Šestnáct miniatur

Matematické aplikace lineární algebry

Verze 14/VIII/2006

Úvod

Zájemcům se tímto předkládá sbírka aplikací lineární algebry v teoretické informatice, kombinatorice a geometrii. Většina z nich je matematických, na dokazování vět, a několik se týká umného způsobu výpočtů, tedy algoritmů. Lineárně algebraické metody se v nich často objeví nečekaně – ne jako třeba v inženýrském problému, kde se má vyřešit soustava lineárních rovnic a použití lineární algebry je nasnadě.

Výklad je stručný a je určen jednak pro přednášející či cvičící, kteří by chtěli některým z níže uvedených příkladů zpestřit výuku, a jednak pro studenty, kteří mají zájem o pěkné matematické myšlenky i za cenu vlastního přemýšlení. Jednotlivé oddíly lze číst nezávisle, a seřadil jsem je podle svého subjektivního hodnocení zhruba od nejpřístupnějších k nejnáročnějším. Po několika oddílech může čtenář vysledovat jistá společná schémata a tendence v uvedených důkazech, o nichž by se dalo všelijak pojednávat, ale rozhodl jsem se žádné obecné výklady o lineárně algebraických metodách nepřidávat.

Nic v tomto spisku není původní a většina příkladů je poměrně dobře známa a publikována na mnoha místech. Abych text nezahltil citacemi, neuvádím původní prameny. Kdo by je chtěl vystopovat, může se podívat do učebnic zmíněných na konci, případně se na mne obrátit – u některých výsledků bych musel po původu zapátrat.

Uvítám sdělení o chybách, náměty na vylepšení výkladu a případně i návrhy na další vhodné kousky do sbírky.

Obsah

1 Rychlý výpočet Fibonacciho čísel

Fibonacciho čísla $F_0, F_1, F_2, \ldots$ jsou definována vztahy $F_0 = 0$, $F_1 = 1$, a $F_{n+2} = F_{n+1} + F_n$ pro všechna $n = 0, 1, 2, \ldots$. Číslo F_n se zjevně dá spočítat řádově n aritmetickými operacemi.

Následujícím trikem jej můžeme spočítat mnohem rychleji, pomocí řádově $\log n$ aritmetických operací. Označme

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

Potom platí

$$\begin{pmatrix} F_{n+2} \\ F_{n+1} \end{pmatrix} = M \begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix},$$

a tudíž

$$\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = M^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

(využíváme asociativity násobení matic). Pro $n = 2^k$ můžeme mocninu M^n spočítat opakovaným umocňováním na druhou, pomocí k operací násobení matic typu 2×2. Obecné n zapíšeme ve dvojkové soustavě, čímž ho vyjádříme ve tvaru $n = 2^{k_1} + 2^{k_2} + \cdots + 2^{k_t}$, $k_1 < k_2 < \cdots < k_t$, a mocninu M^n pak vypočteme ve tvaru $M^n = M^{2^{k_1}} M^{2^{k_2}} \cdots M^{2^{k_t}}$, na což stačí nejvýš $2k_t \leq 2\log_2 n$ násobení matic 2×2.

Poznámky. Podobného triku můžeme použít pro posloupnosti $(y_0, y_1, y_2, \ldots)$ dané rekurencemi tvaru $y_{n+k} = a_{k-1}y_{n+k-1} + \cdots + a_0 y_n$, kde k a $a_0, a_1, \ldots, a_{k-1}$ jsou konstanty.

Při výpočtu se musí dát pozor na to, že Fibonacciho čísla rostou velmi rychle. Ukazuje se, že desítkový zápis F_n má řádově n číslic, a tedy musíme použít vhodnou násobnou aritmetiku. Aritmetické operace pak budou poměrně pomalé.

