerova věta o pevném bodě. Než řekneme, co tvrdí, uvedeme velmi jednoduchou větu o pevném bodě jako motivaci.

6.1.2 Tvrzení. *Pro každou spojitou funkci* $f : [0,1] \to [0,1]$ *existuje bod* $x \in [0,1]$ *takový, že* $f(x) = x$.

Takové x se jmenuje *pevný bod* funkce f. Tvrzení můžeme dokázat takto: funkce $g(x) = f(x) - x$ je spojitá, $g(0) \geq 0$, $g(1) \leq 0$ a intuitivně se zdá celkem zřejmé, že graf spojité funkce g nemůže osu x nijak přeskočit a tedy ji musí protnout, čili g nabývá někde v intervalu $[0,1]$ hodnoty 0. Odvodit to logicky přesně z vlastností reálných čísel dá trochu práce, příslušné tvrzení se jmenuje Darbouxova věta.

Obecně, věty o pevném bodě tvrdí, že za jistých okolností má nějaká funkce f pevný bod, t.j. existuje x takové, že $f(x) = x$. Taková tvrzení jsou klíčová v mnoha oblastech matematiky (i aplikované). Odvozují se z nich různé výsledky zaručující, že nějaká rovnice má řešení a podobně, a hrají dokonce roli například i v teorii sémantiky programů.

V Brouwerově větě o pevném bodě je jednorozměrný interval z tvrzení 6.1.2 nahrazen trojúhelníkem v rovině, čtyřstěnem v třídimenzionálním prostoru nebo jejich analogií ve vyšších dimenzích. Zde dokážeme pouze dvoudimenzionální verzi (protože jsme dokázali jenom dvoudimenzionální Spernerovo lemma, ale viz cv. 2). Důkaz patří spíše do matematické analýzy. Zde se jej pokusíme formulovat tak, abychom z analýzy potřebovali co nejméně; věci, které potřebovat budeme, připomeneme.

Nechť Δ označuje trojúhelník v rovině. Pro určitost vezmeme pravoúhlý rovnoramenný trojúhelník s vrcholy $A_1 = (0,1)$, $A_2 = (1,0)$ a $A_3 = (0,0)$ (jako na obr. 6.1(a)). Funkce $f : \Delta \to \Delta$, jak je nejspíš čtenáři známo, se nazývá *spojitá*, pokud pro každé $a \in \Delta$ a pro každé $\varepsilon > 0$ existuje $\delta > 0$ tak, že je-li $b \in \Delta$ libovolný bod vzdálený od a nejvýš o δ, potom $f(a)$ a $f(b)$ mají vzdálenost nejvýš ε (heslovitě: f zobrazuje blízké body na blízké body).

6.1.3 Věta (Brouwerova věta o pevném bodě v rovině). *Každá spojitá funkce $f : \Delta \to \Delta$ má pevný bod.*

Důkaz. Zavedeme tři pomocné reálné funkce $\beta_1, \beta_2, \beta_3$ na trojúhelníku Δ: Je-li $a \in \Delta$ bod o souřadnicích (x, y), bude

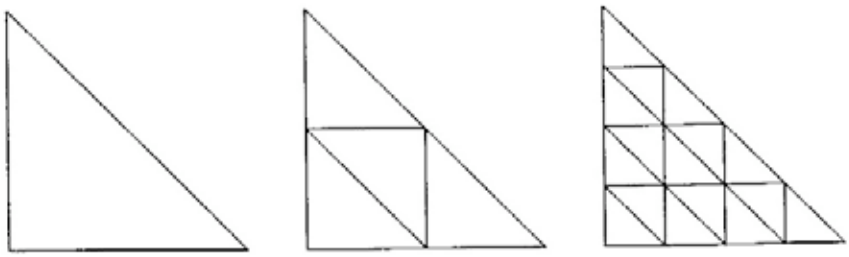
$$\beta_1(a) = y, \quad \beta_2(a) = x, \quad \beta_3(a) = 1 - x - y.$$

Podstatné vlastnosti těchto funkcí, které si hned napíšeme, jsou $\beta_i(a) \geq 0$ a $\beta_1(a) + \beta_2(a) + \beta_3(a) = 1$ pro každé $a \in \Delta$.

Dále definujeme 3 množiny $M_1, M_2, M_3 \subseteq \Delta$, $M_i = \{a \in \Delta;\ \beta_i(a) \geq \beta_i(f(a))\}$, $i = 1, 2, 3$. Pro představu, M_i je množina těch bodů, které funkce f nevzdálí od strany protilehlé vrcholu A_i.

Všimneme si, že každý bod $p \in M_1 \cap M_2 \cap M_3$ je pevným bodem funkce f. (Pokud by funkce f bodem p někam pohnula, vždy jej vzdálí od některé ze stran; formálně přesný důkaz přenecháváme čtenářově píli.) Naším cílem je tedy najít bod ve zmíněném průniku.

Uvažme posloupnost jemnějších a jemnějších triangulací trojúhelníku Δ (první 3 triangulace jsou nakresleny na obr. 6.2). Pro každou triangulaci očíslujeme vrcholy trojúhelníčků čísly 1,2,3. Budeme požadovat, aby vrchol očíslovaný i patřil do množiny M_i, a dále aby očíslování bylo



Obrázek 6.2: Zjemňování triangulace.

podle pravidel ve Spernerově lemmatu. Musíme se přesvědčit, že to vždy jde udělat.

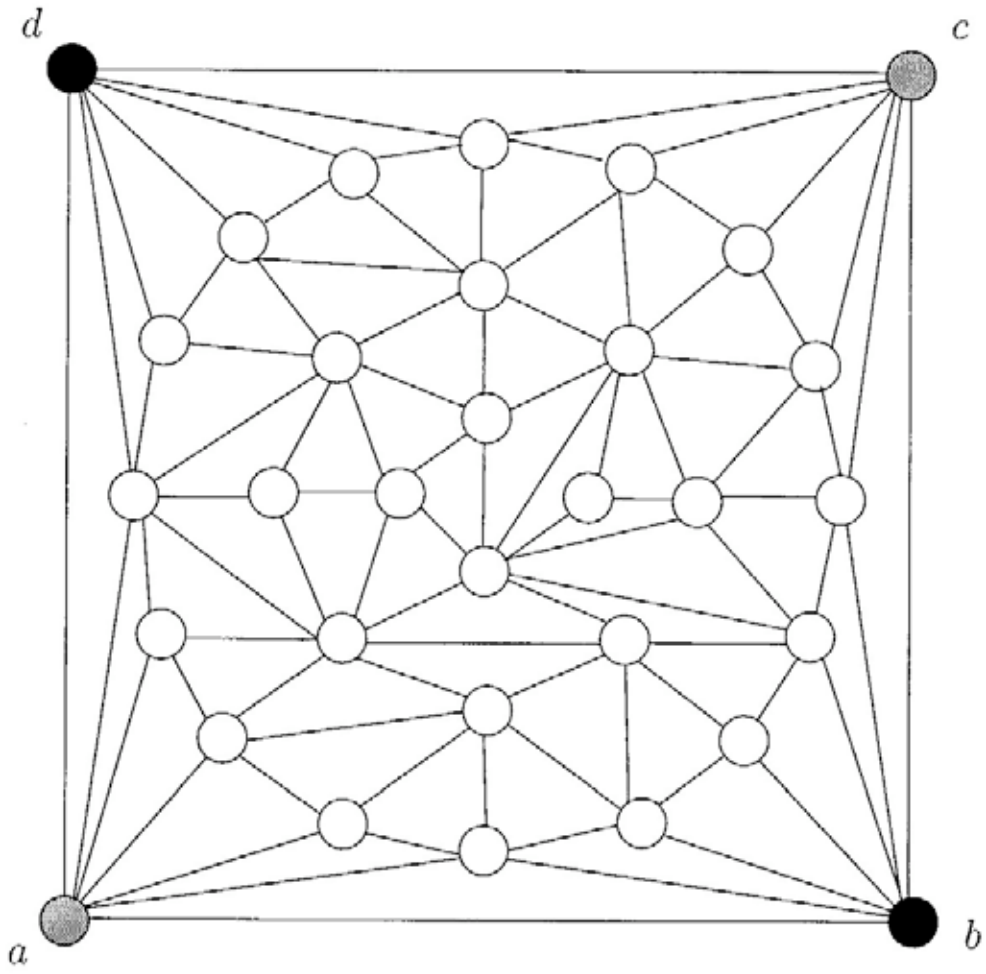
Vrchol A_1 je vůbec nejvzdálenější od své protilehlé strany, takže funkce f jej nemůže ještě vzdálit. Proto $A_1 \in M_1$, takže tomuto vrcholu můžeme přidělit číslo 1 (podobně pro A_2, A_3). Každý bod a na straně A_1A_2 má $\beta_1(a) + \beta_2(a) = 1$, tedy $f(a)$ nemůže zároveň splňovat $\beta_1(f(a)) > \beta_1(a)$ a $\beta_2(f(a)) > \beta_2(a)$. Odtud $a \in M_1 \cup M_2$, neboli nic nám nebrání očíslovat vrcholy na straně A_1A_2 jen jedničkami a dvojkami (podobně pro ostatní strany). Konečně každý bod Δ patří do aspoň jedné z množin M_i, protože žádný bod nelze vzdálit od všech tří stran současně (formální ověření opět vynecháme).

Tím jsme připraveni aplikovat Spernerovo lemma 6.1.1. Každá z triangulací má tedy trojúhelníček očíslovaný 1,2,3. Označme vrcholy nějakého takového trojúhelníčku pro j-tou z oněch zjemňujících se triangulací symboly $a_{j,1}$, $a_{j,2}$ a $a_{j,3}$, a to ještě tak, že vždy $a_{j,i} \in M_i$.

Uvážíme posloupnost bodů $(a_{1,1}, a_{2,1}, a_{3,1}, \ldots)$. Tady potřebujeme, že z této posloupnosti můžeme vybrat nějakou nekonečnou konvergentní podposloupnost. Ale z každé posloupnosti bodů v trojúhelníku se dá vybrat nekonečná konvergentní podposloupnost (tato vlastnost trojúhelníka — sdílená například i každou omezenou a uzavřenou podmnožinou roviny — se nazývá *kompaktnost*). Řekněme, že jsme vybrali takovou podposloupnost $(a_{j_1,1}, a_{j_2,1}, a_{j_3,1}, \ldots)$, $j_1 < j_2 < j_3 < \ldots$, a bod, k němuž konverguje, pojmenujeme p.

Bod p náleží do množiny M_1. Podle definice M_1 totiž pro každé $a_{j_k,1}$ máme $\beta_1(a_{j_k,1}) \geq \beta_1(f(a_{j_k,1}))$, a podle základních vět o limitách se taková neostrá nerovnost mezi spojitými funkcemi zachovává přechodem k limitě.

Poněvadž průměr trojúhelníčků v použitých triangulacích se zmenšoval k nule, musí i posloupnosti ostatních vrcholů, to znamená $(a_{j_1,2}$,



Obrázek 6.3: Hrací plán.

$a_{j_2,2}, a_{j_3,2}, \ldots)$ a $(a_{j_1,3}, a_{j_2,3}, a_{j_3,3}, \ldots)$ konvergovat k bodu p, takže také $p \in M_2$ a $p \in M_3$. Bod p je kýžený pevný bod funkce f. □

Složitější věty podobného typu (jako například, že zobrazíme-li povrch koule spojitě do roviny, nějaké dva protilehlé body se musí zobrazit na sebe) se dokazují v odvětví matematiky zvaném *algebraická topologie*. Potřebuje se k tomu většinou poměrně složitý technický aparát, ale v jádru takových důkazů je často nějaký argument založený na sudosti/lichosti a pod.

Ukážeme ještě jeden pěkný příklad úvahy pomocí principu sudosti. Budeme analyzovat jednu hru (podobnou hře HEX). Na hracím plánu, jaký je nakreslen na obr. 6.3 (ale triangulace uvnitř čtverce může být

libovolná), se hraje následující hra. Hráči pro sebe zabírají políčka (tj. kroužky na hracím plánu); např. A je zamalovává světlejší barvou — na našem obrázku šedou — a B černě. Na začátku má A zabraná a a c. B má b a d, střídají se v tazích, A začíná, a v jednom tahu může hráč zabrat jedno libovolné dosud nezabrané políčko. Hráč A vyhraje, podaří-li se mu obsadit všechna políčka nějaké cesty z a do c, B usiluje o cestu z b do d. Kdyby se stalo, že hráč, který je na tahu, už nemá kam táhnout, ale ani jeden z hráčů svoji cestu nedokončil, hra by končila remízou.

6.1.4 Tvrzení. *Tato hra na hracím plánu uvedeného typu (vnější stěna čtverec, všechny vnitřní trojúhelníky) nemůže skončit remízou.*

Důkaz. Pro spor předpokládejme, že remíza nastala, nechť A je množina políček zabraných hráčem A a B množina políček zabraných hráčem B.

Označíme políčka čísly 1,2,3 podle takovéhoto pravidla: Jedničkou bude označeno políčko, které je v A a vede z něj cesta do políčka a, jejíž všechna políčka leží v A. Dvojkou označíme políčka z B, která lze spojit s b cestou ležící celou v B, a trojka připadne zbývajícím políčkům. Podle předpokladu pak budou c i d mít označení 3 (jinak by jeden z hráčů býval vyhrál).

Nyní se ukáže, že existuje některá vnitřní trojúhelníková stěna, jejíž políčka jsou označena 1,2 a 3. To bude spor: Políčko s číslem 3 nemůže být v A, protože sousedí s políčkem označeným 1, do kterého tedy vede cesta z a používající jen políček v A, a takovou cestu bychom mohli protáhnout do onoho políčka s číslem 3 (a to by správně mělo mít číslo 1). Z podobného důvodu není políčko s číslem 3 ani v B — spor.

Jak se ukáže existence trojúhelníka označeného 1,2,3? Přesně jako Spernerovo lemma. Ještě jedno velmi podobné tvrzení je ve cvičení 1. □

Poznamenejme, že uvedený důkaz podstatně využívá toho, že všechny vnitřní stěny hracího plánu jsou trojúhelníkové, a vnější stěna

má jen 4 vrcholy a, b, c, d. Povolíme-li například čtyřúhelníkové vnitřní stěny, remíza v principu nastat může.

Cvičení

1. Mějme nakreslený rovinný graf, jehož každá stěna včetně vnější je trojúhelník (t.j., má 3 vrcholy). Každému vrcholu přiřadíme, zcela libovolně, některé z čísel 1,2,3. Dokažte, že existuje sudý počet stěn, jejichž vrcholy mají všechna 3 čísla.

2. (Spernerovo lemma v dimenzi 3)

   (a) Uvažme čtyřstěn $A_1A_2A_3A_4$, a nějaké jeho rozdělení na malé čtyřstěny tak, že každá stěna každého z malých čtyřstěnů buď leží na stěně velkého čtyřstěnu, nebo tvoří zároveň stěnu ještě jednoho malého čtyřstěnu. Očíslujeme vrcholy malých čtyřstěnů čísly 1,2,3,4 tak, že A_i dostane i, na hraně A_iA_j se vyskytují pouze i a j, a ve stěně $A_iA_jA_k$ jenom i, j a k. Dokažte, že potom existuje malý čtyřstěn očíslovaný 1,2,3,4.

   (b) Vyslovte a dokažte 3-dimenzionální verzi Brouwerovy věty o pevném bodě (o zobrazení čtyřstěnu do sebe).

3. K tématu vět o pevném bodě náleží dosti známá úloha o turistovi stoupajícím na horu. Turista tedy jednoho dne ráno v 6:00 začne stoupat na horu. Na vrchol dorazí v 6:00 večer, přenocuje tam (v budce k tomu účelu tam vystavěné, řekněme) a druhý den zase v 6:00 vyrazí po přesně stejné trase zpět, cestou se zastavuje, rozhlíží a podobně, takže do výchozího místa přijde zase v 6 večer. Má se dokázat, že na některém místě trasy byl v oba dny přesně ve stejný čas.

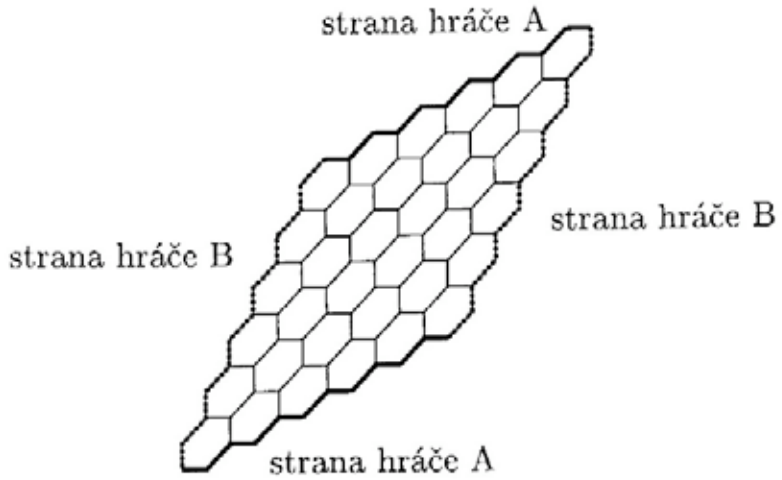
4. Uvažme hru jako v tvrzení 6.1.4.

   (a)* Dokažte, že vždy buď hráč A nebo hráč B má vyhrávající strategii (t.j., pokud neudělá chybu, vyhraje, ať už druhý hraje jakkoli).

   (b) Najděte příklad hracího plánu (splňující podmínky jako v tvrzení 6.1.4) takového, že vyhrávající strategii má hráč B.

   (c)* Dokažte, že je-li hrací plán symetrický vzhledem k otočení o pravý úhel kolem středu (t.j. jeví se stejně z pohledu hráče A i hráče B), potom má vyhrávající strategii vždy hráč A.

5. Hru HEX, jak možná čtenář ví, vynalezl Piet Hein. Hrací plán vypadá zhruba následovně:



Hráči střídavě obsazují prázdná políčka svými figurkami. Cílem hráče A je spojit jeho dvě strany souvislým řetězcem políček, a podobně B chce spojit své dvě strany. Objevte a vysvětlete souvislost této hry s verzí hry HEX diskutované v textu.

6.2 Spernerova věta o nezávislém systému množin

Ano, v této kapitole potkáváme jméno Sperner už podruhé, ale Spernerova věta, již dokážeme, bude o něčem zcela jiném než Spernerovo lemma z předchozí části. Bude o n-prvkové množině X a nějakém systému $\mathcal{M}$ jejích podmnožin. Systém $\mathcal{M}$ nazveme *nezávislý*, pokud v něm nejsou žádné dvě různé množiny A, B takové, že $A \subset B$. Než budete číst dál, zkuste najít nezávislý systém množin na čtyřprvkové množině. Jaký největší počet množin může takový systém obsahovat?

6.2.1 Věta (Spernerova věta). *Libovolný nezávislý systém podmnožin n-prvkové množiny má nejvýš $\binom{n}{\lfloor n/2 \rfloor}$ množin.*

To je vlastně věta o částečně uspořádaných množinách. Uvažme totiž množinu 2^X (t.j., systém všech podmnožin množiny X). Relace $\subseteq$, „býti podmnožinou“, je částečným uspořádáním na množině 2^X; je to dokonce jeden z nejdůležitějších příkladů částečně uspořádaných množin, viz část 1.7. Nezávislý systém podmnožin je množinou po dvou neporovnatelných prvků v uspořádané množině $(2^X, \subseteq)$. Množina po dvou neporovnatelných prvků v částečně uspořádané množině

se zpravidla nazývá *antiřetězec*. Spernerova věta tedy omezuje maximální možnou velikost antiřetězce v $(2^X, \subseteq)$.

Spernerova věta dává nejlepší možný horní odhad, neboť opravdu existují nezávislé systémy s právě $\binom{n}{\lfloor n/2 \rfloor}$ množinami. Jeden takový nezávislý systém je systém všech podmnožin množiny X velikosti právě $\lfloor n/2 \rfloor$.

Důkaz věty 6.2.1. Nejprve definujeme, co je to *řetězec* podmnožin množiny X: je to každá posloupnost podmnožin X tvaru $A_1 \subset A_2 \subset \ldots \subset A_k$. V řeči uspořádání na 2^X je to prostě lineárně uspořádaná podmnožina částečně uspořádané množiny $(2^X, \subseteq)$.

Základní pozorování je, že každý řetězec má s libovolným antiřetězcem (čili nezávislým systémem podmnožin) společný nejvýš jeden prvek. Kdyby se nám například podařilo ukázat, že celá uvažovaná uspořádaná množina se dá vyjádřit jako sjednocení nejvýš r řetězců, potom žádný antiřetězec nemá více než r prvků. V našem důkazu nicméně využijeme uvedené pozorování trochu složitějším způsobem.

Uvažme množinu všech *maximálních řetězců* v $(2^X, \subseteq)$, kde maximální řetězec je řetězec, ke kterému už nelze nic přidat tak, aby zůstal řetězcem. Je snadné nahlédnout, jak maximální řetězce vypadají: obsahují jednu podmnožinu X každé z možných velikostí, t.j., mají tvar

$$\emptyset \subset \{x_1\} \subset \{x_1, x_2\} \subset \{x_1, x_2, x_3\} \subset \ldots \subset \{x_1, x_2, \ldots, x_n\}, \quad (6.1)$$

kde $x_1, x_2, \ldots, x_n$ jsou všechny prvky X vypsané v nějakém pořadí. Každý takový maximální řetězec tudíž určuje pořadí prvků X, a obráceně, z každého pořadí dostaneme právě jeden maximální řetězec. Proto maximálních řetězců je stejně jako permutací, neboli $n!$.

Nechť $\mathcal{M}$ je libovolný antiřetězec (nezávislý systém množin). Utvořme všechny uspořádané dvojice $(\mathcal{R}, M)$, kde $M \in \mathcal{M}$ a $\mathcal{R}$ je maximální řetězec, obsahující M. Budeme počet takových dvojic počítat dvěma způsoby.

Z jedné strany, podle zmíněného pozorování, každý řetězec obsahuje nejvýš jednu $M \in \mathcal{M}$, takže uvažovaných dvojic $(\mathcal{R}, M)$ není více než maximálních řetězců, tedy než $n!$.

Z druhé strany, vezmeme jednu množinu $M \in \mathcal{M}$ a ptáme se, v kolika maximálních řetězcích je obsažena. Maximální řetězec tvaru (6.1)

obsahuje M jako jednu ze svých množin, právě když $\{x_1, x_2, \ldots, x_k\} = M$, kde $k = |M|$. Prvky množiny M můžeme stále ještě uspořádat $k!$ způsoby, čímž volíme počátečních k množin řetězce, a prvky mimo M můžeme uspořádat $(n-k)!$ způsoby, čímž je dán zbytek řetězce. Celkem je tedy M obsažena v $k!(n-k)!$ maximálních řetězcích. Počet uvažovaných uspořádaných dvojic $(\mathcal{R}, M)$ je proto roven

$$\sum_{M \in \mathcal{M}} |M|!(n-|M|)!,$$

přitom podle předchozího způsobu počítání je tento počet nejvýš $n!$. Vydělíme-li vzniklou nerovnost číslem $n!$, dostaneme

$$\sum_{M \in \mathcal{M}} \frac{|M|!(n-|M|)!}{n!} = \sum_{M \in \mathcal{M}} \frac{1}{\binom{n}{|M|}} \leq 1.$$

Využijeme toho, že $\binom{n}{\lfloor n/2 \rfloor}$ je aspoň tak velké jako libovolné kombinační číslo tvaru $\binom{n}{k}$ (viz část 2.5). Proto

$$1 \geq \sum_{M \in \mathcal{M}} \frac{1}{\binom{n}{|M|}} \geq |\mathcal{M}| \frac{1}{\binom{n}{\lfloor n/2 \rfloor}},$$

a odtud $|\mathcal{M}| \leq \binom{n}{\lfloor n/2 \rfloor}$. □

Ještě jeden důkaz Spernerovy věty. Spernerova věta se dá dokazovat několika podstatně odlišnými metodami. Popíšeme ještě dvě z nich. První z nich chytře pokrývá 2^X řetězci speciálního typu. Mějme nějaký řetězec v $(2^X, \subseteq)$, t.j. posloupnost do sebe zařazených množin $M_1 \subset M_2 \subset \ldots \subset M_t$. Nazvěme takový řetězec *symetrickým*, jestliže pro nějaké k obsahuje množiny velikostí právě $k, k+1, \ldots, n-k$. *Rozklad na symetrické řetězce* bude pak vyjádření 2^X jako disjunktního sjednocení několika symetrických řetězců.

Je vidět, že libovolný rozklad na symetrické řetězce (existuje-li vůbec) sestává z přesně $\binom{n}{\lfloor n/2 \rfloor}$ symetrických řetězců, jelikož každý symetrický řetězec obsahuje právě jednu množinu velikosti $\lfloor n/2 \rfloor$. Každý řetězec má s nezávislým systémem množin nejvýš jednu společnou množinu (na tom byl založen i předchozí důkaz Spernerovy věty). Spernerova věta tudíž vyplývá z následujícího:

Tvrzení. *Pro každou konečnou množinu X existuje rozklad na symetrické řetězce.*

Důkaz. Předpokládejme, že $X = \{1, 2, \ldots, n\}$. Základem důkazu je takováto konstrukce:

Každé podmnožině $M \subseteq X$ přiřadíme posloupnost $(m_1, m_2, \ldots, m_n)$ levých a pravých závorek „(“ „)“ předpisem

$$m_i = \begin{cases} \text{„(“} & \text{jestliže } i \in M \\ \text{„)“} & \text{jestliže } i \notin M. \end{cases}$$

Tak například pro $n = 7$ a množinu $M = \{2, 6\}$ máme

$$(m_1, \ldots, m_7) = \text{„)()))()“}.$$

Posloupnost závorek je zcela obecná (tedy ne správně uzávorkovaná). Můžeme ji však „částečně uzávorkovat“: nejdříve spárujeme všechny dvojice „()“ stojící bezprostředně vedle sebe, a dále pokračujeme v párování dosud nepoužitých závorek stejným způsobem (přičemž již spárované závorky ignorujeme). Dva příklady:

$$) \underbrace{(\,)}\,)) \underbrace{(\,)}$$

$$))) ((\underbrace{(\,)\ (\,)}\,) (.$$

Při tomto postupu samozřejmě mohou některé závorky zůstat nespárovány. Z pravidla částečného závorkování nicméně plyne, že posloupnost zbývajících závorek má na začátku jen pravé závorky a potom, od jistého místa, už jen levé závorky.

Řekneme, že dvě posloupnosti závorek mají *stejné částečné uzávorkování*, pokud spárované závorky jsou v obou posloupnostech stejné (i na stejných pozicích). Tak je tomu například pro posloupnosti tří následujících množin: (podmnožin množiny $\{1, 2, \ldots, 11\}$):

$$\begin{array}{lll} M_1 = \{4,5,6,8,11\} & \ldots &))) ((( ) ( )) (\\ M_2 = \{5,6,8,11\} & \ldots &)))) (( ) ( )) (\\ M_3 = \{5,6,8\} & \ldots &)))) (( ) ( ))) \end{array}$$

Jediný způsob, jak se mohou dvě posloupnosti závorek se stejným částečným uzávorkováním lišit, je že jedna z nich má zleva více nespárovaných levých závorek, nebo zprava více nespárovaných pravých závorek. Z toho

je snadno vidět, že dvě množiny se stejným částečným uzávorkováním (příslušných posloupností) musí být jedna podmnožinou druhé.

Definujeme nyní na množině 2^X ekvivalenci $\sim$ předpisem $M \sim M'$ právě když M i M' mají stejné částečné uzávorkování. Tvrdíme, že třídy této ekvivalence jsou symetrické řetězce. Ověření necháváme jako cvičení. Tím jsme ještě jednou dokázali Spernerovu větu. □

Nakonec předvedeme ještě jeden důkaz Spernerovy věty. Ten je zajímavý tím, že se v něm vlastně vůbec nepočítá s kombinačními čísly, ačkoliv Spernerova věta o nich hovoří. Místo toho se využívá značné symetrie uspořádané množiny $(2^X, \subseteq)$.

Začneme trochu obecnější definicí (již zmíněnou ve cvičení 1.7.9). Mějme nějaké uspořádané množiny $(X, \leq)$ a $(Y, \preceq)$. Zobrazení $f : X \to Y$ nazveme *isomorfismem* uspořádaných množin, jestliže f je bijekce a pro každé dva prvky $x, y \in X$ platí $x \leq y$ právě když $f(x) \preceq f(y)$. Isomorfismus uspořádané množiny $(X, \leq)$ s ní samotnou se jmenuje *automorfismus*. Automorfismus zachovává všechny vlastnosti, které můžeme definovat pomocí relace $\leq$. Tak například x je největším prvkem nějaké podmnožiny $A \subseteq X$ právě když $f(x)$ je největším prvkem množiny $f(A)$.

Třetí důkaz Spernerovy věty. Nechť X je daná konečná množina s n prvky. Každá permutace $f : X \twoheadrightarrow X$ indukuje zobrazení $f^{\#} : 2^X \to 2^X$, dané předpisem $f^{\#}(A) = \{f(x);\, x \in A\}$. Je zřejmé, že $f^{\#}$ je bijekce[1] $2^X \to 2^X$, a dokonce automorfismus uspořádané množiny $(2^X, \subseteq)$.

Uvažme nyní nějaký systém $\mathcal{M}$ podmnožin množiny X. Pro každou permutaci f množiny X můžeme uvážit systém

$$\{f^{\#}(M);\, M \in \mathcal{M}\},$$

tedy systém obrazů množin z $\mathcal{M}$ při zobrazení $f^{\#}$. Definujeme tak vlastně nové zobrazení

$$f^{\#\#} : 2^{2^X} \to 2^{2^X}$$

(t.j. množinovým systémům přiřazuje množinové systémy) předpisem

$$f^{\#\#}(\mathcal{M}) = \{f^{\#}(M);\, M \in \mathcal{M}\}.$$

[1] V části 1.6 jsme přijali konvenci, podle níž se pro obraz množiny může použít stejné formy zápisu jako pro obraz prvku, t.j. v našem případě bychom mohli množinu $\{f(x);\, x \in A\}$ zapsat též jako $f(A)$. Momentálně ale bude lepší přísněji rozlišovat mezi obrazem prvku a obrazem množiny. Proto jsme zavedli odlišné značení, $f^{\#}$, pro zobrazení množin

Zobrazení $f^{\#\#}$ je opět bijekce.

Na systémech množin, t.j. na množině 2^{2^X}, zavedeme teď relaci $\lhd$ následujícím předpisem:

$$\mathcal{M} \lhd \mathcal{N} \quad \Leftrightarrow \quad \text{pro každé } M \in \mathcal{M} \text{ existuje } N \in \mathcal{N} \text{ tak, že } M \subseteq N.$$

Všimněte si, že relace $\lhd$ je něco jiného než inkluze mezi systémy množin. Je to relace větší (tedy z $\mathcal{M} \subseteq \mathcal{N}$ plyne $\mathcal{M} \lhd \mathcal{N}$). Čtenář může sám ověřit, že relace $\lhd$ je reflexivní a transitivní. Nemusí to však být relace antisymetrická (najděte příklad na tříprvkové množině X, abyste se přesvědčili, že pojmu rozumíte).

Písmenem Ξ budeme značit množinu všech nezávislých systémů na množině X (tedy $\Xi \subset 2^{2^X}$). Tvrdíme, že relace $\lhd$ zúžená na množinu Ξ již antisymetrická je, a tudíž to je částečné uspořádání. Když totiž $\mathcal{M}$ a $\mathcal{N}$ jsou nezávislé systémy a platí $\mathcal{M} \lhd \mathcal{N}$ i $\mathcal{N} \lhd \mathcal{M}$, uvažme libovolnou množinu $M \in \mathcal{M}$. Systém $\mathcal{N}$ musí obsahovat nějakou $M' \supseteq M$, a pak také $\mathcal{M}$ obsahuje nějakou $M'' \supseteq M'$. Máme tedy $M, M'' \in \mathcal{M}$, $M \subseteq M''$, a proto (z nezávislosti) $M = M'' = M'$, takže $M \in \mathcal{N}$. Tím jsme ukázali $\mathcal{M} \subseteq \mathcal{N}$, a symetricky dostaneme $\mathcal{N} \subseteq \mathcal{M}$, neboli $\mathcal{M} = \mathcal{N}$. Proto $(\Xi, \lhd)$ je uspořádaná množina.

Dále tvrdíme, že pro každou permutaci f je zobrazení $f^{\#\#}$ automorfismem uspořádané množiny $(\Xi, \lhd)$ — ověření přenecháváme čtenáři (tím si ověří i své zvládnutí pojmů jako Ξ a $f^{\#\#}$).

Základem důkazu Spernerovy věty je takovéto lemma:

6.2.2 Lemma. *Označme $\Xi_0 \subseteq \Xi$ množinu všech nezávislých systémů, které mají největší možný počet množin (mezi všemi nezávislými systémy). Množina Ξ_0 má největší prvek, $\mathcal{N}_0$, vzhledem k uspořádání $\lhd$. To znamená, že pro každé $\mathcal{M} \in \Xi_0$ platí $\mathcal{M} \lhd \mathcal{N}_0$.*

Důkaz lemmatu. Protože nezávislých systémů na množině X je pouze konečně mnoho, stačí dokázat, že pro libovolné dva systémy $\mathcal{M}, \mathcal{M}' \in \Xi_0$ existuje systém $\mathcal{N} \in \Xi_0$ splňující $\mathcal{M} \lhd \mathcal{N}$ a $\mathcal{M}' \lhd \mathcal{N}$.

Mějme tedy libovolné $\mathcal{M}, \mathcal{M}' \in \Xi_0$ a uvažme systém $\bar{\mathcal{M}} = \mathcal{M} \cup \mathcal{M}'$. Poněvadž jak $\mathcal{M}$, tak $\mathcal{M}'$ jsou nezávislé systémy množin, má nejdelší řetězec v $\bar{\mathcal{M}}$ (vzhledem k uspořádání $\bar{\mathcal{M}}$ inkluzí) délku nejvýš 2. Označme dále $\bar{\mathcal{M}}_{min}$ systém všech množin z $\bar{\mathcal{M}}$, pro něž $\bar{\mathcal{M}}$ už neobsahuje žádnou jejich vlastní podmnožinu, jinak řečeno systém všech množin z $\bar{\mathcal{M}}$ minimálních vzhledem k $\subseteq$. Podobně zavedeme systém $\bar{\mathcal{M}}_{max}$

jako systém všech množin z $\bar{\mathcal{M}}$ maximálních vzhledem k $\subseteq$. Chceme ověřit, že $\bar{\mathcal{M}}_{max}$ splňuje podmínky kladené výše na systém $\mathcal{N}$.

Oba systémy $\bar{\mathcal{M}}_{min}$ i $\bar{\mathcal{M}}_{max}$ jsou nezávislé, a $\bar{\mathcal{M}} = \bar{\mathcal{M}}_{min} \cup \bar{\mathcal{M}}_{max}$. Zřejmě také $\bar{\mathcal{M}}_{max} \rhd \mathcal{M}$ a $\bar{\mathcal{M}}_{max} \rhd \mathcal{M}'$. Zbývá ověřit $|\bar{\mathcal{M}}_{max}| = |\mathcal{M}|$. Všimneme si, že z nezávislosti $\mathcal{M}$ a $\mathcal{M}'$ plyne $\mathcal{M} \cap \mathcal{M}' \subseteq \bar{\mathcal{M}}_{min} \cap \bar{\mathcal{M}}_{max}$. Proto $|\bar{\mathcal{M}}_{min}| + |\bar{\mathcal{M}}_{max}| = |\bar{\mathcal{M}}_{min} \cup \bar{\mathcal{M}}_{max}| + |\bar{\mathcal{M}}_{min} \cap \bar{\mathcal{M}}_{max}| \leq |\mathcal{M} \cup \mathcal{M}'| + |\mathcal{M} \cap \mathcal{M}'| = |\mathcal{M}| + |\mathcal{M}'|$, a tedy kdyby $|\bar{\mathcal{M}}_{max}| < |\mathcal{M}| = |\mathcal{M}'|$, potom bychom měli $|\bar{\mathcal{M}}_{min}| > |\mathcal{M}|$, a systémy $\mathcal{M}$ a $\mathcal{M}'$ by neměly maximální velikost. Tím je lemma dokázáno.

Zbývá dokončit důkaz Spernerovy věty. Uvažme největší prvek $\mathcal{N}_0$ množiny $(\Xi_0, \lhd)$. Pro každou permutaci f množiny X zobrazuje příslušný indukovaný automorfismus $f^{\#\#}$ množinu Ξ_0 (nezávislé systémy maximální velikosti) na ni samotnou, a tedy zobrazuje i její maximální prvek $\mathcal{N}_0$ na něj samotný: $f^{\#\#}(\mathcal{N}_0) = \mathcal{N}_0$. Odtud však plyne, že jestliže do $\mathcal{N}_0$ patří aspoň jedna k-prvková množina, potom tam už musí patřit *všechny* k-prvkové množiny, neboli $\binom{X}{k} \subseteq \mathcal{N}_0$. K systému $\binom{X}{k}$ už nejde přidat žádnou množinu tak, aby zůstal nezávislým, takže $\mathcal{N}_0 = \binom{X}{k}$. Z maximality kombinačních čísel $\binom{n}{\lfloor n/2 \rfloor}$ a $\binom{n}{\lceil n/2 \rceil}$ pak vyplývá, že $\mathcal{N}_0 = \binom{X}{\lceil n/2 \rceil}$. □

Cvičení

1. Řekneme, že systém $\mathcal{N}$ podmnožin X je *polonezávislý*, neobsahuje-li žádné 3 množiny A, B, C takové, že $A \subset B \subset C$.

   (a) Podobnou metodou jako v důkazu Spernerovy věty dokažte, že $|\mathcal{N}| \leq 2\binom{n}{\lfloor n/2 \rfloor}$, kde $n = |X|$.

   (b) Ukažte, že pro liché n odhad z (a) nelze zlepšit.

2. Pro přirozené číslo n definujte uspořádanou množinu $(D_n, |)$, kde D_n značí množinu všech dělitelů čísla n a $|$ je relace dělitelnosti.

   (a) Jaký je nejdelší řetězec v této množině pro $n = 10!$?

   (b) Kolik má tako množina maximálních řetězců (t.j. takových, které již nejdou prodloužit) pro $n = 10!$?

   (c) Kolik prvků má nejdelší antiřetězec v této množině pro $n = 720$?

3. Ověřte, že třídy ekvivalence $\sim$ definované ve druhém důkazu Spernerovy věty jsou doopravdy symetrické řetězce.

4.* Dokažte, že množinové systémy $\binom{X}{\lfloor n/2 \rfloor}$ a $\binom{X}{\lceil n/2 \rceil}$ jsou jediné nezávislé systémy na n-prvkové množině s největším možným počtem množin.

5. Určete, kolik má množina $(2^X, \subseteq)$ automorfismů.

6. Dokažte, že pro každou konečnou částečně uspořádanou množinu $(P, \leq)$ existuje antiřetězec maximální možné velikosti, který se všemi automorfismy množiny $(P, \leq)$ zobrazuje sám na sebe (je jejich *pevným bodem*).

7.* Nechť $a_1, \ldots, a_n$ jsou reálná čísla, $|a_i| \geq 1$. Nechť $p(a_1, \ldots, a_n)$ značí počet vektorů $(\varepsilon_1, \ldots, \varepsilon_n)$, kde $\varepsilon_i = \pm 1$, pro něž

$$-1 < \sum_{i=1}^{n} \varepsilon_i a_i < 1.$$

Dokažte, že $p(a_1, \ldots, a_n) \leq \binom{n}{\lfloor n/2 \rfloor}$ pro každé $a_1, \ldots, a_n$, a že pro jistou volbu a_i nastane rovnost. (Toto je jedna z prvních aplikací Spernerovy věty — tzv. Littlewoodův-Offordův problém.)

8. Nechť n je přirozené číslo, které není dělitelné žádnou druhou mocninou přirozeného čísla. Určete maximální možnou velikost množiny dělitelů čísla n, které se navzájem nedělí (t.j., $\max |M|$, kde $x \in M \Rightarrow x|n$ a $x, y \in M$, $x \neq y \Rightarrow x \nmid y$).

9. Nechť X je částečně uspořádaná množina s n prvky. Nechť r značí délku nejdelšího řetězce v X a a délku nejdelšího antiřetězce.

(a)* Dokažte, že X lze vyjádřit jako (disjunktní) sjednocení nejvýš r antiřetězců (z toho plyne, že existuje nějaký antiřetězec s aspoň $\lceil n/r \rceil$ prvky).

(b)** (Dilworthova věta) Dokažte, že X lze vyjádřit jako (disjunktní) sjednocení nejvýš a řetězců.

10. (Erdősovo-Szekeresovo lemma)

(a)* Ukažte, že pro libovolnou posloupnost $(a_1, a_2, \ldots, a_n)$ navzájem různých reálných čísel existují indexy $i_1, i_2, \ldots, i_k$, kde $1 \leq i_1 < i_2 < \ldots < i_k \leq n$ a $k = \lceil \sqrt{n} \rceil$, tak že buď $a_{i_1} < a_{i_2} < \ldots < a_{i_k}$ (členy a_{i_j} tvoří *rostoucí podposloupnost*), anebo $a_{i_1} > a_{i_2} > \ldots a_{i_k}$ (členy a_{i_j} tvoří *klesající podposloupnost*). Můžete využít cvičení 9(a).

(b) Ukažte, že hodnotu k v (a) obecně nejde zvětšit, t.j. že existuje n-prvková posloupnost, která nemá delší klesající podposloupnost ani rostoucí podposloupnost než $\lceil \sqrt{n} \rceil$.

(c) Tentokrát uvažme dvě posloupnosti reálných čísel, $a = (a_1, \ldots, a_n)$ a $b = (b_1, \ldots, b_n)$, v nichž se žádné číslo neopakuje. Ukažte, že vždy existují indexy $i_1, \ldots, i_k$, $1 \le i_1 < \ldots < i_k \le n$, kde $k = \lceil n^{1/4} \rceil$, takové že jimi určené podposloupnosti v a i b jsou rostoucí nebo klesající (připouští se všechny 4 možné kombinace, např. „rostoucí v a, rostoucí v b“, „klesající v a, rostoucí v b“ atd.).

(d)* Ukažte, že odhad pro k v (c) obecně nelze zlepšit.

6.3 Extremální věta: grafy bez čtyřcyklů

V některých situacích víme, že nějaký graf G, zpravidla s mnoha vrcholy, neobsahuje jistý konkrétní graf nebo graf jistého typu jako podgraf, a ptáme se, kolik může G mít maximálně hran. Například, víme-li, že daný graf na n vrcholech neobsahuje žádnou kružnici, pak je to strom nebo les, a tedy má nanejvýš $n - 1$ hran. Takové tvrzení můžeme použít i obráceným směrem: Má-li graf na n vrcholech aspoň n hran, jistě obsahuje nějakou kružnici. To byl velmi jednoduchý příklad, pro jiné „zakázané“ podgrafy je situace složitější, a některé z příslušných problémů nejsou dodnes uspokojivě vyřešeny. Takovými otázkami se zabývá tzv. *extremální teorie grafů*. Uvedeme jeden její výsledek, týkající se zakázaného $K_{2,2}$ (neboli kružnice délky 4).

6.3.1 Věta. *Buď G graf s n vrcholy. Neobsahuje-li G graf $K_{2,2}$ jako podgraf, potom má nejvýše $\frac{1}{2}(n^{3/2} + n)$ hran.*

Důkaz. Pišme $V = V(G)$. Budeme dvěma způsoby počítat velikost množiny M všech dvojic $(\{u, u'\}, v)$, kde $v \in V$, $\{u, u'\} \in \binom{V}{2}$ a v je spojen hranou jak s u tak s u'. Jinými slovy, počítáme (neindukované) podgrafy tvaru

Pro pevnou dvojici $\{u, u'\}$ může existovat pouze jediný vrchol $v \in V$ spojený s u i s u' (kdyby byly dva takové vrcholy, v a v', seděl by na vrcholech u, u', v, v' podgraf isomorfní $K_{2,2}$). Proto $|M| \le \binom{n}{2}$.

Nyní uvážíme všechny prvky $(\{u,u'\},v)$ z množiny M pro jeden pevný vrchol $v \in V$. Každá dvojice $\{u,u'\}$ sousedů vrcholu v přispěje jeden prvek M, proto vrchol v stupně d přispěje $\binom{d}{2}$ prvky. Označíme-li tedy $d_1, d_2, \ldots, d_n$ stupně jednotlivých vrcholů z V, dostáváme $|M| = \sum_{i=1}^{n} \binom{d_i}{2}$.

Spojením s předchozím odhadem máme

$$\sum_{i=1}^{n} \binom{d_i}{2} \leq \binom{n}{2}. \tag{6.2}$$

Přitom počet hran uvažovaného grafu je $E = \frac{1}{2}\sum_{i=1}^{n} d_i$. Zbytek důkazu je již čistě manipulace s nerovnostmi, která se dá dělat mnoha různými způsoby.

Zde ukážeme jeden důkaz, další je naznačen ve cvičení 5 (ten je trochu složitější, ale snáze se zobecní). Nejdříve potřebujeme jednu (důležitou) nerovnost:

6.3.2 Tvrzení (Cauchyho-Schwarzova nerovnost). *Pro libovolná reálná čísla $x_1, \ldots, x_n$ a $y_1, \ldots, y_n$ platí*

$$\sum_{i=1}^{n} x_i y_i \leq \sqrt{\sum_{i=1}^{n} x_i^2}\sqrt{\sum_{i=1}^{n} y_i^2}.$$

Důkaz je naznačen ve cvičení 4 (a většinou se zmiňuje v kurzu analýzy). Poznamenejme ještě, že Cauchyho-Schwarzova nerovnost má názorný geometrický význam. Interpretujeme-li totiž $x = (x_1, \ldots, x_n)$ a $y = (y_1, \ldots, y_n)$ jako vektory v n-dimenzionálním euklidovském prostoru, je levá strana nerovnosti jejich *skalární součin*, zatímco pravá strana je součin jejich délek. Přitom dobře známý vzorec z vektorového počtu říká, že kosinus úhlu dvou vektorů je roven jejich skalárnímu součinu dělenému součinem jejich délek. Cauchyho-Schwarzova nerovnost tedy vyjadřuje, že kosinus úhlu je vždy nejvýš 1 (rozmyslete si to aspoň pro případ $n = 2$, t.j. v rovině).

Dokončení důkazu věty 6.3.1. Zřejmě můžeme předpokládat, že náš graf nemá izolované vrcholy, tedy $d_i \geq 1$ pro každé i. Potom platí $\binom{d_i}{2} \geq (d_i - 1)^2/2$, takže z (6.2) dostaneme

$$\sum_{i=1}^{n} (d_i - 1)^2 \leq n^2.$$

Použijeme nyní Cauchyho-Schwarzovu nerovnost s $x_i = d_i - 1$, $y_i = 1$. Dostaneme

$$\sum_{i=1}^{n}(d_i - 1) \le \sqrt{\sum_{i=1}^{n}(d_i - 1)^2}\sqrt{n} \le \sqrt{n^2}\sqrt{n} = n^{3/2},$$

takže $E = \frac{1}{2}\sum_{i=1}^{n} d_i \le \frac{1}{2}(n^{3/2} + n)$. □

Cvičení

1. Dokažte, že pro libovolné $t \ge 2$ je maximální počet hran grafu neobsahujícího $K_{2,t}$ jako podgraf nejvýš $\frac{1}{2}(\sqrt{t-1}\,n^{3/2} + n)$.

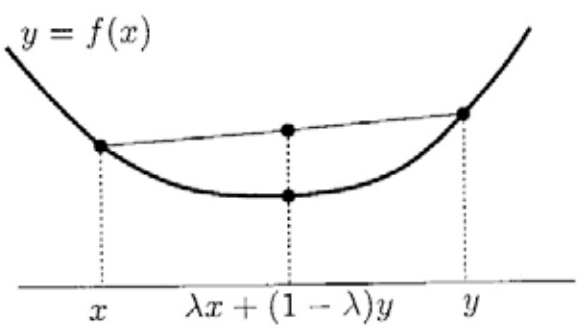
2. Nechť $S_1, S_2, \ldots, S_n$ jsou nějaké podmnožiny nějaké n-prvkové množiny X. Předpokládejme, že platí $|S_i \cap S_j| \le 1$ pro každé i, j, $1 \le i < j \le n$. Ukažte, že některá z množin S_i má nanejvýš $O(\sqrt{n})$ prvků.