2 Vzorec pro Fibonacciho čísla

Najdeme vzorec pro n-té Fibonacciho číslo F_n. Uvažme vektorový prostor všech nekonečných posloupností $(u_0, u_1, u_2, \ldots)$ reálných čísel, se sčítáním a násobením reálným číslem po složkách. V něm definujeme podprostor W všech posloupností splňujících vztah $u_{n+2} = u_{n+1} + u_n$ pro všechna $n = 0, 1, \ldots$. Každá volba prvních dvou členů u_0 a u_1 jednoznačně určuje posloupnost z W, a proto $\dim(W) = 2$. (Podrobněji, například posloupnosti začínající $(0, 1, 1, 2, 3, \ldots)$ a $(1, 0, 1, 1, 2 \ldots)$ tvoří bázi W.)

Teď najdeme šikovnou bázi prostoru W, jejíž prvky jsou dány jednoduchým vzorečkem. „Vnuknutí“: hledejme posloupnost $u \in W$ tvaru $u_n = \tau^n$ pro vhodné číslo τ. Vyjde kvadratická rovnice $\tau^2 = \tau + 1$ se dvěma různými kořeny $\tau_{1,2} = (1 \pm \sqrt{5})/2$. Jak se snadno ověří, posloupnosti $(\tau_1^0, \tau_1^1, \tau_1^2, \ldots)$ a $(\tau_2^0, \tau_2^1, \tau_2^2, \ldots)$ jsou lineárně nezávislé (stačí se podívat na první dva členy), a tedy tvoří bázi W. Fibonacciho čísla vyjádříme v této bázi (použitím prvních dvou členů). Vyjde

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right].$$

Podobně to funguje i pro jiné rekurence tvaru $y_{n+k} = a_{k-1}y_{n+k-1} + \cdots + a_0 y_n$, ale mohou se vyskytnout potíže, třeba pro $y_{n+2} = 2y_{n+1} - y_n$. Pak se musí hledat jiná báze, což zde nebudeme dělat.

3 Kluby města Lišákova

Ve městě žije n občanů, kteří jsou sdruženi v m klubech. Podle vyhlášky městské rady má každý klub *lichý* počet členů, zatímco pro každé dva kluby musí být počet společných členů *sudý*.

Věta. *V této situaci je nutně $m \le n$, tj. klubů není víc než občanů.*

Důkaz. Občany označme $1, 2, \ldots, n$ a kluby $K_1, K_2, \ldots, K_m$. Definujeme matici A typu $m \times n$, kde $a_{ij} = 1$ pokud $j \in K_i$ a $a_{ij} = 0$ jinak (kluby = řádky). Uvažujeme A nad dvouprvkovým tělesem GF(2). Hodnost A je nejvýš n (jasné). Podle vyhlášky městské rady platí $AA^T = I_m$, a protože hodnost součinu matic je nejvýš rovna minimu z hodností činitelů, je hodnost A aspoň m.

Poznámka. Podobnou metodou byla dokázána řada důležitých odhadů pro velikosti různých množinových systémů. Například tzv. Fisherova nerovnost (ve zobecněné podobě) říká, že jsou-li $C_1, C_2, \ldots, C_m$ podmnožiny nějaké n-prvkové množiny a všechny průniky $C_i \cap C_j$, $i \ne j$, mají tutéž velikost, potom $n \ge m$.

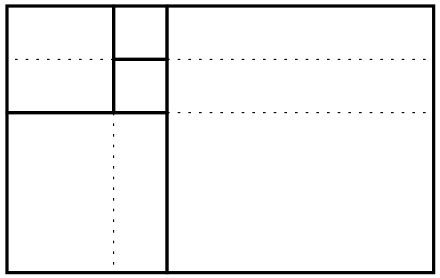
4 Dláždění obdélníka čtverci

Věta. *Obdélník R o stranách 1 a x, kde x je iracionální, nelze „vydláždit“ konečně mnoha čtverci (tak, aby celý R byl pokryt a žádné dva čtverce neměly společný vnitřní bod).*

Důkaz. Pro spor nechť existuje dláždění sestávající ze čtverců $Q_1, Q_2, \ldots, Q_n$, a nechť s_i je délka strany čtverce Q_i. Uvážíme vektorový podprostor V prostoru $\mathbb{R}$ nad $\mathbb{Q}$ generovaný čísly $s_1, s_2, \ldots, s_n$. Definujeme lineární zobrazení $f\colon V \to \mathbb{R}$ tak, aby $f(1) = 1$ a $f(x) = -1$ (a jinak libovolně). To lze, poněvadž 1 a x jsou lineárně nezávislé nad $\mathbb{Q}$.

Pro obdélník A o stranách a a b, $a, b \in V$, definujeme $v(A) = f(a)f(b)$. Tvrdíme, že je-li R vydlážděn čtverci $Q_1, Q_2, \ldots, Q_n$, potom musí platit $v(R) = \sum_{i=1}^n v(Q_i)$. To vede ke sporu, protože $v(R) = -1$, zatímco $v(Q_i) = f(s_i)^2 \ge 0$.

Abychom nahlédli uvedené tvrzení, protáhneme každou ze stran každého čtverce Q_i z hypotetického dláždění napříč celým R, jak je naznačeno na obrázku:



Tím se R rozpadne na malé obdélníčky, a je snadno vidět, že $v(R)$ je rovno součtu $v(O)$ přes všechny tyto malé obdélníčky O. Podobně $v(Q_i)$ je rovno součtu $v(O)$ přes všechny malé obdélníčky ležící v Q_i. Proto skutečně $v(R) = \sum_{i=1}^n v(Q_i)$.

Poznámka. Podobnou metodou se dají dokázat všelijaká další tvrzení o nemožnosti dláždění, například že krychli nelze rozřezat na konečně mnoho částí a z nich složit pravidelný čtyřstěn.

5 Samoopravné kódy

Motivace. Chceme přenášet (nebo zapisovat a číst) nějaká data, třeba řetězec nul a jedniček. Při přenosu mohou vznikat chyby. Předpokládáme, že pravděpodobnost chyby je malá, a pravděpodobnost k chyb při přenosu daného počtu bitů je podstatně menší než pravděpodobnost $k-1$ či méně chyb. Hlavní myšlenka samoopravných kódů je místo řetězce v, který potřebujeme přenést, poslat poněkud delší řetězec w, sestrojený tak, abychom malý počet chyb vzniklých při přenosu w uměli detekovat či dokonce opravit.

Samoopravné kódy se dnes používají v nejrůznějších zařízeních od CD přehrávačů po kosmické sondy a jejich konstrukce je rozsáhlá moderní disciplína. Tady si uvedeme několik obecných definic a jednu elegantní konstrukci založenou na lineární algebře.

Uvažme konkrétní situaci: Chceme posílat libovolné čtyřbitové řetězce v tvaru $abcd$, kde $a, b, c, d \in \{0, 1\}$. Pravděpodobnost dvou nebo více chyb při přenosu je zanedbatelná, zatímco jedna chyba se občas objeví, a chtěli bychom ji umět opravit.

Jeden způsob umožňující opravit 1 chybu je ztrojit každý bit a poslat $w = aaabbbcccddd$ (12 bitů). Například pro $v = 1011$ pošleme $w = 111000111111$. Přijde-li na druhém konci třeba 110000111111, víme, že došlo k chybě ve třetím bitu a bylo posláno 111000111111 (anebo chyby byly přinejmenším dvě).

To je dost marnotratný způsob kódování: Uvidíme, že 1 chybu můžeme opravit pomocí kódu, který ze 4-bitového řetězce dělá 7-bitový, takže kódováním se zpráva neprotáhne třikrát, ale jenom o 75%.

Příklad: Hammingův kód. To je patrně první známý netriviální samoopravný kód a byl objeven v 50. letech. Místo daného čtyřbitového řetězce $v = abcd$ se pošle sedmibitový řetězec $w = abcdefg$, kde $e = a + b + c$ (sčítání modulo 2), $f = a+b+d$ a $g = a+c+d$. Například pro $v = 1011$ máme $w = 1011001$. Tento způsob kódování také dovoluje opravit chybný přenos jednoho (libovolného) bitu, jak brzy elegantně ověříme za pomoci lineární algebry.