3. Nechť A je n-prvková množina, B je m-prvková množina, a nechť G je bipartitní graf na $A \cup B$, jehož každá hrana spojuje vrchol z A s vrcholem z B. Dokažte, že neobsahuje-li G graf $K_{2,2}$ jako podgraf, potom má nejvýš $O(m\sqrt{n} + n)$ hran.

4. (a) Dokažte Cauchyho-Schwarzovu nerovnost indukcí podle n (napřed ji umocněte na druhou).

   (b) Dokažte Cauchyho-Schwarzovu nerovnost přímo: vyjděte z nerovnosti $\sum_{i,j=1}^{n}(x_i y_j - x_j y_i)^2 \ge 0$ a upravte.

5. (a) Nechť $f : \mathbf{R} \to \mathbf{R}$ je *konvexní funkce*, t.j. pro pro libovolné $x, y \in \mathbf{R}$ a $\lambda \in [0,1]$ platí $f(\lambda x + (1-\lambda)y) \le \lambda f(x) + (1-\lambda)f(y)$. Geometricky to znamená, že spojíme-li libovolné dva body na grafu této funkce úsečkou, leží část grafu mezi těmito body pod zmíněnou úsečkou:



Dokažte indukcí, že potom pro libovolná reálná čísla $x_1, x_2, \ldots, x_n$ platí

$$f(\tfrac{1}{n}x_1 + \tfrac{1}{n}x_2 + \cdots + \tfrac{1}{n}x_n) \leq \tfrac{1}{n}f(x_1) + \tfrac{1}{n}f(x_2) + \cdots + \tfrac{1}{n}f(x_n).$$

(b) Definujte funkci f předpisem

$$f(x) = \begin{cases} 0 & \text{pro } x \leq 1 \\ x(x-1)/2 & \text{pro } x > 1. \end{cases}$$

Dokažte, že f je konvexní.

(c) Dokažte ze vztahu (6.2) větu 6.3.1 pomocí (a) a (b) (napřed odvoďte $nf(E/2n) \leq \binom{n}{2}$).

6.* Podobnou metodou jako ve cvičení 5 odvoďte, že neobsahuje-li graf na n vrcholech $K_{3,3}$ jako podgraf, má nejvýš $const.n^{5/3}$ hran.

7

Počet koster

7.1 Cayleyho formule

Pro daný graf G označme $\kappa(G)$ počet všech koster G. V této kapitole předkládáme čtenáři několika důkazů následujícího výsledku:

7.1.1 Věta (Cayleyho formule). *Pro každé $n \geq 2$ je $\kappa(K_n)$, t.j. počet stromů na daných n vrcholech, roven n^{n-2}.*

Ačkoli pro $\kappa(K_n)$ vyjde taková pěkná jednoduchá formule, není znám žádný úplně přímočarý způsob, jak její správnost nahlédnout. Postupem času se přišlo na celou řadu důkazů, jejichž základní myšlenky se od sebe podstatně odlišují, ale každý z nich je založen na umném triku nebo vyplývá z netriviální teorie. Shromáždili jsme několik důkazů do této kapitoly, hlavně jako ilustraci myšlenkového bohatství matematiky.

Rozhodně nechceme tvrdit, že věta 7.1.1 patří k vůbec nejdůležitějším v matematice. Na druhé straně, počet koster grafu (a související teorie) má řadu teoretických i praktických aplikací, a začal se studovat v souvislosti s elektrickými obvody.

Jako ilustraci uvedeme bez důkazu „elektrotechnický“ význam počtu koster. Představme si, že daný graf G je elektrický obvod, kde každá hrana je vodič s jednotkovým odporem (a vrcholy znamenají prostě spojení konců dohromady). Jsou-li x, y vrcholy spojené hranou, potom odpor, který bychom mezi nimi v tomto obvodu naměřili, je roven počtu koster G obsahujících hranu $\{x, y\}$, dělenému celkovým počtem koster

$\kappa(G)$. Přímo tento výsledek není ovšem pro přímou aplikaci příliš už tečný (málokdy máme všechny odpory stejné), ale existuje příslušné z becnění na grafy s ohodnocenými hranami.

V celé kapitole bude množina V vrcholů uvažovaného úplného graf rovna $\{1, 2, \ldots, n\}$.

Cvičení

1. Dokažte, že počet navzájem neisomorfních stromů na n vrcholech nejméně e^n/n^3 (viz též cvičení 4.2.5!).

2.* Předpokládejte platnost věty 7.1.1, a určete počet koster úplného gra na n vrcholech bez jedné hrany.

3. Označme $T_n = \kappa(K_n)$. Dokažte rekurentní vzorec

$$(n-1)T_n = \sum_{k=1}^{n-1} k(n-k)\binom{n-1}{k-1} T_k T_{n-k}.$$

Poznámka: také z této rekurence se dá věta 7.1.1 odvodit, ale není jen tak.

4.* Spočítejte $\kappa(K_{n,m})$ (počet koster úplného bipartitního grafu). Pokus se aplikovat některou z metod z následujících oddílů (např. 7.5, 7.2)

7.2 Důkaz přes skóre

Ukážeme

7.2.1 Tvrzení. *Nechť $d_1, d_2, \ldots, d_n$ jsou kladná celá čísla se součtc $2n-2$. Potom počet koster grafu K_n, v nichž každý vrchol i má stup právě d_i (pro $i = 1, 2, \ldots, n$) je roven*

$$\frac{(n-2)!}{(d_1-1)!(d_2-1)!\ldots(d_n-1)!}.$$

Důkaz. Indukcí podle n. Pro $n = 1, 2$ je tvrzení triviální, nechť te $n > 2$. Protože součet d_i je menší než $2n$, existuje i takové, že $d_i =$ Po případném přejmenování vrcholů můžeme předpokládat, že $d_n =$

(Jinak řečeno: když dokážeme tvrzení za předpokladu $d_n = 1$, bude pak dokázáno i pro libovolnou hodnotu d_n.)

Buď $\mathcal{T}$ množina všech koster grafu K_n, v nichž má každý vrchol i stupeň d_i. Rozdělme kostry z $\mathcal{T}$ do $n-1$ skupin: $\mathcal{T}_j$ budou ty kostry z $\mathcal{T}$, ve kterých je vrchol n spojen s vrcholem j. Nyní uvažme kostru z nějakého $\mathcal{T}_j$, a vymažme z ní vrchol n společně s (jedinou) hranou do něj zasahující. Tím dostaneme kostru grafu K_{n-1}, v níž je stupeň vrcholu i roven d_i pro $i \neq j$ a $d_j - 1$ pro $i = j$. Je snadno vidět, že to definuje bijekci mezi množinou koster $\mathcal{T}_j$ a množinou $\mathcal{T}'_j$ všech koster grafu K_{n-1} se stupni $d_1, d_2, \ldots, d_{j-1}, d_j - 1, d_{j+1}, \ldots, d_{n-1}$ (protože různé kostry z $\mathcal{T}_j$ dávají různé kostry z $\mathcal{T}'_j$, a z každé kostry z $\mathcal{T}'_j$ můžeme dostat kostru z $\mathcal{T}_j$ tím, že přidáme vrchol n a spojíme jej s vrcholem j).

Podle indukčního předpokladu pak máme

$$|\mathcal{T}_j| = |\mathcal{T}'_j| = \frac{(n-3)!}{(d_1-1)!\cdots(d_{j-1}-1)!(d_j-2)!(d_{j+1}-1)!\cdots(d_{n-1}-1)!}$$

$$= \frac{(n-3)!(d_j-1)}{(d_1-1)!(d_2-1)!\cdots(d_{n-1}-1)!}.$$

Tento vzorec platí i když $d_j = 1$ (pak dává 0, což souhlasí s tím, že žádná kostra se stupněm $d_j - 1 = 0$ u vrcholu j neexistuje).

Proto hledaný počet koster na n vrcholech se stupni $d_1, d_2, \ldots, d_n$, kde $d_n = 1$, je roven

$$\sum_{j=1}^{n} |\mathcal{T}_j| = \sum_{j=1}^{n-1} \frac{(n-3)!(d_j-1)}{(d_1-1)!(d_2-1)!\cdots(d_{n-1}-1)!} =$$

$$\left(\sum_{j=1}^{n-1}(d_j-1)\right) \frac{(n-3)!}{(d_1-1)!(d_2-1)!\cdots(d_{n-1}-1)!} =$$

$$= \frac{(n-2)(n-3)!}{(d_1-1)!(d_2-1)!\cdots(d_{n-1}-1)!}.$$

Protože $d_n = 1$, můžeme do jmenovatele beze škody přidat činitel $(d_n - 1)! = 0! = 1$, a tím jsme udělali indukční krok. □

Nyní dokážeme větu 7.1.1. Budeme sčítat přes všechna možná skóre, a využijeme přitom multinomické věty 2.3.4:

$$\kappa(K_n) = \sum_{\substack{d_1,d_2,\dots,d_n \geq 1 \\ d_1+d_2+\cdots+d_n=2n-2}} \frac{(n-2)!}{(d_1-1)!(d_2-1)!\cdots(d_n-1)!} =$$

$$\sum_{\substack{k_1+k_2+\cdots+k_n=n-2 \\ k_1,\dots,k_n \geq 0}} \frac{(n-2)!}{k_1!k_2!\cdots k_n!} = \underbrace{(1+1+\cdots+1)}_{n\times}{}^{n-2} = n^{n-2}.$$

□

Cvičení

1. (a)* Najděte počet stromů (na daných n vrcholech), v nichž každý vrchol má stupeň 1 nebo 3.

   (b)* Co když připustíme stupně 1,2 a 3?

7.3 Důkaz s obratlovci

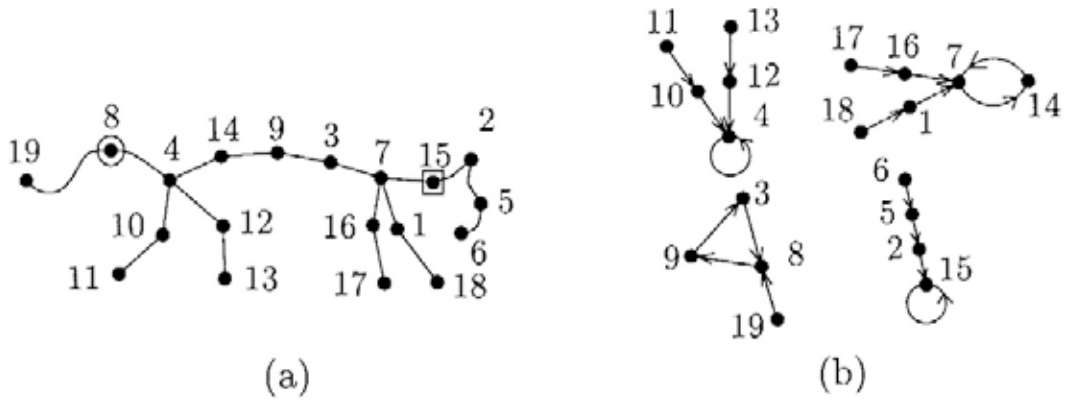
Definujeme, co je *obratlovec* na množině vrcholů V uvažovaného úplného grafu K_n (viz obr. 7.1(a)): je to kostra, u níž navíc je jeden vrchol označen čtverečkem a jeden vrchol kroužkem (nevylučujeme, že týž vrchol je označen čtverečkem i kroužkem). Označme množinu všech obratlovců písmenem $\mathcal{O}$.

Z každé kostry můžeme stvořit právě n^2 různých obratlovců, proto počet všech koster je roven $|\mathcal{O}|/n^2$. Ukážeme nyní

7.3.1 Lemma. *Existuje bijekce F mezi množinou $\mathcal{O}$ všech obratlovců a množinou všech zobrazení množiny V do sebe.*

Počet zobrazení n-prvkové množiny do sebe je n^n, obratlovců je podle lemmatu stejně, a tudíž koster je n^{n-2}.

Důkaz lemmatu. Konstrukci bijekce F ukážeme na příkladu na obr. 7.1. Vyjdeme z obratlovce O nakresleného na obrázku (a). Označené vrcholy □ a ◯ jsou spojeny jedinou cestou, kterou nazveme *páteř*.



Obrázek 7.1: (a) Obratlovec na 19 vrcholech, (b) jemu odpovídající graf zobrazení.

Vypišme si čísla vrcholů páteře do řádky v pořadí podle velikosti, a potom do další řádky znovu v pořadí, jak jdou od ◯ k □:

3	4	7	8	9	14	15
8	4	14	9	3	7	15

Definujeme nyní na vrcholech páteře pomocný orientovaný graf P: uděláme šipku z každého vrcholu z horní řádky do vrcholu napsaného pod ním v dolní řádce. Poněvadž z každého vrcholu vychází právě jedna šipka a také do každého vrcholu jedna šipka vchází, je graf P disjunktním sjednocením orientovaných cyklů (případně samotných vrcholů se smyčkou). Můžeme také říci, že páteř definuje permutaci svých vrcholů a P sestává právě z cyklů této permutace, viz část 2.2. V našem příkladu jsou posloupnosti vrcholů těchto cyklů, srovnané v pořadí podle šipek, $(3, 8, 9)$, (4), $(7, 14)$ a (15).

Podíváme se nyní zpátky na obratlovce O. Odebereme-li z něj na chvíli všechny hrany páteře, rozpadne se na jednotlivé komponenty (opět stromy). Orientujme hrany každé komponenty tak, že směřují k (jedinému) vrcholu páteře v této komponentě. Tím vznikne další množina orientovaných hran na množině V. Definujeme nyní orientovaný graf G na množině V, jehož hranami budou jednak právě definované orientované hrany komponent, jednak všechny hrany pomocného grafu P. Na obrázku je to velmi názorné: nakreslíme cykly grafu P,

a potom ke každému vrcholu (původně z páteře) přikreslíme strom, který přes něj byl zavěšen na páteři obratlovce, viz obrázek (b).

Tvrdíme nyní, že výsledný orientovaný graf G je grafem zobrazení, to znamená, že z každého vrcholu vychází právě jedna hrana. Pro vrcholy páteře jsme to již konstatovali. Pro ostatní vrcholy je to proto, že v obratlovci O z nich vede jediná cesta do páteře. Definujeme tedy konečně zobrazení $f = F(O) : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$, příslušející obratlovci O: pro každé i, což je vrchol grafu G, položíme $f(i) = j$, kde j je ten vrchol G, do nějž jde šipka z i. V našem konkrétním příkladě bychom dostali zobrazení $1 \mapsto 7$, $2 \mapsto 15$, $3 \mapsto 8$, $4 \mapsto 4$, $5 \mapsto 2$, $6 \mapsto 5$, $7 \mapsto 14$, $8 \mapsto 9$, $9 \mapsto 3$, $10 \mapsto 4$, $11 \mapsto 10$, $12 \mapsto 4$, $13 \mapsto 12$, $14 \mapsto 7$, $15 \mapsto 15$, $16 \mapsto 7$, $17 \mapsto 16$, $18 \mapsto 1$ a $19 \mapsto 8$. Takto každý obratlovec určuje zobrazení.

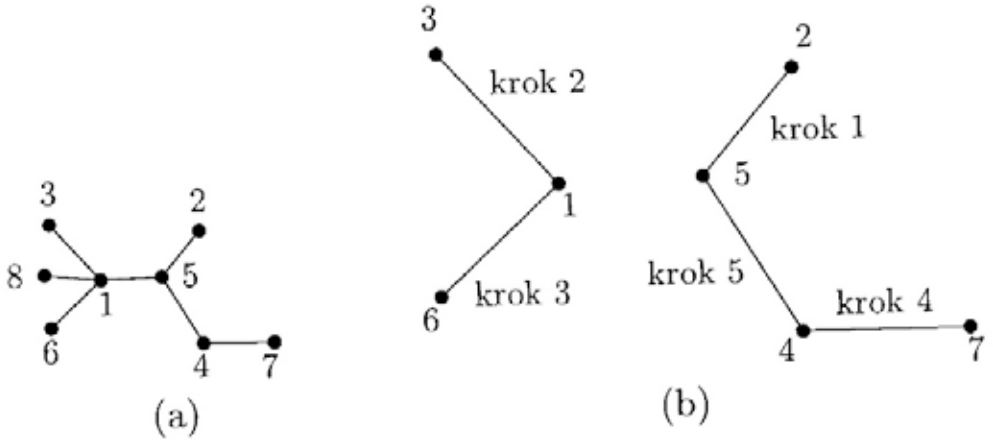
Zbývá ještě ukázat, že z takto sestrojeného zobrazení lze původního obratlovce zpětně rekonstruovat, a že každé zobrazení se dostane z nějakého obratlovce. To ponecháme do cvičení. □

Cvičení

1. Pro dané zobrazení f konečné množiny V do V definujeme *graf* f, což je orientovaný graf s množinou vrcholů V a hranami z každého $i \in V$ do $f(i)$ (takový graf jsme používali v důkazu výše). Dokažte, že každá komponenta takového grafu je orientovaným cyklem, na jehož vrcholy jsou případně přivěšeny stromy s hranami orientovanými směrem k tomuto cyklu.

2. Popište, jak se ze zobrazení $f = F(O) : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ zpětně získá výchozí obratlovec O, a dokažte, že každé zobrazení $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ se dostane jako $F(O)$ pro nějakého obratlovce O (s využitím cvičení 1).

3.* Nechť $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ je funkce. Navrhněte algoritmus, který pro dané i najde délku periody posloupnosti $(i, f(i), f(f(i)), \ldots)$ (t.j. v řeči grafu zobrazení f, délku cyklu, do nějž se dostaneme po šipkách z bodu i), přičemž používá jen konstantní velikost paměti (nezávislou na délce periody). Přitom máte k dispozici podprogram (černou skříňku), vypočítávající hodnoty f.



Obrázek 7.2: (a) Kostra s kódem $(5, 1, 1, 4, 5, 1)$, (b) postup její rekonstrukce z kódu.

7.4 Důkaz pomocí Prüferova kódu

Ukážeme, jak každou kostru grafu K_n zakódovat $(n-2)$-člennou posloupností, jejíž každý člen je některé z čísel $1, 2, \ldots, n$. Toto kódování bude definovat bijekci mezi všemi kostrami a všemi posloupnostmi uvedeného typu. Poněvadž takových posloupností je zřejmě n^{n-2}, bude tím dokázána věta 7.1.1.

Mějme danou kostru T; příklad viz obr. 7.2(a). Popíšeme, jak sestrojit posloupnost $P = P(T) = (p_1, p_2, \ldots, p_{n-2})$, tzv. Prüferův kód kostry T. Základní myšlenka[1] je, že ze stromu T budeme postupně otrhávat listy, dokud z něj nezbude jen jediná hrana. Budeme tedy konstruovat pomocnou posloupnost stromů $T_0 = T, T_1, T_2, \ldots, T_{n-2} = K_2$, a přitom vyrábět posloupnost P. Předpokládejme, že už jsme zkonstruovali T_{i-1} (na začátku máme $T_0 = T$). Jak víme, má aspoň 1 list (vrchol stupně 1). Vezmeme nejmenší z listů T_{i-1} (připomeňme, že vrcholy T jsou čísla $1, 2, \ldots, n$), a utvoříme T_i odstraněním tohoto listu z T_{i-1}, spolu s příslušnou hranou. Přitom definujeme i-tý člen, p_i, konstruované posloupnosti jako *souseda právě utrženého listu* (tedy nikoliv jako list sám, to je hlavní trik!). Uděláme-li toto pro $i = 1, 2, \ldots, n-2$, definovali jsme posloupnost $P = P(T)$.

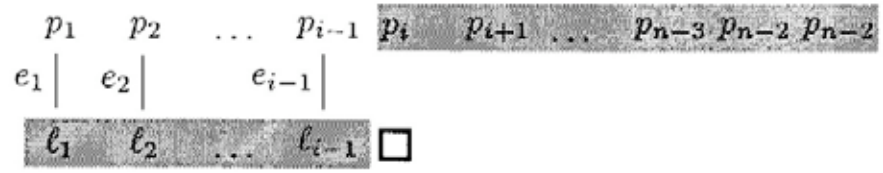
[1] Trochu vandalská.

Předpokládejme teď, že daná posloupnost P vznikla výše uvedenou konstrukcí z nějaké (nám dosud neznámé) kostry T. Odvodíme, jak zpětně vytvořit T. Ptejme se nejdříve, jak z posloupnosti P poznat, který vrchol kostry T byl utržen jako první; označme jej ℓ_1 (musel to být list). Zřejmě ℓ_1 se nesmí vyskytovat nikde v posloupnosti P (protože do P se zapisují jen vrcholy dosud přítomné v otrhaném stromě). Dále, každý vrchol, který není obsažen v množině $\{p_1, p_2, \ldots, p_{n-2}\}$, musí být listem stromu T (jinak bychom od něj v některé fázi odtrhli list, a tím by se octl v posloupnosti P). Podle pravidla otrhávání listů je tudíž ℓ_1 minimum z množiny $\{1, 2, \ldots, n\} \setminus \{p_1, p_2, \ldots, p_{n-2}\}$. Tato množina je vždy neprázdná, a proto je minimum dobře definováno. Můžeme nyní ℓ_1 nakreslit jako první vrchol kostry, a připojit k němu hranou vrchol p_1 (viz obr. 7.2(b)).

Dále postupujeme podobně; známe-li již listy $\ell_1, \ell_2, \ldots, \ell_{i-1}$ utržené v krocích 1 až $i-1$, budeme určovat list ℓ_i. Nemůže to být žádný z vrcholů $p_i, p_{i+1}, \ldots, p_{n-2}$, a ovšem ani z $\ell_1, \ldots, \ell_{i-1}$ — bude to tedy minimum z množiny $\{1, 2, \ldots, n\} \setminus \{p_i, p_{i+1}, \ldots, p_{n-2}, \ell_1, \ell_2, \ldots, \ell_{i-1}\}$ (ta je zase neprázdná). Takto určený list ℓ_i připojíme hranou k vrcholu p_i. Není-li ℓ_i dosud nakreslen, nakreslíme jej ovšem také, podobně pro p_i. Prvních 5 kroků této konstrukce je znázorněno na obr. 7.2(b), v 6. kroku bychom dokreslili hranu $\{1, 5\}$.

Po $n-2$ krocích jsme nakreslili $n-2$ hran kostry T, jmenovitě všechny, které byly při otrhávání odstraněny, a zbývá určit, která byla poslední zbývající hrana. Jeden její konec musí ovšem být p_{n-2}, tedy soused posledně odtrženého listu, a druhý konec je ten vrchol, který se nevyskytuje mezi všemi odtrženými listy $\ell_1, \ldots, \ell_{n-2}$ a je různý od p_{n-2}. Na obr. 7.2 to bude hrana $\{1, 8\}$. Tím je metoda rekonstrukce popsána. Ještě ji pro přehlednost jednou shrňme.

Použijeme dvouřádkového zápisu. Do prvního řádku zapíšeme čísla $p_1, p_2, \ldots, p_{n-3}, p_{n-2}, p_{n-2}$ (tedy $n-1$ čísel, přičemž p_{n-2} na konci se opakuje — tímto opakováním se elegantně zahrne poslední, výjimečný krok do obecného pravidla). Do druhého řádku postupně vyplňujeme čísla $\ell_1, \ell_2, \ldots, \ell_{n-1}$. Byla-li již vyplněna ℓ_1 až ℓ_{i-1}, pak číslo ℓ_i je nejmenší takové, jež se nevyskytuje mezi předchozími čísly v dolním řádku ani mezi čísly v horním řádku od $i$té pozice (včetně) vpravo:



Na silně orámovanou pozici přijde nejmenší číslo, které není mezi čísly vyznačenými šedě. Hrany $e_1, e_2, \ldots$ rekonstruované kostry spojují vždy vrchol z horního řádku s vrcholem napsaným pod ním.

Pro libovolnou $(n-2)$-člennou posloupnost P vytvoří právě uvedený algoritmus nějaký graf G na množině vrcholů $\{1, 2, \ldots, n\}$ s $n-1$ hranami. Též víme, že pokud posloupnost P pocházela z nějaké kostry T, platí $G = T$. Náš úkol ale ještě nekončí: Musíme se přesvědčit, že vzniklý graf G je *vždycky* strom, a že jeho zpětným překódováním do posloupnosti dostaneme tu posloupnost, z níž jsme vyšli.

Označme $G_i = (\{1, 2, \ldots, n\}, \{e_i, e_{i+1}, \ldots, e_{n-1}\})$. Z algoritmu vyplňování dolního řádku je vidět, že do vrcholu ℓ_i zasahuje hrana e_i a žádná z hran $e_{i+1}, \ldots, e_{n-1}$ už do ℓ_i zasahovat nemůže, takže ℓ_i má v G_i stupeň 1. Tedy G_i vznikne z G_{i+1} přidáním listu, a z tvrzení 4.1.3 o postupné výstavbě stromu vidíme, že G je strom. Obecněji, G_i je strom plus $i-1$ izolovaných vrcholů.

Zbývá ověřit, že ℓ_i je nejmenší z listů grafu G_i. Podle definice ℓ_i by menší list mohl být jedině mezi $\ell_1, \ldots, \ell_{i-1}$ nebo mezi $p_i, \ldots, p_{n-2}$. První skupina nepřichází v úvahu (poněvadž $\ell_1, \ldots, \ell_{i-1}$ mají v G_i stupně 0). Uvažme vrchol p_k, $i < k \leq n-2$. V grafu G_k je to soused listu ℓ_k, a protože G_k sestává z izolovaných vrcholů a jedné další komponenty, která má aspoň 2 hrany, má p_k v grafu G_k stupeň minimálně 2. Takže ani v G_i není p_k listem.

Tudíž ℓ_i je nejmenší list v G_i, a G_{i+1} opravdu vznikne z G_i podle procedury Prüferova kódování kostry. Důkaz věty 7.1.1 je hotov. □

7.5 Důkaz pracující s determinanty

Důkaz věty 7.1.1 uvedený v tomto oddílu je založen na lineární algebře, a ilustruje pěkný kombinatorický význam determinantu matice. Je

o něco těžší než předchozí důkazy (a potřebují se v něm základní věty o determinantech), zato ale určuje počet koster pro libovolný graf.

Buď G libovolný graf s vrcholy $1, 2, \ldots, n$, $n \geq 2$, a hranami e_1, e_2, $\ldots$, e_m. Zavedeme $n \times n$ matici Q, zvanou *Laplaceova matice* grafu G, jejíž prvky q_{ij} jsou určeny následujícím předpisem:

$$\begin{aligned} q_{ii} &= \deg_G(i) && i = 1, 2, \ldots, n \\ q_{ij} &= \begin{cases} -1 & \text{pro } \{i,j\} \in E(G) \\ 0 & \text{jinak} \end{cases} && i, j = 1, 2, \ldots, n,\ i \neq j. \end{aligned}$$

Dále nechť Q_{ij} značí matici $(n-1) \times (n-1)$, která vznikne z matice Q vyškrtnutím i-tého řádku a j-tého sloupce.

Platí následující pozoruhodná

7.5.1 Věta. *Pro každý graf G je $\kappa(G) = \det Q_{11}$.*

Poznamenejme, že je též pravda $\kappa(G) = |\det Q_{ij}|$ pro libovolné dva indexy $i, j \in \{1, 2, \ldots, n\}$. To tady nebudeme dokazovat, důkaz je naznačen ve cvičení.

Než začneme větu dokazovat, odvoďme z ní větu 7.1.1. Pro $G = K_n$ má Laplaceova matice na diagonále všude čísla $n-1$, a mimo diagonálu -1. Vymažeme-li první řádek a první sloupec, dostaneme $(n-1) \times (n-1)$ matici tvaru

$$\begin{pmatrix} n-1 & -1 & -1 & \ldots & -1 \\ -1 & n-1 & -1 & \ldots & -1 \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ -1 & -1 & -1 & \ldots & n-1 \end{pmatrix}.$$

Determinant spočítáme šikovnými řádkovými a sloupcovými úpravami: odečteme-li od všech řádků kromě prvního první řádek, a potom k prvnímu sloupci přičteme součet všech ostatních, vznikne matice, která na diagonále má $1, n, n, n, \ldots, n$ a všude pod diagonálou nuly. Determinant je pak součin diagonálních prvků, čili n^{n-2}.

Přejdeme k důkazu věty 7.5.1. Nejdříve pevně zvolíme libovolnou *orientaci* $\vec{G}$ grafu G, t.j. pro každou hranu e_k vybereme jeden její

vrchol jako *začátek* a druhý jako *konec* (terminologie pro orientované grafy se probírá v části 3.7). Příslušnou orientovanou hranu budeme značit také e_k. Je zajímavé, že pro důkaz nějakou orientaci potřebujeme, přestože výsledek na ní nebude záležet! Definujeme teď pomocnou matici $D = D_{\vec{G}}$ (zvanou *matice incidence* pro zvolenou orientaci $\vec{G}$). Ta bude mít n řádků (ty odpovídají vrcholům grafu $\vec{G}$) a m sloupců (odpovídají hranám $\vec{G}$), a bude zadána takto:

$$d_{ik} = \begin{cases} -1 & \text{je-li } i \text{ začátek hrany } e_k \\ 1 & \text{je-li } i \text{ konec hrany } e_k \\ 0 & \text{jinak, tedy pro } i \notin e_k \end{cases}$$

Všimněme si, že matice D má v každém sloupci právě jednu 1, jednu -1 a zbytek 0, speciálně tedy součet všech řádek je nulový vektor.

Připomeňme, že je-li A matice, značí A^T matici k ní transponovanou, t.j. A^T má na místě (i,j) prvek a_{ji}. Označme dále B matici vzniklou z D odebráním prvního řádku. Nejprve uvedeme do souvislosti matici D a Laplaceovu matici grafu G:

7.5.2 Lemma. *Platí* $DD^T = Q$ *a* $BB^T = Q_{11}$ *(kde* $D = D_{\vec{G}}$ *pro nějakou libovolnou orientaci* $\vec{G}$ *grafu* G*).*

Důkaz. Podle definice násobení matic je prvek v pozici (i,j) v součinu DD^T roven $\sum_{k=1}^{m} d_{ik}d_{jk}$. Pro $i = j$ je $d_{ik}d_{jk} = d_{ik}^2$ rovno 1, pokud i je začátek nebo konec hrany e_k, a 0 jinak, tedy uvedený součet je právě stupeň vrcholu i v grafu G. Pro $i \neq j$ je součin $d_{ik}d_{jk}$ nenulový v jediném případě, totiž když $e_k = \{i,j\}$, a tehdy je roven -1. Srovnáním s definicí Laplaceovy matice vidíme, že $DD^T = Q$. Druhá rovnost v lemmatu plyne prostě z definice násobení matic. □

Teď první souvislost koster s determinanty:

7.5.3 Lemma. *Buď* T *nějaký graf na množině vrcholů* $\{1,2,\ldots,n\}$ *s* $n-1$ *hranami* $(n \geq 2)$*, a* $\vec{T}$ *nějaká jeho orientace. Buď* $D_{\vec{T}}$ *matice incidence orientovaného grafu* $\vec{T}$*, a nechť* C *označuje matici vzniknou z matice* $D_{\vec{T}}$ *vynecháním jejího prvního řádku. Potom* $\det C$ *má jednu*

z hodnot 0, 1, −1, a je nenulový právě když T je strom (t.j. kostra úplného grafu na $\{1, 2, \ldots, n\}$).

Důkaz povedeme indukcí podle n, počtu vrcholů. Pro $n = 2$ je situace jednoduchá — T má jedinou hranu a je tedy kostrou, a jediný prvek matice C je 1 nebo -1.

Uvažme tedy obecné $n > 2$, a rozlišme dva případy podle toho, jestli některý z vrcholů $2, 3, \ldots, n$ má v grafu T stupeň 1.

Nejprve předpokládejme že takový vrchol stupně 1 existuje. Můžeme případně přečíslovat vrcholy tak, aby stupeň 1 měl vrchol n. To znamená, že matice C má v posledním řádku jediný nenulový prvek (rovný 1 nebo -1), a sice v k-tém sloupci.

Podle vzorce z lineární algebry pro rozvoj determinantu podle řádku matice, použitého na i-tý řádek naší $(n-1) \times (n-1)$ matice C, můžeme psát

$$\det C = \sum_{j=1}^{n-1} (-1)^{i+j} c_{ij} \det C_{ij},$$

(C_{ij} je matice C po vynechání i-tého řádku a j-tého sloupce). Speciálně, vezmeme-li $i = n-1$, máme pouze jediný nenulový člen (protože pouze prvek v k-tém sloupci je nenulový):

$$\det C = (-1)^{n-1+k} c_{n-1,k} \det C_{n-1,k},$$

a tedy $|\det C| = |\det C_{n-1,k}|$.

Tuto zmenšenou matici $C' = C_{n-1,k}$ můžeme dostat vymazáním prvního řádku z incidenční matice $D_{\vec{T}'}$ menšího orientovaného grafu $\vec{T}'$, vzniklého z $\vec{T}$ vynecháním vrcholu n a hrany e_k. Podle indukčního předpokladu tedy víme, že $|\det C'|$ je 1 nebo 0 podle toho, je-li T' (t.j „neorientovaná verze“ $\vec{T}'$) kostra nebo ne. Protože jsme ale z T odstranili vrchol stupně 1 (list), je T' kostra právě když T je kostra. Tím jsme udělali indukční krok pro případ, že některý z vrcholů $2, 3, \ldots, n$ má v T stupeň 1.

Přejděme k druhému případu, kdy žádný z vrcholů $2, 3, \ldots, n$ nemá v T stupeň 1. Nejprve nahlédneme, že za této situace má T izolovaný

vrchol (kdyby tomu tak nebylo, má vrchol 1 stupeň aspoň 1 a ostatní vrcholy stupeň aspoň 2, tedy součet stupňů je aspoň $2n-1$, na což $n-1$ hran grafu T nestačí).

Z existence izolovaného vrcholu vyplývá, že T není kostra; k završení důkazu potřebujeme ukázat, že $\det C = 0$. Je-li izolovaným vrcholem některý z $2, 3, \ldots, n$, určuje v matici C nulový řádek. Je-li izolovaným vrcholem 1, je součet všech řádků matice C roven nulovému vektoru (protože součet všech řádek matice $D_{\overline{T}}$ je nulový). V obou případech máme $\det C = 0$. □

Podle právě dokázaného lemmatu teď víme, že počet koster grafu G je přesně roven počtu čtvercových $(n-1)\times(n-1)$ podmatic matice B s nenulovým determinantem. K dokončení důkazu věty 7.5.1 využijeme jednoho tvrzení o determinantech.

7.5.4 Věta (Binetova-Cauchyho věta). *Nechť A je libovolná matice s n řádky a m sloupci. Potom*

$$\det(AA^T) = \sum_I \det(A_I)^2,$$

kde se sčítá přes všechny n-prvkové podmnožiny $I \in \binom{\{1,2,\ldots,m\}}{n}$, a kde A_I značí matici vzniklou z A vyškrtáním všech sloupců, jejichž indexy neleží v I.

Pro úplnost uvedeme důkaz této věty, ale nejdříve se podíváme, jak z ní plyne věta 7.5.1. S tím, co už víme, je to velmi prosté. Podle lemmatu 7.5.2 a potom podle věty 7.5.4 je

$$\det Q_{11} = \det(BB^T) = \sum_{I \in \binom{\{1,2,\ldots,m\}}{n-1}} \det(B_I)^2,$$

a podle lemmatu 7.5.3 vidíme, že posledně uvedený výraz je právě počet koster G. □

Důkaz věty 7.5.4. Označme $M = AA^T$. Rozvineme determinant matice M podle definice, tedy

$$\det M = \sum_\pi \operatorname{sgn}(\pi) \prod_{i=1}^{n} m_{i,\pi(i)},$$

kde se sčítá přes všechny permutace π množiny $\{1, 2, \ldots, n\}$, a kd
$\operatorname{sgn}(\pi)$ značí *znaménko* permutace π (pro každou permutaci je +
nebo -1). Definice znaménka zde nebudeme přímo potřebovat, prot
si připomeneme pouze následující

7.5.5 Fakt. *Pro libovolnou permutaci π množiny $\{1, 2, \ldots, n\}$ a in
dexy i, j, $1 \leq i < j \leq n$, označme symbolem $\pi_{i \leftrightarrow j}$ permutaci, jejíž hod
nota pro i je $\pi(j)$, hodnota pro j je $\pi(i)$ a hodnoty pro všechna ostatn
čísla se shodují s hodnotami π. Potom platí* $\operatorname{sgn}(\pi) = -\operatorname{sgn}(\pi_{i \leftrightarrow j})$.

Dosadíme do rozvoje determinantu M hodnoty prvků m_{ij}, t.
$m_{ij} = \sum_{k=1}^{m} a_{ik} a_{jk}$, a roznásobíme každý ze součinů. Dostáváme

$$\det M = \sum_{\pi} \operatorname{sgn}(\pi) \sum_{k_1, k_2, \ldots, k_n = 1}^{m} \prod_{i=1}^{n} a_{i,k_i} a_{\pi(i),k_i}.$$

Přejdeme nyní k zápisu, který bude v dalším lépe vyhovovat. Volb
n-tice sumačních indexů $k_1, \ldots, k_n$ ve vnitřní sumě můžeme chápa
jako volbu zobrazení $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, m\}$, kde $f(i) = k$
V tomto novém zápisu tedy máme

$$\det M = \sum_{\pi} \operatorname{sgn}(\pi) \sum_{f : \{1,2,\ldots,n\} \to \{1,2,\ldots,m\}} \prod_{i=1}^{n} a_{i,f(i)} a_{\pi(i),f(i)}.$$

V uvedené sumě dále zaměníme pořadí sumace; napřed budeme sčíta
podle funkce f, a potom podle permutace π. Přitom ještě pro poho
dlnější zápis zavedeme označení

$$P(f, \pi) = \prod_{i-1}^{n} a_{i,f(i)} a_{\pi(i),f(i)},$$

$$S(f) = \sum_{\pi} \operatorname{sgn}(\pi) P(f, \pi)$$

a potom máme

$$\det M = \sum_{f : \{1,2,\ldots,n\} \to \{1,2,\ldots,m\}} S(f).$$

Klíčové pro celý důkaz je následující

7.5.6 Lemma. *Pokud funkce $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, m\}$ není prostá, potom $S(f) = 0$ (pro libovolnou volbu matice A).*

Důkaz lemmatu: Nechť i, j jsou indexy takové, že $f(i) = f(j)$. Potom pro libovolnou permutaci π jsou součiny $P(f, \pi)$ a $P(f, \pi_{i \leftrightarrow j})$ (kde užíváme označení z faktu 7.5.5) stejné. Probíhá-li π všechny permutace, potom také $\pi_{i \leftrightarrow j}$ probíhá všechny permutace, takže máme

$$S(f) = \sum_{\pi} \operatorname{sgn}(\pi_{i \leftrightarrow j}) P(f, \pi_{i \leftrightarrow j}) = \sum_{\pi} -\operatorname{sgn}(\pi) P(f, \pi) = -S(f),$$

tedy $S(f) = 0$ jak tvrdí lemma. □

Dokončení důkazu věty 7.5.4. Podle lemmatu můžeme psát

$$\det(AA^T) = \sum_{f:\{1,2,\ldots,n\} \hookrightarrow \{1,2,\ldots,m\}} S(f),$$

kde se sčítá přes všechny *prosté* funkce z $\{1, 2, \ldots, n\}$ do $\{1, 2, \ldots, m\}$.

Zvolme nyní nějakou množinu $I \in \binom{\{1,2,\ldots,m\}}{n}$, a počítejme

$$\det(A_I)^2 = \det(A_I) \det(A_I^T) = \det(A_I A_I^T).$$

Tento determinant můžeme rozvinout přesně stejným postupem, jak jsme to udělali pro determinant AA^T; tentokrát dostaneme

$$\det(A_I A_I^T) = \sum_{f:\{1,2,\ldots,n\} \hookrightarrow I} S(f).$$

Máme tedy

$$\sum_{I \in \binom{\{1,2,\ldots,m\}}{n}} \det(A_I)^2 = \sum_{I \in \binom{\{1,2,\ldots,m\}}{n}} \sum_{f:\{1,2,\ldots,n\} \hookrightarrow I} S(f) =$$

$$\sum_{f:\{1,2,\ldots,n\} \hookrightarrow \{1,2,\ldots,m\}} S(f) = \det(AA^T)$$

(předposlední rovnost plyne z toho, že prostá funkce

$$f : \{1, 2, \ldots, n\} \hookrightarrow \{1, 2, \ldots, m\}$$

jednoznačně určuje n-prvkovou množinu I svých hodnot). Tím je věta 7.5.4 dokázána. □

Cvičení

1. V tomto cvičení G je graf na n vrcholech, Q jeho Laplaceova matice a Q^* značí matici, jejíž prvek v pozici (i,j) je roven $(-1)^{i+j} \det Q_{ij}$.

   (a) Ukažte $\det Q = 0$.

   (b) Ukažte, že je-li graf G souvislý, má jeho Laplaceova matice hodnos $n-1$.

   (c)* Ukažte, že pro nesouvislý graf G má Laplaceova matice hodnos nejvýš $n-2$. Z toho odvoďte, že pro nesouvislý G je Q^* nulová matice.

   (d) Ukažte, že je-li G souvislý a $x \in \mathbf{R}^n$ je libovolný vektor, pak $Qx =$ právě když x je násobkem vektoru $(1,1,\ldots,1)$.

   (e)* Dokažte, že součin QQ^* je nulová matice. Pomocí (d) pak odvoďte že všechny prvky matice Q^* jsou stejné.

2. Buď G graf, který může (výjimečně pro účely tohoto cvičení) obsaho vat smyčky a násobné hrany. Nechť e je hrana, která není smyčkou definujme $G - e$ jako G po vynechání hrany e, a $G : e$ jako graf vzniklý vypuštěním hrany e z G a následným slepením jejích konco vých vrcholů do jednoho vrcholu (ostatní hrany se přitom zachovají touto operací se mohou objevit nové smyčky nebo nové násobné hran — to je rozdíl proti operaci kontrakce hrany zavedené v části 5.4).

   (a) Ukažte, že $\kappa(G) = \kappa(G-e) + \kappa(G:e)$.

   (b) Pokuste se rekurzivním počítáním, založeným na (a), určit poče koster grafu (trojrozměrné) krychle.

   (c) Najděte počet koster v (b) pomocí věty 7.5.1.

3. Řešte cvičení 2 k úvodu této kapitoly pomocí věty 7.5.1.

4.* Buď G (neorientovaný) graf, a M jeho matice incidence; t.j., má-li G vrcholy $v_1, v_2, \ldots, v_n$ a hrany $e_1, e_2, \ldots, e_k$, pak M je $n \times m$ matic splňující

$$m_{ik} = \begin{cases} 1 & \text{jestliže } v_i \in e_k \\ 0 & \text{jinak.} \end{cases}$$

   Dokažte, že následující dvě podmínky jsou ekvivalentní:

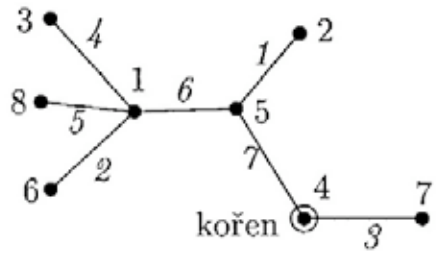
   (i) G je bipartitní.

   (ii) Libovolná čtvercová podmatice M (vzniklá z M vypuštěním někte rých řádků a sloupců) má determinant 0,1 nebo -1 (matice M s tout vlastností se jmenuje *unimodulární*).

7.6 Důkaz zatím asi nejjednodušší

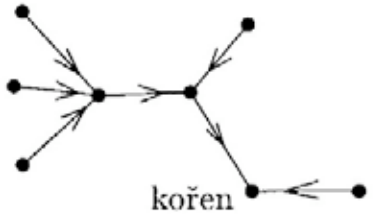
I v dobře prozkoumaných oblastech matematiky je stále co objevovat. Tak například zcela nedávno našel matematik–statistik Jim Pitman z Kalifornské university v Berkeley nový, velmi jednoduchý důkaz Cayleyho formule. Zazáří v něm počítání dvěma způsoby, zdánlivě velmi jednoduchý trik, o jehož užitečnosti jsme se již přesvědčili v předchozí kapitole. Nepoužije se přímo, ale na vhodné zjemnění původní úlohy.

V tomto důkazu Cayleyho formule budeme počítat dvěma způsoby *povykosy*. Co je to povykos? Zkrácený název pro *po*stup *vý*roby *ko*řenového *s*tromu (o kořenových stromech viz část 4.2). Formálně je povykos definován jako uspořádaná trojice $(T, r, č)$, kde T je strom na množině vrcholů $V = \{1, 2, \ldots, n\}$, $r \in V$ je jeho kořen, a $č$ je očíslování hran, neboli bijekce $č : E(T) \to \{1, 2, \ldots, n-1\}$. Na obrázku je příklad povykosu:



Můžeme si představovat, že začneme s prázdným grafem na množině vrcholů V a vyrábíme kořenový strom postupným přidáváním hran; očíslování $č$ kóduje pořadí přidávání hran. Pro každý strom T můžeme kořen r volit n způsoby a pro očíslování hran $č$ je $(n-1)!$ možností, takže počet povykosů je $n(n-1)!\,\kappa(K_n)$.

Pro druhý způsob počítání povykosů budeme kořenový strom uvažovat jako orientovaný strom, kde všechny šipky směřují ke kořenu:



Naopak, každá orientace stromu, pro niž existuje právě jeden vrcho který není počátkem žádné šipky, odpovídá jednoznačně kořenovém stromu (zmíněný jediný vrchol je kořen). I povykos teď budeme inte pretovat v této orientované podobě, a budeme počítat, kolik povykos můžeme dostat, začneme-li z prázdného orientovaného grafu a budem postupně přidávat šipky v $n-1$ krocích.

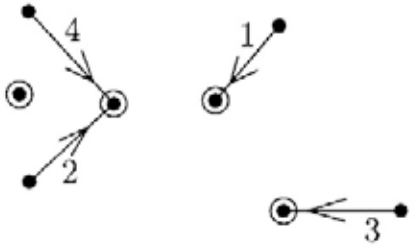
První šipka musí spojovat dva různé vrcholy, a tudíž ji můžem přidat $n(n-1)$ způsoby. Pro druhou šipku máme ještě další omezujíc podmínku: nesmí vycházet z téhož vrcholu jako šipka první. Jaká jso obecně omezení na přidání další šipky?

(A) Nesmíme vytvořit kružnici (v neorientovaném smyslu), tedy nov šipka musí spojovat dvě různé komponenty již vytvořeného graf (komponenty se opět myslí bez ohledu na orientaci).

(B) Na konci musí z každého vrcholu až na jediný vycházet nějak šipka, přičemž máme k dispozici celkem $n-1$ šipek. Nesmím tedy promarnit ani jedinou, a každá nová šipka musí vycháze z vrcholu, z nějž dosud žádná šipka nevycházela.

Klíčové pozorování je, že *v každé komponentě již vytvořeného graf je právě jeden vrchol, z nějž nevychází žádná šipka.* To je proto, ž komponenta má nějakých m vrcholů a $m-1$ hran, a z každého vr cholu vychází nejvýš jedna šipka, neboť jsme i v předchozím postup dodržovali podmínku (B).

Po přidání k šipek s dodržením (A) a (B) má graf $n-k$ komponen (ověřte). Obrázek ukazuje situaci po přidání čtyř šipek podle povykos na prvním obrázku:

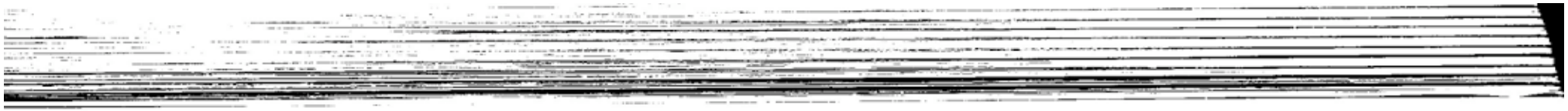


Další šipka, číslo $k+1$, může nyní vést do libovolného vrcholu v nějak z komponent, a vycházet musí z kořene některé jiné komponenty, a pr její přidání máme proto $n(n-k-1)$ možností.

Každý takový postup dává po $n-1$ krocích právě jeden povykos. Proto povykosů je

$$\prod_{k=0}^{n-2} n(n-k-1) = (n-1)!\, n^{n-1}.$$

Porovnáním obou výrazů pro počet povykosů dostáváme $\kappa(K_n) = n^{n-2}$. □



8

Konečné projektivní roviny

Matematika se často zajímá o objekty, vyznačující se v nějakém smyslu velkou pravidelností, mnoha symetriemi atd. (viz například pravidelné mnohostěny v části 5.3). V této kapitole se budeme zabývat jistými hodně pravidelnými systémy konečných množin, tzv. konečnými projektivními rovinami, a s nimi úzce souvisejícími čtvercovými tabulkami čísel, tzv. ortogonálními latinskými čtverci.

8.1 Definice a vlastnosti konečné projektivní roviny

Konečná projektivní rovina bude množinový systém s jistými speciálními vlastnostmi.

8.1.1 Definice (Konečná projektivní rovina). *Nechť X je nějaká konečná množina, a nechť $\mathcal{P}$ je systém podmnožin množiny X. Dvojice $(X, \mathcal{P})$ se nazývá* konečná projektivní rovina, *pokud splňuje následující axiomy:*

(P0) *Existuje čtyřbodová množina $\check{C} \subseteq X$ taková, že $|P \cap \check{C}| \leq 2$ pro každou množinu $P \in \mathcal{P}$.*

(P1) *Každé dvě různé množiny $P_1, P_2 \in \mathcal{P}$ se protínají právě v jednom bodě, t.j. $|P_1 \cap P_2| = 1$.*

(P2) *Pro každé dva různé body $x_1, x_2 \in X$ existuje právě jedna množina $P \in \mathcal{P}$ taková, že $x_1 \in P$ a $x_2 \in P$.*

Je-li $(X, \mathcal{P})$ konečná projektivní rovina, budeme prvkům X říkat *body* a množinám z $\mathcal{P}$ *přímky*. Vztah $x \in P$ (kde $x \in X$ a $P \in \mathcal{P}$) budeme vyjadřovat obratem „bod x leží na přímce P" nebo taky „přímka P prochází bodem x". Vyjádříme-li axiomy (P0)–(P2) v této řeči, začnou se podobat povědomým geometrickým tvrzením. Axiom (P1) říká, že každé dvě (různé) přímky se protínají právě v jednom bodě, a (P2) praví, že každými dvěma různými body prochází právě jediná přímka. Axiom (P0) potom požaduje existenci 4 bodů, z nichž žádné 3 neleží na přímce. Jsou-li $a, b \in X$ dva body konečné projektivní roviny, budeme jedinou přímku $P \in \mathcal{P}$ obsahující a i b značit symbolem $\overline{ab}$. Jsou-li $P, P' \in \mathcal{P}$ dvě přímky, budeme jediný bod jejich průniku nazývat jejich *průsečíkem*.

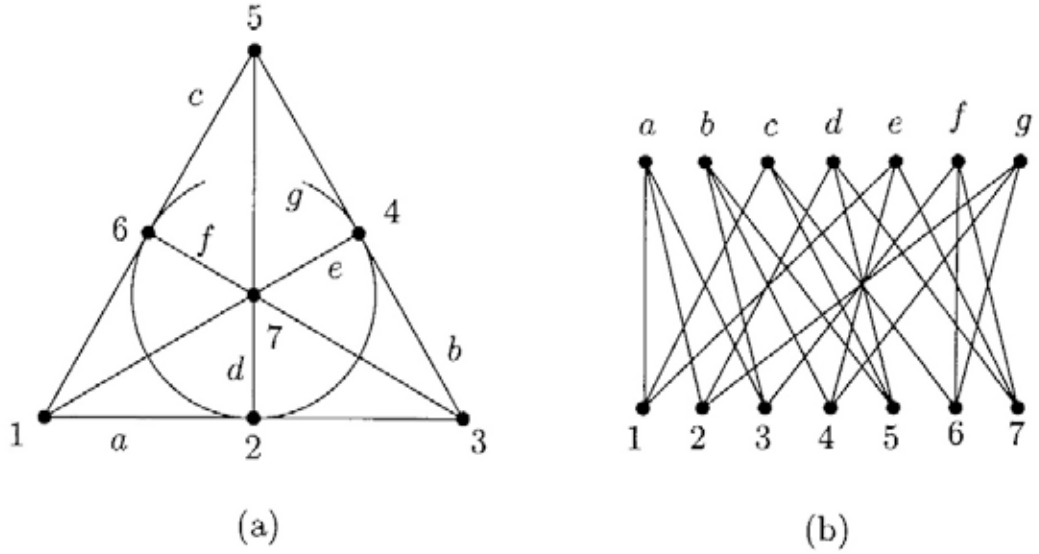
Konečné projektivní roviny jsou konečnou analogií tzv. projektivní roviny (přesněji *reálné projektivní roviny*) známé z geometrie. Zmíněná terminologie („projektivní rovina", „přímky") poukazuje na tuto analogii. Krátce tedy odbočíme a nastíníme, co je reálná projektivní rovina (což beztak patří k všeobecnému matematickému vzdělání).

V obvyklé (euklidovské) rovině se každé dvě přímky protínají v jednom bodě, až na jednu výjimku — rovnoběžky se neprotínají nikde. V mnoha geometrických úvahách je taková výjimka dosti nepříjemná, neboť vyžaduje rozbor různých speciálních případů v důkazech i v analytických výpočtech. Reálná projektivní rovina je vhodné rozšíření euklidovské roviny o množinu dalších bodů, nazývající se *body v nekonečnu*. Populárně řečeno, každému směru přímek v rovině odpovídá jeden bod v nekonečnu, v němž se všechny přímky rovnoběžné s tímto směrem protínají. Všechny body v nekonečnu leží na jedné společné *přímce v nekonečnu*. Tím se dosáhne toho, že nyní se skutečně každé dvě přímky protínají právě v jednom bodě (který ovšem může ležet v nekonečnu).

Body v nekonečnu zde nejsou nějakou filosofickou záhadností, projektivní rovina je matematickou konstrukcí trochu podobného typu, jako třeba konstrukce racionálních čísel z celých čísel nebo reálných čísel z racionálních, tedy jakési zúplnění. Zájemci najdou tuto konstrukci v části 8.2.

Každé dvě přímky v reálné projektivní rovině se protínají právě v jednom bodě (to je podmínka (P1)), a každými dvěma body prochází právě jedna přímka (to je podmínka (P2)). Mnoho geometrických úvah a konstrukcí v reálné projektivní rovině se opírá pouze o tyto dva axiomy.

Analogie konečných projektivních rovin s reálnou projektivní rovinou je užitečná jako motivace pojmů a často i pro intuici. Nesmí se však



Obrázek 8.1: Fanova rovina (a), a její graf incidence (b).

zapomínat, že přísně vzato konečná projektivní rovina je pouze systém konečných množin s vlastnostmi (P0)–(P2), a nelze na ni automaticky přenášet různé další geometrické pojmy a představy. Nejdůležitější rozdíl asi je, že zatímco body na obyčejné geometrické přímce jsou přirozeně uspořádány „podél" přímky, v konečné projektivní rovině žádné takové přirozené uspořádání nemáme.

8.1.2 Příklad. *Nejmenší konečná projektivní rovina má 7 bodů a 7 přímek (všechny přímky jsou tříbodové), a nazývá se* Fanova rovina. *Je znázorněna na obrázku 8.1(a): body jsou vyznačeny puntíky označenými 1–7, a trojice bodů každé přímky je spojena úsečkou, v jednom případě kruhovým obloukem*[1]*; tyto spojnice jsou v obrázku označeny a–g.*

Fanova rovina je užitečný matematický objekt, často je nejmenším protipříkladem na různě domněnky a pod.

Dokážeme teď několik tvrzení, která ilustrují, že při konstrukci projektivní roviny máme mnohem menší svobodu, než je na první pohled patrné.

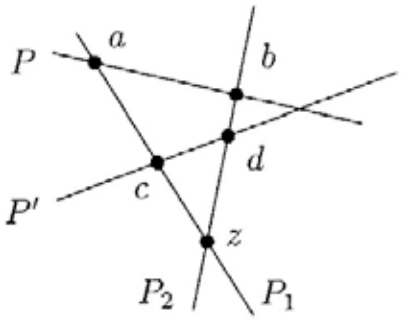
[1] Dá se ukázat, že sedmici bodů nelze nakreslit do roviny tak, aby každá trojice odpovídající přímce ve Fanově rovině ležela na euklidovské přímce — viz cvičení 6.

8.1.3 Tvrzení. *Buď $(X, \mathcal{P})$ konečná projektivní rovina. Potom všechny její přímky mají stejný počet bodů, t.j. $|P| = |P'|$ pro každé $P, P' \in \mathcal{P}$.*

Důkaz. Zvolme libovolné 2 přímky $P, P' \in \mathcal{P}$. Nejprve dokážeme pomocné tvrzení: *Existuje bod $z \in X$, neležící na P ani na P'.*

Důkaz pomocného tvrzení. Uvažme množinu $\check{C} \subseteq X$ jako v axiomu (P0); máme $|P \cap \check{C}| \leq 2$, $|P' \cap \check{C}| \leq 2$. Pokud $\check{C}$ není obsaženo v $P \cup P'$, jsme hotovi. Jediná zbývající možnost je, že P protíná $\check{C}$ ve dvou bodech (označme je a, b), a P' protíná $\check{C}$ ve dvou zbývajících bodech (označme je c, d). Uvážíme potom přímky $P_1 = \overline{ac}$ a $P_2 = \overline{bd}$. Nechť z je bod, v němž se P_1 a P_2 protínají.

Následující geometrický obrázek situaci ilustruje:

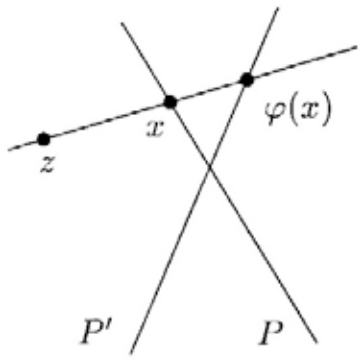


Musíme ale dávat dobrý pozor, abychom v našem důkazu používali jedině podmínek (P0)–(P2), a na intuitivní geometrickou představu podle obrázku nespoléhali — koneckonců konečné projektivní roviny vypadají v mnoha ohledech úplně jinak než „obyčejná“ rovina.

Tvrdíme, že $z \notin P \cup P'$. Přímky P a P_1 se protínají v jediném bodě, totiž v a, takže kdyby $z \in P$, muselo by být $z = a$. To ale není možné, poněvadž pak by přímka P_2 obsahovala body $z = a$, b a d, tedy 3 body z $\check{C}$, což je zakázáno podmínkou (P0). Proto $z \notin P$, a analogicky se ukáže $z \notin P'$. Tím je dokázáno pomocné tvrzení.

Ukážeme teď, že přímky P a P' jsou stejně velké; za tím účelem definujeme zobrazení $\varphi : P \to P'$, o němž se pak ověří, že je to bijekce.

Obraz $\varphi(x)$ bodu $x \in P$ definujeme jako průsečík přímek $\overline{zx}$ a P', kde z je bod jako v pomocném tvrzení. Obrázek tomu opět dodá názornosti:



Podle axiomů (P1) a (P2) je bod $\varphi(x)$ dobře definován. Přitom je-li $y \in P'$ libovolný bod, uvažme přímku $\overline{zy}$, a buď x její průsečík s přímkou P. Pak $\overline{zy}$ a $\overline{zx}$ je tatáž přímka, a proto máme $y = \varphi(x)$. Zobrazení φ je tedy bijekce, a proto $|P| = |P'|$. □

8.1.4 Definice (Řád projektivní roviny). Řádem *konečné projektivní roviny* $(X, \mathcal{P})$ *rozumíme číslo* $|P| - 1$, *kde* $P \in \mathcal{P}$ *je libovolná přímka (podle předchozího tvrzení řád nezávisí na tom, kterou konkrétní přímku* P *vybereme).*

Například Fanova rovina je řádu 2 (přímky jsou tříbodové), a dá se dokázat, že je to jediná projektivní rovina řádu 2 (až na případné přejmenování bodů, t.j. až na isomorfismus).

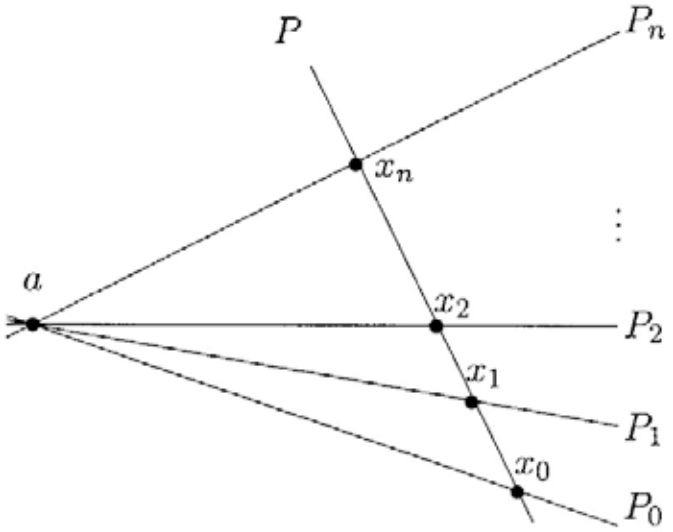
Budeme pokračovat v dokazování vlastností konečných projektivních rovin.

8.1.5 Tvrzení. *Nechť* $(X, \mathcal{P})$ *je projektivní rovina řádu* n. *Potom platí*

(i) *Každým bodem* $x \in X$ *prochází právě* $n + 1$ *přímek.*

(ii) $|X| = n^2 + n + 1$.

(iii) $|\mathcal{P}| = n^2 + n + 1$.



Obrázek 8.2: Ilustrace k důkazu 8.1.5(ii).

Důkaz (i). Uvažme libovolný bod $x \in X$. Nejdříve nahlédneme, že existuje přímka P jím neprocházející. Je-li totiž $\check{C}$ konfigurace 4 bodů jako v (P0) a a, b, c jsou 3 její body různé od x, potom aspoň jedna z přímek $\overline{ab}$ a $\overline{ac}$ neobsahuje x, jak se snadno zkontroluje. Každým z $n+1$ bodů takové přímky P prochází právě jedna přímka obsahující též x. Přitom každá přímka, procházející bodem x, protne P v nějakém bodě y, a tedy je to přímka tvaru $\overline{xy}$, takže bodem x prochází přesně $n+1$ přímek.

Důkaz (ii). Zvolíme nějakou přímku $P = \{x_0, x_1, x_2, \ldots, x_n\} \in \mathcal{P}$ a bod $a \notin P$, viz obr. 8.2. Označme P_i přímku $\overline{ax_i}$, $i = 0, 1, \ldots, n$. Podle (P1) se každé dvě z těchto přímek, P_i a P_j, protínají právě v jednom bodě, a tím je právě a. Přímky $P_0, P_1, \ldots, P_n$ mají každá kromě a ještě dalších n bodů, a celkem tedy obsahují $(n+1)n+1 = n^2+n+1$ různých bodů. Ukážeme, že libovolný bod $x \in X$ již leží na některé přímce P_i; tím bude dokázáno tvrzení (ii).

Body x a a můžeme podle (P2) proložit nějakou přímku Q. Tato přímka protne, podle (P1), přímku P v některém bodě x_i, a podle (P2) (jednoznačnost) je tedy totožná s přímkou P_i.

Důkaz části (iii) nyní vynecháme. Řekneme si v dalším jeden důležitý princip, podle něhož uvidíme, že (iii) plyne okamžitě z toho, co jsme už dokázali. □

Dualita. Heslovitě se dualita dá vyjádřit jako „záměna rolí bodů a přímek". Abychom to mohli formulovat přesně, zavedeme nejdříve obecnou definici. Mějme nějaký (zatím libovolný) systém $\mathcal{S}$ podmnožin množiny X. Definujeme *duální množinový systém* $(Y, \mathcal{T})$ k systému $(X, \mathcal{S})$. Prvky tohoto nového množinového systému budou množiny z $\mathcal{S}$, t.j. $Y = \mathcal{S}$. Pro každý bod $x \in X$ zařadíme do systému $\mathcal{T}$ množinu všech množin $S \in \mathcal{S}$ takových, že $x \in S$. Tím dostaneme soubor $\mathcal{T}$ podmnožin $\mathcal{S}$, jehož množiny odpovídají bodům z X. Zapsáno formulí, máme

$$\mathcal{T} = \Big\{ \{S \in \mathcal{S};\ x \in S\};\ x \in X \Big\}.$$

Jestliže například $X = \{1, 2, 3\}$ a $\mathcal{S} = \{A, B\}$, kde $A = \{1, 2\}$, $B = \{1, 3\}$, potom duální systém $(Y, \mathcal{T})$ bude mít $Y = \mathcal{S} = \{A, B\}$, $\mathcal{T} = \{\{A, B\}, \{A\}, \{B\}\}$.

Ještě jinak si můžeme představit konstrukci duálního množinového systému takto: Definujeme na množině $X \cup \mathcal{S}$ bipartitní graf, tzv. *graf incidence*, v němž každá množina $S \in \mathcal{S}$ bude spojena hranou právě se všemi svými body $x \in S$ (a tudíž bod $x \in X$ bude spojen právě se všemi množinami jej obsahujícími). Stručně můžeme říci, že hrany grafu odpovídají relaci náležení. Pro Fanovu rovinu (což je jistý množinový systém) je tento graf nakreslen na obr. 8.1(b) (vrcholy jsou popsány označením příslušných bodů a přímek)[2]. Potom uvedený přechod k duálnímu systému prostě znamená, že ty vrcholy bipartitního grafu, které jsme dříve chápali jako body, budeme nyní chápat jako množiny, a obráceně, t.j. na obrázku bychom jenom překlopili graf vzhůru nohama. V kontextu konečných projektivních rovin se tedy zaměňují body za přímky a přímky za body (podobná dualita se používá i v reálné projektivní rovině).

8.1.6 Tvrzení. *Množinový systém duální ke konečné projektivní rovině je opět konečná projektivní rovina.*

[2]Tento graf se jmenuje *Heawoodův graf* a je to pěkný a zajímavý příklad grafu — i když naše nakreslení moc pěkně nevypadá; dokážete najít hezčí?

Důkaz. Buď $(X, \mathcal{P})$ konečná projektivní rovina, a $(Y, \mathcal{Q})$ množinový systém k ní duální. Pro něj je potřeba ověřit podmínky (P0)–(P2). Začneme podmínkou (P0). Přeložíme-li ji do řeči výchozího systému $(X, \mathcal{P})$, znamená to, že máme najít 4 přímky $P_1, P_2, P_3, P_4 \in \mathcal{P}$, z nichž žádné 3 nemají společný bod. Uvažme 4-bodovou množinu $\check{C} = \{a, b, c, d\} \subseteq X$ jako v podmínce (P0), a definujme $P_1 = \overline{ab}$, $P_2 = \overline{cd}$, $P_3 = \overline{ad}$, $P_4 = \overline{bc}$. Podíváme-li se na libovolné 3 z těchto 4 přímek, mají vždy 2 z nich společný nějaký bod z $\check{C}$, jímž třetí z nich neprochází. Proto libovolné 3 z přímek $P_1, \ldots, P_4$ mají prázdný průnik. Tím jsme ověřili (P0) pro duální množinový systém.

Přeložíme-li podobně podmínku (P1) pro duální systém, zjistíme, že se požaduje následující: jsou-li $x, x' \in X$ dva různé body, potom existuje právě jedna přímka $P \in \mathcal{P}$ obsahující oba — a to je přesně podmínka (P2) pro $(X, \mathcal{P})$. Podobně zjistíme, že (P2) pro duální systém vyplývá z (P1) pro původní systém $(X, \mathcal{P})$. □

Teď tedy můžeme množinový systém duální ke konečné projektivní rovině oprávněně nazvat *duální projektivní rovina*. Z tvrzení 8.1.5(i) vyplývá, že přechodem k duální projektivní rovině se zachovává řád. Také je vidět, že části (ii) a (iii) tvrzení 8.1.5 jsou navzájem duální, a pokud jsme dokázali jedno z nich, musí platit i druhé.

Obecně, máme-li nějaké pravdivé tvrzení o projektivní rovině řádu n, a zaměníme v něm všude navzájem slova „bod“ a „přímka“, dostaneme opět pravdivý výrok. Přitom ovšem musíme náležitě interpretovat příslušné pojmy, například kde v původním výroku bylo „přímku P_1, P_2 se protínají v bodě x“, bude nyní „body x_1, x_2 jsou spojeny přímkou P“ a pod. To je tedy jakýsi „recept na výrobu vět“ a nazývá se *princip duality*. Všimli si ho geometři studující reálnou projektivní rovinu.

Cvičení

1. (a) Najděte příklad množinového systému $(X, \mathcal{P})$ na konečné množině X, který splňuje podmínky (P1), (P2), ale nesplňuje (P0).

   (b) Najděte X a $\mathcal{P}$ jako v (a), kde navíc $|X| \geq 10$, $|\mathcal{P}| \geq 10$, a každá $P \in \mathcal{P}$ má aspoň 2 body.

2. Nechť X je konečná množina a $\mathcal{P}$ systém jejích podmnožin, splňující podmínky (P1), (P2) a následující (P0′):

   > Existují aspoň 2 různé přímky $P_1, P_2 \in \mathcal{P}$, z nichž každá má aspoň 3 body.

   Dokažte, že potom $(X, \mathcal{P})$ je konečná projektivní rovina.

3.* Popište všechny množinové systémy $(X, \mathcal{P})$ (kde $X \neq \emptyset$ je konečné), splňující (P1),(P2), ale nikoli (P0).

4. Dokažte část (iii) tvrzení 8.1.5 přímo, bez použití duality.

5.* Nechť X je množina s n^2+n+1 prvky a $\mathcal{P}$ je systém tvořený n^2+n+1 jejími $(n+1)$-prvkovými podmnožinami, z nichž každé 2 se protínají nejvýš v jednom bodě.

   (a) Dokažte, že každá dvojice bodů z X je obsažena v právě jedné množině z $\mathcal{P}$.

   (b) Dokažte, že každým bodem prochází nejvýš $n+1$ množin.

   (c) Dokažte, že každým bodem prochází právě $n+1$ množin.

   (d) Dokažte, každé 2 množiny z $\mathcal{P}$ se protínají.

   (e) Ověřte, že $(X, \mathcal{P})$ je projektivní rovina řádu n.

   (V tomto cvičení se hojně využije počítání dvěma způsoby.)

6. Ukažte, že Fanovu rovinu nelze vnořit do „obyčejné“ (euklidovské) roviny, to znamená, že neexistuje 7 přímek a 7 bodů v euklidovské rovině tak, že každá dvojice bodů leží na jedné z přímek a každá dvojice přímek má průsečík v jednom z bodů. Využijte cvičení 5.3.6.

8.2 Konstrukce projektivních rovin

Projektivní roviny řádu 2, 3, 4 a 5 existují, ale žádná projektivní rovina řádu 6 neexistuje! (Dokázat to je dost pracné, musí se rozebrat velmi mnoho případů.) Projektivní roviny řádů 7,8, a 9 opět existují, řádu 10 nikoliv. Kde je v tom nějaká pravidelnost? Konečná projektivní rovina řádu n existuje, kdykoliv existuje konečné těleso[3] s přesně n

[3] V algebraickém smyslu, t.j. množina s operacemi sčítání, odčítání, násobení a dělení splňující jisté podmínky; viz dodatek o algebře.

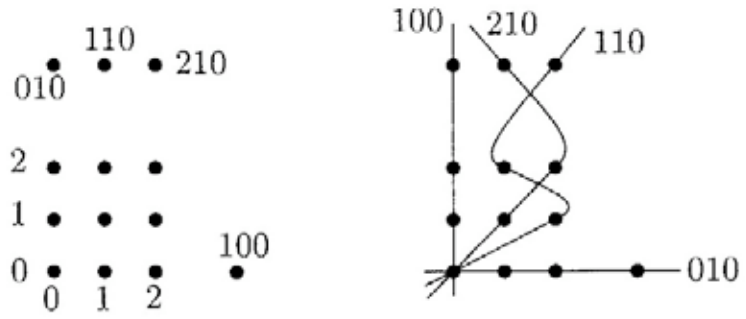
prvky, což je právě když n je mocninou nějakého prvočísla (speciálně tedy existují projektivní roviny libovolně velkých řádů).

Pro n dělitelné aspoň dvěma různými prvočísly sice n-prvkové těleso neexistuje, ale neví se, zda nemůže přesto existovat nějaká projektivní rovina řádu n. Je známo, že pokud číslo n dává při dělení 4 zbytek 1 nebo 2 a přitom se nedá napsat jako součet dvou čtverců celých čísel, potom projektivní rovina řádu n neexistuje (je to dost těžká věta). To například vylučuje existenci projektivní roviny řádu 6 nebo 14 a mnoha dalších řádů, ale zdaleka nepokrývá všechny možné řády, např. o $n = 10$ nebo 12 to nic neříká.

Existence konečné projektivní roviny řádu 10 je také vyloučena. Tyto výsledky mají zajímavou historii. Pro řád 6 se neexistanci projektivní roviny pokoušel dokázat již Euler, podařilo se to ale až G. Tarrymu kolem roku 1900. Pro řád 10 se to prokázalo nedávno neobyčejně rozsáhlými výpočty na počítačích (dokonce armádních, totiž armády Spojených států). Pro nejbližší vyšší řád, 12, je existence projektivní roviny stále otevřený problém. Je sice jasné, že takový problém se dá vyřešit probráním konečně mnoha poměrně malých konfigurací, nicméně počet konfigurací je pro soudobou výpočetní techniku příliš obrovský.

Algebraická konstrukce projektivní roviny. Pro zájemce uvedeme, jak se zkonstruuje projektivní rovina. Obzvlášť nás samozřejmě budou zajímat konečné projektivní roviny, ale půvab konstrukce je i v tom, že přesně stejně funguje pro reálnou projektivní rovinu. Konstrukce vychází z nějakého tělesa K. Pro reálnou projektivní rovinu (t.j. vhodné rozšíření obvyklé euklidovské roviny o body v nekonečnu) se vezme za K těleso $\mathbf{R}$ všech reálných čísel. Budeme-li za K volit n-prvkové těleso, zkonstruujeme konečnou projektivní rovinu řádu n. Průběžně budeme konstrukci ilustrovat pro tříprvkové těleso K, t.j. množinu $\{0, 1, 2\}$ s operacemi sčítání a násobení modulo 3.

Nejprve uvážíme množinu $T = K^3 \setminus \{(0,0,0)\}$, čili množinu všech uspořádaných trojic (x, y, t), kde $x, y, t \in K$ a x, y, t nejsou všechna zároveň rovna nule. Na T definujeme ekvivalenci $\approx$ takto: $(x_1, y_1, t_1) \approx (x_2, y_2, t_2)$ právě když existuje nenulové $\lambda \in K$ takové, že $x_2 = \lambda x_1$, $y_2 = \lambda y_1$ a $t_2 = \lambda t_1$ (není těžké ověřit, že to opravdu je ekvivalence). Body konstruované projektivní roviny budou třídy této ekvivalence. Takto vy-



Obrázek 8.3: Ilustrace ke konstrukci projektivní roviny řádu 3.

robená projektivní rovina[4] se v literatuře zpravidla označuje PK^2, kde místo K se případně píše konkrétní těleso; např. reálná projektivní rovina se značí $P\mathbf{R}^2$.

Abychom získali o projektivní rovině lepší představu, vybereme si z každé třídy ekvivalence $\approx$ jednu trojici jako reprezentanta. Jako reprezentanty vezmeme ty trojice, *jejichž poslední nenulová složka je rovna 1.* Budou to tedy trojice tvaru $(x, y, 1)$, $(x, 1, 0)$ $(x, y \in K)$ a trojice $(1, 0, 0)$; je snadné si rozmyslet, že každá jiná trojice je ekvivalentní některé z uvedených, a naopak že žádné dvě trojice zmíněných tvarů nemohou být ekvivalentní.

Bylo by nepohodlné mluvit stále o třídách ekvivalence. Proto nadále budeme říkat „bod (x, y, t)" pro nějakou trojici z T, a budeme tím myslet celou třídu ekvivalence $\approx$ obsahující tento bod.

Je-li K n-prvkové těleso, můžeme spočítat, kolik dostaneme bodů. Bodů tvaru $(x, y, 1)$ je n^2, bodů tvaru $(x, 1, 0)$ je n a navíc jeden bod $(1, 0, 0)$ — dohromady tedy $n^2 + n + 1$ jak to má být. Pro $n = 3$ jsou všechny body nakresleny na obr. 8.3 vlevo; body tvaru $(x, y, 1)$ jsou popsány hodnotami x, y na souřadnicových osách, ostatní body přímo příslušnými trojicemi.

Pro reálnou projektivní rovinu, bod tvaru $(x, y, 1)$ zpravidla ztotožňujeme s bodem (x, y) euklidovské roviny, body s nulovou poslední složkou jsou body v nekonečnu. Jinak řečeno, trojici (x, y, t) s $t \neq 0$ odpovídá „obyčejný" bod $(\frac{x}{t}, \frac{y}{t})$.

Teď je třeba definovat přímky. Pro každou trojici $(a, b, c) \in K^3 \setminus$

[4]Pro konečné těleso jsme ještě nedokázali, že touto konstrukcí dostaneme projektivní rovinu ve smyslu definice 8.1.1, dokonce jsme ještě ani nedefinovali, co jsou přímky, takže přísně vzato bychom neměli konstruovaný objekt nazývat projektivní rovinou. Ale k takové přísnosti zde snad není důvod.

$\{(0,0,0)\}$ definujeme přímku $P(a,b,c)$ jako množinu bodů (x,y,t) naší projektivní roviny, splňujících rovnici

$$ax + by + ct = 0. \tag{8.1}$$

Dvě ekvivalentní trojice (x,y,t) a $(\lambda x, \lambda y, \lambda t)$ tuto rovnici buď obě zároveň splňují nebo obě zároveň nesplňují, tedy jsme skutečně definovali jistou množinu bodů projektivní roviny. Je také vidět, že pro každé nenulové $\lambda \in K$, trojice $(\lambda a, \lambda b, \lambda c)$ definuje stejnou přímku jako trojice (a,b,c). Na trojicích definujících přímky tedy máme přesně stejnou ekvivalenci jako na trojicích, definujících body, a můžeme pro tyto trojice vybrat stejné reprezentanty, jako jsme to udělali pro body, t.j. trojice s poslední nenulovou složkou rovnou 1. Na obrázku 8.3 vpravo jsou vyznačeny a popsány příslušnými trojicemi všechny přímky, procházející bodem $(0,0,1)$.

Abychom ukázali, že pro n-prvkové těleso jsme opravdu zkonstruovali projektivní rovinu řádu n, je třeba ověřit podmínky (P0)–(P2). Začneme podmínkou (P1) (2 přímky se protínají v 1 bodě). Nechť tedy (a_1,b_1,c_1) a (a_2,b_2,c_2) jsou dvě trojice definující přímky, a předpokládejme, že nejsou ekvivalentní, t.j. jedna není násobkem druhé.

Mohli bychom teď přímo vypočítat bod, který je jejich průsečíkem, a ověřit jeho jednoznačnost. Uvedeme jiný důkaz, pomocí základních výsledků z lineární algebry (zkusí-li si čtenář udělat důkaz přímým výpočtem, bude si pak možná lineární algebry cenit více než předtím).

Dívejme se na trojice (a_1,b_1,c_1) a (a_2,b_2,c_2) jako na třírozměrné vektory nad tělesem K. Oba jsou nenulové, a to, že jeden není násobkem druhého, tedy znamená, že jsou lineárně nezávislé. Proto matice

$$\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{pmatrix}$$

má hodnost 2. Podívejme se nyní na sloupce této matice jako na dvourozměrné vektory. Především víme, že všechny tři jsou lineárně závislé; existují tedy nějaká 3 čísla $x,y,t \in K$, ne všechna zároveň rovná 0 taková, že

$$x(a_1,a_2) + y(b_1,b_2) + t(c_1,c_2) = (0,0). \tag{8.2}$$

Rozepíšeme-li to po složkách, znamená to přesně to, že bod (x,y,t) leží na obou uvažovaných přímkách.

Na druhé straně, protože hodnost matice je 2, musí existovat 2 sloupcové vektory, které jsou lineárně nezávislé; nechť jsou to třeba (a_1,a_2) a

(b_1, b_2). Z toho plyne, že pro každý vektor (u, v) má rovnice $x(a_1, a_2) + y(b_1, b_2) = (u, v)$ jen jediné řešení. Jinými slovy, předepíšeme-li hodnotu t v rovnici (8.2), jsou x a y už dána jednoznačně, a tedy všechna řešení této rovnice jsou násobky jediného vektoru, což znamená, že uvažované přímky se protínají v jediném bodě.

Uvedený argument se dá říci ještě trochu učeněji a stručněji: Zobrazení přiřazující vektoru $(x, y, t) \in K^3$ vektor $x(a_1, a_2) + y(b_1, b_2) + t(c_1, c_2) \in K^2$ má hodnost 2, čili je na a tedy jeho jádro je 1-dimenzionální.

Tak jsme dokázali (P1). Podmínku (P2) bychom mohli dokazovat podobně, nebo můžeme rovnou říci, že v rovnici (8.1) jsou role trojice (x, y, t) a trojice (a, b, c) zcela symetrické, tedy mezi body a přímkami máme (opět) dualitu. Konečně ověření podmínky (P0) přenecháváme čtenáři. □

Poznámka. Uvedená konstrukce může vzbudit dojem, že některé body v nekonečnu se nějak odlišují od ostatních. Ve skutečnosti jsou všechny body rovnocenné, a nekonečno můžeme v jistém smyslu umístit kam chceme — projektivní rovina vypadá „lokálně všude stejně".

Cvičení

1.** Dokažte neexistenci projektivní roviny řádu 6. (Můžete si pomoci počítačovým programem, který probere a vyloučí konfigurace přicházející v úvahu. Musí se postupovat obratně, protože např. probírání všech systémů 43 sedmic na 43 bodech by trvalo příliš dlouho.)

8.3 Ortogonální latinské čtverce

Latinský čtverec řádu n je čtvercová tabulka $n \times n$, v níž v každém políčku je zapsáno jedno číslo z množiny $\{1, 2, \ldots, n\}$ a taková, že každé číslo se v každém řádku i sloupci vyskytuje právě jednou. Dva latinské čtverce 3×3 jsou znázorněny na obr. 8.4(a).

Nyní řekneme, co to znamená, že dva latinské čtverce téhož řádu jsou *ortogonální*: Představme si, že jeden ze čtverců je nakreslen na průhledné fólii, a že jej položíme přes druhý čtverec tak, že odpovídající políčka jsou nad sebou (obr. 8.4(b) znázorňuje takové položení čtverců z (a) přes sebe). Tím vznikne n^2 uspořádaných dvojic, každá z nich je tvořena číslem ze spodního čtverečku a odpovídajícím číslem

1	2	3
2	3	1
3	1	2

1	2	3
3	1	2
2	3	1

(a)

1_1	2_2	3_3
2_3	3_1	1_2
3_2	1_3	2_1

(b)

Obrázek 8.4: Dva ortogonální latinské čtverce řádu 3 (a), a jejich položení přes sebe (b).

z horního čtverečku. Čtverce jsou ortogonální, pokud se žádná dvojice neopakuje. Protože všech možných uspořádaných dvojic čísel od 1 do n je také n^2, musí se dokonce každá dvojice objevit právě jednou.

8.3.1 Věta. *Nechť M je množina latinských čtverců řádu n, z nichž každé dva jsou navzájem ortogonální. Potom $|M| \leq n-1$.*

Důkaz. Nejdříve jedno pozorování. Nechť A, B jsou dva ortogonální latinské čtverce řádu n, a nechť π je nějaká permutace čísel $1, 2, \ldots, n$. Utvořme nový latinský čtverec A', který v políčku (i, j) bude mít číslo $\pi(a_{ij})$, kde a_{ij} je číslo v políčku (i, j) čtverce A. Z definice ortogonality není těžké nahlédnout, že potom i A' a B budou ortogonální latinské čtverce. Toto pozorování můžeme vyjádřit heslem „ortogonalita latinských čtverců se nezmění přejmenováním symbolů v jednom z nich".

Mějme nyní latinské čtverce $A_1, A_2, \ldots, A_t$, z nichž každé 2 jsou ortogonální. Pro každé A_i zvolíme tu permutaci čísel $1, 2, \ldots, n$, jejíž aplikací na čísla v políčcích A_i se dosáhne toho, že v první řádce budou stát čísla $1, 2, \ldots, n$ *v pořadí podle velikosti*; výsledný čtverec označíme A'_i. Podle uvedeného pozorování budou $A'_1, \ldots, A'_t$ stále po dvou ortogonální. Podívejme se nyní, jaká čísla mohou stát v prvním políčku druhé řádky čtverců $A'_1, \ldots, A'_t$. Především tam nemůže

být číslo 1, protože to už je v prvním sloupci použito. Dále, žádné dva čtverce A'_i, A'_j nemohou mít v uvažované pozici $(2,1)$ stejná čísla. Kdyby totiž měly, položením A'_i, A'_j přes sebe vznikne v pozici $(2,1)$ dvojice stejných čísel, řekněme (k,k), ale tato dvojice také vznikne na k-tém místě prvního řádku! Tedy každé z čísel $2,3,\ldots,n$ může na pozici $(2,1)$ stát jen v jednom z A'_i, a proto $t \leq n-1$. □

Následující věta dává do souvislosti konečné projektivní roviny a latinské čtverce.

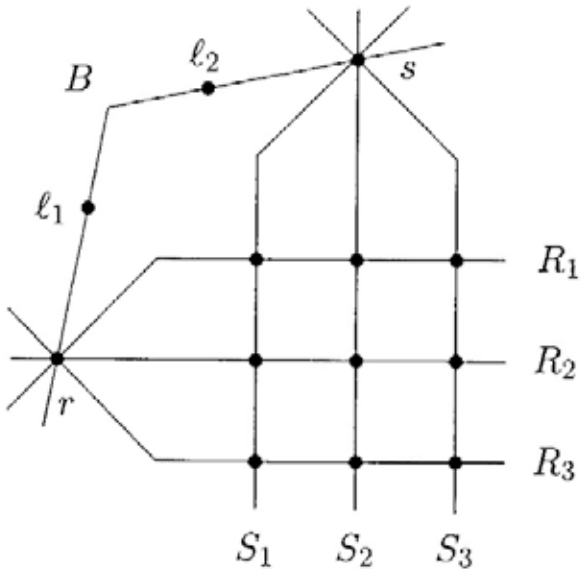
8.3.2 Věta. *Pro $n \geq 2$, projektivní rovina řádu n existuje právě když existuje soubor $n-1$ po dvou ortogonálních latinských čtverců řádu n.*

Poznamenejme jen, že existence projektivní roviny řádu 10 byla vyloučena právě přes hledání ortogonálních latinských čtverců řádu 10.

Důkaz nebudeme dělat do detailů, ale popíšeme si příslušnou konstrukci. Řekněme, že máme dáno $n-1$ ortogonálních latinských čtverců L_1, L_2, $\ldots$, L_{n-1} řádu n, budeme vyrábět projektivní rovinu řádu n. Zvolíme 2 body projektivní roviny, r a s, přímku B je spojující, a zbývající body na přímce B označíme $\ell_1,\ldots,\ell_{n-1}$. Potom nazveme $R_1,\ldots,R_n$ zbývající přímky procházející bodem r (mimo B) a $S_1,\ldots,S_n$ zbývající přímky bodem s. Nyní každý z dosud neoznačených bodů je průsečíkem některé dvojice přímek R_i a S_j. Schematicky je situace znázorněna na obr 8.5 (pro $n=3$).

Body konstruované projektivní roviny mimo bodů r, s, ℓ_1, $\ell_2,\ldots$, ℓ_{n-1} máme sestaveny do čtverce $n \times n$; pozice bodu v tomto čtverci bude odpovídat pozici políčka v latinském čtverci; tak např. 2. políčko v 3. řadě latinského čtverce odpovídá v projektivní rovině průsečíku přímek S_2 a R_3.

To, co jsme dosud označili a zakreslili, musí být stejné v každé projektivní rovině řádu n; nyní podle latinských čtverců doplníme přímky procházející body $\ell_1,\ldots,\ell_{n-1}$; jak označení napovídá, přímky procházející bodem ℓ_i budou určeny čtvercem L_i. Přímky bodem ℓ_i budou odpovídat jednotlivým číslům (symbolům) v latinském čtverci L_i. Kdyby např. L_1 byl latinský čtverec na obr. 8.4 vlevo, potom bodem ℓ_1 budou procházet takovéto přímky: přímka odpovídající číslu 1 v latinském čtverci, ta obsahuje mimo ℓ_1 body $R_1 \cap S_1$, $R_2 \cap S_3$ a $R_3 \cap S_2$, t.j. body odpovídající políčkům s 1, dále přímka odpovídající číslu 2, s body $R_1 \cap S_2$, $R_2 \cap S_1$ a $R_3 \cap S_3$, a konečně podobně utvořená přímka odpovídající číslu 3.



Obrázek 8.5: Konstrukce projektivní roviny z latinských čtverců

Tím jsme popsali konstrukci projektivní roviny, zbývá ověřit axiomy. Snadno spočteme, že celkový počet bodů i přímek je $n^2 + n + 1$. Podle cvičení 5 v části 8.1 stačí ověřit, že každé 2 přímky se protínají nejvýš v 1 bodě. Přitom se využije jak toho, že každý L_i je latinský čtverec, tak toho, že každé 2 z použitých čtverců jsou ortogonální; přenecháváme to do cvičení.

Obrácený postup, konstrukce $n-1$ ortogonálních latinských čtverců z projektivní roviny, sleduje totéž schéma. V projektivní rovině libovolně zvolíme body r, s, a zafixujeme další označení jako na obr. 8.5. Potom i-tý latinský čtverec L_i vyplníme podle přímek procházející bodem ℓ_i. Tolik k důkazu věty 8.3.2. □

Cvičení

1. Projděte konstrukci v důkazu věty 8.3.2 pro $n = 2$ (kdy existuje jen 1 latinský čtverec), ověřte, že vznikne Fanova rovina.
2. Ověřte, že každé 2 přímky zkonstruované v důkazu věty 8.3.2 se protínají nejvýš v 1 bodě, a uveďte, kde se využije vlastnosti latinského čtverce a kde ortogonality.
3. Ukažte, že obrácená konstrukce v důkazu věty 8.3.2 opravdu dává $n-1$ ortogonálních latinských čtverců.

4. Definujme *osvobozený čtverec* řádu n jako čtvercovou tabulku $n \times n$, v jejímž každém políčku je některé z čísel $1, 2, \ldots, n$. Ortogonalitu pro osvobozené čtverce definujeme stejně jako pro čtverce latinské. Pro nějaké číslo $t \geq 0$, uvažme následující dvě podmínky:

   (i) Existuje t navzájem ortogonálních latinských čtverců řádu n.

   (ii) Existuje $t + 2$ navzájem ortogonálních osvobozených čtverců řádu n.

   (a) Dokažte, že z (i) plyne (ii).

   (b)* Dokažte, že z (ii) plyne (i).

5. Buď T konečné těleso s n prvky, které označíme $t_0, t_1, \ldots, t_{n-1}$, přičemž $t_0 = 0, t_1 = 1$. Pro $k = 1, 2, \ldots, n-1$ definujme $n \times n$ matice $L^{(k)}$, přičemž prvek matice $L^{(k)}$ v pozici (i, j), je roven $t_i t_k + t_j$ (násobení a sčítání v tomto vzorci je v tělese T). Dokažte, že $L^{(1)}, \ldots, L^{(n-1)}$ jsou navzájem ortogonální latinské čtverce řádu n. (Tím se pomocí věty 8.3.2 podá také jiná konstrukce projektivní roviny řádu n.)

6. Pro $m \leq n$ definujme *latinský* $m \times n$ *obdélník* jako obdélníkovou tabulku $m \times n$, v jejímž každém políčku je zapsáno jedno číslo z množiny $\{1, 2, \ldots, n\}$ tak, že v žádném řádku ani sloupci se čísla neopakují. Spočítejte počet všech možných latinských $2 \times n$ obdélníků.

8.4 Použití konečných projektivních rovin

Konečné projektivní roviny mají řadu aplikací v matematice i mimo ni; několik jich zmiňme. Projektivní rovina je velmi stejnorodá, to znamená, že každé dva body (nebo i např. každé dvě dvojice bodů) jsou zcela rovnocenné. Proto se konečné projektivní roviny a jejich zobecnění, tzv. *bloková schémata*, používají jako schémata organizace různých pokusů, viz část 11.1. Podobná použití mají i latinské čtverce. Motocyklové závody jednotlivců na ploché dráze se rozepisují podle schématu daného projektivní rovinou řádu 4 (k čemuž však nejspíše organizátoři závodů dospěli empiricky); podrobněji se o této souvislosti lze dočíst v knížce [10]. Konečné projektivní roviny se objevují v teorii šifer a kódů, tzv. kryptografii.

V samotné matematice slouží konečné projektivní roviny jako příklady množinových systémů s mnoha pozoruhodnými vlastnostmi. Hle-

dáme-li pro nějakou domněnku o množinových systémech protipříklad nebo naopak chceme-li příklad množinového systému cosi splňujícího, často neprohloupíme, zkusíme-li jako jeden z prvních pokusů nějakou konečnou projektivní rovinu (to trochu připomíná situaci v teorii grafů, která má také svoji zásobárnu zajímavých grafů sloužících jako „notorické protipříklady").

8.4.1 Příklad (Barvení dvěma barvami). *Buď X konečná množina bodů a $\mathcal{M}$ nějaký systém podmnožin X. Řekneme, že $(X, \mathcal{M})$ je 2-obarvitelný, pokud můžeme každý bod z X obarvit jednou ze dvou barev (např. červenou nebo bílou) tak, že v každé množině z $\mathcal{M}$ se vyskytují body obou barev. Nejmenší počet tříbodových množin, z nichž lze utvořit systém, jenž není 2-obarvitelný, je 7, a jediný takový systém je projektivní rovina řádu 2. Více o tom v příkladu 9.1.3*

8.4.2 Příklad. Věta 6.3.1 praví, že je-li G graf na m vrcholech neobsahující $K_{2,2}$ jako podgraf, potom G má nejvýš $\frac{1}{2}(m^{3/2} + m)$ hran. Pomocí konečných projektivních rovin ukážeme, že tento odhad je obecně téměř nejlepší možný: pro nekonečně mnoho hodnot m existuje graf na m vrcholech s aspoň $0.35\, m^{3/2}$ hranami neobsahující $K_{2,2}$ jako podgraf.

Důkaz. Vezmeme projektivní rovinu řádu n, a uvážíme její graf incidence (jako v odstavci o principu duality v části 8.1). Budeme tedy mít celkem $m = 2(n^2 + n + 1)$ vrcholů. Každá z $n^2 + n + 1$ přímek má $n + 1$ bodů, takže tento graf má $(n^2 + n + 1)(n + 1) \geq (n^2 + n + 1)^{3/2} = m^{3/2}/2^{3/2} \approx 0.35 m^{3/2}$ hran.

Co by znamenalo, kdyby uvažovaný graf incidence obsahoval $K_{2,2}$? V pojmech projektivní roviny by to říkalo, že existují dva body x, x' a dvě přímky P, P' takové, že $\{x, x'\} \subseteq P \cap P'$, to ale v projektivní rovině není možné. □

Poznámka. Konstanta 0.35 se dá ještě poněkud vylepšit, viz cvičení 2.

Cvičení

1. Dokažte tvrzení z příkladu 8.4.1: Fanova rovina není 2-obarvitelná.

2. Nechť n je mocnina prvočísla, a nechť K je n-prvkové těleso. Uvažte třídy ekvivalence $\approx$ na množině všech trojic z $K^3 \setminus \{(0,0,0)\}$ (zavedené

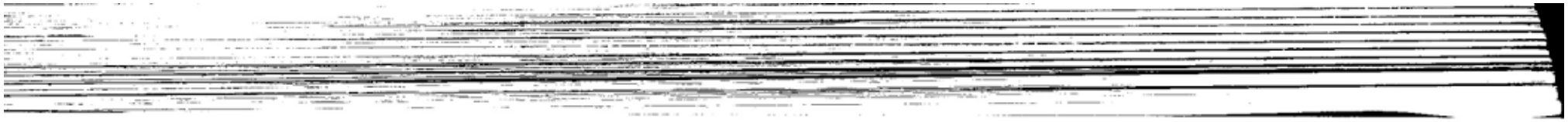
v části 8.2). Tyto třídy budou vrcholy grafu G, a vrcholy (a, b, c) a (x, y, z) budou spojené hranou právě když $ax + by + cz = 0$. Ověřte

(a) že tato definice je korektní,

(b)* že definovaný graf neobsahuje $K_{2,2}$ jako podgraf,

(c) že každý vrchol má aspoň n sousedů, a

(d) že je-li $m = n^2 + n + 1$ počet vrcholů, potom počet hran je aspoň $\frac{1}{2}m^{3/2} - m$.



9

Pravděpodobnostní důkazy

Čtenář asi zná nějaké úlohy na počítání pravděpodobnosti nějakého jevu (v jiných kapitolách je ostatně několik takových také roztroušeno). Nejčastěji to asi budou příklady, které jsou takzvaně „ze života" nebo to aspoň předstírají: ve školských úlohách se nejčastěji hovoří o hracích kostkách, kartách, mincích, v učebnicích z let padesátých bychom možná našli otázky o zmetcích mezi hutními výrobky, a pod. V téhle kapitole chceme ukázat pozoruhodnou matematickou aplikaci, totiž jak se některá tvrzení dají dokazovat pomocí pravděpodobnosti, ačkoli v nich o pravděpodobnosti ani náhodnosti není ani zmínka.

9.1 Důkazy počítáním

Ve dvou úvodních příkladech se zatím o pravděpodobnosti mluvit nebude.

9.1.1 Příklad. *Uvažme balíček 32 karet srovnaných tak, jak přišly z továrny. Budeme ho míchat tzv. řezáním: rozdělíme jej na 2 stejně velké části, a smísíme karty z jedné části s kartami z druhé části, přičemž pořadí karet z každé části se zachová. Dokážeme, že opakujeme-li to nejvýš 4×, nemůžeme dostat všechna možná pořadí karet (což naznačuje, že takové míchání nemůže dát opravdu náhodné pořadí).*

Důkaz. Celkem je 32! možných pořadí karet. Spočítáme, kolika pořadí se dá dosáhnout popsaným mícháním. Kolika způsoby můžeme

TADY CHYBI 10 STRANEK

Tohle je tu, aby vychazely sude/liche stranky.

Ahoj, jak se mate? Ta skola nic moc, co. Taky si myslim. Stejne to z toho vubec neni k pochopeni.
Radsi byste se sli opit. Nebo tak neco. Nojo. Ale co, vy se k tomu uceni nakonec dokopete. Urcite jo. Jinak byste si tohle nestahovali a az sem to nedocetli, zejo. Mno. Tak jo.

- největší číslo není mezi prvními 50 kartičkami, a
- druhé největší číslo je na některé z prvních 50 kartiček.

Při uvedené strategii záleží očividně jen na pořadí čísel na kartičkách podle velikosti, a tedy můžeme předpokládat, že na kartičkách je náhodná permutace množiny $\{1, 2, \ldots, 100\}$, t.j. elementární jev z výše definovaného prostoru $\mathcal{S}_{100}$. Zajímat nás pak bude jev $A = \{\pi \in \mathcal{S}_{100};\ \pi(100) > 50 \text{ a } \pi(99) \leq 50\}$. Tady bude užitečné dívat se na permutaci jako na pořadí. Pozici čísla 100 můžeme zvolit 50 způsoby, pozici 99 nezávisle na tom 50 způsoby, a pro každou takovou volbu pak zbývající čísla můžeme na zbývající pozice rozestavit 98! způsoby. Proto

$$P(A) = \frac{50 \times 50 \times 98!}{100!} = \frac{50 \times 50}{99 \times 100} \doteq 0.2525 > \frac{1}{4}.$$

Ještě několik poznámek. Jev A není jediná situace, kdy naše strategie vyhrává, proto pravděpodobnost A je jen dolní odhad pro šanci na výhru. Číslo 50 v popsané strategii optimalizuje pravděpodobnost jevu A, ale vezmeme-li v úvahu i jiné možnosti výhry, dostaneme poněkud lepší výsledky s jiným „prahovým" počtem kartiček; zde podrobnější analýzu už dělat nebudeme.

9.2.6 Definice (Náhodný graf). *Graf (obyčejný, neorientovaný) na množině vrcholů $V = \{1, 2, \ldots, n\}$ je zadán tím, že pro každou dvojici $\{i, j\} \in \binom{V}{2}$ specifikujeme, zda tvoří hranu nebo ne. Existuje tedy $2^{\binom{n}{2}}$ grafů (mnohé z nich jsou ovšem isomorfní, to nás zde ale nebude zajímat). Vybíráme-li náhodný G graf na V, přičemž všechny grafy jsou stejně pravděpodobné, můžeme na to nahlížet též jako na $\binom{n}{2}$ hodu symetrickou mincí — pro každou dvojici vrcholů hodíme mincí, zda se má stát hranou nebo ne. Příslušný pravděpodobnostní prostor $\mathcal{G}_n$ bude mít jako prvky všechny možné grafy na V, a všechny budou mít stejnou pravděpodobnost, totiž $2^{-\binom{n}{2}}$.*

Jako příklady jevů můžeme studovat nejrůznější grafové vlastnosti, jako jev S =„graf G je souvislý" nebo B =„graf G je bipartitní", a podobně. Vypočítat pravděpodobnosti takových jevů přesně je někdy obtížné, ale většinou nás zajímá jen nějaký přibližný odhad. Pro dva zmíněné jevy lze ukázat, že pro $n \to \infty$ se pravděpodobnost $P(S)$ velmi rychle blíží 1, zatímco pravděpodobnost $P(B)$ se velmi rychle blíží 0

To se někdy vyjadřuje frázemi „náhodný graf je skoro jistě souvislý“ a „náhodný graf skoro jistě není bipartitní“.

9.2.7 Úloha. *Dokažme, že náhodný graf skoro jistě není bipartitní, t.j.* $\lim_{n\to\infty} P(B) = 0$.

Důkaz. Následující postup je poučný i pro mnoho jiných tvrzení tohoto typu. Jak víme, množinu vrcholů V bipartitního grafu lze rozdělit na dvě části, U a W, tak, že všechny hrany jsou mezi U a W. Pro danou podmnožinu $U \subseteq V$ označme B_U jev, že všechny hrany grafu G spojují vrcholy z U s vrcholy z $W = V \setminus U$. Je-li $k = |U|$, máme $k(n-k)$ dvojic $\{u, w\}$ s $u \in U$, $w \in V \setminus U$, tedy jev (množina) B_U sestává z $2^{k(n-k)}$ grafů, a proto $P(B_U) = 2^{k(n-k)-\binom{n}{2}}$. Není těžké se přesvědčit, že funkce $k \mapsto k(n-k)$ nabývá maxima pro $k = n/2$, a toto maximum je rovno $n^2/4$. Proto můžeme pro každé U odhadnout

$$P(B_U) \le 2^{n^2/4-\binom{n}{2}} = 2^{-n(n-2)/4}.$$

Každý bipartitní graf patří některému B_U (pro vhodnou množinu U). Pro různé volby U nemusí být jevy B_U navzájem disjunktní, avšak pravděpodobnost sjednocení jevů je vždy nejvýš rovna součtu jejich pravděpodobností, a proto

$$P(B) \le \sum_{U\subseteq V} P(B_U) \le 2^n 2^{-n(n-2)/4} = 2^{-n(n-6)/4} \to 0.$$

□

V uvedeném výsledku jsme se zajímali o jistou kvalitativní vlastnost „velkého“ náhodného grafu. To trochu připomíná např. otázky fyziky pevných látek; tam se totiž studují nějaké makroskopické vlastnosti souboru velkého množství mikroskopických částic. Předpokládá se přitom, že jednotlivé částice si vedou ve vhodném smyslu náhodně, a makroskopické vlastnosti jsou výslednicí jejich náhodného chování. I matematické metody studia takových souborů částic jsou příbuzné metodám pro náhodné grafy.

Nezávislé jevy. Musíme probrat ještě jeden klíčový pojem. Dva jevy A, B v nějakém pravděpodobnostním prostoru (Ω, P) se nazývají *nezávislé*, platí-li

$$P(A \cap B) = P(A)P(B).$$

Nezávislost znamená, že rozdělíme-li Ω na 2 části, A a jeho doplněk, j
B „rozřízne" obě tyto části v témže poměru. Jinak řečeno, kdybych
prvek $\omega \in \Omega$ volili náhodně nikoliv ze všech prvků Ω, ale jenom me
prvky z A, byla by pravděpodobnost toho, že $\omega \in B$, přesně rov
$P(B)$ (za předpokladu $P(A) \neq 0$).

S nezávislými jevy se nejčastěji setkáme v takovéto situaci: prvk
Ω, t.j. elementární jevy, si můžeme představovat jako uspořádané dv
jice, neboli Ω modeluje výsledek jednoho „složeného" experiment
sestávajícího ze dvou experimentů konaných jeden po druhém. Pře
pokládejme, že průběh prvního experimentu nijak neovlivní průbě
experimentu druhého. Je-li $A \subseteq \Omega$ nějaký jev, závisející jen na v
sledku prvního experimentu (t.j., známe-li tento výsledek, můžen
rozhodnout, zda A nastal nebo ne) a podobně B závisí jen na v
sledku druhého experimentu, potom jevy A a B budou nezávislé.

Prostor $\mathcal{C}_n$ (náhodná posloupnost 0/1) je typickým zdrojem situa
tohoto druhu. Zde máme složený experiment sestávající z n po sob
jdoucích hodů mincí, o nichž předpokládáme, že se navzájem nij
neovlivňují. Závisí-li tedy jev A např. jen na hodech se sudým poř
dovým číslem („v suchých hodech nepadl žádný líc") a jev B jen n
hodech s lichým pořadovým číslem („v lichých hodech padly aspoň
ruby"), budou takové jevy nezávislé. Podobně v prostoru $\mathcal{G}_n$ (náhodn
graf) jsou jednotlivé hrany nezávislé, a např. jevy „graf G má asp
jeden trojúhelník na vrcholech 1,2,...,10" a „graf G obsahuje nějak
lichou kružnici s vrcholy mezi $11, 12, \ldots, n$" jsou nezávislé.

Subtilnější situace můžeme demonstrovat na pravděpodobnostní
prostoru $\mathcal{S}_n$ (náhodná permutace). Jevy $A = \{\pi(1) = 1\}$ a B
$\{\pi(2) = 1\}$ zjevně nezávislé nejsou (protože $P(A), P(B) > 0$, a
$A \cap B = \emptyset$, a tudíž $P(A \cap B) = 0$). Bude-li jev $C = \{\pi(2) = 2$
je vidět, že B a C určitě nejsou nezávislé, ale možná už není t
zřejmé, že ani A a C nejsou nezávislé: máme $P(A) = P(C) = \frac{1}{n}$, a
$P(A \cap C) = \frac{1}{n(n-1)} \neq P(A)P(C)$. Intuitivně, víme-li, že nastal A, t
že $\pi(1) = 1$, vyloučili jsme tím zároveň jednu z n možností pro $\pi(2$
a tedy $\pi(2)$ má malinko větší šanci být rovno 2. Naproti tomu jevy
a $D = \{\pi(2) < \pi(3)\}$ jsou nezávislé, jak se lze přesvědčit výpočte
příslušných pravděpodobností.

Pojem nezávislosti můžeme rozšířit i na více jevů $A_1, A_2, \ldots, A_n$.

9.2.8 Definice. *Jevy $A_1, \ldots, A_n \subseteq \Omega$ se nazývají* nezávislé, *pokud pro každou množinu indexů $I \subseteq \{1, 2, \ldots, n\}$ platí*

$$P\left(\bigcap_{i \in I} A_i\right) = \prod_{i \in I} P(A_i).$$

Speciálně tato definice požaduje, aby každé dva z těchto jevů byly nezávislé, ale musíme varovat, že z nezávislosti všech dvojic obecně neplyne nezávislost!

V prostorech $\mathcal{C}_n$ (náhodná posloupnost 0/1) i $\mathcal{G}_n$ (náhodný graf) máme typické situace s mnoha nezávislými jevy. Definujme jev A_i v prostoru $\mathcal{C}_n$, tvořený všemi posloupnostmi s jedničkou na i-tém místě. Pak jevy $A_1, \ldots, A_n$ jsou nezávislé. Obecněji, závisejí-li nějaké jevy na po dvou disjunktních skupinách složek posloupnosti, jsou nezávislé (důkaz vynecháme, není obtížný).

V různých pravděpodobnostních výpočtech a důkazech se příslušné pravděpodobnostní prostory zpravidla výslovně nepopisují, jen se s nimi mlčky pracuje. Přesto je samozřejmě důležité mít jasno v těchto základních pojmech.

Na závěr tohoto oddílu ještě jeden pěkný pravděpodobnostní důkaz.

9.2.9 Úloha. *Uvažme turnaj n hráčů, řekněme v tenisu, v němž každý hraje s každým (a žádná dvojice neremizuje). Mají-li jednotliví hráči velké výkonnostní odstupy, můžeme čekat, že nejlepší s nich vyhraje se všemi, druhý nejlepší se všemi kromě prvního, atd., t.j., turnaj přesvědčivě určí pořadí. Turnaj s vyrovnanými hráči ovšem může dopadnout složitějším způsobem. Může například turnaj dopadnout tak, aby* pro každou trojici hráčů existoval nějaký jiný hráč, který je všechny porazil? *(Podobně se ovšem můžeme ptát pro libovolné k místo trojky.)*

Když si matematikové položili tuto otázku, dlouho se nedařilo najít řešení; konstrukce takových turnajů je obtížná. Pravděpodobnostní

metodou se ukáže existence takového výsledku turnaje, pro dost velk n, poměrně snadno.

Uvažme náhodný turnaj, kde si představujeme, že výsledek každého zápasu je určen nestranným losem. Podíváme se na pevně zvolenou trojici hráčů x, y, z. Pravděpodobnost, že nějaký jiný hráč u s nimi se všemi vyhraje, je $2^{-3} = \frac{1}{8}$, tedy pravděpodobnost že w prohraje aspoň s jedním je $\frac{7}{8}$. Jaká je pravděpodobnost, že každý z $n-3$ hráčů w (různých od x, y, z) prohraje aspoň s jedním z x, y, z? Pro různé hráče w jsou výsledky jejich zápasů s x, y, z na sobě nezávislé a tedy tato pravděpodobnost je $(\frac{7}{8})^{n-3}$. Trojici $\{x, y, z\}$ lze volit $\binom{n}{3}$ způsoby, proto pravděpodobnost, že pro aspoň jednu z těchto trojic x, y, z není žádný další hráč, jenž x, y i z porazil, je nejvýš $\binom{n}{3}(\frac{7}{8})^{n-3}$. Pro $n \geq 91$ je tato pravděpodobnost menší než 1, proto existuje nějaký výsledek turnaje n hráčů s požadovanou vlastností. □

Cvičení

1. Ukažte, že náhodný graf skoro jistě obsahuje trojúhelník (tím podáte jiné řešení příkladu 9.2.7).

2.* Ukažte, že náhodný graf je skoro jistě souvislý.

3. Najděte příklad 3 jevů v nějakém pravděpodobnostním prostoru takových, že každé dva jsou nezávislé, ale všechny 3 nezávislé nejsou.

4. Ukažte, že jsou-li A, B nezávislé jevy, pak také jejich doplňky $\Omega \setminus A$, $\Omega \setminus B$ jsou nezávislé.

5. (a) Ukažte podle definice, že jevy $A_1, \ldots, A_n$ v prostoru $\mathcal{C}_n$, definované v textu za definicí 9.2.8, jsou skutečně nezávislé.

   (b)* Buď (Ω, P) konečný pravděpodobnostní prostor, v němž existuje n nezávislých jevů $A_1, \ldots, A_n$ takových, že $0 < P(A_i) < 1$ pro každé i. Dokažte, že $|\Omega| \geq 2^n$.

6. Nechť (Ω, P) je konečný pravděpodobnostní prostor, v němž všechny prvky mají pravděpodobnost $1/|\Omega|$. Ukažte, že je-li $|\Omega|$ prvočíslo, pak žádné dva netriviální jevy (různé od $\emptyset$ a Ω) nejsou nezávislé.

7. Pro jednoduchost předpokládejme, že pravděpodobnost narození kluka i holky je stejná (což ve skutečnosti není zcela tak). O jisté rodině

víme, že mají přesně dvě děti, a aspoň jedno z nich je kluk. Jaká je pravděpodobnost, že mají dva kluky?

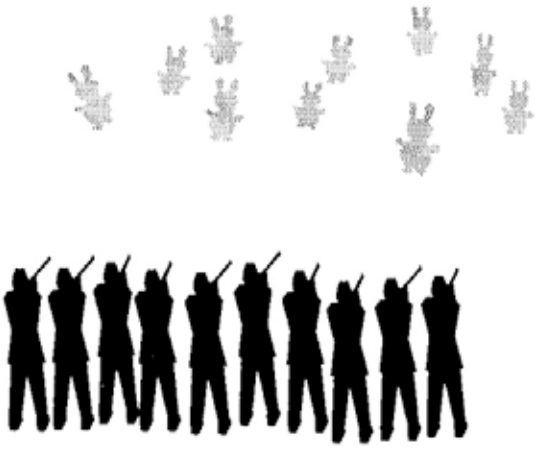
9.3 Střední hodnota

9.3.1 Definice. *Nechť (Ω, P) je nějaký konečný pravděpodobnostní prostor.* Náhodnou veličinou *na Ω nazveme každé zobrazení $f : \Omega \to \mathbf{R}$.*

Náhodná veličina f tedy přiřazuje každému elementárnímu jevu $\omega \in \Omega$ nějaké reálné číslo $f(\omega)$. Teď několik příkladů náhodných veličin:

9.3.2 Příklad (Počet jedniček). *Je-li $\mathcal{C}_n$ prostor všech n-prvkových posloupností nul a jedniček, můžeme definovat náhodnou veličinu f_1 takto: pro posloupnost s, $f_1(s)$ je počet jedniček v s.*

9.3.3 Příklad (Počet živých zajíců). *Každý z n lovců zamíří na jednoho náhodně vybraného z n zajíců, a všichni naráz vystřelí. Náhodná veličina f_2 je počet přeživších zajíců (za předpokladu, že se každý lovec trefí). Formálně, pravděpodobnostní prostor zde bude množina všech zobrazení μ množiny $\{1, 2, \ldots, n\}$ do sebe, každé s pravděpodobností n^{-n}, a $f_2(\mu)$ je počet bodů mino obraz μ.*



9.3.4 Příklad (Počet levých maxim). *Na pravděpodobnostním prostoru $\mathcal{S}_n$ všech permutací na množině $\{1, 2, \ldots, n\}$, definujeme náhodnou veličinu f_3: $f_3(\pi)$ je počet* levých maxim *permutace π, t.j. počet i takových, že $\pi(i) > \pi(j)$ pro všechna $j < i$. Představme si závod třeba ve vrhu koulí, a pro jednoduchost předpokládejme, že každý závodník podává stabilní výkon, t.j., pokaždé hodí stejně. V první sérii hodů hází n závodníků v náhodném pořadí. Potom f_3 bude udávat, kolikrát se v této první sérii hodů měnil závodník s dosud nejlepším výkonem.*

9.3.5 Příklad (Složitost třídícího algoritmu). *A ještě jedna složitější náhodná veličina. Nechť A je nějaký třídicí algoritmus, to znamená, A dostane jako vstup n-tici čísel $x_1, \ldots, x_n$, a na výstup vypíše táž čísla setříděná podle velikosti. Předpokládejme, že počet kroků výpočtu algoritmu A závisí jen na pořadí vstupních čísel podle velikosti, takže si můžeme představovat, že na vstupu je nějaká permutace π čísel $\{1, 2, \ldots, n\}$ (tuto podmínku splňuje mnoho skutečně používaných algoritmů). Definujeme náhodnou veličinu f_4 na prostoru $\mathcal{S}_n$; $f_4(\pi)$ je počet kroků, vykonaných algoritmem A pro vstupní permutaci π.*

9.3.6 Definice. *Nechť (Ω, P) je konečný pravděpodobnostní prostor, f náhodná veličina na něm.* Střední hodnota *f bude reálné číslo, které značíme $\mathbf{E}f$ a definujeme předpisem*

$$\mathbf{E}f = \sum_{\omega \in \Omega} P(\{\omega\}) f(\omega)$$

(písmeno **E** *je zkratka z anglického „expectation“, v překladu „očekávání“).*

Střední hodnotu si můžeme představovat takto: opakujeme-li mnohokrát náhodnou volbu prvku z Ω, bude se průměrná hodnota f přes tyto náhodně zvolené prvky blížit $\mathbf{E}f$. Jsou-li speciálně všechny elementární jevy $\omega \in \Omega$ stejně pravděpodobné (jak je tomu téměř ve všech našich příkladech), je střední hodnota f prostě aritmetický průměr všech hodnot f:

$$\mathbf{E}f = \frac{1}{|\Omega|} \sum_{\omega \in \Omega} f(\omega).$$

Pokračování příkladu 9.3.2 (Počet jedniček). Pro ilustraci vypočteme střední hodnotu náhodné veličiny f_1, počtu jedniček v náhodné n-členné posloupnosti nul a jedniček, podle definice. Veličina f_1 má hodnotu 0 pro jedinou posloupnost (samých nul), hodnotu 1 pro n posloupností,..., hodnotu k pro $\binom{n}{k}$ posloupností z $\mathcal{C}_n$. Proto

$$\mathbf{E}f_1 = \frac{1}{2^n} \sum_{k=1}^{n} \binom{n}{k} k.$$

Jak se počítá v příkladu 10.1.2, je suma na pravé straně rovna $n2^{n-1}$, takže $\mathbf{E}f_1 = n/2$. To ovšem souhlasí s intuicí, že při n hodech mincí v průměru padne polovina líců.

Hodnota $\mathbf{E}f_1$ se dá stanovit jednodušeji, následujícím trikem. Pro každou posloupnost $s \in \mathcal{C}_n$ uvažme posloupnost $\bar{s}$, která vznikne ze s záměnou jedniček na nuly a obráceně. Platí $f_1(s) + f_1(\bar{s}) = n$. Toho využijeme takto:

$$\mathbf{E}f_1 = 2^{-n} \sum_{s \in \mathcal{C}_n} f_1(s) = \frac{1}{2^n \cdot 2} \sum_{s \in \mathcal{C}_n} (f_1(s) + f_1(\bar{s})) = 2^{-n-1} |\mathcal{C}_n| n = \frac{n}{2}.$$

Popíšeme nyní metodu, jíž se střední hodnota často dá spočítat velmi jednoduše (viděli jsme, že výpočet podle definice je i v jednoduchých případech pracný). Potřebujeme na to definici a jednoduchou větu.

9.3.7 Definice. *Buď $A \subseteq \Omega$ jev v nějakém pravděpodobnostním prostoru (Ω, P).* Indikátorem *jevu A nazveme náhodnou veličinu, $I_A : \Omega \to \{0, 1\}$, definovanou následovně*

$$I_A(\omega) = \begin{cases} 1 & \text{pro } \omega \in A \\ 0 & \text{pro } \omega \notin A. \end{cases}$$

9.3.8 Pozorování. *Pro každý jev A, $\mathbf{E}I_A = P(A)$.*

Důkaz. Podle definice střední hodnoty je

$$\mathbf{E}I_A = \sum_{\omega\in\Omega} I_A(\omega)P(\{\omega\}) = \sum_{\omega\in A} P(\{\omega\}) = P(A).$$

□

Následující tvrzení je skoro škoda nazývat větou, jeho důkaz z definice je bezprostřední a přenecháváme jej čtenáři. Je to však tvrzení, které nám bude v dalším velice užitečné.

9.3.9 Věta (O linearitě střední hodnoty). *Buďte f a g libovolné náhodné veličiny na konečném pravděpodobnostním prostoru (Ω, P), α reálné číslo. Potom $\mathbf{E}(\alpha f) = \alpha\mathbf{E}f$, $\mathbf{E}(f+g) = (\mathbf{E}f) + (\mathbf{E}g)$.*

Zdůrazněme, že f a g mohou být naprosto libovolné, nemusí tedy být v žádném smyslu nezávislé nebo tak něco. Pokračujeme několika příklady toho, jak se 9.3.7–9.3.9 dají využít.

Další pokračování příkladu 9.3.2 (Počet jedniček). Spočítáme $\mathbf{E}f_1$, průměrný počet jedniček, asi nejelegantnějším způsobem. Jev A_i na prostoru $\mathcal{C}_n$ bude „v i-tém hodu padne líc", čili množina všech posloupností, majících na i-tém místě jedničku. Zřejmě $P(A_i) = \frac{1}{2}$ pro každé i. Všimněme si, že pro každou posloupnost $s \in \mathcal{C}_n$ je $f_1(s) = I_{A_1}(s) + I_{A_2}(s) + \cdots + I_{A_n}(s)$ (triviální tvrzení jsme jen zapsali v trošku komplikovanějším značení). Z linearity střední hodnoty a pak z pozorování 9.3.8 dostaneme

$$\mathbf{E}f_1 = \mathbf{E}I_{A_1} + \mathbf{E}I_{A_2} + \cdots + \mathbf{E}I_{A_n} = P(A_1) + P(A_2) + \cdots + P(A_n) = \frac{n}{2}.$$

□

Pokračování příkladu 9.3.3 (Počet živých zajíců). Budeme počítat $\mathbf{E}f_2$, střední hodnotu počtu nezastřelených zajíců. Tentokrát A_i bude jev „i-tý zajíc přežije", formálně A_i bude množina všech

zobrazení μ, která nic nezobrazí na i. Pravděpodobnost, že j-tý lovec střelí i-tého zajíce je $\frac{1}{n}$, a protože lovci si vybírají nezávisle, je $P(A_i) = (1 - 1/n)^n$. Dále postupujeme jako v předchozím příkladě:

$$\mathbf{E}f_2 = \sum_{i=1}^{n} \mathbf{E}I_{A_i} = \sum_{i=1}^{n} P(A_i) = \left(1 - \frac{1}{n}\right)^n n \approx \frac{n}{e}$$

(jak známo z analýzy, $(1 - 1/n)^n$ konverguje k e^{-1}). □

Pokračování příkladu 9.3.4 (Počet levých maxim). Budeme teď počítat střední hodnotu počtu levých maxim náhodné permutace, $\mathbf{E}f_3$. Zde A_i bude jev „i je levé maximum π", t.j. $A_i = \{\pi;\ \pi(i) > \pi(j)$ pro $j = 1, 2, \ldots, i-1\}$. Tvrdíme, že $P(A_i) = \frac{1}{i}$. Nejnázornější je si představit, že náhodnou permutaci π vyrábíme takovýmto postupem: Začneme s „hromádkou" čísel $\{1, 2, \ldots, n\}$. Vytáhneme z hromádky jedno náhodně zvolené číslo, a prohlásíme jej za $\pi(n)$. Potom ze zbývajících čísel v hromádce vytáhneme další náhodné číslo, to bude $\pi(n-1)$, atd. Hodnota $\pi(i)$ se volí v okamžiku, kdy v hromádce zbývá právě i čísel. Pravděpodobnost, že jako $\pi(i)$ zvolíme největší z těchto i čísel (což je právě jev A_i), je tudíž $\frac{1}{i}$. Zbytek výpočtu je jako v předchozím:

$$\mathbf{E}f_3 = \sum_{i=1}^{n} \mathbf{E}I_{A_i} = \sum_{i=1}^{n} P(A_i) = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}.$$

Hodnota součtu převrácených hodnot, k němuž jsme dospěli, je přibližně $\ln n$, viz cvičení 2.4.12. □

Cvičení

1. Ukažte na příkladech, že pro libovolné náhodné veličiny f, g obecně neplatí ani jedna z rovností $\mathbf{E}(fg) = (\mathbf{E}f)(\mathbf{E}g)$, $\mathbf{E}(f^2) = (\mathbf{E}f)^2$, $\mathbf{E}(1/f) = 1/\mathbf{E}f$.
2. Dokažte, že pro libovolnou náhodnou veličinu f platí $\mathbf{E}(f^2) \geq (\mathbf{E}f)^2$.
3. Nechť $f(\pi)$ je počet pevných bodů permutace π (viz část 2.7). Spočtěte $\mathbf{E}f$ pro náhodnou permutaci $\pi \in \mathcal{S}_n$.

4. Buď π náhodná permutace množiny $\{1, 2, \ldots, n\}$.
   (a)* Určete střední délku cyklu π obsahujícího číslo 1.
   (b)* Určete střední počet cyklů π.

5. Hodíme $n\times$ po sobě desetikorunovou mincí, na níž padá lev i Hradčana s pravděpodobností $\frac{1}{2}$. Kolik je střední počet „sérií" (série jsou souvislé úseky, kdy padá stejná strana)?

6. Předpokládejme, že jeden z milionu lidí má místo levé nohy kopyto, a že tito lidé jsou mezi populací náhodně rozděleni. Detektiv zjistil, že pachatelem zločinné finanční machinace je člověk s kopytem místo levé nohy žijící v Praze (předpokládejme 1 milion obyvatel). Policejní inspektor pak člověka s tímto anatomickým znakem zatkl. Jaká je teď pravděpodobnost, že v Praze žije nejméně ještě jeden další takový člověk?

7.* V první nádobě je n červených kuliček a ve druhé n modrých kuliček. Vezmeme náhodně vybranou kuličku z první nádoby, náhodně vybranou kuličku z druhé nádoby, a dáme je do opačných nádob než ze kterých jsme je vytáhli. Dokažte, že opakujeme-li to $k\times$, je střední hodnota počtu červených kuliček v první nádobě rovna $\frac{1}{2}n\bigl(1+\bigl(1-\frac{2}{n}\bigr)^k\bigr)$.

9.4 Několik aplikací

V této části jsou shromážděny příklady — drobné matematické skvosty — na použití linearity střední hodnoty.

9.4.1 Věta (Existence velkých bipartitních podgrafů). *Buď G graf se sudým počtem, $2n$, vrcholů a s $m > 0$ hranami. Potom množinu $V = V(G)$ lze rozdělit na dvě disjunktní n-prvkové podmnožiny A a B tak, že více než $m/2$ hran G spojuje vrchol z A s vrcholem z B.*

Důkaz. Zvolme n-prvkovou množinu A náhodně mezi všemi n-prvkovými podmnožinami V, položme $B = V \setminus A$. Nechť X označuje počet hran grafu G jdoucích „napříč", t.j., tvaru $\{a, b\}$, kde $a \in A$, $b \in B$. Spočteme střední hodnotu $\mathbf{E}X$ náhodné veličiny X. Pro každou hranu $e = \{u, v\} \in E(G)$ definujeme jev N_e, který nastane pro všechny volby množiny A takové, že hrana e jde napříč, to znamená

$|A \cap \{u,v\}| = 1$. Platí $X = \sum_{e \in E(G)} I_{N_e}$, a tedy $\mathbf{E}X = \sum_{e \in E(G)} P(N_e)$. Potřebujeme stanovit pravděpodobnost $P(N_e)$.

Celkem existuje $\binom{2n}{n}$ možností volby množiny A. Požadujeme-li, aby $u \in A$ a $v \notin A$, můžeme zbývajících $n-1$ prvků A zvolit $\binom{2n-2}{n-1}$ způsoby, a podobně pro symetrickou situaci $u \notin A$, $v \in A$. Proto

$$P(N_e) = \frac{2\binom{2n-2}{n-1}}{\binom{2n}{n}} = \frac{n}{2n-1} > \frac{1}{2}.$$

Odtud dostaneme $\mathbf{E}X = \sum_{e \in E(G)} P(N_e) > m/2$. Střední hodnota X je průměrem hodnot X přes všechny volby množiny A. Průměr nemůže být větší než maximum z těchto hodnot, a tedy existuje volba A, pro niž více než polovina hran jde napříč. □

Nezávislé množiny. Kolik nejvýš hran může obsahovat graf na n vrcholech, neobsahující úplný graf na k vrcholech jako podgraf? Speciálně, pro $k = 3$, kolik hran může mít graf bez trojúhelníků? Na tuto otázku odpovídá Turánova věta, jeden z významných výsledků extremální teorie grafů. Tato věta se dá formulovat různými způsoby, nejsilnější verze přesně popisuje, jak musí graf s takovým maximálním možným počtem hran vypadat. Tady předvedeme velmi vtipný pravděpodobnostní důkaz trošku slabšího výsledku, který jen omezuje zmíněný počet hran. Turánova věta se nejčastěji používá v „obrácené" podobě: *má-li graf na n vrcholech více než jistý počet hran, pak obsahuje K_k*. Vezmeme-li doplněk grafu G, t.j. hrany budou právě tam, kde G hrany neměl, Turánova věta tvrdí *má-li graf na n vrcholech méně než jistý počet hran, pak obsahuje nezávislou množinu velikosti aspoň k* (nezávislá množina je množina vrcholů, mezi nimiž nejde žádná hrana). V této podobě zde větu zformulujeme a dokážeme.

9.4.2 Věta (Turánova věta). *Pro každý graf na n vrcholech platí*

$$\alpha(G) \geq \frac{n^2}{2|E(G)| + n},$$

kde $\alpha(G)$ značí velikost největší nezávislé množiny v grafu G.

Pravděpodobnostní metodu použijeme v důkazu takovéhoto lemmatu

9.4.3 Lemma. *Pro každý graf G platí*

$$\alpha(G) \geq \sum_{v \in V(G)} \frac{1}{\deg_G(v) + 1}$$

($\deg_G(v)$ značí stupeň vrcholu v v grafu G).

Důkaz. Předpokládejme, že vrcholy grafu G jsou $1, 2, \ldots, n$, a zvolme náhodnou permutaci π těchto vrcholů. Definujeme množinu $M \subseteq V(G)$, obsahující všechny vrcholy v takové, že pro všechny sousedy u vrcholu v platí $\pi(u) > \pi(v)$, t.j., vrchol v je v uspořádání podle hodnot π menší než všichni jeho sousedi. Všimněme si, že množina M je nezávislá v grafu G, tedy $|M| \leq \alpha(G)$ pro libovolnou permutaci, a tudíž i $\mathbf{E}|M| \leq \alpha(G)$.

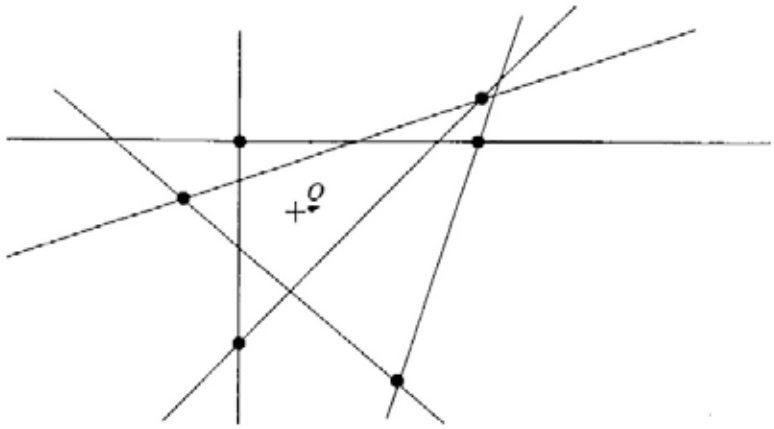
Pro každý vrchol v buď A_v jev „$v \in M$“. Je-li N_v množina všech sousedů vrcholu v, jsou všechna uspořádání množiny $N_v \cup \{v\}$ permutací π stejně pravděpodobná, a tedy pravděpodobnost, že v bude nejmenší z této množiny, je rovna $1/(|N_v| + 1) = 1/(\deg_G(v) + 1)$. Proto $P(A_v) = 1/(\deg_G(v) + 1)$, a můžeme počítat střední hodnotu jako již několikrát:

$$\alpha(G) \geq \mathbf{E}|M| = \sum_{v \in V(G)} \mathbf{E} I_{A_v} = \sum_{v \in V(G)} P(A_v) = \sum_{v \in V(G)} \frac{1}{\deg_G(v) + 1}.$$

□

Důkaz věty 9.4.2. To už je čistě počítání s nerovnostmi. Počet hran grafu $e = |E(G)|$ je polovina součtu stupňů všech vrcholů. Máme tedy takovouto situaci: pro nezáporná reálná čísla $d_1, d_2, \ldots, d_n$ víme $\sum_{i=1}^{n} d_i = 2e$, a ptáme se, jaká je nejmenší možná hodnota součtu

$$\sum_{i=1}^{n} \frac{1}{d_i + 1}.$$



Obrázek 9.1: Průsečíky úrovně 1 pro množinu přímek

Lze ukázat, že tento součet je minimální pro $d_1 = d_2 = \ldots = d_n = 2e/n$ (ponecháme do cvičení), a tehdy má hodnotu $n^2/(2e+n)$ jako v tvrzení věty. □

Počet průsečíků úrovně $\leq k$. Mějme množinu L sestávající z n přímek v rovině, z nichž žádné 3 se neprotínají v jednom bodě a žádné 2 nejsou rovnoběžné, a dále nějaký bod o, který neleží na žádné z přímek. Budeme se zabývat průsečíky přímek z L. Celkem je jich $\binom{n}{2}$ (každá dvojice přímek určuje právě 1 průsečík). Řekneme, že průsečík v má *úroveň* k, pokud úsečka ov protíná, kromě dvou přímek procházejících průsečíkem v, ještě k dalších přímek (obr. 9.1 znázorňuje všechny průsečíky úrovně 1). Kolik maximálně může být průsečíků úrovně nejvýš k, pro dané n a k? Tato otázka vzniká při analýze efektivity některých geometrických algoritmů. Následující věta dává horní odhad, který je nejlepší možný až na hodnotu konstanty úměrnosti:

9.4.4 Věta. *Existuje maximálně $3(k+1)n$ průsečíků úrovně nejvýš k.*

Důkaz. Nejdříve se podíváme na případ $k = 0$. Zjišťujeme, že průsečíky úrovně 0 jsou přesně vrcholy ohraničující konvexní mnohoúhelník, jenž obsahuje bod o. Protože každá přímka přispívá nejvýš jednou

stranou tohoto mnohoúhelníka, je takových vrcholů nejvýš n. Toho využijeme v dalším. Přikročíme k obecnému případu.

Nechť p označuje jisté číslo v intervalu $(0, 1)$, jehož hodnotu vhodně zvolíme na konci důkazu. Představíme si takovýto náhodný pokus: Náhodně vybereme podmnožinu přímek $R \subseteq L$, přičemž každou přímku $\ell \in L$ dáme do R s pravděpodobností p, a výběry jednotlivých přímek jsou na sobě nezávislé.

> Tady je asi na místě říci více o příslušném pravděpodobnostním prostoru. Je to zobecnění prostoru $\mathcal{C}_n$ z příkladu 9.2.2, modelujícího n hodů symetrickou mincí, na níž padá rub a líc se stejnou pravděpodobností, totiž $\frac{1}{2}$. V našem případě bychom používali jakousi nesymetrickou minci, na níž padá líc s pravděpodobností p a rub s pravděpodobností $1 - p$. Pro každou přímku $\ell \in L$ bychom jednou hodili, a zahrnuli bychom ji do R jestliže padne líc. Formálně, náš pravděpodobnostní prostor je množina všech podmnožin $R \subseteq L$, a pravděpodobnost množiny $R \subseteq L$, tedy elementárního jevu, je $p^r(1-p)^{n-r}$, kde $r = |R|$ (abychom dostali právě množinu R, musí v určitých r hodech padnout líc a ve zbývajících $n - r$ hodech rub). To je příklad pravděpodobnostního prostoru, kde elementární jevy nemají všechny stejnou pravděpodobnost.

Vraťme se k naší geometrické situaci. Představme si, že bychom do roviny nakreslili jen přímky z takové náhodně vybrané podmnožiny R. Zavedeme náhodnou veličinu $f = f(R)$, což bude počet průsečíků přímek z R úrovně 0, jinak řečeno těch průsečíků, jimž žádná přímka z R nezabraňuje ve výhledu na bod o. Budeme dvěma způsoby počítat střední hodnotu $\mathbf{E}f$. Na jedné straně víme, podle poznámky na začátku důkazu, že pro každou konkrétní množinu R je $f(R) \leq |R|$, a proto $\mathbf{E}f \leq \mathbf{E}|R|$. Lze snadno spočítat (ponecháváme do cvičení), že $\mathbf{E}|R| = pn$.

Nyní jiný způsob počítání $\mathbf{E}f$. Pro každý průsečík v přímek z L definujeme jev A_v, který nastane, pokud v bude jedním z průsečíků úrovně 0 přímek z R, t.j. přispěje 1 k hodnotě $f(R)$. Jev A nastane, právě když jsou splněny tyto dvě podmínky:

- Obě přímky, určující průsečík v, padnou do R.
- Žádná z přímek, protínajících úsečku ov ve vnitřním bodě (t.j., zakrývající bodu o výhled na bod v) nepadne do R.

Z toho je vidět, že $P(A_v) = p^2(1-p)^{u(v)}$, kde $u(v)$ značí úroveň průsečíku v.

Označme M množinu všech průsečíků přímek z L, a $M_k \subseteq M$ množinu průsečíků úrovně nejvýš k. Máme

$$\mathbf{E}f = \sum_{v\in M} \mathbf{E}I_{A_v} = \sum_{v\in M} P(A_v) \geq \sum_{v\in M_k} P(A_v) = \sum_{v\in M_k} p^2(1-p)^{u(v)} \geq$$

$$\geq \sum_{v\in M_k} p^2(1-p)^k = |M_k|p^2(1-p)^k.$$

Celkem jsme tedy odvodili $np \geq \mathbf{E}f \geq |M_k|p^2(1-p)^k$, neboli

$$|M_k| \leq \frac{n}{p(1-p)^k}.$$

Zvolíme teď číslo p tak, abychom na pravé straně dostali co nejmenší hodnotu. Vhodná volba je například $p = 1/(k+1)$. Je známo, že pro každé $k \geq 1$ je $(1-\frac{1}{k+1})^k > e^{-1} > \frac{1}{3}$, takže vyjde $|M_k| \leq 3(k+1)n$, jak se tvrdí ve větě. □

Poznamenejme ještě, že problém odhadnout maximální možný počet průsečíků úrovně *přesně* k je mnohem obtížnější a dosud nevyřešený.

Průměrný počet porovnání v algoritmu QUICKSORT. Známý třídící algoritmus QUICKSORT (česky „rychlotřídič"?), dostane-li jako vstup posloupnost prvků $(x_1, x_2, \ldots, x_n)$, pracuje takto: porovnáním s x_1 rozdělí ostatní prvky na dvě skupiny, na prvky menší než x_1 a prvky aspoň tak velké jako x_1 (přitom v obou skupinách zachová pořadí prvků jako bylo na vstupu). Každou skupinu pak zvlášť setřídí rekurzivním voláním sebe sama. Rekurze se zastaví u triviálně malých skupin (např. nejvýš dvouprvkových).

Tento algoritmus v nejhorším případě může potřebovat řádově až n^2 kroků (nejhorší, co mu můžeme provést, je dát mu již setříděnou posloupnost). V praxi je však velmi oblíben a bere se jako jeden z nejrychlejších třídících algoritmů. Jeden z důvodů je následující výsledek o jeho průměrném chování:

9.4.5 Věta. *Nechť $x_1 < x_2 < \ldots < x_n$ jsou tříděné prvky v pořadí podle velikosti. Buď π permutace množiny $\{1, 2, \ldots, n\}$, a nechť $T(\pi)$ značí počet porovnání (dvojic čísel podle velikosti) provedených algoritmem QUICKSORT pro vstupní posloupnost $(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)})$. Potom při náhodné volbě permutace π platí $\mathbf{E}T \leq 2n \ln n$.*

Důvod takového chování není těžké vidět. Jsou-li vstupní čísla srovnána náhodně, lze čekat, že první prvek většinou rozdělí ostatní na dvě zhruba stejně velké skupiny. Rekurze pak bude mít $\log n$ úrovní, a na každé úrovni se spotřebuje celkem $O(n)$ porovnání. To ale není pořádný důkaz. Následující elegantní analýza dává i správnou konstantu úměrnosti.

Důkaz. Nechť T_i je počet prvků porovnávaných s prvkem $x_{\pi(i)}$ ve fázi, kdy se stane dělicím prvkem. Například $T_1 = n - 1$, protože $x_{\pi(1)}$ je první prvek na vstupu a porovnávají se s ním všechny ostatní prvky. Pokud $\pi(2) < \pi(1)$, T_2 bude $\pi(1) - 2$, a pro $\pi(2) > \pi(1)$ je $T_2 = n - \pi(1) - 1$. Obecně si můžeme T_i představit podle obrázku:

Kroužky na tomto obrázku znázorňují $x_1, x_2, \ldots, x_n$ seřazené podle velikosti, plně jsou kresleny prvky s indexy $\pi(1), \pi(2), \ldots, \pi(i-1)$, dvojitě je označen $x_{\pi(i)}$, a prázdné jsou kroužky pro ostatní prvky. Není těžké si rozmyslet, že T_i je právě počet prázdných kroužků, které „vidí“ prvek $x_{\pi(i)}$, přičemž skrz plné kroužky vidět není.

Budeme hledat $\mathbf{E}T_i$. Představme si, že indexy probíráme pozpátku a sledujeme příslušný obrázek s plnými a prázdnými kroužky. Nejprve jsou všechny kroužky plné, postupně se jeden po druhém v náhodném pořadí vyprazdňují. V okamžiku, kdy zbývá i plných kroužků, vezmeme náhodně jeden zbývající plný kroužek, $x_{\pi(i)}$, a T_i bude počet prázdných kroužků, které vidí.

Použijeme jednoduché počítání dvěma způsoby. Každý *prázdný* kroužek vidí nejvýš dva plné kroužky. Proto celkový počet dvojic (plný

kroužek, prázdný kroužek), které se vidí, je nejvýš $2(n-i)$. Na jeden z i plných kroužků tedy připadá v průměru nejvýš $\frac{2(n-i)}{i}$ prázdných kroužků, a to je potřebný odhad pro $\mathbf{E}T_i$. Z linearity střední hodnoty konečně dostáváme

$$\mathbf{E}T = \sum_{i=1}^{n} \mathbf{E}T_i \leq \sum_{i=1}^{n} \frac{2(n-i)}{i} = 2n \sum_{i=1}^{n} \frac{1}{i} - 2n \leq 2n \ln n$$

(součet převrácených hodnot jsme odhadli podle cvičení 2.4.12). □

Poznámky. Složitější analýzou se dá dokázat, že při náhodné vstupní permutaci je nepříznivé chování algoritmu (t.j. počet porovnání podstatně větší než řádově $n \log n$) velmi málo pravděpodobné. Přesto skutečnost, že algoritmus pracuje špatně zrovna pro setříděné nebo skoro setříděné posloupnosti, je nepříjemná. Existuje řada verzí algoritmu QUICKSORT, které se různými modifikacemi snaží toto odstranit. Modifikace se týkají způsobu výběru prvku, podle nějž se ostatní prvky rozdělí.

Cvičení

1. Dokažte z věty 9.4.2, že graf na n vrcholech bez trojúhelníků má nejvýš $n^2/4$ hran.

2.* Ukažte, že jsou-li $d_1, \ldots, d_n$ nezáporná reálná čísla se součtem 1, potom výraz $\sum_{i=1}^{n} 1/(d_i + 1)$ je minimální pro $d_1 = d_2 = \ldots = d_n = \frac{1}{n}$.

3. Nechť podmnožina $R \subseteq L$ je zvolena náhodně jako v důkazu věty 9.4.4. Ukažte $\mathbf{E}|R| = pn$.

4.* Uvažme přímky jako ve větě 9.4.4, z nichž navíc žádná není svislá. Řekneme, že průsečík v je *špice*, pokud jedna z přímek jej definujících má kladnou směrnici (zleva doprava stoupá) a druhá má zápornou směrnici (zleva doprava klesá). Dokažte, že existuje nejvýš $6(k+1)^2$ špic úrovně nejvýš k.

10

Vytvořující funkce

V této kapitole probereme jednu užitečnou početní techniku. Základní myšlenkou je sdružit se studovanou nekonečnou posloupností reálných čísel jistou spojitou funkci, tzv. vytvořující funkci této posloupnosti. Úlohy o posloupnostech lze pak řešit využitím různých operací s funkcemi a poznatků o funkcích. Takový přechod je velmi nesamozřejmý a mnohé aplikace vytvořujících funkcí, ač technicky nejsou příliš hluboké, můžeme právem nazvat podivuhodnými.

V tomto úvodním textu se dostaneme pouze k jednodušším příkladům, u nichž se řešení většinou dá najít i bez použití vytvořujících funkcí. V některých úlohách různé triky dokonce vedou k cíli rychleji než počítání přes vytvořující funkce (nemusí však být snadné na takové triky přijít). To by čtenáře nemělo odrazovat od zvládnutí technik s vytvořujícími funkcemi, neboť tyto jsou mocným nástrojem i pro složitější problémy, kde jiné postupy selhávají nebo se stávají příliš složitými.

U některých řešení jsou alternativní postupy zmíněny, jinde jsou naznačeny ve cvičeních. Někdy čtenář možná najde ještě jednodušší řešení.

10.1 Kombinatorické aplikace mnohočlenů

Jak vynásobit mnohočleny $p(x) = x+x^2+x^3+x^4$ a $q(x) = x+x^3+x^4$? Třeba podle tohoto jednoduchého pravidla: vynásobíme každý člen z $p(x)$ každým členem z $q(x)$, a všechny tyto součiny sečteme, přesněji řečeno sloučíme součiny se stejnými mocninami x. Součin takto vyjde $x^8 + 2x^7 + 2x^6 + 3x^5 + 2x^4 + x^3 + x^2$.

Ptejme se teď jinak: vybereme si nějakou mocninu x, například x^5, a chceme vědět, jaký bude její koeficient v součinu, aniž bychom celý součin počítali. Člen s x^5 se v součinu může objevit vynásobením nějakého členu x^i z $p(x)$ členem x^{5-i} z $q(x)$. Koeficient u x^5 v součinu bude tedy právě počet způsobů, kterými se dá vyhovující i zvolit. Jinak řečeno, koeficient u x^5 bude počet dvojic (i,j), kde $i \in \{1,2,3,4\}$ (to je „množina exponentů" mnohočlenu $p(x)$), $j \in \{1,3,4\}$ (to jsou exponenty v $q(x)$) a přitom $i+j=5$.

To, co jsme právě řekli, vyjádříme trochu obecněji. Nechť I, J jsou konečné množiny přirozených čísel. Utvoříme mnohočleny $p(x) = \sum_{i\in I} x^i$, $q(x) = \sum_{j\in J} x^j$ (všechny koeficienty v takových mnohočlenech jsou rovny 1). Potom pro každé přirozené číslo r,

> počet řešení (i,j) rovnice
>
> $$i+j=r$$
>
> splňujících $i \in I$, $j \in J$ je roven koeficientu u x^r v součinu $p(x)q(x)$.

Další, zajímavější zobecnění tohoto pozorování je na součin 3 a více mnohočlenů. Ilustrujeme jej nejdřív na příkladu.

10.1.1 Úloha. *Kolika způsoby lze zaplatit částku 21 korun, máme-li 6 korunových mincí, 5 dvoukorun a 4 pětikoruny?*

Hledaný počet je zřejmě roven počtu řešení rovnice

$$i_1 + i_2 + i_3 = 21,$$

kde $i_1 \in \{0,1,2,3,4,5,6\}$, $i_2 \in \{0,2,4,6,8,10\}$, $i_3 \in \{0,5,10,15,20\}$ — i_1 je částka zaplacená korunami, i_2 částka zaplacená dvoukorunami a i_3 pětikorunami.

Tentokrát tvrdíme, že počet řešení této rovnice je roven koeficientu u x^{21} v součinu

$$\left(1+x+x^2+x^3+x^4+x^5+x^6\right)\left(1+x^2+x^4+x^6+x^8+x^{10}\right)\times$$

$$\left(1 + x^5 + x^{10} + x^{15} + x^{20}\right)$$

(samozřejmě poté, co ho roznásobíme a upravíme). Člen s x^{21} totiž dostáváme tak, že vezmeme nějaký člen x^{i_1} z první závorky, nějaký člen x^{i_2} ze druhé závorky a x^{i_3} ze třetí, přičemž $i_1 + i_2 + i_3 = 21$. Každý takový možný výběr přispěje 1 k uvažovanému koeficientu.

Čím nám toto pomůže v řešení úlohy? Z čistě praktického hlediska, usnadní to použití počítače na její řešení, máme-li ovšem k dispozici nějaký program pro násobení mnohočlenů (systémů pro počítání s formulemi, které zvládnou násobení mnohočlenů i mnoho dalších rutinních matematických úloh, existuje řada, mezi nejznámější patří Reduce, Maple, Mathematica, Macsyma, Derive, Mupad,...). Tak byla také zjištěna odpověď k tomuto příkladu: 9. Hledaný počet můžeme samozřejmě najít probráním všech možností (máme také jen celkem málo mincí), ale snadno se může stát, že na nějakou zapomeneme. Nejvýznamnější je však uvedený postup jako předehra ke složitějším metodám.

Kombinatorický význam binomické věty. Binomická věta tvrdí

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n. \qquad (10.1)$$

Na levé straně máme součin n mnohočlenů, každý z nich je $1 + x$. Podle výše uvedeného, koeficient u x^r po roznásobení bude počet řešení rovnice

$$i_1 + i_2 + \cdots + i_n = r,$$

kde $i_1, i_2, \ldots, i_n \in \{0, 1\}$. Ale každé řešení takové rovnice znamená vybrat r proměnných mezi $i_1, i_2, \ldots, i_n$, které budou rovny 1 — ostatní pak budou rovny 0. Takových výběrů je stejně jako r-prvkových podmnožin n-prvkové množiny, tedy $\binom{n}{r}$. To znamená, že koeficient při x^r v mnohočlenu $(1 + x)^r$ je $\binom{n}{r}$. Právě jsme kombinatoricky dokázali binomickou větu!

Pohráváme-li si šikovně s mnohočlenem $(1 + x)^n$ a jemu podobnými, můžeme odvodit hodnoty různých sum s binomickými koeficienty. Nejjednodušší příklad jsme viděli už v části 2.3, jmenovitě vzorce $\sum_{k=0}^{n}\binom{n}{k} = 2^n$ a $\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0$, které dostaneme dosazením $x = 1$, resp. $x = -1$ do (10.1).

10.1.2 Příklad. *Platí rovnost*

$$\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}.$$

Důkaz. Tento vztah můžeme odvodit derivováním obou stran vzorce (10.1) jako funkce proměnné x. Na obou stranách musí samozřejmě vyjít týž mnohočlen. Derivováním levé strany dostaneme $n(1+x)^{n-1}$, derivováním pravé strany člen po členu obdržíme $\sum_{k=0}^{n} k\binom{n}{k}x^{k-1}$. Dosazením $x = 1$ vznikne požadovaná rovnost.

Příklad jiného typu je založen na rovnosti koeficientů ve dvou vyjádřeních téhož mnohočlenu.

Jiný důkaz tvrzení 2.3.3. Uvažme identitu

$$(1+x)^n(1+x)^n = (1+x)^{2n}.$$

Koeficient při x^n na pravé straně je $\binom{2n}{n}$. Na levé straně můžeme rozvinout obě mocniny $(1+x)^n$ podle binomické věty, a potom násobit dva vzniklé mnohočleny. Koeficient u x^n v jejich součinu můžeme vyjádřit jako $\binom{n}{0}\binom{n}{n} + \binom{n}{1}\binom{n}{n-1} + \binom{n}{2}\binom{n}{n-2} + \cdots + \binom{n}{n}\binom{n}{0}$, a to musí být totéž jako koeficient na pravé straně, t.j.

$$\sum_{i=0}^{n} \binom{n}{i}\binom{n}{n-i} = \binom{2n}{n}.$$

Tím jsme znovu dokázali tvrzení 2.3.3. □

Podobným způsobem se lze spočítat i řadu dalších, komplikovanějších sum. Pokusíme-li se však o nějaké složitější výpočty, brzy začneme pociťovat jako nepříjemné omezení to, že pracujeme jen s mnohočleny, jež mají jen konečný počet členů. „Správným" nástrojem pro podobné aplikace se ukazují být analogie mnohočlenů, u nichž však připouštíme nekonečný počet mocnin proměnné x, tzv. mocninné řady.

Cvičení

1. V cukrárně prodávají 3 druhy zákusků — větrníky, kremrole a punčové dortíky. Kolika způsoby lze koupit 12 zákusků tak, aby se od každého druhu koupily aspoň 2 zákusky a přitom nejvýš 3 kremrole? Vyjádřete hledaný počet jako koeficient vhodné mocniny x ve vhodném součinu mnohočlenů.
2. Kolika způsoby lze rozdělit 10 stejných balónků 2 chlapečkům a 2 holčičkám, má-li každý chlapeček dostat aspoň 1 balónek a každá holčička nejméně 2? Vyjádřete hledaný počet jako koeficient vhodné mocniny x ve vhodném součinu mnohočlenů.
3. Dokažte multinomickou větu 2.3.4 podobnou úvahou, jako jsme zde dokazovali větu binomickou.
4. Spočtěte sumu v příkladu 10.1.2 vhodnou početní úpravou výrazu $k\binom{n}{k}$ a použitím binomické věty.
5. Spočítejte sumu $\sum_{i=0}^{n}(-1)^i\binom{n}{i}\binom{n}{n-i}$.

10.2 Rozšíření na nekonečné řady

Vlastnosti mocninných řad. *Mocninnou řadou* budeme rozumět nekonečnou řadu tvaru $a_0 + a_1x + a_2x^2 + \cdots$, kde $a_0, a_1, a_2, \ldots$ jsou reálná čísla a x je proměnná, nabývající reálných hodnot[1]. Uvedenou mocninnou řadu budeme zpravidla označovat $a(x)$.

Jednoduchým příkladem mocninné řady je

$$1 + x + x^2 + x^3 + \cdots \tag{10.2}$$

(všechna a_i jsou rovna 1). Ze vzorce pro součet geometrické řady víme, že pro každé $x \in (-1, 1)$ tato řada konverguje, a její součet je roven $1/(1-x)$. V tomto smyslu řada (10.2) určuje funkci $1/(1-x)$. Obráceně, uvedená funkce v sobě naopak obsahuje veškerou informaci o řadě (10.2), protože koeficienty řady jsou, jak se může čtenář přesvědčit, právě koeficienty Taylorova rozvoje funkce $1/(1-x)$ v bodě

[1] Velmi užitečné je též rozšíření na komplexní čísla a aplikace metod z teorie funkcí komplexní proměnné. Tak daleko se však v tomto úvodním textu nedostaneme.

0. Takové převtělování nekonečné posloupnosti čísel ve funkci a zpět je klíčovým obratem v technice vytvořujících funkcí.

Následující tvrzení říká, že nerostou-li členy posloupnosti $(a_0, a_1, a_2, \ldots)$ příliš rychle, definuje příslušná nekonečná řada $a(x) = a_0 + a_1 x + a_2 x^2 + \cdots$ skutečně funkci reálné proměnné x (aspoň na malém okolí 0), a ze znalosti hodnot této funkce můžeme posloupnost $(a_0, a_1, a_2, \ldots)$ zpětně rekonstruovat.

10.2.1 Tvrzení. *Buď $(a_0, a_1, a_2, \ldots)$ posloupnost reálných čísel. Předpokládejme, že pro nějaké číslo K platí $|a_n| \leq K^n$ pro všechna $n \geq 1$. Potom pro každé $x \in (-\frac{1}{K}, \frac{1}{K})$ řada $a(x) = \sum_{i=0}^{\infty} a_i x^i$ konverguje (dokonce absolutně), a hodnota jejího součtu definuje tedy funkci proměnné x na uvedeném intervalu; tuto funkci budeme označovat též $a(x)$. Hodnotami funkce $a(x)$ na libovolně malém okolí 0 jsou všechny členy posloupnosti $(a_0, a_1, a_2, \ldots)$ jednoznačně určeny: funkce $a(x)$ má totiž v bodě 0 derivace všech řádů, a pro $n = 0, 1, 2, \ldots$ platí*

$$a_n = \frac{a^{(n)}(0)}{n!}$$

($a^{(n)}(0)$ značí n-tou derivaci funkce $a(x)$ v bodě 0).

Důkaz plyne z poznatků z matematické analýzy a zde jej nebudeme uvádět, podobně jako u několika dalších tvrzení v tomto oddílu. Nejpřirozenější důkazy se dostanou z teorie funkcí komplexní proměnné, která se zpravidla probírá až v pokročilejších přednáškách. Nicméně pro naše účely potřebujeme velice málo, a to se dá trochu pracněji dokázat i elementárně, ze základních vět o limitách a derivování. V následujících příkladech nebudeme pro uvažované mocninné řady předpoklad tvrzení 10.2.1 výslovně ověřovat. V mnoha případech můžeme tomu uniknout následujícím alibistickým způsobem: Najdeme-li jednou správné řešení úlohy pomocí vytvořujících funkcí jakkoli podezřelou metodou, můžeme potom ověřit správnost řešení jinak, třeba indukcí.

Teď konečně řekneme, co je vytvořující funkce:

10.2.2 Definice. *Nechť* $(a_0, a_1, a_2, \ldots)$ *je posloupnost reálných čísel.* Vytvořující funkcí *této posloupnosti*[2] *rozumíme mocninnou řadu*

$$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots .$$

Má-li posloupnost $(a_0, a_1, a_2, \ldots)$ jen konečně mnoho nenulových členů, její vytvořující funkce je mnohočlen. V předchozím oddílu jsme tedy různě využívali vytvořujících funkcí konečných posloupností (aniž jsme jim tak říkali).

Operace s posloupnostmi a jejich vytvořujícími funkcemi. Operace popsané dále můžeme použít pro nalezení šikovného vyjádření vytvořující funkce pro danou posloupnost (t.j. pro otázky typu „Jaká je vytvořující funkce posloupnosti $(1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots)$?"), nebo někdy i pro hledání posloupnosti pro danou vytvořující funkci (ptáme-li se třeba „Která posloupnost má vytvořující funkci $\ln(1-x)$?"). V dalším budou $(a_0, a_1, a_2, \ldots)$ a $(b_0, b_1, b_2, \ldots)$ posloupnosti a $a(x), b(x)$ jejich vytvořující funkce.

A. Sčítáme-li posloupnosti člen po členu, odpovídá tomu zřejmě *sčítání* vytvořujících funkcí, t.j. posloupnost $(a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots)$ má vytvořující funkci $a(x) + b(x)$.

B. Jiná jednoduchá operace je *násobení reálným číslem* α: posloupnost $(\alpha a_0, \alpha a_1, \alpha a_2, \ldots)$ má vytvořující funkci $\alpha a(x)$.

C. Je-li n nějaké přirozené číslo, vytvořující funkce $x^n a(x)$ odpovídá posloupnosti

$$(\underbrace{0, 0, \ldots, 0}_{n\times}, a_0, a_1, a_2, \ldots) ;$$

to je velmi užitečné pro *posunutí posloupnosti doprava* o potřebný počet míst.

[2] Obšírnější název používaný v literatuře je *obyčejná vytvořující funkce*. Jak toto napovídá, používají se i jiné typy vytvořujících funkcí, z nichž pro kombinatorické aplikace nejdůležitější jsou patrně *exponenciální vytvořující funkce*. Exponenciální vytvořující funkce posloupnosti $(a_0, a_1, a_2, \ldots)$ je mocninná řada $\sum_{i=0}^{\infty} a_i/i!$, t.j. např. pro posloupnost $(1, 1, 1, \ldots)$ dostaneme exponenciální vytvořující funkci e^x. V dalším se omezíme na obyčejné vytvořující funkce.

D. Co dělat, chceme-li naopak *posunout doleva*, neboli získat vytvořující funkci např. pro posloupnost $(a_3, a_4, a_5, \ldots)$? Je ovšem potřeba dělit x^3, ale nesmíme zapomenout odečíst první 3 členy; správná vytvořující funkce pro uvedenou posloupnost je

$$(a(x) - a_0 - a_1 x - a_2 x^2)/x^3.$$

E. *Dosazení αx za x*: Utvoříme-li funkci $c(x) = a(\alpha x)$, kde α je opět pevné reálné číslo, bude $c(x)$ vytvořující funkcí pro posloupnost $(a_0, \alpha a_1, \alpha^2 a_2, \ldots)$. Kupříkladu: Jak už víme, je $1/(1-x)$ vytvořující funkce posloupnosti samých jedniček, a podle právě uvedeného pravidla bude tedy $1/(1-2x)$ vytvořující funkcí pro posloupnost mocnin dvojky, $(1, 2, 4, 8, \ldots)$. Na této operaci je založen i trik pro nahrazení všech členů posloupnosti s lichým indexem nulou: jak se může čtenář přesvědčit, odpovídá funkce $(a(x) + a(-x))/2$ posloupnosti $(a_0, 0, a_2, 0, a_4, 0, \ldots)$.

F. Jinou možností je *dosazení x^n za x*. Tím vznikne posloupnost, v níž nk-tý člen bude roven k-tému členu původní posloupnosti, a všechny ostatní členy budou nulové. Tak např. funkce $a(x^3)$ dává posloupnost $(a_0, 0, 0, a_1, 0, 0, a_2, 0, 0, \ldots)$. Se složitějšími případy, jako je dosazení jedné mocninné řady do druhé, se v našich příkladech nesetkáme, ale v komplikovanějších úvahách se objevují také.

10.2.3 Úloha. *Jaká je vytvořující funkce posloupnosti*

$$(1, 1, 2, 2, 4, 4, 8, 8, \ldots),$$

t.j. $a_n = 2^{\lfloor n/2 \rfloor}$?

Řešení. Jak jsme zmínili v E, posloupnost $(1, 2, 4, 8, \ldots)$ má vytvořující funkci $1/(1-2x)$. Podle F dostaneme vytvořující funkci $1/(1-2x^2)$ pro posloupnost $(1, 0, 2, 0, 4, 0, \ldots)$, a podle C odpovídá posloupnosti $(0, 1, 0, 2, 0, \ldots)$ vytvořující funkce $x/(1-2x^2)$. Sečtením konečně dostaneme vytvořující funkci pro původní posloupnost, t.j. odpověď je $(1+x)/(1-2x^2)$. □

G. Populární operace z matematické analýzy, *derivování a integrování* podle proměnné x, znamenají v řeči posloupností toto: derivace funkce $a(x)$, čili $a'(x)$, má jako svoji posloupnost

$$(a_1, 2a_2, 3a_3, \ldots),$$

člen s indexem k je $(k+1)a_{k+1}$ (mocninnou řadu derivujeme člen po členu, podobně jako mnohočlen). Vytvořující funkce $\int_0^x a(t)\mathrm{d}t$ odpovídá posloupnosti $(0, a_0, \frac{1}{2}a_1, \frac{1}{3}a_2, \frac{1}{4}a_3, \ldots)$, pro $k \geq 1$ je člen s indexem k roven $\frac{1}{k}a_{k-1}$.

10.2.4 Úloha. *Jaká je vytvořující funkce pro posloupnost druhých mocnin* $(1^2, 2^2, 3^2, \ldots)$, *t.j. posloupnost* $(a_0, a_1, a_2, \ldots)$, *kde* $a_k = (k+1)^2$?

Řešení. Začneme s posloupností samých jedniček, pro niž známe vytvořující funkci: $1/(1-x)$. První derivace této funkce, $1/(1-x)^2$, dává posloupnost $(1, 2, 3, 4, \ldots)$ podle bodu G. Druhá derivace je $2/(1-x)^3$, a její posloupnost je $(2\times 1, 3\times 2, 4\times 3, \ldots)$ opět podle G; člen s indexem k je $(k+2)(k+1) = (k+1)^2 + k + 1$. My ale potřebujeme $a_k = (k+1)^2$, takže odečteme ještě vytvořující funkci pro posloupnost $(1, 2, 3, \ldots)$, a dostaneme

$$a(x) = \frac{2}{(1-x)^3} - \frac{1}{(1-x)^2}.$$

□

H. Nakonec jsme si nechali nejzajímavější operaci, totiž násobení vytvořujících funkcí. Součin $a(x)b(x)$ je vytvořující funkcí posloupnosti $(c_0, c_1, c_2, \ldots)$, kde čísla c_k jsou dána vztahy

$$\begin{aligned} c_0 &= a_0b_0 \\ c_1 &= a_0b_1 + a_1b_0 \\ c_2 &= a_0b_2 + a_1b_1 + a_2b_0 \\ &\vdots \end{aligned}$$

obecně můžeme napsat

$$c_k = \sum_{i,j\geq 0;\ i+j=k} a_ib_j. \tag{10.3}$$

To se snadno zapamatuje — členy v součinu až do k-tého jsou tytéž jako v součinu mnohočlenů $(a_0 + a_1 x \cdots + a_k x^k)(b_0 + b_1 x + \cdots + b_k x^k)$.

Násobení vytvořujících funkcí má názornou kombinatorickou interpretaci, kterou nyní vysvětlíme na příkladu (pravda dětinském), přirozený příklad přijde v oddílu 10.4. Představme si, že máme zásobu stejných kostek, a že víme, že z i kostek můžeme a_i různými způsoby postavit hrad, a z j kostek můžeme b_j různými způsoby zbudovat pyramidu. Máme-li celkem k kostek, pak $c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0$ bude počet způsobů, jak postavit nějaký hrad a zároveň nějakou pyramidu (přitom pyramida a hrad nemají nikdy společné kostky). Heslovitě řečeno, vytvořující funkci pro počet uspořádaných dvojic (hrad, pyramida) získáme jako součin vytvořující funkce pro počet hradů a vytvořující funkce pro počet pyramid.

Výchozí funkce. K práci s vytvořujícími funkcemi je užitečné mít, kromě různých operací, k dispozici i zásobu funkcí, pro něž známe příslušné mocninné řady. Příklady mocninných řad, uváděné v kursu diferenciálního počtu, mohou patřit do takové zásoby; tak třeba někdy se může hodit poznatek, že $\ln(1-x)$ je vytvořující funkcí pro posloupnost $(0, 1, \frac{1}{2}, \frac{1}{3}/, \frac{1}{4}, \ldots)$. My zde uvedeme jedno snadné tvrzení, které se využívá zvlášť často:

10.2.5 Tvrzení (Zobecněná binomická věta). *Pro libovolné reálné číslo r a nezáporné celé číslo k definujme kombinační číslo $\binom{r}{k}$ předpisem*

$$\binom{r}{k} = \frac{r(r-1)(r-2)\ldots(r-k+1)}{k!}$$

(speciálně klademe $\binom{r}{0} = 1$). Potom funkce $(1+x)^r$ je vytvořující funkcí pro posloupnost $(\binom{r}{0}, \binom{r}{1}, \binom{r}{2}, \binom{r}{3}, \ldots)$ (přičemž mocninná řada $\binom{r}{0} + \binom{r}{1}x + \binom{r}{2}x^2 + \cdots$ vždy konverguje pro $|x| < 1$).

Důkaz je opět záležitostí matematické analýzy, a udělá se snadno pomocí Taylorova rozvoje. Pro r celé záporné můžeme binomický koeficient $\binom{r}{k}$ upravit na $(-1)^k\binom{-r+k-1}{k} = (-1)^k\binom{-r+k-1}{-r-1}$ (což je „obyčejný“ binomický koeficient), takže pro celé záporné mocniny $(1-x)$

speciálně dostaneme

$$\frac{1}{(1-x)^n} = \binom{n-1}{n-1} + \binom{n}{n-1}x + \binom{n+1}{n-1}x^2 + \cdots + \binom{n+k-1}{n-1}x^k + \cdots .$$

Uvedeme jednoduchý příklad na použití vytvořujících funkcí, další jsou ve cvičeních. Pokročilejší příklady pak následují v samostatných oddílech.

10.2.6 Úloha. *V krabici je 30 červených, 40 modrých a 50 bílých míčků, míčky téže barvy se od sebe nepoznají. Kolik je různých možností, jak vybrat z takové krabice soubor 70 míčků?*

Poučeni úvahami z oddílu 10.1 zjistíme, že hledaný počet je roven koeficientu při x^{70} v součinu

$$(1+x+x^2+\cdots+x^{30})(1+x+x^2+\cdots+x^{40})(1+x+x^2+\cdots+x^{50}).$$

Toto není potřeba skutečně roznásobovat, místo toho přepíšeme

$$1+x+x^2+\cdots+x^{30} = \frac{1-x^{31}}{1-x}.$$

Abychom nahlédli tuto rovnost, můžeme se rozpomenout na vztah pro součet prvních n členů geometrické řady. Kdybychom se nerozpomněli, můžeme si pomoci takto: začneme s vytvořující funkcí posloupnosti $(1,1,1,\ldots)$, což je $1/(1-x)$, a od ní odečteme vytvořující funkci posloupnosti

$$(\underbrace{0,0,\ldots,0}_{31\times},1,1,\ldots),$$

což je $x^{31}/(1-x)$ podle bodu C. Výsledkem je $(1-x^{31})/(1-x)$, což je vytvořující funkce pro posloupnost

$$(\underbrace{1,1,\ldots,1}_{31\times},0,0,\ldots).$$

Celý součin tedy upravíme na

$$\frac{1-x^{31}}{1-x}\cdot\frac{1-x^{41}}{1-x}\cdot\frac{1-x^{51}}{1-x}=\frac{1}{(1-x)^3}(1-x^{31})(1-x^{41})(1-x^{51}).$$

Nyní podle zobecněné binomické věty rozvineme činitel $(1-x)^{-3}$, a v součinu zbývajících 3 činitelů spočteme koeficienty u mocnin až do x^{70}, což je velmi snadné. Vychází

$$\left(\binom{2}{2}+\binom{3}{2}x+\binom{4}{2}x^2+\cdots\right)(1-x^{31}-x^{41}-x^{51}+\cdots),$$

kde tečky $\cdots$ zastupují mocniny vyšší než x^{70}. Koeficient u x^{70} v tomto součinu bude tedy $\binom{70+2}{2}-\binom{70+2-31}{2}-\binom{70+2-41}{2}-\binom{70+2-51}{2}=1061$.

Cvičení

1. (a) Určete koeficient při x^{15} v $(x^2+x^3+x^4+\cdots)^4$.
   (b) Určete koeficient při x^{50} v $(x^7+x^8+x^9+x^{10}+\cdots)^6$.
   (c) Určete koeficient při x^5 v $(1-2x)^{-2}$.
   (d) Určete koeficient při x^4 v $\sqrt[3]{1+x}$.
   (e) Určete koeficient při x^3 v $(2+x)^{3/2}/(1-x)$.
   (f) Určete koeficient při x^4 v $(2+3x)^5\sqrt{1-x}$.
   (g) Určete koeficient při x^3 v $(1-x+2x^2)^9$.
2. Najděte vytvořující funkce pro následující posloupnosti (nepoužívejte v jejich zápisu nekonečné řady!)
   (a) $0,0,0,0,-6,6,-6,6,-6,\ldots$
   (b) $1,0,1,0,1,0\ldots$
   (c) $1,2,1,4,1,8,\ldots$
   (d) $1,1,0,1,1,0,1,1,0,\ldots$
3. Zjistěte, jaká je pravděpodobnost, že při hodu 12 hracími kostkami hodíme dohromady přesně 30 ok.
4. Buď a_n počet uspořádaných r-tic $(i_1,\ldots,i_r)$ celých nezáporných čísel takových, že $i_1+i_2+\cdots+i_r=n$; přitom r je nějaké pevné přirozené číslo.
   (a) Napište vytvořující funkci pro posloupnost $(a_0,a_1,a_2,\ldots)$.
   (b) Najděte vzorec pro a_n. (To jsme jiným způsobem řešili v části 2.3.)

5. Řešte úlohu 10.2.4 bez použití derivace — místo toho využijte zobecněnou binomickou větu.

6. Buď a_n počet způsobů, jímž lze zaplatit částku n korun pomocí korunových, dvoukorunových a pětikorunových mincí.

   (a) Napište vytvořující funkci pro posloupnost $(a_0, a_1, \ldots)$.

   (b)* Pomocí (a) najděte vzorec pro a_n (k odvození vzorce pomůže přečtení následujícího oddílu).

7. (a) Ověřte, že je-li $a(x)$ vytvořující funkce pro posloupnost $(a_0, a_1, a_2, \ldots)$, potom $a(x)/(1-x)$ je vytvořující funkce pro posloupnost částečných součtů $(a_0, a_0 + a_1, a_0 + a_1 + a_2, \ldots)$.

   (b) Pomocí (a) a řešení úlohy 10.2.4 vypočítejte součet $\sum_{k=1}^{n} k^2$.

   (c) Podobnou metodou vyjádřete součet $\sum_{k=1}^{n} k^3$.

   (d) Podobnou metodou — a pomocí zobecněné binomické věty — spočítejte $\sum_{k=r}^{n} \binom{k}{r}$ (r, n jsou daná přirozená čísla).

   (e) Pro přirozená čísla n, m vypočítejte součet $\sum_{k=0}^{m} (-1)^k \binom{n}{k}$.

   (f) Teď by se mohlo zdát, že uvedenou metodou můžeme spočítat téměř jaké sumy se nám zachce, ale není to tak jednoduché. Co se stane, budeme-li takto počítat $\sum_{k=1}^{n} \frac{1}{k}$?

8.* Dokažte vzorec pro součin mocninných řad, t.j. ukažte, že jsou-li $a(x)$, $b(x)$ mocninné řady vyhovující předpokladům tvrzení 10.2.1, potom funkce $a(x)b(x)$ je též mocninná řada, a její koeficienty jsou dány formulí (10.3).

9. Buď $a(x) = a_0 + a_1 x + a_2 x^2 + \cdots$ mocninná řada s nezápornými koeficienty, t.j. $a_i \geq 0$ pro každé i. Definujme její *poloměr konvergence* jako

$$\rho = \sup\{x \geq 0;\ a(x) \text{ konverguje}\}.$$

   (a)* Dokažte, že $a(x)$ konverguje pro každé $x \in [0, \rho)$, a že funkce $a(x)$ je na intervalu $[0, \rho)$ spojitá.

   (b) Najděte příklad posloupnosti $(a_0, a_1, a_2, \ldots)$, pro niž $\rho = 1$ a řada $a(\rho)$ diverguje.

   (c) Najděte příklad posloupnosti $(a_0, a_1, a_2, \ldots)$, pro niž $\rho = 1$ a řada $a(\rho)$ konverguje.

10. (Varovný příklad) Definujme funkci f předpisem

$$f(x) = \begin{cases} e^{-1/x^2} & \text{pro } x \neq 0 \\ 0 & \text{pro } x = 0 \end{cases}$$

(a)* Ukažte, že všechny derivace funkce f v bodě 0 existují a rovnají se 0.

(b) Odvoďte, že funkce f není v žádném okolí 0 dána mocninnou řadou.

10.3 Fibonacciho čísla a zlatý řez

Budeme vyšetřovat posloupnost $(F_0, F_1, F_2, \ldots)$ danou předpisem

$$F_0 = 0,\ F_1 = 1,\ F_{n+2} = F_{n+1} + F_n \quad \text{pro } n = 0, 1, 2, \ldots.$$

Tuto posloupnost studoval ve 13. století ve svém spise Leonardo z Pisy zvaný Fibonacci, a je známa pod jménem Fibonacciho čísla. Prvních několik členů je

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots.$$

V matematice i v teoretické informatice se tato čísla vynořují často a v rozličných souvislostech.

Ukážeme, jak se najde formule pro n-té Fibonacciho číslo použitím vytvořujících funkcí. Nechť tedy $F(x)$ značí vytvořující funkci této posloupnosti. Hlavní myšlenka je vyjádřit vytvořující funkci posloupnosti, jejíž k-tý člen je pro $k \geq 2$ roven $F_k - F_{k-1} - F_{k-2}$. Podle vztahu definujícího Fibonacciho čísla je tato posloupnost od druhého členu počínaje nulová. Na druhé straně lze takovou vytvořující funkci zkonstruovat z $F(x)$ pomocí operací probraných v oddílu 10.2, a tím vyjde rovnice určující $F(x)$.

Konkrétně, vezmeme funkci $F(x) - xF(x) - x^2F(x)$, odpovídající posloupnosti

$$(F_0, F_1 - F_0, F_2 - F_1 - F_0, F_3 - F_2 - F_1, \ldots) = (0, 1, 0, 0, \ldots).$$

V řeči vytvořujících funkcí to znamená $(1 - x - x^2)F(x) = x$, a odtud

$$F(x) = \frac{x}{1 - x - x^2}. \tag{10.4}$$

Kdybychom teď začali zjišťovat Taylorovu řadu této funkce derivováním, příliš neuspějeme. Musíme ještě uplatnit jeden obrat, který je dobře znám v integrálním počtu pod názvem *rozklad na částečné (parciální) zlomky*. V našem případě tato metoda zaručuje, že můžeme racionální funkci na pravé straně (10.4) přepsat do tvaru

$$\frac{x}{1-x-x^2} = \frac{A}{x-x_1} + \frac{B}{x-x_2},$$

kde x_1, x_2 jsou kořeny kvadratického mnohočlenu $1-x-x^2$ a A, B jsou vhodné konstanty. Pro naše účely se bude lépe hodit ještě trochu pozměněné vyjádření, totiž ve tvaru

$$\frac{x}{1-x-x^2} = \frac{a}{1-\lambda_1 x} + \frac{b}{1-\lambda_2 x},$$

kde $\lambda_1 = 1/x_1$, $\lambda_2 = 1/x_2$ a a, b jsou jiné vhodné konstanty (toto vyjádření se dostane z výše uvedeného dělením čitatele i jmenovatele prvního zlomku číslem $-x_1$ a druhého zlomku $-x_2$). Z tohoto vyjádření je už snadné napsat vzorec pro F_n; jak čtenář může ověřit, vychází $F_n = a\lambda_1^n + b\lambda_2^n$.

Výpočet kořenů kvadratické rovnice jakož i stanovení konstant a, b vynecháme, a uvedeme jen výslednou formuli

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right].$$

Je pozoruhodné, že tento výraz plný iracionálních čísel dává pro každé přirozené n celé číslo.

S přibližnými numerickými hodnotami konstant vypadá tento vzorec takto:

$$F_n = (0.4472135\ldots)\,[(1.6180339\ldots)^n - (-0.6180339\ldots)^n]$$

Z toho vidíme, že pro velká n se čísla F_n chovají zhruba jako $\lambda_1^n/\sqrt{5}$. Také dostáváme, že poměr F_n/F_{n+1} má limitu $1/\lambda_1 = 0.6180339\ldots$. Tento poměr byl znám a ceněn již v antice; nazývá se *zlatý řez*. Obdélník s poměrem stran rovným zlatému řezu se považoval za nejuměřenější a nejkrásnější. Oddělíme-li od takového obdélníku čtverec, zbylý obdélník má opět poměr zlatého řezu. Podobně jako s Fibonacciho čísly, se zlatým řezem se v matematice setkáme překvapivě často.

Jiné odvození: schody. Uvažme schodiště s n stupni. Kolika způsoby je lze vyjít, když každým krokem vyjdeme jeden nebo dva schody? Jinak řečeno, kolika způsoby lze zapsat číslo n jako součet jedniček a dvojek, neboli kolik řešení má rovnice

$$s_1 + s_2 + \cdots + s_k = n,$$

kde $s_i \in \{1, 2\}$, $i = 1, 2, \ldots, k$, $k = 0, 1, 2, \ldots$? Označíme-li tento počet S_n, máme $S_1 = 1$, $S_2 = 2$, a není těžké ověřit, že pro $n \geq 1$ splňují čísla S_n rekurentní vztah $S_{n+2} = S_{n+1} + S_n$ (rozmyslete si to!). Z toho je indukcí vidět, že S_n je právě Fibonacciho číslo F_{n-1}. Odvodíme teď vytvořující funkci pro posloupnost $(S_0, S_1, S_2, \ldots)$ jiným způsobem. Podle návodu z části 10.1 dostaneme, že pro dané k je počet řešení rovnice $s_1 + s_2 + \cdots + s_k = n$, kde $s_i \in \{1, 2\}$, roven koeficientu při x^n v součinu $(x + x^2)^k$. My ale můžeme zvolit k libovolně (není řečeno, kolika kroky máme schody vyjít), a proto S_n bude koeficient při x^n v součtu $\sum_{k=0}^{\infty}(x + x^2)^k$, takže tento součet je vytvořující funkcí pro čísla S_n. Tuto vytvořující funkci můžeme ještě dále upravit: uvedený součet je geometrická řada s kvocientem $x + x^2$ (tedy pro dost malé x konverguje), a její součet je $1/(1 - x - x^2)$. Vytvořující funkce pro Fibonacciho čísla je tudíž $x/(1 - x - x^2)$, jak jsme předtím nahlédli jinou metodou.

Recepty. Výše uvedenou metodou můžeme najít obecný tvar posloupnosti splňující vztah

$$y_{n+k} = a_{k-1}y_{n+k-1} + a_{k-2}y_{n+k-2} + \cdots + a_1 y_{n+1} + a_0 y_n \qquad (10.5)$$

pro $n = 0, 1, 2, \ldots$, kde k je konstanta, $a_0, a_1, \ldots, a_{k-1}$ jsou daná čísla (reálná nebo komplexní) a $(y_0, y_1, \ldots)$ je neznámá posloupnost reálných (nebo komplexních) čísel; tak například pro Fibonacciho čísla bychom měli $k = 2$, $a_0 = a_1 = 1$. Označme nyní písmenem $\mathcal{Y}$ množinu všech posloupností $(y_0, y_1, \ldots)$ splňujících vztah (10.5). V této množině bude obecně mnoho posloupností, protože prvních k členů posloupnosti $(y_0, y_1, \ldots)$ můžeme libovolně zvolit a ostatní členy postupně vypočítat ze vztahu (10.5). V dalším popíšeme, jak vypadají všechny posloupnosti z $\mathcal{Y}$, nejprve však terminologická odbočka.

Rovnice (10.5) se učeně nazývá *homogenní lineární diferenční rovnice k-tého stupně s konstantními koeficienty.* Pokusme se vysvětlit jednotlivé části názvu:

- *Homogenní* se v názvu objevuje proto, že je-li $(y_0, y_1, \ldots) \in \mathcal{Y}$, pak také pro každé reálné číslo α je $(\alpha y_0, \alpha y_1, \ldots) \in \mathcal{Y}$. Naproti tomu nehomogenní by byla třeba rovnice $y_{n+1} = y_n + 1$.
- Slovo *lineární* zde znamená, že hodnoty y_j se v rovnici objevují vždy v první mocnině. Nelineární diferenční rovnice by byla třeba $y_{n+2} = y_{n+1} y_n$.
- Fráze *s konstantními koeficienty* vyjadřuje, že $a_0, a_1, \ldots, a_{k-1}$ jsou pevná čísla nezávisející na n. Mohli bychom totiž také uvažovat např. rovnici tvaru $y_{n+1} = (n-1)y_n$, kde koeficient na pravé straně je funkcí n.
- Konečně *diferenční rovnice* se užívá jako obecného označení pro rovnice vyjadřující n-tý člen posloupnosti pomocí několika předchozích členů[3]. Název souvisí s tzv. *diferencemi* funkce, což je pojem trochu podobný derivacím. Jak známo, derivace funkce f v bodě x je limita podílu $(f(x+h) - f(x))/h$ pro $h \to 0$; je to tedy míra přírůstku funkce f při zvětšení x o „nekonečně malou" veličinu. Diference funkce f v bodě x je naproti tomu přírůstek funkce f při zvětšení argumentu o 1, t.j. veličina $f(x+1) - f(x)$. Pro dostatečně hladké funkce je diference hrubou aproximací derivace. Čtenář se možná setkal s diferenciálními rovnicemi, což jsou vztahy mezi neznámou funkcí a jejími derivacemi, jako třeba $f'(x) = f(x) + 1$. Diferenční rovnice můžeme podobně chápat jako vztah mezi neznámou funkcí a jejími diferencemi (zde se ovšem můžeme omezit na celočíselné hodnoty x, a psát hodnotu neznámé funkce y v bodě n jako y_n). Analogií k právě zmíněnému příkladu diferenciální rovnice $f'(x) = f(x) + 1$ by byla diferenční rovnice $y_{n+1} - y_n = y_n + 1$, neboli $y_{n+1} = 2y_n + 1$. Takto název diferenční rovnice vznikl, a někdy může analogie mezi diferenčními a diferenciálními rovnicemi opravdu napomoci řešení jedněch pomocí druhých.

Tolik k onomu obšírnému názvu, teď zformulujeme obecný výsledek o řešení uvažovaných diferenčních rovnic. *Charakteristickým polynomem* diferenční rovnice (10.5) nazveme polynom

$$p(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \cdots - a_1 x - a_0$$

(například charakteristický polynom vztahu pro Fibonacciho čísla je $x^2 - x - 1$). Připomeňme, že každý mnohočlen k-tého stupně s koeficientem

[3] Jiný používaný název je *rekurence* nebo *rekurentní relace*.

1 při x^k lze zapsat jako $(x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_k)$, kde $\lambda_1,\ldots,\lambda_k$ jsou (obecně komplexní) čísla, zvaná *kořeny* daného mnohočlenu.

10.3.1 Tvrzení. *Nechť $p(x)$ je charakteristický polynom homogenní lineární diferenční rovnice (10.5).*

(i) (Jednoduché kořeny) *Předpokládejme, že $p(x)$ má k navzájem různých kořenů $\lambda_1,\ldots,\lambda_k$. Potom pro libovolnou posloupnost $y = (y_0, y_1, \ldots) \in \mathcal{Y}$ splňující (10.5) existují komplexní konstanty C_1, C_2, ..., C_k takové, že pro každé n je*

$$y_n = C_1\lambda_1^n + C_2\lambda_2^n + \cdots + C_k\lambda_k^n.$$

(ii) (Obecný případ) *Nechť $\lambda_1,\ldots,\lambda_q$ jsou navzájem různá komplexní čísla a $k_1,\ldots,k_q$ přirozená čísla, $k_1+k_2+\cdots+k_q = k$, taková, že*

$$p(x) = (x-\lambda_1)^{k_1}(x-\lambda_2)^{k_2}\ldots(x-\lambda_q)^{k_q}.$$

Potom pro libovolnou posloupnost $y = (y_0, y_1, \ldots) \in \mathcal{Y}$ splňující (10.5) existují komplexní konstanty C_{ij} ($i = 1,2,\ldots,q$, $j = 0,1,\ldots,k_i-1$) takové, že pro každé n je

$$y_n = \sum_{i=1}^{q}\sum_{j=0}^{k_i-1} C_{ij}\binom{n}{j}\lambda_i^n.$$

Jak podle tohoto řešit diferenční rovnice? Uveďme dva stručné příklady. U rovnice $y_{n+2} = 3y_{n+1} - 2y_n$ je charakteristický polynom $p(x) = x^2 - 3x + 2 = (x-2)(x-3)$. Jeho kořeny jsou tedy $\lambda_1 = 2$, $\lambda_2 = 3$, a tvrzení 10.3.1 říká, že řešení máme hledat ve tvaru $C_1 2^n + C_2 3^n$. Máme-li předepsány počáteční podmínky, např. $y_0 = 2$, $y_1 = 5$, musíme dopočítat konstanty C_1, C_2 tak, aby uvedený vzorec dával tyto požadované hodnoty pro $n = 0, 1$; v našem případě bychom tudíž volili $C_1 = C_2 = 1$.

A ještě dosti umělý příklad na násobné kořeny: rovnice $y_{n+5} = 8y_{n+4} + 25y_{n+3} - 38y_{n+2} + 28y_{n+1} - 8y_n$ má charakteristický polynom[4] $p(x) = (x-1)^2(x-2)^3$, a tvrzení 10.3.1 praví, že řešení bude tvaru $y_n = C_{10} + C_{11}n + C_{20}2^n + C_{21}n2^n + C_{22}\binom{n}{2}2^n$. Hodnoty konstant by se opět dopočítaly podle hodnot prvních 5 členů posloupnosti $(y_0, y_1, \ldots)$.

[4] Samozřejmě autoři vybrali koeficienty tak, aby charakteristický polynom vyšel takhle pěkně. Uvedený návod na řešení (jakož i metoda pomocí vytvořujících funkcí) ponechává stranou otázku, jak v obecnosti najít kořeny. V příkladech z různých sbírek úloh a učebnic mají rekurence stupeň 1 nebo 2 nebo bývají koeficienty zvoleny tak, aby kořeny vyšly pěkně.

Právě uvedený postup řešení rekurence (10.5) se najde téměř ve všech učebnicích, a o vytvořujících funkcích zpravidla nepadne zmínka ani v důkaze tvrzení 10.3.1 — skutečně, toto tvrzení se dá dokázat dosti elegantně pomocí lineární algebry (naznačíme ve cvičeních), a pakliže odněkud víme, že řešení se má hledat ve zmíněném tvaru, vytvořující funkce už nepotřebujeme. Postup, který jsme uvedli pro Fibonacciho čísla, však ukazuje, jak správný tvar řešení opravdu odvodit. Navíc je to pěkný příklad na práci s vytvořujícími funkcemi, a podobný přístup se někdy dá s úspěchem použít i pro diferenční rovnice jiného tvaru, kde už obecný návod k řešení znám není (nebo je pracné ho v literatuře najít).

Cvičení

1.* Zjistěte, kolik existuje n-členných posloupností nul a jedniček, v nichž se nikde nevyskytují 2 nuly po sobě.

2. Vyjádřete obecný člen posloupností určených následovně (zobecněte postup použitý pro Fibonacciho čísla, příp. použijte výše uvedený obecný návod na řešení homogenních lineárních diferenčních rovnic s konstantními koeficienty):

   (a)
   $$a_0 = 2,\ a_1 = 3,\ a_{n+2} = 3a_n - 2a_{n+1} \quad (n = 0, 1, 2, \ldots)$$

   (b)
   $$a_0 = 0,\ a_1 = 1,\ a_{n+2} = 2a_{n+1} - 4a_n \quad (n = 0, 1, 2, \ldots)$$

   (c)
   $$a_0 = 1, a_{n+1} = 2a_n + 3 \quad (n = 0, 1, 2, \ldots)$$

3. V posloupnosti $(a_0, a_1, a_2, \ldots)$ je vždy následující člen aritmetickým průměrem předchozích dvou členů. Určete limitu $\lim_{n\to\infty} a_n$ (jako funkci a_0, a_1).

4. Řešte rekurenci $a_{n+2} = \sqrt{a_{n+1}a_n}$ s počátečními podmínkami $a_0 = 2$, $a_1 = 8$, najděte $\lim_{n\to\infty} a_n$.

5. (a) Řešte rekurenci $a_n = a_{n-1} + a_{n-2} + \ldots + a_1 + a_0$ s počáteční podmínkou $a_0 = 1$.

   (b) * Řešte rekurenci $a_n = a_{n-1} + a_{n-3} + a_{n-4} + a_{n-5} + \cdots + a_1 + a_0$ $(n \geq 3)$, pro $a_0 = a_1 = a_2 = 1$.

6.* Kolik existuje n-členných posloupností, tvořených písmeny a, b, c, d, v nichž a nikdy nesousedí s b?

7. Dokažte tvrzení 10.3.1 zobecněním postupu předvedeného pro Fibonacciho čísla (využijte obecný tvar věty o rozkladu racionální funkce na částečné zlomky z analýzy).

8. Dokažte tvrzení 10.3.1 přímo použitím lineární algebry, podle následujících bodů.

   (a) Ověřte, že množina $\mathcal{Y}$ všech řešení tvoří vektorový prostor vzhledem ke sčítání posloupností po složkách a násobení komplexním číslem po složkách.

   (b) Ukažte, že dimenze $\mathcal{Y}$ je rovna k.

   (c) * Ukažte, že v situaci části (i) tvrzení 10.3.1 posloupnosti $(\lambda_i^0, \lambda_i^1, \lambda_i^2, \ldots)$ pro $i = 1, 2, \ldots, k$ náleží do $\mathcal{Y}$, a jsou lineárně nezávislé, t.j. podle (b) tvoří bázi vektorového prostoru $\mathcal{Y}$; tím dokážete část (i).

   (d) Ověřte, že v situaci části (ii) tvrzení 10.3.1 je každá z posloupností $(\binom{n}{j}\lambda_i^n)_{n=0}^{\infty}$ prvkem množiny řešení $\mathcal{Y}$.

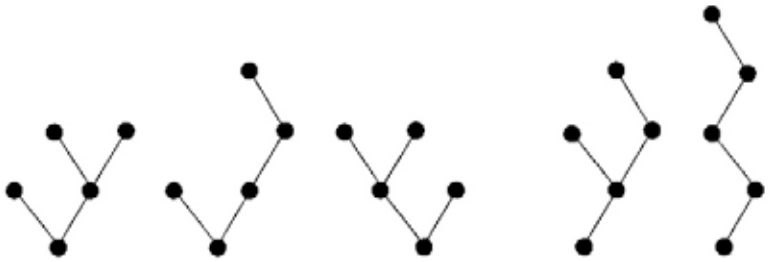
   (e) ** Dokažte, že posloupnosti z předchozího bodu (d) jsou lineárně nezávislé v $\mathcal{Y}$, t.j. tvoří bázi.

10.4 Binární stromy

Budeme uvažovat tzv. binární stromy, takové, jaké se často používají v datových strukturách. Na obr. 10.1 je nakresleno několik různých binárních stromů s 5 vrcholy. Pro naše účely můžeme binární strom definovat krátce takto: binární strom je buď prázdný (nemá žádný vrchol), nebo sestává z jednoho význačného vrcholu (zvaného *kořen*) plus z uspořádané dvojice binárních stromů[5] (levého a pravého podstromu).

Nechť b_n označuje počet binárních stromů s n vrcholy. Naším úkolem bude najít vzorec pro b_n. Probráním malých případů zjistíme $b_0 = 1$, $b_1 = 1$, $b_2 = 2$, $b_3 = 5$; to může sloužit jako kontrola správnosti výsledků v dalším.

[5] Toto je vlastně definice indukcí; nejdříve řekneme, co je binární strom s 0 vrcholy (prázdný strom), a potom definujeme binární strom s n vrcholy pomocí již definovaných binárních stromů s menším počtem vrcholů. Tím, že připouštíme prázdný strom, se vyhneme popisu různých speciálních případů, jako když kořen má jen levý či jen pravý podstrom.



Obrázek 10.1: Několik různých binárních stromů na 5 vrcholech.

Jako obvykle, $b(x) = b_0 + b_1 x + b_2 x^2 + \cdots$ bude příslušná vytvořující funkce. Pro $n \geq 1$, počet binárních stromů s n vrcholy je podle definice roven počtu uspořádaných dvojic tvaru (B, B'), kde B, B' jsou binární stromy s dohromady $n-1$ vrcholy, t.j. má-li B k vrcholů, má B' $n-k-1$ vrcholů. Počet takových uspořádaných dvojic je

$$b_n = b_0 b_{n-1} + b_1 b_{n-2} + \cdots + b_{n-1} b_0. \tag{10.6}$$

To je ale podle definice násobení vytvořujících funkcí přesně koeficient při x^{n-1} v součinu $b(x).b(x) = b(x)^2$ (to je příklad na kombinatorický význam násobení vytvořujících funkcí, slíbený v oddílu 10.2), a tedy koeficient při x^n ve funkci $xb(x)^2$. Tím pádem je $xb(x)^2$ vytvořující funkce pro tutéž posloupnost jako funkce $b(x)$, až na to, že funkce $b(x)$ má absolutní člen b_0 rovný 1, zatímco ve funkci $xb(x)^2$ je absolutní člen 0 (to proto, že vzorec (10.6) je správný jen pro $n \geq 1$). Můžeme tudíž napsat následující rovnost mezi vytvořujícími funkcemi:

$$b(x) = 1 + xb(x)^2.$$

Na to se můžeme dívat jako na kvadratickou rovnici s neznámou $b(x)$ (přitom x si představujeme jako libovolné, ale pevné číslo). Podle dobře známého vzorečku jsou její kořeny

$$b(x)_{1,2} = \frac{1 \pm \sqrt{1-4x}}{2x}.$$

To vypadá, jako by byla dvě možná řešení, my však víme, že posloupnost $(b_0, b_1, b_2, \ldots)$ a tedy i její vytvořující funkce jsou určeny

jednoznačně! Podíváme-li se však na řešení se znaménkem „+“, zjistíme, že pro $x \to 0+$ má limitu ∞, zatímco vytvořující funkce pro naši posloupnost musí mít limitu $b_0 = 1$. Toto řešení tedy vyloučíme. Řešení se znaménkem „−“ se ukazuje být hledané vyjádření vytvořující funkce, zbývá určit jeho koeficienty.

K tomu využijeme zobecněné binomické věty 10.2.5. Podle ní máme rozvoj

$$\sqrt{1-4x} = \sum_{k=0}^{\infty} (-4)^k \binom{1/2}{k} x^k.$$

Koeficient u x^0 je 1, takže $1 - \sqrt{1-4x}$ má po rozvinutí v řadu nulový absolutní člen, a tak můžeme tuto řadu vydělit $2x$ (posunutím o 1 člen doleva a dělením 2). Z toho dostáváme pro $n \geq 1$

$$b_n = -\frac{1}{2}(-4)^{n+1} \binom{1/2}{n+1}. \tag{10.7}$$

Dalšími úpravami (které ponecháváme do cvičení) lze získat pěknější tvar

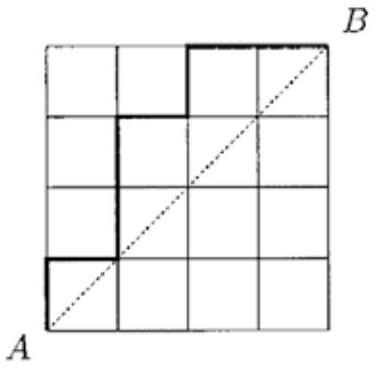
$$b_n = \frac{1}{n+1} \binom{2n}{n}.$$

Takto definovaná čísla b_n jsou v literatuře známa pod jménem *Catalanova čísla*. Kromě toho, že udávají počet binárních stromů, mají i několik dalších kombinatorických významů.

Cvičení

1. Upravte pravou stranu rovnice (10.7) na tvar uvedený pod touto rovnicí.

2. Uvažme šachovnici $n \times n$ čtverečků:



Uvažujme cesty z bodu A do bodu B, které jdou po hranách čtverečků šachovnice a jsou nejkratší (t.j. používají $2n$ hran).

(a) Kolik je všech takových cest?

(b)* Ukažte, že cest, které nikdy nejdou pod diagonálu šachovnice (t.j. přímku AB) je právě b_n, t.j. Catalanovo číslo. Jedna taková cesta je na obrázku vyznačena.

(c)** Dokažte vzorec $b_n = \frac{1}{n+1}\binom{2n}{n}$ elementárně, bez použití vytvořujících funkcí.

3. Uvažme součin 4 čísel, $abcd$. Ten lze „uzávorkovat" 5 způsoby: $((ab)c)d$, $(a(bc))d$, $(ab)(cd)$, $a((bc)d)$ a $a(b(cd))$. Dokažte, že počet uzávorkování součinu n čísel je právě Catalanovo číslo b_{n-1}.

4. Ve frontě na lístky po 50 Kč kus je $2n$ lidí, každý kupuje 1 lístek, přitom n z nich má padesátikorunu a n stokorunu. Na začátku nemá pokladní žádné peníze.

   (a) Kolik je seřazení lidí do fronty, pro něž pokladní bude mít pro každého majitele 100 Kč bankovky nazpět padesátikorunu?

   (b) Jaká je pravděpodobnost toho, že při náhodném seřazení fronty bude mít pokladní pro každého nazpět?

5. *Uvažme pravidelný n-úhelník. Rozdělme jej na trojúhelníky zakreslením $n-3$ neprotínajících se úhlopříček. Ukažte, že takových triangulací existuje právě b_{n-2}.

6. V tomto a několika dalších cvičeních budeme používat pojmy *kořenový strom* a *pěstovaný strom* z části 4.2 (oba jsou stromy s kořenem, u pěstovaných stromů záleží na pořadí synů každého vrcholu, u kořenových stromů nikoli).

   (a) Označme c_n počet (navzájem neisomorfních) pěstovaných stromů s n vrcholy, kde každý vrchol je buď koncový, nebo má právě 2 syny (příklady dvou takových neisomorfních stromů jsou první a třetí strom na

obr. 10.1). Ukažte, že příslušná vytvořující funkce $c(x)$ splňuje rovnici $c(x) = x + xc(x)^2$, a vypočítejte výraz pro c_n.

(b)* Uměli byste odvodit hodnotu c_n ze znalosti b_n (počtu binárních stromů vyšetřovaných textu této části)?

(c) Najděte d_n, počet neisomorfních pěstovaných vrcholů s n vrcholy, kde každý nekoncový vrchol má jednoho nebo dva syny.

7. Nechť t_n značí počet neisomorfních pěstovaných stromů s n vrcholy.

(a) Ukažte, že příslušná vytvořující funkce $t(x)$ splňuje rovnici

$$t(x) = \frac{x}{1 - t(x)},$$

a vypočítejte výraz pro t_n.

(b)* Uměli byste odvodit hodnotu t_n ze znalosti b_n (počtu binárních stromů vyšetřovaných textu této části)?

8. Řekneme, že pěstovaný strom je *starý*, nemá-li žádný *mladý vrchol*, přičemž mladý vrchol je koncový vrchol přímo připojený ke kořeni. Nechť s_n je počet starých pěstovaných stromů s n vrcholy. Vyjádřete vytvořující funkci $s(x)$ pomocí vytvořující funkce $t(x)$ pro pěstované stromy z předchozího cvičení.

9.* Teď uvažme kořenové stromy, kde každý nekoncový vrchol má právě 2 syny (u kořenového stromu nezáleží na pořadí synů vrcholu, t.j. první a třetí strom na obr. 10.1 budou nyní isomorfní). Nechť $\bar{b}(x)$ je příslušná vytvořující funkce. Odvoďte rovnici

$$\bar{b}(x) = 1 + \frac{x}{2}\left(\bar{b}(x)^2 + \bar{b}(x^2)\right).$$

10. Uvažme *alkanové radikály*, což jsou acyklické uhlovodíky, kde každý atom uhlíku má 4 jednoduché vazby, až na jeden, který má 3 jednoduché vazby a jednu „volnou“ vazbu. Takové molekuly si můžeme představovat jako kořenové stromy (vrcholy odpovídají atomům uhlíku), kde každý nekoncový vrchol má 1,2 nebo 3 syny (přičemž pořadí synů jednoho vrcholu není důležité). Buď r_n počet takových stromů s n vrcholy (neboli alkanových radikálů s n uhlíky), a $r(x)$ příslušná vytvořující funkce.

(a)** Odvoďte rovnici $r(x) = 1 + \frac{x}{6}\left(r(x)^3 + 3r(x^2)r(x) + 2r(x^3)\right)$.

(b) Vypočítejte pomocí této rovnice tabulky r_n pro malá n. Srovnejte s hodnotami uvedenými v nějaké encyklopedii chemie.

Více o metodách počítání různých typů grafů, stromů atd. se najde např. v knize [9].

10.5 O házení kostkou

10.5.1 Úloha. *Budeme-li házet kostkou tak dlouho, až poprvé padne šestka, kolik hodů v průměru potřebujeme*[6]*?*

Pravděpodobnost, že v prvním hodu padne šestka, je $p = \frac{1}{6}$. Pravděpodobnost, že v prvním hodu šestka nepadne a v druhém padne, je $(1-p)p$, a obecně pravděpodobnost toho, že šestka padne poprvé v i-tém hodu je rovna číslu $q_i = (1-p)^{i-1}p$. Průměrný počet hodů (neboli střední hodnota počtu hodů) bude pak

$$S = \sum_{i=0}^{\infty} iq_i = \sum_{i=1}^{\infty} i(1-p)^{i-1}p\,.$$

Zavedeme vytvořující funkci $q(x) = q_1x + q_2x^2 + \cdots$. Derivujeme-li tuto řadu člen po členu, dostáváme $q'(x) = 1 \times q_1 + 2 \times q_2x + 3 \times q_3x^2 + \cdots$, a hledaný průměrný počet hodů pak bude roven hodnotě $q'(1)$.

Po jistém úsilí spočítáme, že naše vytvořující funkce má vyjádření

$$q(x) = \frac{p}{1-p} \cdot \frac{1}{1-(1-p)x} - \frac{p}{1-p}.$$

Po malém cvičení v derivování vyjde $q'(x) = p/(1-(1-p)x)^2$, neboli $S = q'(1) = \frac{1}{p}$. V našem případě pro $p = \frac{1}{6}$ tedy průměrný počet hodů je 6.

Zde je způsob usuzování, který dává ještě mnohem kratší řešení: V každém případě hodíme kostkou aspoň jednou. S pravděpodobností $1-p$ nehodíme napoprvé šestku, a v tomto případě nás čeká v průměru ještě S dalších hodů (kostka nemá paměť). Odtud

$$S = 1 + (1-p)S,$$

a $S = \frac{1}{p}$ vyjde okamžitě.

[6] Po úvaze jsme dali přednost této formulaci před jinou, která se nabízí, totiž s tzv. ruskou ruletou.

Cvičení

1. Podobným postupem jako v textu této části najděte

   (a) průměrný počet líců, které padnou při n hodech mincí (se stejnou pravděpodobností rubu i líce),

   (b) průměrný počet šestek, které padnou při n hodech kostkou,

   (c)* průměrnou hodnotu výrazu $(i-6)^2$, kde i je počet hodů do první šestky (to je jakási míra „typické odchylky" od průměrného počtu hodů, t.j. od 6).

10.6 Náhodná procházka

Představme si číselnou osu nakreslenou v rovině, na níž jsou celá čísla vyznačena kroužky. Po těchto kroužcích se bude pohybovat figurka podle následujících pravidel náhodné procházky:

- Na začátku (před prvním tahem) stojí figurka v čísle 1.
- V každém tahu se pohne z čísla, kde právě stojí, buď o 2 čísla doprava nebo o 1 číslo doleva. Jedna z těchto možností se vždy zvolí náhodně, a obě možnosti mají stejnou pravděpodobnost (t.j. jako bychom hodili mincí a rozhodli se podle výsledku hlava/orel).

10.6.1 Úloha. *Jaká je pravděpodobnost, že figurka vůbec někdy dospěje do čísla 0?*

Nejdříve je potřeba vyjasnit, co se vůbec takovou pravděpodobností míní. Je celkem zřejmé, jak definovat pravděpodobnost, že se figurka aspoň jednou octne v 0 během prvních řekněme 7 tahů (označme ji P_7): Prvních 7 tahů náhodné procházky má 2^7 různých možných průběhů, protože v každém tahu se rozhodne mezi dvěma možnostmi, a tato rozhodnutí lze libovolně zkombinovat. Podle pravidla náhodné procházky v naší úloze jsou všechny tyto průběhy stejně pravděpodobné. Výše zmíněná pravděpodobnost P_7 bude potom rovna počtu takových průběhů, které projdou 0 (čtenář si může ověřit, že je jich 75), dělenému celkovým počtem průběhů, t.j. 2^7.

Hledanou pravděpodobnost P v naší úloze potom můžeme definovat jako limitu $P = \lim_{i\to\infty} P_i$, kde definice P_i byla objasněna výše pro $i = 7$ (tato limita určitě existuje, protože zřejmě $P_1 \leq P_2 \leq \ldots$).

Nechť a_i značí počet průběhů prvních i tahů náhodné procházky takových, že figurka dorazí do 0 po i-tém tahu, a zároveň nikdy předtím (t.j. před 1., 2.,..., i-tým tahem) v 0 nebyla. Platí tedy

$$P = \sum_{i=1}^{\infty} \frac{a_i}{2^i}.$$

Zavedeme-li vytvořující funkci $a(x) = a_1x + a_2x^2 + a_3x^3 + \cdots$, máme $P = a(\frac{1}{2})$.

Pro řešení úlohy bude užitečné podívat se i na procházky, které začínají v jiných číslech než 1 (ale pokračují podle stejného pravidla). Jaký bude například počet procházek začínajících v čísle 2, které dospějí poprvé do 0 v i-tém tahu (označme jej třeba b_i)? Aby taková procházka došla do 0, musí nejprve po nějakém j-tém tahu, $1 \leq j < i$, poprvé dosáhnout čísla 1, a potom v dalších $i - j$ tazích poprvé vstoupit do 0. Pro dosažení čísla 1 poprvé v j-tém kroku je a_j možností, (jde totiž pouze o „posunutou kopii" procházky, která by začala v 1 a po j tazích došla do 0). Je-li figurka v j-tém kroku v 1, má ještě a_{i-j} možností dosažení 0 po $i - j$ dalších tazích. Celkem tedy dostaneme[7]

$$b_i = \sum_{j=1}^{i-1} a_j a_{i-j},$$

v řeči vytvořujících funkcí to znamená $b(x) = a(x)^2$.

Analogicky, c_i bude počet procházek začínajících v čísle 3, jež poprvé dorazí do 0 po i tazích. Podobně jako v předchozím nahlédneme že $c(x) = a(x)b(x) = a(x)^3$.

Zkoumejme teď procházky začínající v 1 z trochu jiného pohledu. Při prvním tahu můžeme rovnou dojít do 0 (což dává $a_1 = 1$), nebo se octneme v čísle 3, a potom máme c_{i-1} možností, jak poprvé vstoupit

[7] Všimněte si, že jsme podstatně využili toho, že doleva se chodí vždy jen o 1, takže se nelze dostat z 2 do 0 a přitom přeskočit 1.

do 0 po dalších $i-1$ tazích. Pro $i > 1$ tedy $a_i = c_{i-1}$. Převedeno na vztah mezi vytvořujícími funkcemi

$$a(x) = x + xc(x) = x + xa(x)^3. \tag{10.8}$$

Speciálně pro $x = \frac{1}{2}$ odtud dostaneme pro $P = a(\frac{1}{2})$ rovnici

$$P = \frac{1}{2} + \frac{1}{2}P^3.$$

Ta má tři řešení, $1, (\sqrt{5}-1)/2$ a $-(\sqrt{5}+1)/2$. Záporné řešní můžeme vyloučit ihned, a ani 1 nemůže být odpovědí v naší úloze (řada pro $a(x)$ má nezáporné koeficienty a konverguje pro $x = \frac{1}{2}$, tedy definuje spojitou rostoucí funkci na intervalu $[0, \frac{1}{2}]$, a proto hodnota $a(\frac{1}{2})$ je nejmenší kladný kořen naší rovnice — rozmyslete si a případně nakreslete obrázek). Zbývá tedy $P = (\sqrt{5}-1)/2 = 0,618033988\ldots$ a jedině toto číslo může být hledaná hodnota P (zase zlatý řez!).

Z rovnice (10.8) bychom v principu mohli spočítat i funkci $a(x)$ a potom se snažit vyjádřit čísla a_i třeba pomocí jejího Taylorova rozvoje (což je ale dost pracné). Půvab výše uvedeného řešení je v tom, že jsme nic takového dělat nepotřebovali.

Cvičení

1. Uvažme náhodnou procházku začínající v 0, při níž se postupuje o 1 číslo doleva nebo o 1 číslo doprava, každá volba má pravděpodobnost $\frac{1}{2}$.

   (a)* Dokažte, že s pravděpodobností 1 se někdy vrátíme do 0.

   (b) Dokažte, že každé číslo k někdy navštívíme, s pravděpodobností 1.

11

Aplikace lineární algebry

Několik pěkných použití lineární algebry v problémech diskrétní matematiky jsme ukázali už v předchozích kapitolách (obzvlášť v části 7.5). Zde předvedeme nejdříve dvě použití jednoduchých vlastností hodnosti matice pro úlohy, v nichž by lineární algebru na první pohled asi hledal málokdo: otázka existence blokových schémat a problém o pokrytí úplnými bipartitními grafy. O podobných důkazech se zájemce dočte mnohem více například ve svěží (ale bohužel dosud nedokončené) učebnici [2]. V dalších oddílech této kapitoly pak přiřadíme každému grafu několik vektorových prostorů, což vede k přehlednému popisu zdánlivě velmi složitých množin.

11.1 Bloková schémata

Nechť V je konečná množina a nechť $\mathcal{B}$ je systém podmnožin[1] množiny V. Abychom zdůraznili, že množinový systém $\mathcal{B}$ je na množině V, budeme jej zapisovat jako uspořádanou dvojici $(V, \mathcal{B})$. Na takovou dvojici se můžeme také dívat jako na zobecnění grafu (proto jiný termín pro takovou dvojici je *hypergraf*). Speciálně, mají-li všechny množiny $B \in \mathcal{B}$ stejnou velikost k, potom $(V, \mathcal{B})$ můžeme rovněž nazývat k-graf (2-graf tedy splývá s pojmem grafu).

S důležitým příkladem k-grafu jsme se setkali v kapitole 8 o konečných projektivních rovinách. Ukázali jsme tam, že jestliže V označuje

[1] Volbu písmen V, $\mathcal{B}$ jsme podřídili dalším souvislostem této kapitoly.

množinu vrcholů projektivní roviny a $\mathcal{B}$ označuje množinu jejích přímek, potom množinový systém $(V, \mathcal{B})$ je $(k+1)$-graf pro vhodné k (a navíc $|V| = |\mathcal{B}| = k^2 + k + 1$). Tento příklad poslouží i ke snažšímu pochopení následující, na první pohled technické, definice. Nenechte se odradit.

11.1.1 Definice. *Nechť v, k, t, λ jsou celá čísla. Předpokládáme $v > k > t \geq 1$, $\lambda \geq 1$.* Blokové schéma *typu t-(v, k, λ) je množinový systém $(V, \mathcal{B})$ splňující následující podmínky:*

(1) *V má v prvků.*

(2) *Každá množina $B \in \mathcal{B}$ má k prvků. Prvky $\mathcal{B}$ se nazývají* bloky.

(3) *Každá t prvková podmnožina V je obsažena právě v λ blocích $B \in \mathcal{B}$.*

Definici pochopíme uvážením několika případů.

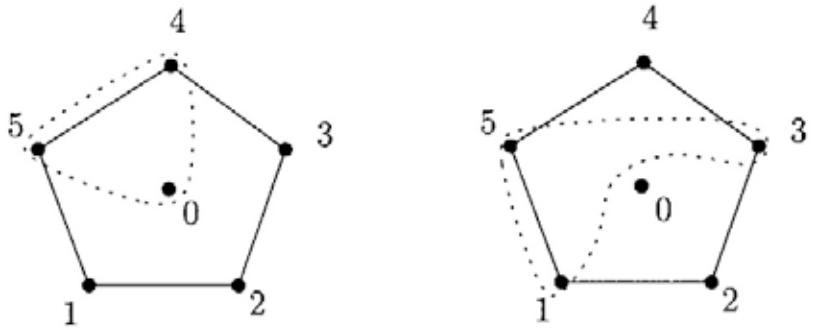
11.1.2 Příklad. *Nechť $\mathcal{B} = \binom{V}{k}$; $(V, \mathcal{B})$ se nazývá* triviální blokové schéma. *Snadno se přesvědčíme, že $(V, \mathcal{B})$ je t-(v, k, λ) blokové schéma pro $v = |V|$ a $\lambda = \binom{v-t}{k-t}$. (Zvolte libovolnou t-prvkovou podmnožinu T množiny V a přesvědčte se, že náleží právě $\binom{v-t}{k-t}$ blokům $B \in \mathcal{B}$.)*

11.1.3 Příklad. *Nechť $\mathcal{B} = \{B_1, \ldots, B_b\}$ označuje třídy rozkladu množiny V na stejně velké části. Položme $|B_i| = k$. Potom $(V, \mathcal{B})$ je blokové schéma typu 1-$(|V|, k, 1)$.*

11.1.4 Příklad. *Nechť V označuje body projektivní roviny řádu n, a pro tuto chvíli označme $\mathcal{B}$ množinu jejích přímek. Takové $(V, \mathcal{B})$ je blokové schéma typu 2-$(n^2+n+1, n+1, 1)$. Tuto netriviální skutečnost jsme ukázali v části 8.1.*

11.1.5 Příklad. *Nechť $V = \{0, 1, 2, 3, 4, 5\}$ a $\mathcal{B}$ tvoří následující trojice:* $\{0,1,2\}$, $\{0,2,3\}$, $\{0,3,4\}$, $\{0,4,5\}$, $\{0,1,5\}$, $\{1,2,4\}$, $\{2,3,5\}$, $\{1,3,4\}$, $\{2,4,5\}$, $\{1,3,5\}$.

Snadno se přesvědčíte, že $(V, \mathcal{B})$ je 2-$(6, 3, 2)$ blokové schéma. Toto schéma můžeme definovat také tak, že uvážíme kružnici s vrcholy 1, 2, 3, 4, 5 a jeden další vrchol 0. Systém $\mathcal{B}$ pak sestává ze všech trojic obsahujících právě jedinou hranu kružnice, viz obrázek:



Tyto příklady mají ve čtenáři vyvolat (správnou) představu, že bloková schémata představují jistý druh pravidelnosti, že představují příklad *pravidelných konfigurací*. Zpravidla není jednoduché blokové schéma sestrojit a základní otázkou v této celé oblasti je otázka existenční.

Základní problém. *Pro dané hodnoty v, k, λ, t rozhodněte, zda existuje blokové schéma typu t-(v, k, λ).*

Zde odvodíme některé nutné podmínky pomocí algebraických prostředků (teorie matic).

Na závěr tohoto úvodu zmiňme, že bloková schémata vznikla a dosud se používají v matematické statistice při návrhu experimentů. Tato motivace ovlivnila i standardní značení, které jsme výše zavedli.

Představme si, že chceme vyhodnotit účinnost několika způsobů ošetření určité rostliny. Porovnávaných způsobů ošetření je v (v od „variety"). Budeme je porovnávat sérií pokusů, a v každém z nich budeme vyhodnocovat k ošetření (to je dáno nějakými technickými podmínkami pokusů). Každý pokus bude tvořit *blok* příslušných ošetření. Mohli bychom samozřejmě vyšetřit všechny k-tice — všechny bloky — možných ošetření. V situaci polních pokusů je tento triviální způsob (odtud triviální blokové schéma) holou nemožností již pro malé hodnoty v a k. Proto začali statistikové používat návrhy experimentů, kde se nevyšetřují všechny k-tice, ale jen některé vybrané bloky. Tím samozřejmě může docházet k chybám, neboť návrh pokusu je neúplný, některé bloky nebyly uvažovány (a tedy

některá možná vzájemná působení ošetření byla zanedbána). Abychom alespoň částečně kompenzovali tuto (vynucenou) neúplnost návrhu experimentu, požadujeme, aby se každá dvojice ošetření vyskytovala ve stejném počtu pokusů-bloků. Schéma takového návrhu experimentu, tedy „blokové schéma", bude právě blokové schéma s parametry 2-(v, k, λ). Budeme-li požadovat, aby se každá trojice ošetření objevila ve stejném počtu λ pokusů, dostaneme blokové schéma typu 3-(v, k, λ), atd.

Pro rozlišení aplikace se bloková schémata vyskytují pod různými jmény: *Balanced Incomplete Block Design* (čili BIBD) pro schémata typu 2-(v, k, λ), *Steinerovy systémy* (pro $\lambda = 1$), *taktické konfigurace* (pro $t > 2$) atd.

Podmínky celočíselnosti. Je zřejmé, že blokové schéma typu t-(v, k, λ) nebude obecně existovat na každé množině, tedy pro každé v. Například 1-$(v, k, 1)$ schéma je rozklad, a tedy v musí být dělitelné k. Jiný, méně triviální příklad představovaly projektivní roviny, kde jsme určili velikost v jako funkci velikosti přímky. Následující věta popisuje nejdůležitější třídu nutných podmínek pro existenci blokového schématu typu t-(v, k, λ).

11.1.6 Věta (Podmínky celočíselnosti). *Nechť existuje blokové schéma s parametry t-(v, k, λ). Potom následující zlomky jsou celá čísla:*

$$\lambda\frac{v(v-1)\cdots(v-t+1)}{k(k-1)\cdots(k-t+1)},\ \lambda\frac{(v-1)\cdots(v-t+1)}{(k-1)\cdots(k-t+1)},\ \ldots,\ \lambda\frac{v-t+1}{k-t+1}.$$

Důkaz je snadnou aplikací počítání dvěma způsoby. Nechť $(V, \mathcal{B})$ je blokové schéma typu t-(v, k, λ). Zvolme pevné číslo s, kde $0 \le s \le t$, a s-prvkovou podmnožinu $S \subseteq V$. Počítejme dvěma způsoby počet dvojic (T, B), kde $S \subseteq T \in \binom{V}{t}$ a $T \subseteq B \in \mathcal{B}$.

Na jedné straně T lze zvolit $\binom{v-s}{t-s}$ způsoby, přičemž každé T je podmnožinou právě λ bloků B. Na druhé straně každý blok obsahující S obsahuje $\binom{k-s}{t-s}$ podmnožin $T \supseteq S$. Celkem tedy zlomek

$$\lambda\frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}} = \lambda\frac{(v-s)\cdots(v-t+1)}{(k-s)\cdots(k-t+1)}$$

vyjadřuje počet bloků B obsahujících množinu S, a tedy je to celé číslo. □

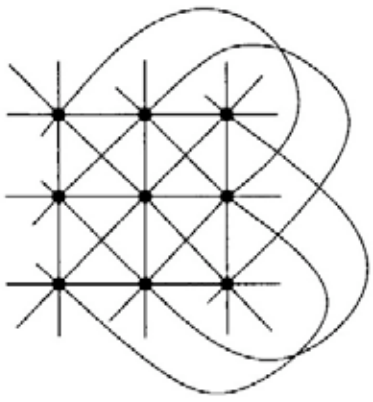
Poznámka. Použijeme-li uvedený důkaz pro $s = 0$ a $s = 1$, vidíme, že $\lambda\frac{v(v-1)\cdots(v-t+1)}{k(k-1)\cdots(k-t+1)}$ určuje počet bloků a $\lambda\frac{(v-1)\cdots(v-t+1)}{(k-1)\cdots(k-t+1)}$ určuje počet bloků obsahujících daný prvek $x \in V$ (tedy „stupeň vrcholu x“). Ve statistické interpretaci, kterou jsme uvedli výše, toto číslo vyjadřuje, kolikrát se prvek x vyskytuje v různých pokusech (čili kolikrát byl x ošetřen). Proto se číslo $\lambda\frac{(v-1)\cdots(v-t+1)}{(k-1)\cdots(k-t+1)}$ zpravidla značí r („repetice“).

11.1.7 Příklad (Steinerovy systémy trojic). *V jistém smyslu „první“ netriviální případ blokového schématu typu t-(v, k, λ) dostaneme pro $t = 2$, $\lambda = 1$, $k = 3$. To je systém trojic kde každá dvojice bodů je obsažena v právě jedné trojici (jinými slovy, pokrytí množiny hran úplného grafu disjunktními trojúhelníky).*

V tomto případě podmínky celočíselnosti z věty 11.1.6 vyžadují, aby čísla

$$\frac{v(v-1)}{6} \quad \text{a} \quad \frac{v-1}{2}$$

byla celá, z čehož je snadné odvodit, že buď $v \equiv 1 \pmod 6$ nebo $v \equiv 3 \pmod 6$. Tedy v musí být prvkem posloupnosti 3, 7, 9, 13, 15, 19, 21, 25, 27, ... Pro všechny tyto hodnoty blokové schéma typu 2-$(v, 3, 1)$ existuje. Tato schémata se nazývají *Steinerovy systémy trojic* (viz cvičení 3). Pro $v = 7$ tvoří Steinerův systém projektivní rovinu řádu 2 (viz obr. 8.1(a)). Pro $v = 9$ máme takovýto Steinerův systém:



(což lze považovat za tzv. afinní rovinu — ta vznikne z projektivní roviny řádu 3 vypuštěním bodů ležících na jedné přímce).

11.1.8 Příklad (Bloková schémata). *Pro $t = 2$ (t.j., požadujeme-li, aby každá dvojice byla právě v λ k-ticích z $\mathcal{B}$) vypadají podmínky celočíselnosti takto:*

$$\begin{aligned} \lambda v(v-1) &\equiv 0 \pmod{k(k-1)} \\ \lambda(v-1) &\equiv 0 \pmod{k-1}. \end{aligned} \tag{11.1}$$

Tyto podmínky již v obecnosti nejsou postačující. Platí ale základní (teoretický) výsledek, který uvádíme pro ilustraci:

11.1.9 Věta (Wilsonova věta). *Pro každou volbu čísel k, λ existuje takové číslo $v_0(k,\lambda)$, že pro všechny hodnoty $v \geq v_0(k,\lambda)$ splňující podmínky celočíselnosti (11.1) již existuje blokové schéma typu 2-(v,k,λ).*

Jinak řečeno, pro $t = 2$ jsou podmínky celočíselnosti postačující pro dostatečně velké množiny. Věta nic nesděluje o malých hodnotách v, jako například o existenci blokových schémat typu 2-$(k^2+k+1, k+1, 1)$ (neboli projektivních rovin).

Cvičení

1. (a) Ověřte, že projektivní rovina řádu p je blokové schéma typu 2-$(p^2+p+1, p+1, 1)$.
   (b)* Ukažte, že naopak blokové schéma typu 2-$(p^2+p+1, p+1, 1)$ je projektivní rovina řádu p.
2. Sestrojte Steinerův systém trojic s 15 prvky.
3.* Položme $n = 3m$, m je liché číslo. Definujme množinový systém $(X, \mathcal{M})$ následovně: $X = \{(x,i);\ i = 1,2,3, x = 0,1,\ldots,m-1\}$, a $\mathcal{M}$ obsahuje všechny trojice tvaru $\{(x,1),(x,2),(x,3)\}$, a pro každé $i = 1,2,3$ všechny trojice tvaru $\{(x,i),(y,i),(z,i+1)\}$, kde $x \neq y$ a $x + y \equiv 2z \pmod{m}$. Ukažte, že $(X, \mathcal{M})$ je Steinerův systém trojic.

11.2 Fisherova nerovnost

Jedním ze zakladatelů teorie blokových schémat byl anglický statistik R. A. Fisher. Ačkoliv dílčí příklady blokových schémat byly známy dlouhou dobu (např. Steinerovy systémy trojic již téměř 100 let), Fisher byl

první, kdo rozpoznal obecnou definici a její význam ve statistickém kontextu. Také našel další důležité omezující podmínky pro existenci blokových schémat.

11.2.1 Věta (Fisherova nerovnost). *Nechť $(V, \mathcal{B})$ je blokové schéma typu 2-(v, k, λ), kde $v > k$. Potom $|\mathcal{B}| \geq |V|$. (Tedy návrh experimentu pro v odrůd vyžaduje alespoň v pokusů.)*

Tato nerovnost se dá dokázat zajímavým využitím elementární lineární algebry, jak objevil indický matematik R. C. Bose. Než začneme s vlastním důkazem, zaveďme matici incidence množinového systému $(V, \mathcal{B})$. Označme prvky množiny V jako $x_1, \ldots, x_v$, a množiny z $\mathcal{B}$ jako $B_1, \ldots, B_b$. Definujme $b \times v$ matici $A = (a_{ij})$ předpisem

$$a_{ij} = \begin{cases} 1 & \text{jestliže } x_j \in B_i \\ 0 & \text{jinak.} \end{cases}$$

Matici A nazýváme *matice incidence* systému $(V, \mathcal{B})$. Řádky matice incidence jsou tedy charakteristické vektory množin $B_1, \ldots, B_b$.

Důkaz Fisherovy nerovnosti. Pro dané blokové schéma $(V, \mathcal{B})$ uvažme matici incidence $A = (a_{ij})$. Matice k ní transponovaná, A^T, má rozměr $v \times b$, a tedy součin $A^T A$ má rozměr $v \times v$. Ukážeme, že matice $B = A^T A$ má velmi jednoduchý tvar. Uvažme její člen b_{ij}; podle definice násobení matic máme

$$b_{ij} = \sum_{k=1}^{b} a_{ki} a_{kj}$$

(člen v i-tém řádku a k-tém sloupci matice A^T je a_{ki}). Člen b_{ij} tudíž vyjadřuje počet bloků B_k obsahujících zároveň x_i a x_j. Proto b_{ij} nabývá pouze dvou možných hodnot:

$$b_{ij} = \begin{cases} \lambda & \text{pro } i \neq j \\ \lambda \frac{v-1}{k-1} & \text{pro } i = j. \end{cases}$$

Číslo $\lambda \cdot \frac{v-1}{k-1}$ jsme výše označili r (počet opakování), a tedy matice B má tvar

$$\begin{pmatrix} r & \lambda & \dots & \lambda \\ \lambda & r & \dots & \lambda \\ & & \ddots & \\ \lambda & \lambda & \dots & r \end{pmatrix}.$$

Elementárními úpravami dostaneme

$$\begin{aligned} \det B &= \det \begin{pmatrix} r+(v-1)\lambda & r+(v-1)\lambda & \dots & r+(v-1)\lambda \\ \lambda & r & \dots & \lambda \\ \vdots & \vdots & \vdots & \\ \lambda & \lambda & \dots & r \end{pmatrix} \\ &= \Big(r+(v-1)\lambda\Big) \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ \lambda & r & & \lambda \\ \vdots & \vdots & & \\ \lambda & \lambda & & r \end{pmatrix} \\ &= \Big(r+(v-1)\lambda\Big) \cdot \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & r-\lambda & \dots & 0 \\ \vdots & \vdots & & \\ 0 & 0 & & r-\lambda \end{pmatrix} \\ &= (r+(v-1)\lambda) \cdot (r-\lambda)^{v-1}. \end{aligned}$$

Připomeňme nyní, že $r = \lambda \cdot \frac{v-1}{k-1}$, a tedy $r+(v-1)\lambda = rk$. Protože $v > k$, máme i $r > \lambda$, a tak $\det B \neq 0$, čili matice B má hodnost[2] v. Kdyby ale $b < v$, potom hodnost matic A i A^T by byla ostře menší než v, a potom i $B = A^T A$ by měla hodnost $< v$ (zde používáme jednoduché vlastnosti hodnosti matice, viz cvičení 2). Tedy $b \geq v$. □

Jiný důkaz toho, že matice B má hodnost v, je naznačen ve cvičení 4.

[2] Připomeňme: *hodnost* nějaké matice M, označovaná zpravidla symbolem $r(M)$, je dimenze vektorového prostoru generovaného řádky této matice, nebo jinak řečeno je to maximální počet lineárně nezávislých řádků M (a totéž pro sloupce). Viz dodatek o algebře.

Toto použití hodnosti matice incidence se stalo základem mnoha podobných (a důležitých) důkazů.

Cvičení

1. Pro $\lambda = 1$ dokažte Fisherovu nerovnost přímo (bez použití lineární algebry).

2. Ukažte, že je-li A matice typu $n \times k$ a B matice typu $k \times m$, potom $r(AB) \leq \max(r(A), r(B))$.

3. Nechť F je nějaké těleso, a $G \subseteq F$ jeho podtěleso (představujte si např. pod F reálná čísla a pod G racionální čísla). Buď A matice s prvky z tělesa G. Hodnost matice A můžeme uvažovat nad tělesem G (lineární závislost s koeficienty v G) nebo nad tělesem F (lineární závislost s koeficienty v F). Zdůvodněte, proč v obou případech dostaneme tutéž hodnost.

4. Čtvercová $n \times n$ reálná matice B se nazývá *pozitivně definitní*, pokud platí $x^T B x > 0$ pro každý nenulový (sloupcový) vektor $x \in \mathbf{R}^n$.

   (a) Proč má pozitivně definitní $n \times n$ matice plnou hodnost n?

   (b) Ukažte, že matice B, použitá v důkazu v textu, je pozitivně definitní (a tedy B má hodnost v, bez počítání determinantu).

5. (a) Nechť $C_1, C_2, \ldots, C_m$ jsou podmnožiny nějaké n-prvkové množiny X. Předpokládejme, že každá C_i má lichou velikost, a že velikost každého průniku $C_i \cap C_j$ (pro $i \neq j$) je sudá. Dokažte, že potom $m \leq n$. Podobně jako v textu, uvažte matici $A^T A$, kde A je matice incidence uvažovaného množinového systému, ale pracujte nad dvouprvkovým tělesem $GF(2)$.

   (b) Uvažme podobný problém jako v (a), ale tentokrát požadujeme, aby velikosti množin samotných byly *sudé*, zatímco velikosti průniků $|C_i \cap C_j|$ jsou všechny *liché*. Dokažte, že zase $m \leq n$.

   (c) A tentokrát požadujeme, aby všechny množiny C_i byly navzájem různé, a jejich velikosti i velikosti všech průniků byly *sudé*. Ukažte, že lze zkonstruovat $2^{\lfloor n/2 \rfloor}$ takových množin.

6. (Zobecněná Fisherova nerovnost) Buď X nějaká n-prvková množina, a q celé číslo, $1 \leq q < n$. Nechť $C_1, C_2, \ldots, C_m$ jsou podmnožiny X, a předpokládejme, že všechny průniky $C_i \cap C_j$ (pro $i \neq j$) mají velikost přesně q.

(a)* Použitím metody z cvičení 4 dokažte, že platí $m \leq n$. (Zvlášť ošetřete případ, kdy $|C_i| = q$ pro některé i.)

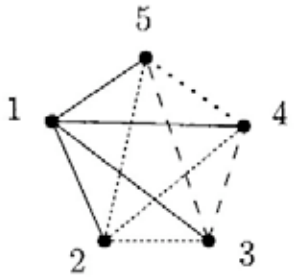
(b) Proč se tvrzení v (a) asi nazývá „zobecněná Fisherova nerovnost"? Odvoďte z něj Fisherovu nerovnost!

11.3 Pokrývání úplnými bipartitními grafy

R. Graham and H. O. Pollak, dva matematici v laboratořích firmy Bell, studovali následující otázku, motivovanou problémem z oblasti telekomunikací:

11.3.1 Úloha. *Množina hran úplného grafu K_n se má vyjádřit jako disjunktní sjednocení množin hran m úplných bipartitních grafů. Pro jakou minimální hodnotu $m = m(n)$ je to možné?*

Jedno možné vyjádření $E(K_n)$ pomocí $n-1$ úplných bipartitních grafů se snadno vyrobí z grafů typu K_{1,n_i} („hvězd"). Předpokládejme, že jsme již vyjádřili $E(K_{n-1})$ pomocí $n-2$ takových grafů. V grafu K_n uvážíme jeden vrchol, a hranami grafu $K_{1,n-1}$ pokryjeme všechny hrany z něj vycházející; pak zbývá pokrýt hrany K_{n-1}, což už umíme. Takhle vypadá vzniklé pokrytí pro $n = 5$:



Graham s Pollakem přišli na jednoduchý způsob, jak ukázat, že lepší pokrytí neexistuje:

11.3.2 Věta (Grahamova-Pollakova věta). *Platí $m(n) \geq n-1$.*

Důkaz. Předpokládejme, že úplné bipartitní grafy $B_1, \ldots, B_m$ disjunktně pokrývají všechny hrany K_n, t.j. $V(B_k) \subseteq V(K_n) =$

$\{1, 2, \ldots, n\}$, $E(K_n) = E(B_1) \dot\cup E(B_2) \dot\cup \ldots \dot\cup E(B_m)$. Nechť (X_k, Y_k) je rozklad množiny vrcholů B_k na dvě části takové, že hrany B_k jdou jen mezi nimi.

Každému grafu B_k přiřadíme $n \times n$ matici A_k, jejíž prvek v i-tém řádku a j-tém sloupci je

$$a_{ij}^{(k)} = \begin{cases} 1 & \text{pokud } i \in X_k \text{ a } j \in Y_k \\ 0 & \text{jinak} \end{cases}$$

(definice A_k je trochu podobná matici sousednosti grafu B_k, až na to, že A_k není symetrická — každá hrana grafu B_k přispěje jenom jednou jedničkou). Tvrdíme, že každá z matic A_k má hodnost 1. To je proto, že všechny nenulové řádky matice A_k jsou rovny témuž vektoru, totiž vektoru s jedničkami v pozicích, jejichž indexy náležejí Y_k, a s nulami všude jinde.

Uvažme teď matici $A = A_1 + A_2 + \cdots + A_m$. Každá hrana $\{i, j\}$ náleží právě jednomu z grafů B_k, a proto pro každé $i \neq j$ platí buď $a_{ij} = 1$, $a_{ji} = 0$, anebo $a_{ij} = 0$, $a_{ji} = 1$, kde a_{ij} označuje prvek matice A v pozici (i, j) (přitom a_{ii}=0). Odtud plyne $A + A^T = J_n - I_n$, kde J_n je $n \times n$ matice samých jedniček a I_n je $n \times n$ jednotková matice (s jedničkami na hlavní diagonále a nulami jinde). Chceme teď ukázat, že hodnost takové matice A je aspoň $n-1$. Budeme-li to vědět, dostaneme $n - 1 \leq r(A) \leq r(A_1) + \cdots + r(A_m) \leq m$, poněvadž pro hodnost libovolných dvou matic M_1 a M_2 platí $r(M_1 + M_1) \leq r(M_1) + r(M_2)$ — to je snadné ověřit z definice hodnosti.

Předpokládejme tedy $r(A) \leq n - 2$. Připíšeme-li k matici A ještě jeden řádek ze samých jedniček, má vzniklá $(n + 1) \times n$ matice pořád hodnost $\leq n - 1$, a tedy existuje netriviální lineární kombinace jejích sloupců rovná nule. Jinými slovy, existuje (sloupcový) vektor $x \in \mathbf{R}^n$, $x \neq (0, 0, \ldots, 0)^T$ takový, že $Ax = 0$ a zároveň $\sum_{i=1}^n x_i = 0$.

Z posledně uvedeného vztahu plyne $J_n x = 0$. Spočítáme

$$x^T \left(A + A^T\right) x = x^T (J_n - I_n) x = x^T (J_n x) - x^T (I_n x) =$$

$$0 - x^T x = -\sum_{i=1}^n x_i^2 < 0.$$

Na druhé straně ale

$$x^T \left(A^T + A\right) x = \left(x^T A^T\right) x + x^T (Ax) = 0 \times x + x \times 0 = 0,$$

a to je spor. □

Cvičení

1. (a) Ukažte, že chceme-li pokrýt hrany K_n hranami bipartitiních podgrafů K_n, a přitom netrváme na disjunktním pokrytí (t.j., jedna hrana může být pokryta i mnohokrát), potom existuje pokrytí $\lceil \log_2 n \rceil$ bipartitními grafy.

   (b)* Dokažte, že pokrytí jako v (a) skutečně vyžaduje aspoň $\lceil \log_2 n \rceil$ bipartitních grafů.

2.* Tentokrát chceme pokrýt všechny hrany grafu K_n hranami bipartitních podgrafů tak, aby každá hrana byla pokryta lichým počtem bipartitních podgrafů. Dokažte, že potřebujeme aspoň $(n-1)/2$ bipartitních podgrafů. Postupujte podobně jako v důkazu v textu, ale pracujte s maticemi nad dvouprvkovým tělesem $GF(2)$. Místo matice A_k pak uvažte „skutečnou" matici sousednosti grafu B_k, jež má hodnost 2.

11.4 Prostor kružnic grafu

Nechť $G = (V, E)$ je neorientovaný graf. Označme symbolem $\mathcal{K}_G$ množinu všech kružnic (všech možných délek) v grafu G. Je vidět, že tato množina si zasluhuje složitější označení (kroucenými písmenkami), protože je značně veliká. Přesvědčte se, že např. pro úplný graf K_n platí

$$|\mathcal{K}_{K_n}| = \sum_{k=3}^{n} \binom{n}{k} \cdot \frac{(k-1)!}{2}, \tag{11.2}$$

a pro úplný bipartitní graf $K_{n,n}$ je

$$|\mathcal{K}_{K_{n,n}}| = \sum_{k=2}^{n} \binom{n}{k}^2 \cdot \frac{k!(k-1)!}{2}. \tag{11.3}$$

Na druhé straně $\mathcal{K}_G = \emptyset$ právě když G je les.

Zdálo by se, že struktura množiny $\mathcal{K}_G$ je nepřehledná a není možné ji nějak vhodně popsat. V této části zavedeme vhodné zobecnění pojmu kružnice, které souvisí s látku vyloženou v části 3.5, a které „doplní" množinu všech kružnic na větší množinu s velmi jednoduchou strukturou — strukturou vektorového prostoru. Myšlenky vyložené v dalším původně vznikly v souvislosti se studiem elektrických obvodů.

11.4.1 Definice (Eulerovská množina hran). *Nechť $G = (V, E)$ je (neorientovaný) graf. Množina $E' \subseteq E$ se nazývá* eulerovská, *jestliže graf (V, E') má všechny stupně sudé.*

Tedy prázdná množina a množina hran libovolné kružnice jsou eulerovské množiny.

V dalším bude pro nás výhodné ztotožňovat kružnici s její množinou hran.

11.4.2 Lemma. *Množina E' je eulerovská právě když existují kružnice $E_1, \ldots, E_t$ tak, že E_i jsou navzájem disjunktní množiny a E' je jejich sjednocením.*

Důkaz. Je-li E' neprázdná eulerovská množina, potom (V, E') není les a tedy obsahuje kružnici E_1. Množina $E' \setminus E_1$ je opět eulerovská, a lze tedy postupovat indukcí. □

Popíšeme algebraickým způsobem strukturu všech eulerovských množin v daném grafu $G = (V, E)$. Hrany grafu G očíslujeme $e_1, \ldots, e_m$, a každé podmnožině $A \subseteq E$ přiřadíme charakteristický vektor $\mathbf{v}_A = (v_1, \ldots, v_m)$ definovaný předpisem

$$v_i = \begin{cases} 1 & \text{jestliže } e_i \in A \\ 0 & \text{jinak.} \end{cases}$$

Vektory budeme sčítat a násobit ve dvojkové soustavě (kde $1+1=0$). Snadno potom sami nahlédnete, že

$$\mathbf{v}_A + \mathbf{v}_B = \mathbf{v}_C,$$

kde $C = (A \setminus B) \cup (B \setminus A)$ je *symetrický rozdíl* množin A a B.

Symbolem $\mathcal{C}$ označme množinu všech charakteristických vektorů eulerovských množin v G. Kvůli snadné formulaci zobecněme trochu pojem kostry grafu: kostra libovolného grafu G je každý jeho podgraf neobsahující kružnice a maximální vzhledem k této vlastnosti (t.j. přidáním libovolné další hrany z $E(G)$ kružnice vznikne). Pro souvislý graf toto splývá s definicí z části 4.3, pro nesouvislý graf dostáváme les, sestávající z koster všech komponent.

11.4.3 Věta (O prostoru kružnic).

(1) Pro každý graf G tvoří množina $\mathcal{C}$ vektorový prostor nad dvouprvkovým tělesem[3] *$GF(2)$ dimenze $|E| - |V| + k$, kde k je počet komponent grafu G.*

(2) Zvolme libovolnou kostru (V, E') grafu G, a pro každou hranu $e \in E \setminus E'$ označme K_e jedinou kružnici obsaženou v grafu $(V, E' \cup \{e\})$. Charakteristické vektory kružnic K_e (vzhledem ke zvolené kostře G) potom tvoří bázi $\mathcal{C}$.

Kružnici K_e nazýváme *elementární kružnice* (určená hranou e, vzhledem k dané kostře).

Důkaz. Nejprve ukážeme, že $\mathcal{C}$ je vektorový prostor. K tomu musíme zkontrolovat, že sčítáním vektorů z $\mathcal{C}$ i jejich násobením prvky tělesa $GF(2)$ dostaneme zase vektory z $\mathcal{C}$. Protože $0\mathbf{v}_A = \mathbf{v}_\emptyset$, $1\mathbf{v}_A = \mathbf{v}_A$, stačí ověřit, že množina $\mathcal{C}$ je uzavřena na sčítání vektorů. Vzhledem k poznámce před touto větou stačí ukázat, že pro eulerovské množiny A a B je i jejich symetrický rozdíl eulerovská množina. Zvolme tedy libovolný vrchol $v \in V$. Nechť k_A hran vycházejících z v náleží do A, k_B do B a k do obou těchto množin (kde k_A, k_B jsou sudá čísla). Potom do symetrického rozdílu $(A \setminus B) \cup (B \setminus A)$ patří zřejmě $k_A + k_B - 2k$ hran vycházejících z vrcholu v, a tedy stupeň v v symetrickém rozdílu množin A a B je sudý. Proto tento symetrický rozdíl je také eulerovská množina.

[3] GF je zkratka Galois Field, neboli Galoisovo těleso. Viz dodatek o algebře.

Nechť (V, E') je libovolná kostra grafu G. Potom $|E'| = |V| - k$, kde k je počet komponent grafu G. Stačí tedy ukázat, že charakteristické vektory všech elementárních kružnic tvoří bázi vektorového prostoru $\mathcal{C}$.

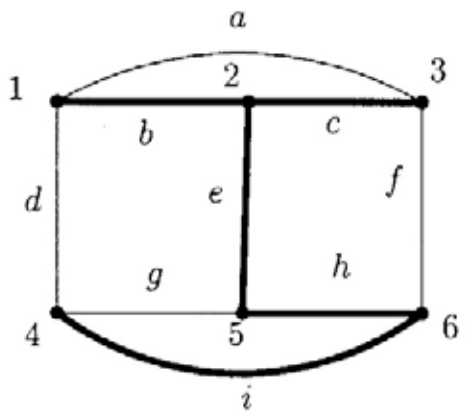
Můžeme předpokládat, že $E' = \{e_1, \ldots, e_t\}$, kde $t = |V| - k$ (případně přeznačíme hrany z E tak, aby hrany z E' byly na začátku). Ukážeme nejprve, že elementární kružnice jsou lineárně nezávislé. Uvážíme-li libovolnou hranu $e_i \notin E'$ (t.j. $i > t$), pak vektor odpovídající elementární kružnici K_{e_i} je jediný mezi vektory elementárních kružnic, jenž má 1 v pozici i. Z tohoto důvodu nemůže být žádný z vektorů elementárních kružnic lineární kombinací jiných.

Dokažme teď, že elementární kružnice generují $\mathcal{C}$. Zvolme eulerovskou množinu A a definujme množinu B předpisem

$$\mathbf{v}_B = \sum_{e \in A \setminus E'} \mathbf{v}_{K_e}.$$

Jaké prvky množina B obsahuje? Právě ty hrany, které náleží lichému počtu elementárních kružnic (vzhledem k E'). Zajisté tedy B obsahuje množinu $A \setminus E'$ (každá její hrana náleží jediné elementární kružnici). Označme C symetrický rozdíl množin A a B. To je eulerovská množina, a přitom je obsažena v E', a E' neobsahuje kružnici — proto $C = \emptyset$. Odtud $A = B$, takže jsme (libovolně zvolený) vektor $\mathbf{v}_A \in \mathcal{C}$ vyjádřili jako lineární kombinaci elementárních kružnic. □

Příklad. Uvažme následující graf $G = (V, E)$:



Dimenze prostoru kružnic je $9 - 6 + 1 = 4$. Zvolíme-li silně vytaženou kostru, potom odpovídající báze prostoru kružnic je tvořena vektory elementárních kružnic

$$\begin{aligned} K_a &= \{a, b, c\} \\ K_d &= \{b, e, h, i, d\} \\ K_g &= \{g, h, i\} \\ K_f &= \{c, f, h, e\}. \end{aligned}$$

Například pro kružnici $K = \{a, f, i, d\}$ máme vyjádření $\mathbf{v}_K = \mathbf{v}_{K_a} + \mathbf{v}_{K_d} + \mathbf{v}_{K_f}$.

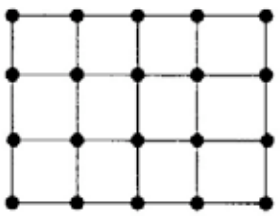
Z věty 11.4.3 snadno plyne toto:

11.4.4 Důsledek. *Počet eulerovských množin grafu $G = (V, E)$ s k komponentami je $2^{|E|-|V|+k}$.*

Přes obrovský počet eulerovských podmnožin je jejich struktura jednoduchá a lze je rovněž snadno generovat (z mnohem menší báze). To byla rovněž jedna z původních motivací. Číslo $|E| - |V| + k$ se nazývá *cyklomatické číslo* grafu $G = (V, E)$.

Cvičení

1. Ověřte vzorce (11.2) a (11.3).
2. Dokažte důsledek 11.4.4.
3. Určete cyklomatické číslo (=dimenzi prostoru kružnic) $m \times n$ mřížky, například:



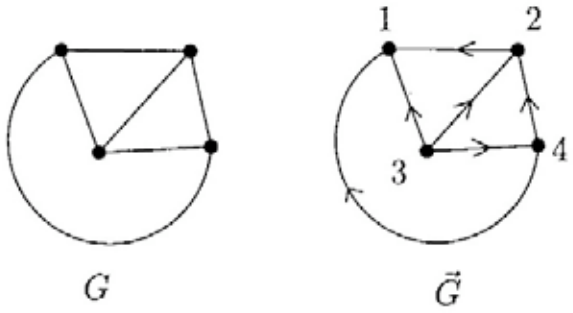
3×4

4. Dokažte, že pro každý topologický rovinný 2-souvislý graf (t.j. 2-souvislý graf s daným rovinným nakreslením) tvoří bázi prostoru C kružnice ohraničující omezené stěny.
5. Dokažte, že počet eulerovských množin v grafu G je vždy sudé číslo.

11.5 Cirkulace a řezy: prostor kružnic podruhé

V tomto článku vyložíme látku předchozího odstavce v poněkud jiném světle, za pomoci základů teorie matic. Budeme rovněž pracovat jak s grafy, tak s jejich orientacemi. Při tomto zesložitění se dostane věta 11.4.3 do nových souvislostí.

Z části 7.5 si připomeňme pojem *orientace*: Orientace grafu $G = (V, E)$ je orientovaný graf tvaru $\vec{G} = (V, \vec{E})$, kde množina $\vec{E}$ obsahuje pro každou hranu $\{x, y\} \in E$ právě jednu ze šipek (x, y) a (y, x). Následující obrázek ukazuje příklad grafu a jednu z jeho možných orientací:



(Všech možných orientací grafu G je $2^{|E|}$, mnoho jich však může být isomorfních.)

Orientaci $\vec{G} = (V, \vec{E})$ budeme pokládat za pevně zvolenou. Reálná funkce $f : \vec{E} \to \mathbf{R}$ se nazývá *cirkulace*, jestliže pro každý vrchol v grafu G platí

$$\sum_{x \in V;\, (v,x) \in \vec{E}} f(v, x) = \sum_{x \in V;\, (x,v) \in \vec{E}} f(x, v). \tag{11.4}$$

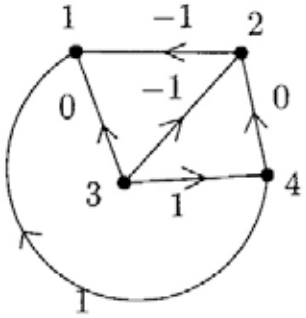
(Poznamenejme, že cirkulace může nabývat záporných hodnot.)

Pojem cirkulace má různé názorné interpretace. Například, je-li $\vec{G}$ schéma elektrického obvodu a $f(e)$ vyjadřuje proud tekoucí hranou e, potom (11.4) říká, že do každého vrcholu vtéká stejně, jako z něj vytéká — což je první Kirchhoffův zákon. Tato interpretace byla jednou z původních motivací pro teorii vyloženou v tomto článku.

Jeden příklad cirkulace se dostane následovně. Buď $K = (v_1, v_2, \ldots, v_{k+1} = v_1)$ kružnice (neorientovaná) v grafu G. Definujeme cirkulaci f (v orientaci $\vec{G}$) předpisem

$$\begin{aligned} f(v_i, v_{i+1}) &= 1 && \text{jestliže } (v_i, v_{i+1}) \in \vec{E} \\ f(v_{i+1}, v_i) &= -1 && \text{jestliže } (v_{i+1}, v_i) \in \vec{E} \\ f(x, y) &= 0 && \text{pokud } \{x, y\} \text{ není hrana kružnice } K. \end{aligned}$$

Cirkulace tedy závisí na směru, v němž jsme (neorientovanou) kružnici zapsali. O takto definované cirkulaci říkáme, že přísluší kružnici K. Pro graf na předchozím obrázku a kružnici s pořadím vrcholů 1 2 3 4 vypadá cirkulace takto:



Snadno nahlédneme, že jsou-li f_1 a f_2 cirkulace, je rovněž funkce $f_1 + f_2$ cirkulace na G. Pro reálné číslo c je také cf_1 cirkulace. (V obou případech stačí ověřit podmínku (11.4).) Odtud dostáváme, že každá eulerovská množina dává vzniknout přirozeným způsobem cirkulaci. Definujeme *nosič* dané cirkulace jako množinu

$$\big\{\{x,y\} \in E;\ \text{aspoň jedna z hodnot } f(x,y),\ f(y,x) \text{ je nenulová}\big\}.$$

S trochou nepřesnosti označíme $\mathcal{C}$ množinu všech cirkulací. Množina $\mathcal{C}$ tvoří vektorový prostor, který nazýváme prostor cirkulací a nebo rovněž *prostor kružnic* (stejný název jako v předchozím článku). Oba pojmy jsou si velmi příbuzné. Hlavní rozdíl mezi tímto a předcházejícím článkem spočívá v tom, že zde pracujeme nad tělesem reálných čísel, zatímco v předcházejícím článku nad tělesem $GF(2)$.

Nechť nyní $p : V \to \mathbf{R}$ je libovolná funkce (p od slova potenciál). Definujme funkci δp na šipkách $\vec{G}$ předpisem

$$\delta p(x,y) = p(x) - p(y) \tag{11.5}$$

pro každou šipku $(x,y) \in \vec{E}$.

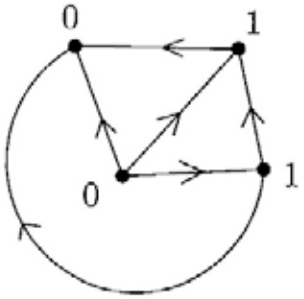
Funkce $\delta p : \vec{E} \to \mathbf{R}$ se nazývá *potenciálový rozdíl* (kdo si pamatuje trochu fyziky, vidí jistě souvislost s elektrickými obvody). Každá funkce $g : \vec{E} \to \mathbf{R}$, pro niž existuje potenciál p splňující $g = \delta p$, se také nazývá *potenciálový rozdíl.*

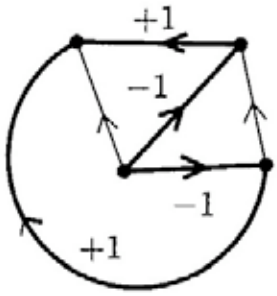
Snadno se opět přesvědčíme (ověřením podmínky (11.5)), že součet potenciálových rozdílů je opět potenciálový rozdíl, stejně tak číselný násobek. Množinu všech potenciálových rozdílů označíme $\mathcal{R}$ a nazýváme ji *prostor řezů.*

Proč jsme zvolili tento název? Uvažme následující situaci: Nechť potenciál p nabývá pouze hodnot 0 a 1. Položme $A = \{v \in V;\, p(v) = 1\}$, $B = V \setminus A$. Potom potenciálový rozdíl $g = \delta p$ nabývá nenulové hodnoty pouze pro šipky s jedním vrcholem v A a druhým v B:

$$\begin{array}{lcll} g(x,y) & = & 1 & \text{pro } x \in A,\ y \in B \\ g(x,y) & = & -1 & \text{pro } x \in B,\ y \in A \\ g(x,y) & = & 0 & \text{jinak.} \end{array}$$

Je přitom přirozené množinu všech hran mezi množinami A a B nazývat *řezem*, protože po jejím odejmutí bude mít vzniklý graf více komponent (samozřejmě pokud existuje alespoň jedna hrana mezi A a B). Na obrázku jsme znázornili potenciál p





a příslušný potenciálový rozdíl, hrany řezu jsou vyznačeny silněji.

Nyní celou situaci popíšeme pomocí matice incidence. Očíslujeme proto vrcholy $V = \{v_1, \ldots, v_n\}$ a hrany $E = \{e_1, \ldots, e_m\}$. Symbol $\vec{e}_i$ bude označovat šipku příslušející hraně e_i. Jako v části 7.5 zavedeme *matici incidence* orientace $\vec{G}$. Tato matice, D, je typu $n \times m$ a má prvky d_{ik} definované předpisem

$$d_{ik} = \begin{cases} -1 & \text{je-li } v_i \text{ začátek šipky } \vec{e}_k \\ 1 & \text{je-li } v_i \text{ konec šipky } \vec{e}_k \\ 0 & \text{jinak.} \end{cases}$$

Platí následující elegantní popis prostoru cyklů a prostoru řezů:

11.5.1 Věta. *Pro každý graf G je prostor řezů $\mathcal{R}$ generován řádky matice incidence D, prostor cirkulací $\mathcal{C}$ je ortogonální doplněk $\mathcal{R}$ (t.j. $\mathcal{C} = \{x \in \mathbf{R}^m;\, x^T y = 0\ \forall y \in \mathcal{R}\}$).*

Důkaz. Nechť $D = (d_{ij})$ je $n \times m$ matice incidence. Nejprve uvažme libovolný potenciálový rozdíl $g = \delta p$. Podle definice potenciálového rozdílu pro každou šipku $(v_r, v_s) = \vec{e}_j$ platí $g(\vec{e}_j) = p(v_r) - p(v_s) = \sum_{i=1}^{n} d_{ij} p(v_i)$ (porovnáním (11.5) s definicí matice incidence). Funkce g (chápaná jako

řádkový vektor) je tedy lineární kombinací řádků matice incidence. Obrácením postupu vidíme, že řádky matice generují prostor $\mathcal{R}$.

Přepišme nyní podmínku (11.4) pro cirkulaci f pomocí matice incidence. Ze vztahu

$$\sum_{x\in V;\,(x,v)\in\vec{E}} f(x,v) = \sum_{x\in V;\,(v,x)\in\vec{E}} f(v,x)$$

plyne

$$\sum_{(x,v)\in\vec{E}} f(x,v) - \sum_{(v,x)\in\vec{E}} f(v,x) = 0,$$

což pro $v = v_i$ můžeme jinak zapsat

$$\sum_{j=1}^{m} f(\vec{e}_j)d_{ij} = 0.$$

Funkce f, chápaná jako m-členný řádkový vektor, má tedy s i-tým řádkem matice D nulový skalární součin. Tudíž f je kolmá na každý řádek D, a proto prostor $\mathcal{C}$ tvoří ortogonální doplněk $\mathcal{R}$ (v prostoru všech m-členných reálných vektorů). □

Jakou má prostor $\mathcal{R}$ dimenzi? Podle předchozí věty stejnou jako prostor generovaný řádky matice incidence D. Nyní přijde častý a užitečný trik: protože hodnost matice je stejná jako hodnost matice transponované, uvažme lineární nezávislost sloupců matice D. Symbolem d_j označme j-tý sloupec matice D (odpovídající šipce $\vec{e}_j$).

Uvažme nějakou množinu $J \subseteq \{1, 2, \ldots, m\}$ indexů sloupců, a ptejme se, kdy je množina sloupců $\{d_j;\ j \in J\}$ lineárně závislá. Lineární závislost znamená, že existují čísla c_j, $j \in J$, z nichž alespoň jedno je nenulové, tak, že $\sum_{j\in J} c_j d_j$ je nulový sloupcový n-členný vektor. Rozepišme to po složkách: i-tá složka, odpovídající vrcholu v_i, má tvar

$$\sum_{j\in J} c_j d_{ij} = 0.$$

Definujeme-li $c_t = 0$ pro $t \notin J$, dostáváme podmínku (11.4), a tedy $c = (c_1, \ldots, c_m)$ je nenulová cirkulace. Tím pádem nosič c obsahuje kružnici.

Na druhé straně, jak již víme, pro každou kružnici K existuje nenulová cirkulace s nosičem K. Celkem dostáváme, že množina sloupců $\{d_j;\ j \in J\}$ je lineárně nezávislá právě když množina hran $\{e_j;\ j \in J\}$ grafu G neobsahuje kružnici. Tedy hodnost matice D je $m - n + k$, kde k je počet komponent grafu G. Touto úvahou jsme tedy dokázali:

11.5.2 Věta. *Pro graf G s n vrcholy, m hranami a k komponentami má prostor řezů $\mathcal{R}$ dimenzi $n-k$, a prostor cirkulací $\mathcal{C}$ dimenzi $m-n+k$.*

Toto je jakási verze věty 11.4.3 pro vektorový prostor nad tělesem reálných čísel.

Vztah mezi eulerovskými množinami (nebo cirkulacemi) a řezy má povahu duality. Uvedené úvahy lze rozšířit na další struktury (nejenom grafy). Tímto se zabývá tzv. teorie matroidů.

Cvičení

1. Podejte definici „elementární cirkulace vzhledem k dané kostře".

Dodatek: opakování algebry

V této kapitolce zopakujeme základní skutečnosti o maticích, tělesech, vektorových prostorech a několika dalších algebraických objektech, které potřebujeme na některých místech knížky. Narozdíl od ostatních kapitol, tato část není míněna jako úvod do problematiky, nýbrž jako stručné shrnutí, v němž si může čtenář osvěžit své případně již zasuté znalosti.

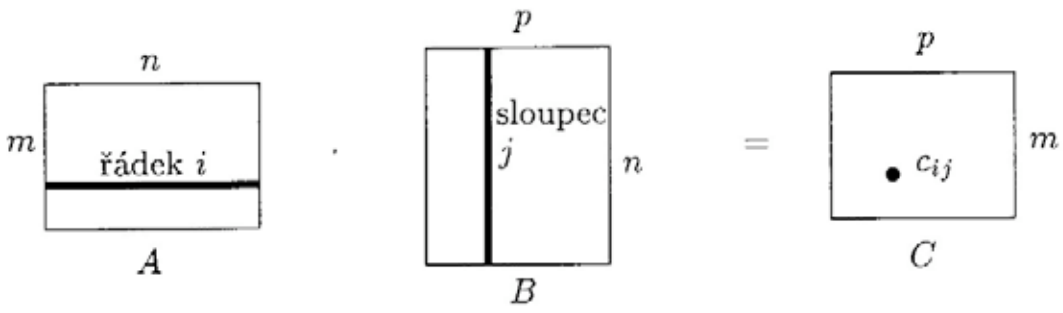
Matice. Matice je obdélníková tabulka čísel. Její položky mohou být reálná nebo komplexní čísla, případně i prvky dalších algebraických struktur. Matice typu $m \times n$ má m řádků n sloupců. Prvek v i-tém řádku a j-tém sloupci matice zvané A se obvykle označuje a_{ij}. Takže například matice A typu 3×2 má obecný tvar

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix}.$$

Matice se sčítají po složkách, a sčítané matice musejí mít týž typ. Jsou-li tedy A a B matice typu $m \times n$ a $C = A + B$, pak $c_{ij} = a_{ij} + b_{ij}$. Podobně pro násobení číslem α: matice αA má v pozici (i, j) prvek αa_{ij}. Složitější a na první pohled nečekaná je však definice *násobení matic*. Součin AB je definován jen když počet sloupců matice A souhlasí s počtem řádků matice B. Je-li A typu $m \times n$ a B typu $n \times p$, pak součin $C = AB$ je matice typu $m \times p$ daná vzorcem

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}.$$

Obrázkově:



Buď $x = (x_1, x_2, \ldots, x_n)$ vektor. V souvislosti s maticemi, takový vektor se zpravidla považuje za matici typu $n \times 1$ (představujeme si jej napsaný ve sloupečku), a je-li A matice typu $m \times n$, výraz Ax čteme jako součin dvou matic.

Zápis A^T, kde A je matice typu $m \times n$, znamená *matici transponovanou* k A, což je matice typu $n \times m$, která má v i-tém řádku a v j-tém sloupci prvek a_{ji}. Je snadné ověřit vzoreček pro transpozici součinu: $(AB)^T = B^T A^T$.

Skalární součin dvou n-složkových vektorů x a y je číslo $\sum_{i=1}^{n} x_i y_i$. Skalární součin x a y se mnohdy zapisuje $x^T y$. Přísně vzato, součin $1 \times n$ matice x^T a $n \times 1$ matice y je matice typu 1×1, jejíž jediný prvek je skalární součin definovaný výše, ale mezi maticí 1×1 a jejím prvkem se většinou nerozlišuje. Vektory x a y jsou *kolmé* pokud $x^T y = 0$.

Čtvercová matice je typu $n \times n$ pro nějaké $n \geq 1$. Její *diagonála* (někdy zvaná *hlavní diagonála*) sestává z prvků $a_{11}, a_{22}, a_{33}, \ldots, a_{nn}$. *Horní trojúhelníková matice* má nuly všude pod diagonálou; jinak řečeno $a_{ij} = 0$ pro $i > j$. *Diagonální matice* smí mít nenulové prvky jen na diagonále. *Jednotková matice* typu $n \times n$, označovaná zpravidla I_n, má jedničky na diagonále a všude jinde nuly.

Determinanty. Každé čtvercové matici A je přiřazeno číslo $\det(A)$ zvané *determinant* A. Definuje se formulí

$$\det(A) = \sum_{\pi \in S_n} \operatorname{sgn}(\pi)\, a_{1,\pi(1)} a_{2,\pi(2)} \cdots a_{n,\pi(n)},$$

kde se sčítá přes všechny permutace π množiny $\{1, 2, \ldots, n\}$, a kde $\operatorname{sgn}(\pi)$ značí *znaménko* permutace π. Znaménko permutace je vždycky

buď $+1$ nebo -1, a krátce se dá definovat jako

$$\operatorname{sgn}(\pi) = \prod_{1 \le i < j \le n} \frac{\pi(j) - \pi(i)}{j - i}.$$

Kupříkladu determinant matice A typu 2×2 je roven $a_{11}a_{22} - a_{12}a_{21}$. Determinanty větších matic se málokdy počítají podle definice. Účinnější metody vyčíslení determinantu jsou zpravidla založeny na následujících pravidlech:

1. Determinant horní trojúhelníkové matice (a speciálně diagonální matice) je roven součinu všech prvků diagonály.

2. („Elementární řádková operace I“) Vynásobíme-li všechny prvky nějakého řádku matice A nějakým číslem α, determinant se také násobí α. Speciálně, má-li A řádek ze samých nul, potom $\det(A) = 0$. Podobně pro sloupec.

3. („Elementární řádková operace II“) Determinant se nezmění, přičteme-li násobek nějakého řádku k jinému řádku. Jinými slovy, máme-li indexy $i \neq k$ a nahradíme-li prvek a_{ij} prvkem $a_{ij} + \alpha a_{kj}$ pro každé $j = 1, 2, \ldots, n$, kde α je nějaké pevné číslo, determinant zůstane stejný. Podobně pro sloupce.

4. Prohozením dvou řádků (nebo dvou sloupců) změní determinant znaménko. (To se dá odvodit z předchozích dvou pravidel.)

5. Pro libovolné čtvercové matice A, B typu $n \times n$ platí $\det(AB) = \det(A)\det(B)$.

6. („Rozvoj determinantu podle řádku“) Pro každý řádkový index i platí vztah

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} \det(A_{ij}),$$

kde A_{ij} je matice, která vznikne z A vypuštěním i-tého řádku a j-tého sloupce.

Čtvercová matice A je *regulární* pokud $\det(A) \neq 0$ a *singulární* pokud $\det(A) = 0$. *Podmaticí* rozumíme každou matici vzniklou z A vymazáním některých řádků nebo sloupců. Důležitý pojem *hodnosti matice* bude připomenut později v souvislosti s lineární nezávislostí vektorů.

Grupy a tělesa. *Binární operace* na nějaké množině X je libovolné zobrazení $X \times X \to X$; to znamená, že každým dvěma prvkům $a, b \in X$ je přiřazen nějaký prvek X, což je „výsledek" uvažované binární operace. Například sčítání a násobení jsou binární operace na množině všech přirozených čísel, zatímco odčítání není binární operací na této množině. Binární operace se obvykle zapisují symboly jako $*$, $\circ$, $+$, $\cdot$ a podobně. Je-li tedy $*$ nějaká binární operace, zápis $a * b$ označuje prvek přiřazený operací $*$ uspořádané dvojici (a, b).

Binární operaci $*$ nazveme *asociativní*, pokud $a*(b*c) = (a*b)*c$ pro všechna $a, b, c \in X$. *Komutativita* operace $*$ znamená $a * b = b * a$ pro všechna $a, b \in X$. Prakticky veškeré binární operace, s nimiž se v matematice běžně setkáme, bývají asociativní, ale mnohé důležité a často se vyskytující operace jsou nekomutativní, jako třeba násobení matic typu $n \times n$ (pro $n \geq 2$) nebo skládání zobrazení nějaké množiny.

Grupa je množina G s asociativní binární operací $*$ splňující následující podmínky (existuje mnoho různých ekvivalentních verzí těchto podmínek):

(i) Existuje prvek $e \in G$, zvaný *jednotkový prvek* (případně *neutrální prvek*), takový že pro všechna $a \in G$ platí $a * e = e * a = a$. (Je snadno vidět, že pokud takové e existuje, je jen jedno.)

(ii) Pro každé $a \in G$ existuje $b \in G$, pro něž $a * b = b * a = e$, kde e je jednotkový prvek. Takové b se jmenuje *inverzní prvek* k prvku a, a obvykle se označuje a^{-1}. Inverzní prvek je také určen pro každé $a \in G$ jednoznačně[4].

[4]Někdy se grupa definuje jako algebraická struktura se třemi operacemi: binární operací $*$ jako výše, unární operací inverzního prvku ($a \mapsto a^{-1}$) a nulární operací, čili konstantou, e (zatímco v uvedené definici jsou operace inverzního prvku a e odvozené definicí z $*$). To má jisté výhody z hlediska obecné algebry, například podgrupa je pak prostě podmnožina uzavřená na tyto tři operace.

Některé z důležitých příkladů grup jsou celá čísla s operací sčítání, kladná reálná čísla s násobením, množina všech regulárních matic typu $n \times n$ s operací násobení, množina všech permutací dané množiny X s operací skládání permutací a množina všech rotací třídimenzionálního euklidovského prostoru kolem počátku s operací skládání (provedení nejprve jedné rotace a pak druhé dá opět nějakou rotaci). Na druhé straně, přirozená čísla se sčítáním ani reálná čísla s násobením grupu netvoří.

Grupa je komutativní pokud její binární operace je komutativní. Komutativním grupám se někdy říká *abelovské*.

Těleso je množina K se dvěma binárními operacemi+ a $\times$ (tyto symboly zde nemusí nutně znamenat obvyklé operace s čísly!), pro něž platí takovéto axiomy:

1. Množina K s operací $+$ je komutativní grupa. Její jednotkový prvek se značí 0.

2. Množina $K \setminus \{0\}$ s operací $\times$ je komutativní grupa. Její jednotkový prvek se značí 1.

3. Platí *distributivita*: $a \times (b + c) = (a \times b) + (a \times c)$ pro každé $a, b, c \in K$.

Podobně jako u grup, v literatuře se najde mnoho ekvivalentních verzí axiomů tělesa. Násobení $a \times b$ se často zkráceně zapisuje ab. Nejběžnější tělesa jsou racionální čísla, reálná čísla a komplexní čísla (s obvyklým násobením a sčítáním jako operacemi). Naproti tomu celá čísla se sčítáním a násobením tělesem nejsou.

Buď K těleso. Jeho podmnožina L je jeho *podtěleso* pokud je L tělesem s binárními operacemi a prvky 0 a 1 zděděnými z K. Například těleso racionálních čísel je podtělesem tělesa reálných čísel.

V kombinatorice se mnohdy potřebují konečná tělesa. Konečné těleso s q prvky, pokud takové existuje, se často označuje $GF(q)$. Nejjednodušší konečné těleso je $GF(2)$, což je prostě množina $\{0, 1\}$ s obvyklým násobením (jako v celých číslech) a se sčítáním daným rovnostmi $0 + 0 = 1 + 1 = 0$, $0 + 1 = 1 + 0 = 1$. Je známo, že konečné těleso

$GF(q)$ existuje právě když je q mocnina prvočísla. V takovém případě je vždy jen jediné q-prvkové těleso (až na přejmenování prvků). Je-li q prvočíslo, těleso $GF(q)$ se popíše velmi snadno. Je to množina $\{0, 1, 2, \ldots, q-1\}$, kde sčítání a násobení se provádějí jako pro celá čísla, ale po sečtení nebo vynásobení dvou čísel vezmeme zbytek při dělení výsledku číslem q (tomu se říká *aritmetika modulo q*). Výše uvedený popis $GF(2)$ je speciálním případem této konstrukce. Zdůrazněme ale, že pro $q = p^k$, kde p je prvočíslo a $k > 1$, množina $\{0, 1, \ldots, q-1\}$ s aritmetikou modulo q *není* tělesem, a konstrukce tělesa $GF(q)$ je jiná a složitější.

Vektorové prostory. Nechť K je nějaké těleso (nejčastěji uvažujeme těleso všech reálných čísel). *Vektorový prostor* nad K je komutativní grupa V s grupovou operací $+$ a s neutrálním prvkem 0, plus zobrazení $K \times V \to V$. To znamená, že každé dvojici (α, v), kde $\alpha \in K$ a $v \in V$, je přiřazen prvek z V, a tedy každý prvek z V můžeme „vynásobit" libovolným prvkem z K. Tohle násobení se zpravidla zapisuje bez nějakého zvláštního znaménka pro násobení, takže píšeme prostě αv a míníme v vynásobené α. Pro vektorový prostor musí být dále splněný takovéto požadavky, pro libovolná $u, v \in V$ a jakákoli $\alpha, \beta \in K$: $\alpha(u+v) = \alpha u + \alpha v$, $(\alpha+\beta)v = \alpha v + \beta v$ (jakási distributivita), $\alpha(\beta v) = (\alpha\beta)v$ (něco jako asociativita), a $1v = v$. Z těchto axiomů lze už dokázat všelijaké další vlastnosti, jako třeba $0v = 0$ (ta 0 nalevo je v tělese K, zatímco ta napravo je ve vektorovém prostoru V). Prvky V se jmenují *vektory*.

Nejobvyklejší a nejdůležitější příklad vektorového prostoru je tvořen množinou všech uspořádaných n-tic reálných čísel (pro nějaké přirozené číslo n). Tyto n-tice se sčítají a násobí reálným číslem po složkách. Tak dostaneme vektorový prostor nad reálnými čísly, ale podobně můžeme uvažovat vektorový prostor všech uspořádaných n-tic prvků jakéhokoli tělesa K, čímž dostaneme vektorový prostor nad K. Ten se zpravidla označuje K^n.

Množina $A \subset V$ ve vektorovém prostoru V je *lineárně závislá*, pokud existují vektory $v_1, v_2, \ldots, v_n \in A$, $n \geq 1$, a čísla α_1, α_2, …, $\alpha_n \in K$, ne všechna najednou rovná 0, tak, že $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0$. Není-li A lineárně závislá, nazývá se *lineárně nezávislá*.

Největší mohutnost lineárně nezávislé množiny v daném vektorovém prostoru V se jmenuje *dimenze* V, a každá lineárně nezávislá množina této mohutnosti se nazývá *báze* vektorového prostoru V. Vektorový prostor K^n má dimenzi n, jak by každý čekal.

Každý vektorový prostor má nějakou bázi, a každá lineárně nezávislá množina maximální vzhledem k inkluzi (t.j., nelze přidat žádný vektor bez pokažení lineární nezávislosti) je bází. V kombinatorice se skoro vždy setkáváme jen s vektorovými prostory konečné dimenze.

Je-li $(e_1, e_2, \ldots, e_n)$ báze nějakého n-dimenzionálního vektorového prostoru V, pak každý vektor $v \in V$ se dá právě jedním způsobem vyjádřit ve tvaru $v = \sum_{i=1}^{n} \alpha_i e_i$ pro nějaká $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$. Tato jednoznačně určená $\alpha_1, \ldots, \alpha_n$ jsou *souřadnice* vektoru v vzhledem k bázi $(e_1, \ldots, e_n)$. Každému vektoru $v \in V$ je tudíž jednoznačně přiřazen vektor z K^n, totiž n-tice jeho souřadnic. Tím dostaneme bijekci mezi V a K^n (pro daný V je mnoho takových bijekcí, jedna pro každou volbu báze ve V). Všechny n-dimenzionální vektorové prostory nad daným tělesem jsou „stejné", t.j. jsou ve vhodně definovaném smyslu isomorfní. Takže na K^n můžeme pohlížet jako na „jediný" n-dimenzionální vektorový prostor nad K, a vektory si obvykle můžeme představovat jako n-tice čísel. Na druhé straně, často je užitečné pracovat i s jinými konkrétními verzemi n-dimenzionálních vektorových prostorů. V kombinatorických použitích lineární algebry je často rozhodujícím krokem šikovná a nečekaná konstrukce nějakého pomocného vektorového prostoru, a hlavní část důkazu pak spočívá v odhadu jeho dimenze.

Podprostor vektorového prostoru V je podmnožina $W \subseteq V$ uzavřená na sčítání vektorů a na násobení prvky z tělesa K. Je-li $X \subseteq V$ libovolná množina vektorů, definujeme *podprostor generovaný* X jako nejmenší podprostor prostoru V obsahující X. Explicitní popis tohoto podprostoru je $\{\sum_{i=1}^{n} \alpha_i v_i;\ n \in \mathbf{N},\ \alpha_1, \ldots, \alpha_n \in K,\ v_1, \ldots, v_n \in X\}$.

Hodnost matice A typu $m \times n$, jejíž prvky jsou z tělesa K, je definována jako dimenze podprostoru generovaného řádky matice A (chápanými jako n-složkové vektory) v prostoru K^n. Hodnost A se zpravidla označuje $r(A)$. Tato hodnost je také rovna dimenzi podprostoru generovaného sloupci matice A v prostoru K^m, tedy $r(A) =$

$r(A^T)$. Pro hodnost součinu a součtu matic platí nerovnosti $r(AB) \leq \min(r(A), r(B))$ a $r(A+B) \leq r(A) + r(B)$. Čtvercová matice typu $n \times n$ je regulární (má nenulový determinant) právě když má hodnost n—to je významné kriterium lineární nezávislosti pomocí determinantu. Obecněji, platí následující charakterizace hodnosti: $r(A)$ je největší celé číslo k takové, že A (ne nutně čtvercová) má aspoň jednu regulární podmatici typu $k \times k$.

Jsou-li V a W vektorové prostory nad stejným tělesem K, definujeme *lineární zobrazení* prostoru V do prostoru W jako zobrazení $f: V \to W$ splňující $f(\alpha u) = \alpha f(u)$ a $f(u+v) = f(u) + f(v)$ pro všechna $\alpha \in K$ a $u, v \in V$. *Jádro* lineárního zobrazení f je množina $\ker(f) = \{v \in V;\ f(v) = 0\}$. Jádro f je podprostor V, a množina $f(V)$ je podprostor W. Dimenze $f(V)$ je *hodnost* zobrazení f. Pro každé lineární zobrazení $f : V \to W$ je pravda $\dim \ker(f) + \dim f(V) = \dim V$.

Buď $(e_1, e_2, \ldots, e_n)$ nějaká báze V a $(f_1, f_2, \ldots, f_m)$ nějaká báze W. Volbou těchto bází získáme bijekci mezi všemi lineárními zobrazeními $f: V \to W$ a všemi maticemi typu $m \times n$ s prvky z tělesa K. Jak víme, každý vektor $v \in V$ můžeme jednoznačně napsat ve tvaru $v = \sum_{i=1}^{n} \alpha_i e_i$. Lineární zobrazení $f: V \to W$ se dá vyjádřit takto:

$$f(v) = f\Big(\sum_{i=1}^{n} \alpha_i v_i\Big) = \sum_{j=1}^{m} \Big(\sum_{i=1}^{n} a_{ji}\alpha_i\Big) f_j,$$

kde a_{ij} jsou prvky $m \times n$ matice A odpovídající f. Jinými slovy, je-li α sloupcový vektor souřadnic vektoru v vzhledem k bázi $(e_1, \ldots, e_n)$ a β je sloupcový vektor souřadnic $f(v)$ vzhledem k bázi $(f_1, \ldots, f_m)$, potom máme $\beta = A\alpha$.

Takže lineární zobrazení můžeme chápat jako abstraktní verzi matic, nebo matice jako „souřadnicový zápis“ lineárních zobrazení. Násobení matic pak odpovídá skládání lineárních zobrazení. Hodnost lineárního zobrazení je ovšem totéž jako hodnost jeho matice (vzhledem k libovolným bázím).

Geometrická interpretace. Mnohdy je užitečné si některé objekty z lineární algebry představovat geometricky, a naopak lineární algebra samozřejmě pomáhá pracovat s objekty geometrickými. Není žádný recept na nejlepší geometrické interpretace lineárně-algebraických pojmů.

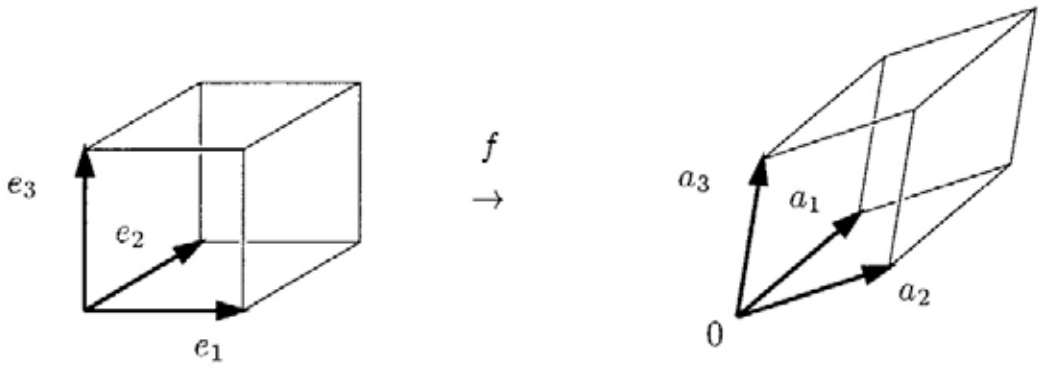
Zde uvedeme několik jednoduchých možností. Budeme se držet vektorového prostoru $\mathbf{R}^3$, i když geometrické představy mohou při určitém cviku pomoci i pro vyšší dimenze.

Podprostory $\mathbf{R}^3$ (jako vektorového prostoru nad $\mathbf{R}$) jsou: bod 0 (počátek), všechny přímky a roviny procházející počátkem, a $\mathbf{R}^3$ sám. Lineární závislost 3 vektorů $a_1, a_2, a_3 \in \mathbf{R}^3$ znamená, že body a_1, a_2, a_3 leží na společné rovině procházející počátkem.

Rovina neprocházející počátkem není (vektorovým) podprostorem. Můžeme ji vyjádřit jako posun nějakého podprostoru o vhodný vektor, nebo též jako řešení jedné lineární rovnice, t.j. jako množinu všech $x = (x_1, x_2, x_3) \in \mathbf{R}^3$, pro něž $a^T x = a_1 x_1 + a_2 x_2 + a_3 x_3 = b_0$, pro nějaké $b_0 \in \mathbf{R}$ a nějaké nenulové $a \in \mathbf{R}^3$.

Je-li A matice typu $m \times 3$ a $b \in \mathbf{R}^m$ je sloupcový m-složkový vektor, $Ax = b$ je soustava m lineárních rovnic pro neznámý vektor $x \in \mathbf{R}^3$. Každý řádek A dává jednu lineární rovnici. S výjimkou patologického případu nulového řádku, taková rovnice určuje rovinu, a geometricky je množina řešení soustavy $Ax = b$ průnikem m rovin (nemá-li A nulové řádky). Pro $m = 2$, příslušné 2 roviny mohou být totožné (řešením jsou všechny body této roviny), rovnoběžné (žádné řešení), nebo různoběžné (řešením jsou body přímky). V prvních dvou případech má A hodnost 1, a ve třetím případě hodnost 2. Podobně můžeme diskutovat případ $m = 3$: matice A hodnosti 3 odpovídá třem rovinám protínajícím se v jediném bodě, a menší hodnosti odpovídají několika možným „degenerovaným" situacím (některé z rovin splývají nebo jsou rovnoběžné, případně průnik dvou rovin je rovnoběžný s rovinou třetí).

Nechť $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, $e_3 = (0, 0, 1)$ je standardní báze prostoru $\mathbf{R}^3$. Lineární zobrazení $f : \mathbf{R}^3 \to \mathbf{R}^3$ je určeno obrazy $a_i = f(e_i)$ bázových vektorů. Vektoru $x \in \mathbf{R}^3$ je přiřazen vektor $f(x) = Ax \in \mathbf{R}^3$, kde A je matice typu 3×3 s a_1, a_2, a_3 jako sloupci (přesněji řečeno, A je matice zobrazení f vzhledem ke dvojici bází (e_1, e_2, e_3) a (e_1, e_2, e_3)). Zobrazení f převádí jednotkovou krychli na rovnoběžnostěn určený vektory a_1, a_2, a_3:



Absolutní hodnota determinantu A je přesně objem tohoto rovnoběžnostěnu! Jako speciální případ, je-li $\det A = 0$, má A hodnost ≤ 2, tudíž a_1, a_2, a_3 leží ve společné rovině procházející počátkem, a místo rovnoběžnostěnu máme placku nulového objemu. Obecněji, je-li $K \subset \mathbf{R}^3$ množina objemu v, potom $f(K)$ má objem $v|\det A|$. Podobný význam má absolutní hodnota determinantu i pro vyšší dimenze. Znaménko determinantu je pak dáno orientací trojice (a_1, a_2, a_3): příkladem trojice s kladnou orientací je (e_1, e_2, e_3), a příkladem trojice se zápornou orientací je $(e_1, e_2, -e_3)$.

Literatura

[1] A. Aho, J. Hopcroft, and J. Ullman: *The Design and Analysis of Computer Algorithms*, Addison-Wesley, Reading, Massachusetts, 1983.

[2] L. Babai and P. Frankl: *Linear algebra methods in combinatorics* (Preliminary version 2), Department of Computer Science, The University of Chicago, 1992.

[3] B. Balcar a P. Štěpánek: *Teorie množin*, Academia Praha 1986.

[4] O. Borůvka: Několik vzpomínek na matematický život v Brně, *Pokroky mat. fyz. a astr.* 22(1977) 91–99.

[5] J. M. Borwein and P. B. Borwein: *Pi and the AGM*, John Wiley & Sons, New York 1987.

[6] K. Chandrasekhar: *Introduction to Analytic Number Theory*, Springer-Verlag 1968.

[7] R. Diestel: *Graph Theory*, Graduate Texts in Mathematics 173, Springer-Verlag, Berlin etc., 1996.

[8] R. Graham, D. Knuth, and O. Patashnik: *Concrete Mathematics: A Foundation for Computer Science*, Addison-Wesley, Reading, Massachusetts, 1989.

[9] F. Harary, E. M. Palmer: *Graphical Enumeration*, Academic Press, New York and London, 1973.

[10] K. Havlíček a kol.: *Cesty moderní matematiky*, Horizont Praha 1976.

[11] D. Karger, P. Klein, and R. Tarjan: A Randomized Linear-Time Algorithm to Find Minimum Spanning Trees, *Journal of the ACM* 42(1995) 321–328.

[12] D. Knuth: *The Art of Computer Programming*, Volume I: Fundamental Algorithms, Addison-Wesley, Reading, MA 1968.

[13] J. H. van Lint, R. M. Wilson: *A Course in Combinatorics*, Cambridge University Press, Cambridge 1992.

[14] L. Lovász: *Combinatorial Problems and Exercises*, 2. vydání, Akadémiai Kiadó Budapest and North-Holland, Amsterdam 1993.

[15] J. Nešetřil: *Teorie grafů*, SNTL Praha 1979.

[16] J. Nešetřil: Kombinatorika a teorie grafů I, skripta, Universita Karlova Praha 1981.

[17] N. Robertson, D. P. Sanders, P. D. Seymour, and R. Thomas: The Four Color Theorem, *Journal of Combinatorial Theory* Ser. B 70(1997), 2–44.

[18] A. de Saint-Exupéry: *Malý princ*, SNDK Praha 1966.

[19] J. Stillwell: *Classical Topology and Combinatorial Group Theory* (Graduate Texts in Mathematics 72), Springer-Verlag 1980.

[20] N. J. Vilenkin: *Kombinatorika*, SNTL Praha 1977.

Rejstřík

Jiří Načeradský a Jaroslav Nešetřil: Modul X

Návody ke cvičením

1.2.2(b). $\lfloor \log_{10} n \rfloor + 1$.

1.2.3. Označíme-li pravou stranu m, je celé číslo m určeno vztahy $m^2 \leq \lfloor x \rfloor < (m+1)^2$. To platí právě když $m = \lfloor \sqrt{x} \rfloor$.

1.2.5(d). Viz část 10.4, cvičení 3.

1.3.3(a). Přidáním další přímky k n přímkám bude právě $n+1$ oblastí rozříznuto na 2.

1.3.3(b). V indukčním kroku použijte (a). Vyjde $(n^3 + 5n + 6)/6$.

1.3.5. Definujte $x_1 = \min(M)$, $x_{i+1} = \min(M \setminus \{x_1, \ldots, x_i\})$. Kdyby M byla nekonečná, nemá podmnožina $\{x_1, x_2, \ldots\}$ největší prvek.

1.3.7. Ukažte, že čitatel se každým krokem zmenší.

1.4.3(a). Existuje jen konečně mnoho relací na X.

1.4.3(c). Vezměte $(\mathbf{N}, <)$.

1.7.4. Definujte relaci $S = \{(x,x);\, x \in X\} \cup R \cup R \circ R \cup R \circ R \circ R \cup \ldots$, dokažte že je to uspořádání.

1.7.6. Např. pro množinu všech racionálních čísel je relace bezprostředního předchůdce prázdná.

1.7.8. Indukcí podle $|X|$. Odeberte z X nějaký minimální prvek, dejte ho jako první v uspořádání podle $\leq$.

1.7.9(b). Konečná lineárně uspořádaná množina má největší prvek. Zobrazte největší prvek na největší prvek, a pokračujte indukcí.

1.7.9(d). Nespočetně: Rozdělte $\mathbf{N}$ na spočetně mnoho disjunktních podmnožin $A_1, A_2, \ldots$. Každou A_i uspořádejte buď jako přirozená čísla, nebo jako záporná celá čísla; potom dejte tyto množiny za sebe v pořadí $A_1, A_2, \ldots$.

1.7.10. Zvolte $A = X$ a $x \in X$ přiřaďte $M_x = \{y \in X; y \leq x\}$.

1.7.11(c). Ukažte, že pro $A \subseteq X$ je $\inf A = \sup\{x \in X;\, x \leq a\, \forall a \in A\}$.

2.1.1. Kódujte dvojici (A, B) zobrazením do množiny $\{0, 1, 2\}$: prvek $x \in A$ dostane 2, $x \in B \setminus A$ dostane 1, a $x \notin B$ 0.

2.1.2(b). První sloupec zvolme jako libovolný nenulový vektor. Druhý sloupec nesmí být násobkem prvního, tím se vylučuje q vektorů. Třetí sloupec nesmí být lineární kombinací prvních dvou, tím se pro něj vylučuje q^2 možností (žádné 2 různé lineární kombinace prvních dvou sloupců nedají týž vektor — ověřte!); obecně pro i-tý sloupec je $q^n - q^i$ možností.

2.2.1. $(n-1)!$.

2.2.2. Uvažte cykly permutace. Jaký je řád permutace s jediným cyklem délky k? S dvěma cykly délky k_1 a k_2?

2.2.3(a). Ukažte, že napíšeme-li permutaci s k úseky pozpátku, dostaneme permutaci s $n+1-k$ úseky.

2.2.3(b). Uvažte permutaci čísel $\{1, 2, \ldots, n-1\}$ s k úseky (v jednořádkovém zápisu), a vložte do ní číslo n na některou z možných $n+1$ pozic. Pro kolik pozic bude mít výsledná permutace $k+1$ úseků, a pro kolik k?

2.2.3(c). Obecný vzorec, odvozený Eulerem, je
$f(n,k) = \sum_{j=0}^{k} (-1)^j (k-j)^n \binom{n+1}{j}$.

2.2.3(d). Rozdělte permutace do tříd podle množiny čísel na prvních $k+1$ místech. Všechna pořadí prvních $k+1$ čísel jsou stejně pravděpodobná. Která z možných rozestavení prvních $k+1$ čísel dávají počáteční úsek délky k? Pravděpodobnost vyjde $k/(k+1)!$.

2.2.4(b). Jsou-li na počátku čísla srovnána podle permutace π, jednou výměnou sousedů ubyde nanejvýš 1 inverze.

2.2.5(b). Kolik z čísel $1, 2, \ldots, n$ je dělitelných p^j pro dané j? Vyjde $\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \cdots$.

2.3.2(b). Pravá strana je počet $(r+2)$-tic nezáporných celých čísel řešících rovnici $X_1 + X_2 + \cdots + X_{r+2} = n - r$. Rozdělte tyto $(r+2)$-tice na $n-r$ skupin podle hodnoty X_{r+2} a spočítejte počet řešení v každé skupině zvlášť, tím se dostane levá strana.

2.3.3. Upravte k-tý člen na $\binom{n}{m}\binom{n-m}{n-k}$, $\binom{n}{m}$ vytkněte. Vyjde $\binom{n}{m} 2^{n-m}$.

2.3.4(a). Užijte $\frac{1}{k}\binom{k}{m} = \frac{1}{m}\binom{k-1}{m-1}$ a vzorec (2.9).

2.3.4(b). Tentokrát $k\binom{k}{m} = (k+1)\binom{k}{m} - \binom{k}{m} = (m+1)\binom{k+1}{m+1} - \binom{k}{m}$.

2.3.5. Buď M nějaká m-prvková množina, N n-prvková. Obě strany počítají počet uspořádaných dvojic (X, Y), kde $X \subseteq M$, $Y \subseteq N \cup X$, $|Y| = m$. Pro levou stranu vybereme napřed X, pak Y, pro pravou nejdřív $Y \cap M$, pak $Y \cap N$, nakonec X.

2.3.6. Označme $k_i = f(i+1) - f(i)$, $k_1 = f(1)$, $k_n = n - f(n)$. Hledaný počet je počet celých nezáporných řešení rovnice $k_1 + \cdots + k_n = n$.

2.3.8. Uvažme k-tici $\{a_1, \ldots, a_k\}$, $a_1 < \cdots < a_k$. Přiřaďme jí k-tici $\{a_1, a_2 - 1, a_3 - 2, \ldots, a_k - k + 1\}$. To je bijekce na $\binom{\{1,2,\ldots,n-k+1\}}{k}$.

2.3.9(c). Počítejte plochu velkého čtverce dvěma způsoby. Jeho strana je $2(1 + 2 + 3 + \cdots + n)$. Přitom k-tá "vrstva" (od středu) má $4k$ čtverečků $k \times k$.

2.3.11. Postupujte třeba indukcí podle n.

2.3.12(b). Ve vzorci pro binomický koeficient, právě 1 z činitelů v čitateli je dělitelný p. Tedy $\binom{n}{p}$ je dělitelné p právě když tento činitel je dělitelný i p^2.

2.3.13(a). Dosaďte postupně do binomické věty $x = 1$, $x = -1$, $x = \mathrm{i}$ a $x = -\mathrm{i}$ (i značí imaginární jednotku) a výsledné rovnice sečtěte. Upravte n-té mocniny pomocí de Moivreova vzorce. Pro hledaný počet vyjde podivuhodná formule $2^{n-2} + 2^{n/2-1} \cos \frac{\pi n}{4}$. Ověřte správnost pro malé hodnoty n.

2.3.13(b). Postupujte podobně jako v (a), ale do binomické věty dosazujte za x všechny 3 kořeny rovnice $x^3 = 1$.

2.3.16. Nejdřív rozestavte čarodějnice, tím je určeno 8 možných pozic pro vodníky, vyberte 5 z nich, a nakonec určete pořadí vodníků.

2.3.18. Nejprve zvolte zastoupené státy, pak pro každý určete jednoho ze 2 senátorů.

2.3.19. Vyjděte z trojúhelníku T_0 který má 2 strany na obvodu n-úhelníka, zvolte k němu přiléhající trojúhelník T_1, T_2 přiléhající k T_1, ... Pro T_0 je n možností, v každém dalším kroku jsou 2 možnosti. Přitom každou triangulaci dostaneme $2\times$ (pro T_0 jsou 2 možnosti). Vyjde $n2^{n-5}$.

2.3.21(a). Levá strana je počet seřazení n předmětů, k_i předmětů i-tého druhu. Pravá strana: nejdříve zvolíme druh předmětu na první pozici, pak rozestavíme zbývající předměty.

2.4.3. Napřed upravte všechny funkce na tvar $e^{f(n)}$.

2.4.4. Přímka $y = x + 1$ je tečnou ke grafu funkce e^x v bodě $(0, 1)$. Dále funkce e^x je konvexní, poněvadž má nezápornou druhou derivaci, a proto nemůže svoji tečnu protínat jinde než v bodě dotyku.

2.4.6(b). Označme $A = (x_1 + x_2 + \cdots + x_{n-1})/(n-1)$. Podle $AG(n)$ aplikovaného na čísla $x_1, \ldots, x_{n-1}$ a A máme $A^n = ((x_1 + x_2 + \cdots + x_{n-1} + A)/n)^n \geq x_1 x_2 \cdots x_{n-1} A$, a odtud po úpravě $A \geq (x_1 \cdots x_{n-1})^{1/(n-1)}$.

2.4.9. Funkce $\ln x$ je konkávní, speciálně každý trojúhelníček s vrcholy v bodech $(i, \ln i)$, $(i+1, \ln i)$ a $(i+1, \ln(i+1))$ leží celý pod jejím grafem (nakres-

lete si). Jeho plocha je $(\ln(i+1) - \ln i)/2$. Proto $\ln n! \le \ln n + \int_1^n \ln x \, dx - \frac{1}{2}\sum_{i=1}^{n-1}(\ln(i+1) - \ln i)$; upravte.

2.4.10. Indukcí podle n.

2.4.11. Dolní odhad: indukcí, dokazujte $2(\sqrt{n} - \sqrt{n-1}) \le 1/\sqrt{n+1}$, levou stranu upravte na zlomek se jmenovatelem $\sqrt{n} + \sqrt{n-1}$. Horní odhad podobně.

2.4.12(a). Aproximujte každý zlomek $1/i$ shora a zdola nejbližším zlomkem tvaru $1/2^k$.

2.5.2(a). Taková prvočísla všechna dělí $\binom{2m}{m}$.

2.5.2(b). Je-li P součin prvočísel jako v (a), máme $\log_2 P \le 2m$, ale na druhé straně $P \ge m^{\pi(2m)-\pi(m)}$. Odtud $\pi(2m) \le \pi(m) + O(m/\ln m)$.

2.5.2(c). Maximální mocnina p dělící $n!$ je $\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \cdots$. Použijte vyjádření $\binom{2m}{m} = (2m)!/(m!)^2$ a vyjádřete rozdíl max. mocnin p pro čitatele i jmenovatele.

2.5.2(d). Podle (c) je $2^{2n}/(n+1) \le \binom{2n}{n} \le (2n)^{\pi(2n)}$.

2.6.2. Postupujte jako ve druhém důkazu principu inkluze a exkluze. t.j. uvažte příspěvek jednoho prvku.

2.7.1. Rozdělte všechny permutace do tříd podle počtu pevných bodů, vyjádřete počet permutací v každé třídě pomocí funkce $š(k)$.

2.7.2(a). První pán si vymění klobouk, který dostal, za svůj klobouk, a odejde. Buď má ten, s nímž první pán měnil, taky svůj klobouk — a odjede — nebo nemá svůj klobouk, a máme situaci s $n-1$ pány.

2.7.4. Zvolte pevný bod, zbytek je permutace bez pevného bodu, užijte výsledek problému šatnářky.

2.7.6(c). Zobrazujte na množinu $\{1, 2, \ldots, m\}$; nechť A_i je množina zobrazení, která nic nezobrazí na prvek i. Použijte princip inkluze a exkluze na určení $|A_1 \cup \ldots \cup A_m|$, t.j. počtu špatných zobrazení. Pro $m = n$ musíme dostat $n!$.

2.7.6(d). Zobrazení f množiny N na m-prvkovou množinu definuje ekvivalenci na N s m třídami. Ukažte, že každá z ekvivalencí na N s m třídami je definována právě $m!$ takovými zobrazeními.

2.7.7(a). Můžete použít návodu k (d) předchozího cvičení a výsledku (c) onoho cvičení.

2.7.7(b). Výsledek (a) sčítáme přes všechna k; vyjde
$\sum_{k=0}^{n} \frac{1}{k!} \sum_{j=0}^{k} (-1)^j \binom{k}{j} (k-j)^n$.

2.7.7(c). Ve vyjádření z (b) pište i místo $k-j$, nechte k formálně probíhat do ∞, a zaměňte pořadí sčítání podle k a j.

2.7.10(b). Každý člen součinu rozepište jako $1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i}$.

2.7.10(c). Buď $n = 2^q \prod_{i=1}^{r} p_i^{\alpha_i}$, p_i lichá prvočísla. Podle (b) musí být $2n = t\prod(p_i^{\alpha_i} + p_i^{\alpha_i - 1} + \cdots + 1)$, $t = 2^{q+1} - 1$. Po vydělení výrazem $t\prod p_i^{\alpha_i}$ máme $1 + 1/t = \prod(1 + 1/p_i + \cdots + 1/p_i^{\alpha_i})$. Přitom některé p_i dělí t. Aby pravá strana nebyla větší než levá, musí být $r = 1$, $t = p_1$.

2.7.11(a). Pro každé prvočíslo $p_i \leq N$, nechť A_i je množina dvojic (m, n) takových, že $p_i | n$ a $p_i | m$. Použijte princip inkluze a exkluze na určení počtu špatných dvojic.

2.7.12(a). Definujte A_i jako množinu všech grafů, v nichž vrchol i je izolovaný, počítejte $|A_1 \cup \ldots \cup A_n|$.

2.7.12(b). Zvolte izolované vrcholy, na zbytek užijte (a).

2.7.13. Definujte A_i jako množinu těch rozsazení, kdy i-tý pár sedí vedle sebe.

3.1.5(a). Protipříklad je třeba graf na obr. 3.2 vpravo (str. 114).

3.1.6. Jak sestrojit $2^{n^2/2 - O(n \log n)}$ neisomorfních (téměř tolik jako se dostane počítáním uvedeným v textu): Buď n dost velké, a buď m nejmenší splňující $2^m \geq n$. Pojmenujme vrcholy a, b, c, d, $u_0, u_1, \ldots, u_{m-1}$ a $v_0, v_1, \ldots, v_{n-m-5}$; pišme $U = \{u_0, \ldots, u_{m-1}\}$, $V = \{v_0, \ldots, v_{n-m-5}\}$. Spojme a s b, a b spojíme s c, s d a se všemi vrcholy z U. Na U zvolme nějaký asymetrický graf, např. cestu $u_0, u_1, \ldots, u_{m-1}$ kde u_0 je ještě propojen s u_3. Vrcholy c, d spojme se všemi vrcholy V (takže teď a je jediný vrchol stupně 1). Na V zvolme libovolný graf, a konečně každý vrchol $v_i \in V$ spojme s vrcholy $u_{j_1}, \ldots, u_{j_k}$, kde $0 \leq u_1 < u_2 < \ldots < u_k \leq m-1$ jsou (jednoznačně určená) čísla pro něž platí $2^{j_1} + 2^{j_2} + \cdots + 2^{j_k} = i$ (to odpovídá dvojkovému zápisu čísla i). Lze snadno ukázat, že pro dva různé grafy na V jsou výsledné grafy neisomorfní, a máme tedy aspoň $2^{\binom{n-m-5}{2}}$ neisomorfních grafů na n vrcholech.

3.2.1. Nejvíce hran zřejmě dostaneme pro sjednocení k úplných grafů; jsou-li jejich velikosti $n_1, \ldots, n_k$, $\sum n_i = k$, potřebujeme maximalizovat výraz $\binom{n_1}{2} + \cdots + \binom{n_k}{2}$. Ukažte, že pokud např. $n_1 \geq n_2 > 1$, zmenšením n_2 a zvětšením n_2 o 1 hodnota neklesne; maximum je tedy pro $n_1 = n - k + 1$ a ostatní $n_i = 1$.

3.2.3. Neobsahuje-li lichou kružnici, předpokládejte, že je souvislý, a označujte vrcholy následujícím algoritmem: libovolný vrchol označte $+1$; dále kdykoli je v vrchol sousedící s vrcholem označeným x, označte v $-x$. Ukažte,

že takto se postupně označí všechny vrcholy a žádné 2 stejně označené vrcholy nesousedí.

3.2.4(a). Je-li v vrchol stupně > 1, musí být spojen se všemi vrcholy své komponenty. Každá komponenta musí být buď K_3, nebo $K_{1,n}$.

3.2.4(b). Uvažme jen souvislé grafy G. Případ kdy max. stupeň je ≤ 2 je snadný; předpokládejme že max. stupeň ≥ 3, a uvažme vrchol v max. stupně. Podle předchozího cvičení musí být graf G_v indukovaný na sousedech v být disjunktním sjednocením trojúhelníků a hvězd (=grafů tvaru $K_{1,n}$). Diskusí možných případů vyjdou následující možnocti pro G: libovolný graf na ≤ 4 vrcholech, dvě hvězdy spojené hranou za středy, trojuhelnik s několika hranami přivěšenými k jednomu vrcholu, a $K_{1,n}$ jehož všechny vrcholy jsou spojeny s jedním dalším vrcholem.

3.2.6. Průměr: $\max\{d_G(u,v);\ u,v \in V(G)\}$.
Poloměr: $\min_{v\in V(G)} \max_{u\in V(G)} d_G(u,v)$.

3.3.2. Graf zadejte seznamem sousedů pro každý vrchol. Uchovávejte vrcholy množiny A spolu s hodnotami $d(v)$ ve vhodné datové struktuře, která umožňuje rychle najít a vymazat vrchol s minimálním $d(v)$ — takovou strukturou je např. tzv. halda (heap).

3.3.4. Pro každý vrchol v uchovávejte vrchol $p(v)$, z nějž se do v přišlo.

3.3.5(b). Algoritmus je totožný s Dijkstrovým algoritmem (v naší formulaci) pro ohodnocení $w = 1$.

3.3.6. Jako v textu se ukáže, že vždy platí $d(v) \geq d_{G,w}(s,v)$. Pro spor, nechť existuje v pro nějž $d(v) > d_{G,w}(s,v)$ v okamžiku, kdy opustil A. V tomto okamžiku uvažte poslední vrchol u na nejkratší cestě z s do v, který není v A, a vrchol u_1 následující na této cestě po u (ve směru od s). Protože $u \notin A$, je $d(u) = d_{G,w}(s,u)$, a $d(u_1) \leq d(u) + w(\{u,u_1\}) = d_{G,w}(s,u_1)$. Dále $d(u_1) + h(u_1) \geq d(v) + h(v) > d_{G,w}(s,v) + h(v)$ (protože u_1 je ještě v A), odtud $d_{G,w}(s,v) - d_{G,w}(s,u_1) < h(u) - h(v)$, a to dává spor s podmínkou pro h.

3.4.1. Např.: první graf neobsahuje žádnou kružnici délky 4, druhý 2 takové kružnice, třetí 5 kružnic délky 4.

3.4.7(a). Ne; musel by mít skóre $(0,1,\ldots,n-1)$, ale má-li vrchol spojený se všemi ostatními nemůže mít zároveň vrchol stupně 0.

3.4.7(b). Pro všechna $n \geq 2$. Indukcí konstruujeme grafy G_n se skóre obsahujícím čísla $0,1,\ldots,n-2$, v němž se opakuje $\lfloor (n-1)/2 \rfloor$: G_2 jsou 2 izolované vrcholy, G_{n+1} vznikne přidáním izolovaného vrcholu k doplňku grafu G_n (*doplněk* grafu $G = (V,E)$ je graf $(V, \binom{V}{2} \setminus E)$).

3.4.8. Uvažte obarvení s nejmenším možným počtem jednobarevných hran.

3.4.9. Uvažte cestu maximální možné délky v G. Její koncový vrchol je spojen aspoň se dvěma dalšími vrcholy této cesty; to dá hledaný podgraf.

3.4.10. Zřejmě musí platit $k \leq n-1$, kn sudé. To je taky postačující; např. $V = \{0, \ldots, n-1\}$, $E = \{\{i,j\}; i - j (\mathrm{mod}\, n) \in S\}$, kde $S = \{1, -1, 2, -2, \ldots, k/2, -k/2\}$ pro k sudé, $S = \{1, -1, \ldots, (k-1)/2, -(k-1)/2, n/2\}$ pro k liché, n sudé.

3.4.13. Stačí ukázat, že je-li $\{u,v\} \in E(G)$, pak $\deg_G(u) = \deg_G(v)$. Buď U množina všech sousedů u mimo v, a V množina všech sousedů v mimo u. Každý vrchol z U musí mít 4 sousedy ve V, a každý vrchol z V má 4 sousedy v U. Proto $|U| = |V|$ (počítání hran mezi U a V dvěma způsoby).

3.4.14. Sporem, nechť žádné 2 takové vrcholy nejsou. Pro libovolný vrchol v se podíváme na podgraf indukovaný jeho sousedy; v něm musí být všechny stupně liché, a proto má v sudý stupeň. Počítejme sledy délky 2 začínající ve v. Celkem je jich sudý počet. Přitom sudý počet se jich vrací zpátky do v, ale každý jiný vrchol dosáhneme lichým počtem sledů, proto je počet vrcholů různých od v sudý — spor.

3.4.15(b). Uvažte trojúhelník xyz (existující podle (a)), a vyjádřete pomocí principu inkluze a exkluze počet vrcholů spojených aspoň s jedním z vrcholů x, y, z.

3.5.5(a). Při pevné množině vrcholů postupujte indukcí podle počtu hran G; ukažte, že je-li $E \neq \emptyset$, má G kružnici, odeberte ji.

3.8.2(b). Např. v K_{n+1} podrozdělte každou hranu.

3.8.2(c). Vezměte strom T, v němž každý vrchol mimo listů má stupeň n, a kde všechny listy mají od kořene vzdálenost n (úplný n-ární strom). Udělejte jeho kopii T_1, a ztotožněte každý list s jeho vzorem v T.

3.8.3(a). Ano.

3.8.3(b). Ano.

3.8.4. Např. indukcí pomocí lemmatu o vytváření 2-souvislých grafů přilepováním uší.

4.1.5. Máme $2n-2 = 2|E(T)| = \sum_{v \in V(T)} \deg_T(v) = \sum_{i=1}^{n-1} i p_i$. Úpravou plyne žádaná rovnost.

4.1.6. (ii)⇒(ii): indukcí podle n; buď $n \geq 3$, $(d_1, \ldots, d_n)$ splňují (ii); pak existuje nějaké $d_i = 1$ a nějaké $d_j > 1$ (např. $d_n = 1$, $d_{n-1} > 1$). Aplikujeme indukční předpoklad na $(d_1, \ldots, d_{n-2}, d_{n-1} - 1)$ a připojíme koncový vrchol za vrchol číslo $n-1$.

4.2.4. Rozdělte posloupnosti do dvou skupin: začínající 0 a začínající 1, a obě skupiny setřiďte rekurzivně. Při skutečném programování algoritmu se posloupnosti ve skutečnosti nepřemisťují, pracuje se jen s vhodnými ukazateli na ně.

4.2.5. Kód stromu na n vrcholech má délku $2n$. Existuje tedy nejvýš 4^n kódů.

4.2.6. Indukcí podle $|V|$.

4.3.1. Dokažte, že jeden vrchol se přeznačuje nejvýš $(\log_2 n)$-krát.

4.3.2. Graf je zadán seznamy S_v hran vycházejících z jednotlivých vrcholů $v \in V(G)$. Udržujte dvousměrný seznam N hran, které jdou mezi množinou V_i a jejím doplňkem. Přitom každá hrana v S_v má navíc ukazatel na svůj případný výskyt v N. Je-li nově přidaný vrchol y_i stupně d, lze všechny seznamy aktualizovat v čase $O(d)$.

4.4.1. Důkaz správnosti Kruskalova algoritmu nevyužívá nikde nezápornosti ohodnocení w. Proto jej lze použít na ohodnocení $-w$, a tím se najde maximální kostra.

4.4.7(a). Pro vrchol v stupně ≥ 7 existují hrany $\{v, u_1\}$ a $\{v, u_2\}$ svírající úhel $< 60°$. Jednu z nich lze nahradit hranou $\{u_1, u_2\}$.

4.4.8. Jedno řešení: rozdělte jednotkový čtverec na síť $\sqrt{n} \times \sqrt{n}$ čtverečků. Očíslujte čtverečky $1, 2, \ldots, n$ tak, že po sobě jdoucí čtverečky vždy sousedí (např. jako když se oře pole). Spojte cestou nejdřív všechny body z V ve čtverečku 1, potom ve čtverečku 2, atd. Jiné řešení: Dokažte, že existují 2 body se vzdáleností $O(n^{-1/2})$. Vymažte jeden z nich, sestrojte kostru indukcí, a připojte vymazaný bod.

4.4.9(a). Buď E_M maximální párování, E_H párování nalezené hladovým algoritmem, a každé hraně $e \in E_M$ přiřaďme první z hran E_H, která ji protíná. Každá $\check{e} \in E_H$ je tak přiřazena nejvýš 2 hranám $e_1, e_2 \in E_M$, $w(e_1), w(e_2) \leq w(\check{e})$.

4.4.10(b). Buďte $e_1, \ldots, e_k$ hrany vybrané hladovým algoritmem, $\check{e}_1, \ldots, \check{e}_t$ hrany nějakého optimálního pokrytí, a buď $k_1 = |\{i;\ e_i \cap (e_1 \cup \ldots \cup e_{i-1}) = \emptyset\}|$, a podobně $t_1 = |\{i;\ \check{e}_i \cap (\check{e}_1 \cup \ldots \cup \check{e}_{i-1}) = \emptyset\}|$. Máme $|V| = k + k_1 = t + t_1$. Klíčové pozorování: v krocích hladového algoritmu pro $i > k_1$ už musel být aspoň 1 bod z každé hrany $\check{e}_j$ přispívající k t_1 pokryt, takže $k_1 \geq t_1/2$. Odtud $k = t + t_1 - k_1 \leq t + t_1/2 \leq \frac{3}{2}t$.

4.4.11. Buď $V = \{1, 2, \ldots, 2^{k+2} - 2\} \cup \{a_1, a_2, b_1, b_2, \ldots, b_k\}$. Vrchol a_1 je spojen s $1, 3, 5, \ldots$, a_2 s $2, 4, 6, \ldots$, b_i s $2^i - 1, 2^i, \ldots, 2^{i+1} - 2$, a a_1, a_2 jsou navíc spojeny se všemi b_i. Hladový algoritmus vybere všechny b_i, optimální je $\{a_1, a_2\}$.

4.5.5(a). Ukažte, že každá komponenta po i-tém kroku má $\geq 2^i$ vrcholů.

4.5.5(b). Pro každou komponentu udržujte seznam hran z ní vycházejících. V každé fázi můžete každý seznam projít a najít v něm hranu minimální váhy.

5.1.3. Indukcí podle počtu hran. Uvažme v nakreslení nějaký vrchol v stupně aspoň 4, a 2 sousední hrany z něj vycházející, a pokud možno zasahující do různých komponent grafu $G - v$. Nahraďte je jedinou hranou spojující jejich druhé konce. (Je výhodné připustit i grafy s násobnými hranami.)

5.2.3(a). Zvolme nějaký kruh D takový, že $k \cap D$ je úsečka. Z každého bodu $\mathbf{R}^2 \setminus k$ můžeme dojít lomenicí, která jde těsně podél k, do nějakého vnitřního bodu D. Přitom $D \setminus k$ má nejvýš 2 třídy ekvivalence.

5.2.8. Na každé pětici vrcholů je indukován K_5, a nějaké 2 jeho hrany se musí protínat; tím dostáváme $\binom{n}{5}$ protínajících se dvojic. Přitom dané 2 protínající se hrany se účastní v $n-4$ pěticích, takže celkem je aspoň $\binom{n}{5}/(n-4)$ křížících se dvojic.

5.3.4. Dokažte, že do stěny s ≥ 6 stranami lze přidat diagonálu. Přitom je třeba dávat pozor, aby nevznikl trojúhelník; spojované vrcholy nesmí být spojeny hranou (vnějškem kružnice) ani mít společného souseda — je asi potřeba rozebrat několik případů.

5.3.5(a). Řekneme, že puntík, z něhož vychází $k \leq 3$ hran, přispívá $3 - k$ stupni volnosti. Na začátku je $3n$ stupňů volnosti, na konci aspoň 1, každým tahem 1 ubude.

5.3.5(c). Ukažte, že na konci hry čouhá do každé stěny přesně jedno rameno křížku (nevyužité). Počet volných ramen se libovolnám tahem zachovává, takže na konci je $4n$ stěn. Přitom $n-1$ tahů spojí dvě komponentý do nové, a zbývající tahy každý zvyšuje počet stěn o 1. Na začátku byla 1 stěna, celkem tedy $5n - 2$ tahů.

5.3.6(a). Platí $e = v + s - 1$ — dokazujte indukcí dle n, při vkládání nové přímky rozlišujte nově vytvořené průsečíky a již existující průsečíky.

5.3.6(c). Z (b) odvoďte $e \geq 3s - n$. Je-li d_i počet přímek procházejících i-tým vrcholem, spočítá se $\sum d_i = e - n$ (každá hrana přispěje dvěma konci až na $2n$ nekonečných hran). Dosazením za s z (a) vyjde $\sum d_i \leq 3v - 3$.

5.3.7. Předpokládejme souvislost. Nechť červenomodrý roh je dvojice (S, v), kde S je stěna a v vrchol na její hranici takový, že obcházíme-li hranici stěny S po směru hodinových ručiček (pro neomezenou stěnu proti směru), vrcholu v předchází červená hrana a následuje po něm modrá hrana. Počítáním dvěma způsoby a pomocí Eulerova vzorce ukažte, že existuje vrchol s nejvýš jedním červenomordým rohem.

5.4.3. Indukcí podle počtu vrcholů.

5.4.4. Podgraf vnějškově rovinného grafu je zase vnějškově rovinný. Podle cvičení 3 stačí tedy ukázat, že vnějškově rovinný graf má vždycky vrchol stupně ≤ 2. To jde z Eulerova vzorce s využitím toho, že 1 stěna sousedí s aspoň n hranami.

5.4.5. Ukažte, že existuje vrchol stupně ≤ 3.

5.4.6(a). Ukažte, že duální graf je bipartitní (neobsahuje lichou kružnici).

5.4.6(b). Obarvěte stěny 2 barvami. Počet hran se dá počítat jako součet obvodů stěn jedné barvy, i jako součet obvodů stěn druhé barvy. Jeden způsob počítání ale dá číslo dělitelné 3, druhý ne.

6.1.1. Definujte graf na stěnách přesně jako v důkazu Spernerova lemmatu.

6.1.2(a). Napodobte důkaz rovinné verze. Spojujte hranou malé čtyřstěny přes stěnu očíslovanou 1,2,3, a užijte rovinné verze na důkaz toho, že stupeň vnějšího vrcholu je lichý.

6.1.3. Názorné řešení — představte si 2 turisty v týž den, jeden vystupuje, druhý sestupuje.

6.1.4(b). Zařiďte, aby z a do c bylo podstatně dále než z b do d.

6.1.4(c). Sporem. Kdyby měl B vyhrávající strategii, A bude ignorovat svůj první tah, tím se octne v situaci B (jedno zabrané políčko navíc z prvního tahu může jen pomoci) a použije jeho vyhrávající strategii.

6.2.4. Nezávislý množinový systém $\mathcal{M}$ splňuje $\sum_{M\in\mathcal{M}} \binom{n}{|M|}^{-1} = 1$, proto množiny největšího systému mají všechny velikost $\lfloor n/2\rfloor$ nebo $\lceil n/2\rceil$ (pro n sudé jsme tím hotovi). Ukažte, že obsahuje-li $\mathcal{M}$ t množin velikosti $\lfloor n/2\rfloor$ a $0 < t < \binom{n}{\lfloor n/2\rfloor}$, potom má $< \binom{n}{\lfloor n/2\rfloor} - t$ množin velikosti $\lceil n/2\rceil$.

6.2.5. Pro automorfismus h definujte zobrazení $f : X \to X$, $f(x)$ je y takové, že $h(\{x\}) = \{y\}$. Ukažte $h = f^{\#}$ (z toho je vidět, že je $n!$ automorfismů).

6.2.7. Aplikujte Spernerovu větu na množinový systém $\{\{i;\ \varepsilon_i = 1\};\ \sum \varepsilon_i a_i \in (-1, 1)\}$.

6.2.8. Buď $n = p_1 p_2 \dots p_n$ rozklad na prvočinitele. Děliteli $d = p_{i_1} p_{i_2} \dots p_{i_k}$ přiřaďte podmnožinu $M_d = \{i_1, \dots, i_k\} \subseteq \{1, 2, \dots, n\}$; pak $d_1 | d_2 \Leftrightarrow M_{d_1} \subseteq M_{d_2}$. Užijte Spernerovy věty.

6.2.9(a). Indukcí podle r. Jako první antiřetězec vezměte množinu všech minimálních prvků X, ukažte že jeho odebráním klesne r o 1.

6.2.9(b). Indkcí dle $|X|$. Nechť x je minimální prvek a y maximální prvek s $x < y$ (neexistují-li, je X antiřetězec). Buď A nejdelší antiřetězec

v $X \setminus \{x, y\}$. Pokud $|A| < a$, použijeme indukční předpoklad. Jinak rozložíme množiny $\{t \in X;\ \exists a \in A : t \leq a\}$ a $\{t \in X;\ \exists a \in A : t \geq a\}$ každou na a řetězců a tyto řetězce napojíme přes prvky z A.

6.2.10. Definujte $i \preceq j$ právě když $i \leq j$ a $a_i < a_j$. Řetězec v $(\{1, \ldots, n\}, \preceq)$ definuje rostoucí podposloupnost, antiřetězec klesající podposloupnost.

6.3.1. Napodobte důkaz pro $K_{2,2}$, jediný rozdíl je, že jeden vrchol v přispěje do M nejvýš $t - 1$ prvky.

6.3.2. Uvažte graf incidence s množinou vrcholů $X \cup \{1, 2, \ldots, n\}$, kde vrcholy $x \in X$ a $i \in \{1, 2, \ldots, n\}$ jsou spojeny právě když $x \in S_i$. Ten neobsahuje $K_{2,2}$, tedy má $O(n^{3/2})$ hran.

6.3.6. Uvažte funkci $f(x)$, rovnou 0 pro $x \leq 2$ a $x(x-1)(x-2)$ pro $x > 2$, ta je konvexní.

7.1.1. Jako pro neisomorfní grafy v 3.1; využijte odhad $n!$ z věty 2.4.4.

7.1.2. Počítejte kostry, obsahující danou hranu; tento počet je pro všechny hrany stejný, přitom každá kostra obsahuje $n - 1$ hran.

7.1.3. Z každé kostry K_n můžeme $n - 1$ způsoby vyjmout hranu, tím dostaneme dvojici stromů. Obráceně, z kostry na k-bodové podmnožině a kostry na doplňku této podmnožiny můžeme udělat kostru celého K_n přidáním hrany, právě $k(n-k)$ způsoby.

7.1.4. Vyjde $n^{m-1} m^{n-1}$, nejsnáze možná pomocí determinantu.

7.2.1(a). Pro liché n 0. Pro n sudé je $n/2 + 1$ listů a $n/2 - 1$ vrcholů stupně 3 (indukcí). Sčítáme tedy výraz $(n-2)!/2^{n/2-1}$ přes všechny volby $(d_1, \ldots, d_n)$, $d_i \in \{1, 3\}$, $\sum d_i = 2n - 2$. Substitucí $k_i = (d_i - 1)/2$ vidíme, že počet sčítanců je roven počtu $(n/2-1)$-prvkových podmnožin n-prvkové množiny, takže odpověď je $(n-2)!\binom{n}{n/2-1} 2^{-n/2+1}$.

7.2.1(b). Asi nejlépe přes vytvořující funkce (viz kapitola 10). Odpověď je koeficient při x^{2n-2} ve výrazu $(n-2)!(x + x^2 + x^3/2)^n$, který se najde podle multinomické věty (podobně se dá řešit i (a)).

7.3.3. Představte si, že na grafu zobrazení vyšlete z bodu i dva chodce — jeden projde jednu šipku za minutu, druhý dvě šipky. Rozmyslete, kdy se budou potkávat.

7.5.1(a). Q má nulový součet řádek.

7.5.1(b). $\kappa(G) > 0$, proto $\det Q_{11} \neq 0$ podle věty o počtu koster.

7.5.1(c). Součet řádků matice Q přes každou komponentu je nulový, tedy prostor generovaný řádky má dimenzi $< n - 1$.

7.5.1(d). Jádro obsahuje $(1, 1, \ldots, 1)$, protože součet řádků je nulový, a podle (b) je jádro Q jednodimenzionální.

7.5.1(e). Součin i-tého řádku Q a i-tého sloupce Q^* je rozvoj $\det Q$ podle i-tého řádku, užijte $\det Q = 0$. Ostatní pozice součinu jsou rozvojem determinantu matice, v níž se 1 řádek opakuje dvakrát, tedy také 0.

7.5.4. Na jednu implikaci stačí spočítat determinant matice incidence pro kružnici liché délky (protože každý ne-bipartitní graf obsahuje kružnici liché délky). Pro bipartitní G se požadovaná vlastnost M dá dokázat indukcí, podobně jako jsme dokazovali lemma 7.5.3.

8.1.1. Viz cvičení 3.

8.1.2. Ukažte, že 2 body z $P_1 \setminus P_2$ a 2 body z $P_2 \setminus P_1$ tvoří dohromady konfiguraci $\check{C}$ jako v (P0).

8.1.3. Jedna možnost je $\mathcal{P} = \{X\}$, další je $\mathcal{P} = \{X \setminus \{a\}\} \cup \{\{a, x\};\ x \in X \setminus \{a\}\}$, kde $a \in X$ je nějaký bod. To jsou jediné množnosti kde všechny přímky jsou aspoň dvoubodové (při důkazu se využije cvičení 2). Pro obě tyto možnosti můžeme k $\mathcal{P}$ dále přidat libovolný soubor jednobodových množin.

8.1.5(a). Jedna dvojice je nejvýš v jedné množině. Jedna množina pokrývá $\binom{n+1}{2}$ dvojic, celkový počet pokrytých dvojic vyjde shodný jako počet všech dvojic, každá dvojice je tedy pokryta nějakou množinou.

8.1.5(b). Kdyby jich bylo více, mají dohromady více než $n^2 + n + 1$ bodů.

8.1.5(c). Počítejte dvěma způsoby dvojice (x, P), $x \in P$. Sčítáním napřed přes množiny je vidět, že jich je $(n+1)|\mathcal{P}|$, kdyby nějaký bod byl v méně než $n + 1$ množinách, vzhledem k (b) dostaneme méně než $(n + 1)|X|$ dvojic.

8.1.5(d). Uvažme nějakou množinu P, v každém z jejích $n + 1$ bodů ji protíná n dalších přímek, celkem $n^2 + n + 1$ přímek, žádná neprotínající P už nezbývá.

8.3.4(a). K daným t ortogonálním latinským čtvercům můžeme přidat jeden čtverec mající v i-tém řádku všude i, a jeden čtverec mající v i-tém sloupci všude i.

8.3.4(b). Aby byl osvobozený čtverec ortogonální k jinému, musí obsahojat každé $i \in \{1, 2, \ldots, n\}$ právě $n\times$. Permutujte políčka daných $t+2$ ortogonálních osvobozených čtverců (všechny čtverce touž permutací) tak, aby první čtverec měl v i-tém řádku samá i, $i = 1, \ldots, n$. Potom ještě permutujte uvnitř každého řádku (zase všechny čtverce stejně) tak, aby druhý čtverec měl v j-tém sloupci samá j. Ověřte, že ortogonalita se neporušila a zbývajících t čtverců je latinských.

8.3.6. Hledaný počet je $n!\times$ počet permutací bez pevného bodu.

9.1.1. Kódujte možné průjezdy vagónů kolejištěm, např. „vagón z A n I, vagón z A na C, vagón z C na II,...“ (stačí vždy uvést z které kolej na kterou se v daném kroku přesunuje, který vagón je jasné z momentáln pozice). Existuje tedy nanejvýš C^n možných kódů (pro vhodnou konstant C), takže vznikne nejvýš C^n různých pořadí na koleji B, což je pro velká méně než $n!$.

9.1.2(a). Funkce n proměnných definuje dvě funkce $n-1$ proměnných, jedn pro $x_n = 0$ a jednu pro $x_n = 1$. Lze postupovat např. indukcí podle n.

9.1.4. Každé vážení má 3 možné výsledky, 3 váženími lze tedy rozlišit ma ximálně 3^3 možností.

9.2.2. Pro nesouvislý graf existuje vlastní podmnožina A vrcholů taková, ž mezi A a jejím doplňkem nejsou hrany. Spočtěte pravděpodobnost tohot jevu pro pevnou A, pak sčítejte přes všechny A.

9.2.5(b). Nahradíme-li některé z A_i jejich doplňky, máme pořád soubo nezávislých jevů, a průnik těchto jevů má nenulovou pravděpodobnost. Takt se vyrobí 2^n disjunktních neprázdných jevů.

9.2.7. Je to $\frac{1}{3}$ (nechť děti jsou A a B; 3 stejně pravděpodobné možné případy A=kluk, B=kluk; A=kluk, B=holka A=holka, B=kluk).

9.3.2. Ukažte $0 \leq \mathbf{E}((f - \mathbf{E}f)^2) = \mathbf{E}(f^2) - (\mathbf{E}f)^2$.

9.3.3. Použijte indikátorů; nechť A_i je jev "$\pi(i) = i$". Vyjde $\mathbf{E}f = 1$.

9.3.4(a). Definujte X_i jako indikátor jevu „jednička je v cyklu délky i“ ukažte že $P(X_i = 1) = \frac{1}{n}$.

9.3.4(b). Hledaný počet je roven $\sum_{i,j=1}^{n} X_{ij}$, kde X_{ij} je indikátor „j je cyklu délky i“.

9.3.5. Počítejte raději rozhraní mezi sériemi. Pravděpodobnost, že na daném místě bude rozhraní, je $\frac{1}{2}$.

9.4.4. Na úrovni 0 jsou jen 2 špice. Počítejte dvěma způsoby střední hodnot počtu špic na úrovni 0 pro náhodnou podmnožinu $R \subseteq L$.

10.1.3. Abychom dostali člen $x_1^{k_1} \dots x_m^{k_m}$ při roznásobování n závorek, mu síme zvolit k_1 závorek z nichž vybereme x_1, ..., k_m závorek z nichž vyberem x_m. Počet možností je právě multinomický koeficient.

10.1.5. Vyjděte z rovnosti $(1-x)^n(1+x)^n = (1-x^2)^n$.

10.2.6(a). Vytvořující funkce je $1/((1-x)(1-x^2)(1-x^5))$.

10.2.7(d). Výsledek: $(-1)^m\binom{n-1}{m}$.

10.2.9(a). Pro spojitost potřebujeme dokázat, že pro $x_0 \in [0, \rho)$ $\lim_{x \to x_0} |a(x) - a(x_0)| = 0$. Užijte $|x_0^i - x^i| \leq |x_0 - x|(x_0^{i-1} + x_0^{i-2}x + \dots + x^{i-1}) \leq |x - x_0| i m^{i-1}$, kde $m = \max(x, x_0)$.

10.2.9(c). Třeba $a_i = 1/i^2$.

10.2.10(a). Napřed indukcí ukažte, že každá derivace funkce f v bodě $x \neq 0$ je tvaru $R(x)e^{-1/x^2}$, kde $R(x)$ je podíl dvou mnohočlenů. Pak indukcí odvoďte podle definice derivace, že všechny derivace v 0 jsou 0.

10.2.10(b). Koeficienty mocninné řady se dají vyjádřit pomocí derivací, musely by tedy být všechny nulové.

10.3.1. Nechť a_n, resp.b_n je počet takových posloupností končících 1, resp. 0. Odvoďte rekurentní vzorce pro a_n a b_n. Vyjdou Fibonacciho čísla.

10.3.4. Uvažte posloupnost $b_n = \log_2 a_n$.

10.3.6. Označme u_n počet takových posloupností začínajících a nebo b, a v_n počet takových posloupností začínajících c nebo d. Vyjdou rekurence $u_n = u_{n-1} + 2v_{n-1}$, $v_n = 2u_{n-1} + 2v_{n-1}$. Napište odpovídající rovnice pro vytvořující funkce $u(x)$ a $v(x)$, vyřešte a spočítejte koeficienty. Vyjde $u_n + v_n = ((\sqrt{17}+1)/4\sqrt{17})((3+\sqrt{17})/2)^{n+1} + ((\sqrt{17}-1)/4\sqrt{17})((3-\sqrt{17})/2)^{n+1}$.

10.3.8(b). Ukažte, že posloupnosti, jejichž j-tý člen je 1 a ostatní členy mezi $y_0, \ldots, y_{k-1}$ jsou nulové, pro $j = 0, 1, \ldots, k-1$ tvoří bázi.

10.3.8(c). Aby se ukázala lineární nezávislost, stačí např. dokázat, že vektory tvořené prvními k členy jsou lineárně nezávislé. Na to se dá použít kritérium pomocí determinantu, a vede to na tzv. Vandermondův determinant probíraný v lineární algebře.

10.3.8(e). Asi nejjednodušší metoda zde je pomocí rychlosti růstu jednotlivých posloupností. Kdyby byly posloupnosti lineárně závislé, šlo by nejrychleji rostoucí z nich vyjádřit jako lineární kombinaci pomaleji rostoucích, což není možné. Potíž v tomto přístupu nastane, má-li několik různých komplexních kořenů stejnou absolutní hodnotu; tento případ se dá řešit zvlášť např. pomocí determinantu jako v návodu k (c).

10.4.2(a). $\binom{2n}{n}$.

10.4.2(b). Cesta, která nikdy nejde pod diagonálu, kóduje binární strom s n vrcholy např. takto: rozdělte cestu na 2 části v bodě, kde poprvé dosáhne diagonály. Od první části odeberte první a poslední úsek, druhou nechte beze změny. Obě části pak rekurzivně kódují levý a pravý podstrom (přitom cesta s 0 úseky kóduje prázdný strom.

10.4.2(c). Zaveďme souřadnice: A je $(0,0)$, B je (n,n). Nastavíme šachovnici o jeden sloupec vpravo. Ukažte, že cesty, které *zasahují* pod diagonálu, se dají vzájemně jednoznačně přiřadit cestám z A do bodu $B_1 = (n+1, n-1)$ — dojděte po cestě až na konec prvního úseku po prvním překročení diagonály, a zbytek cesty překlopte symetricky podle přímky $y = x - 1$.

10.4.3. Najděte korespondenci s cestami nejdoucími pod diagonálu.

10.4.6(b). $c_{2n+1} = b_n$; bijekce mezi pěstovanými stromy jako ve cvičení a binárními stromy uvažovanými v textu se dostane smazáním všech koncových vrcholů pěstovaného stromu.

10.4.7(a). Vyjde $t_n = b_{n-1}$.

10.4.8. Starý strom je buď samotný kořen, nebo vznikne připojením nějakých k pěstovaných stromů, každý aspoň se dvěma vrcholy, ke kořeni. Odtud $s(x) = x + x/(1 - t(x) + x)$.

10.6.1(a). Buď a_i počet cest začínajících v 1 a vstupujících poprvé do 0 po i tazích. Hledaná pravděpodobnost je $a(\frac{1}{2})$. Odvoďte vztah $a(x) = x + xa(x)^2$. Hodnotu a_i lze též explicitně spočítat, např. pomocí Catalanových čísel.

11.1.1(b). Vpodstatě duální úloha ke cvičení 8.1.5.

11.2.2. Každý řádek matice AB je lineární kombinací řádků matice B (koeficienty jsou dány odpovídajícím řádkem A), proto $r(AB) \leq r(B)$.

11.2.3. Regularita čtvercové matice znamená totéž jako nenulovost determinantu, a definice determinantu nezávisí na tom, nad jakým tělesem pracujeme. Hodnost se dá vyjádřit pomocí existence regulárních podmatic.

11.2.4(a). Kdyby měla hodnost $< n$, má soustava $Bx = 0$ nenulové řešení, a takové řešení dá $x^T Bx = 0$.

11.2.4(b). B je součtem diagonální matice D s kladnými prvky na diagonále a matice L ze samých $\lambda > 0$. Pro každé nenulové $x \in \mathbf{R}^v$ platí $x^T Dx > 0$ a $x^T Lx \geq 0$.

11.2.6(a). Je-li A matice incidence systému, potom $A^T A$ je součtem matice Q ze samých q a diagonální matice D, jejíž diagonální prvky jsou $|C_i| - q > 0$ (za předpokladu $|C_i| > q$ který můžeme udělat). Proto je $A^T A$ pozitivně definitní a tudíž regulární.

11.2.6(b). V situaci Fisherovy nerovnosti, uvažte množinový systém duální k $(V, \mathcal{B})$, a aplikujte na něj část (a).

11.3.1(b). Dokažte indukcí podle k, že je-li E sjednocení množin hran k bipartitních grafů na množině vrcholů $\{1, 2, \ldots, n\}$, potom existuje podmnožina aspoň $\lceil n/2^k \rceil$ vrcholů, na níž není žádná hrana z E.

Kapitoly z diskrétní matematiky

prof. RNDr. Jiří Matoušek, DrSc.
prof. RNDr. Jaroslav Nešetřil, DrSc.

Vydala Univerzita Karlova v Praze
Nakladatelství Karolinum, Ovocný trh 3
116 36 Praha 1
Prorektor-editor prof. MUDr. Pavel Klener, DrSc.
Obálku navrhla Kamila Schüllerová s použitím
obrazu Jiřího Načeradského a Jaroslava Nešetřila
Z předloh připravených autory v systému LaTeX
vytiskly Tiskárny Havlíčkův Brod, a.s.
Vychází s podporou centra DIMATIA při MFF UK

Dotisk druhého, opraveného vydání
Praha 2002
ISBN 80-246-0084-6