Než se k tomu dostaneme, připravíme si několik obecných definic z teorie kódů. Nechť S je konečná množina, tzv. *abeceda*, například $S = \{0, 1\}$ nebo $S = \{\mathrm{a}, \mathrm{b}, \mathrm{c}, \check{\mathrm{c}}, \ldots, \check{\mathrm{z}}\}$. Zápis $S^n = \{w = a_1a_2 \ldots a_n : a_1, \ldots, a_n \in S\}$ označuje množinu všech možných **slov** délky n (slovo zde tedy znamená libovolnou konečnou posloupnost písmen abecedy).

Definice. **Kód** *délky n nad abecedou S je libovolná podmnožina $C \subseteq S^n$.*

Například pro Hammingův kód máme $S = \{0, 1\}$, $n = 7$ a C je množina všech sedmibitových slov, která mohou popsanou kódovací procedurou vzniknout ze všech $2^4 = 16$ možných slov čtyřbitových, tj. $C = \{0000000, 0001011, 0010101, 0011110, 0100110, 0101101, 0110011, 0111000, 1000111, 1001100, 1010010, 1011001, 1100001, 1101010, 1110100, 1111111\}$.

Podstatná vlastnost tohoto kódu je, že se každá dvě z jeho slov liší aspoň ve třech bitech. To se dá ověřit jednoduše, i když pracně, srovnáním

každé dvojice slov. Zanedlouho to dokážeme jinak a téměř bezpracně. Pro obecný kód se zavádějí následující pojmy:

- **Hammingova vzdálenost** slov $u, v \in S^n$ je
$$d(u, v) = |\{i : u_i \neq v_i, i = 1, 2, \ldots, n\}|,$$
kde u_i značí i-té písmeno ve slově u. To jest, v se dá z u dostat nejvýš $d(u, v)$ „chybami".

- Kód C **opravuje t chyb**, pokud pro každé $u \in S^n$ existuje nejvýš jedno $v \in C$ takové, že $d(u, v) \leq t$.

- Pro kód C označme $d(C) = \min\{d(u, v) : u, v \in C, u \neq v\}$, to je **minimální vzdálenost** kódu C.

Je snadné ověřit, že dva posledně uvedené pojmy spolu souvisí následovně: *Kód C opravuje t chyb, právě když $d(C) \geq 2t+1$.* Když tedy pro Hammingův kód dokážeme $d(C) \geq 3$, bude z toho vidět, že opravuje 1 chybu.

Kódování a dekódovaní. Většinou si člověk pod kódem představuje nějakou proceduru pro kódování a dekódování zpráv, a uvedená definice kódu může proto vypadat divně. Pro skutečné použití je opravdu potřeba kód C jako v definici doplnit nějakou bijekcí $c\colon \Sigma^k \to C$, kde Σ je abeceda, v níž je napsána původní zpráva, a k je délka původní zprávy (nebo délka bloků, na něž se původní zpráva rozkouskuje). Pro danou zprávu $v \in \Sigma^k$ se vypočte kódové slovo $w = c(v) \in C$ a to se pošle. Pro přijaté slovo $w' \in S^n$ se pak nejprve najde slovo $w'' \in C$ minimalizující $d(w', w'')$, a pro něj se spočte $v' = c^{-1}(w'') \in \Sigma^k$. Pokud při přenosu došlo k nejvýš t chybám a C opravuje t chyb, pak $w'' = w$ a tudíž $v' = v$, čili se dostane přesně původní zpráva.

Hlavní problém teorie kódů je najít, pro danou velikost abecedy S a daná t a n, kód C s co největším počtem slov, aby se přenosový kanál co nejlépe využil. Proto se kód definuje tak, jak je napsáno výše. Je ovšem třeba porovnávat i kvalitu kódů s různými $|S|, t, n$. O tom pojednává *Shannonova teorie* míry informace, jíž se zde zabývat nebudeme.

Při konstrukci kódů se berou v úvahu i další hlediska, jako například rychlost kódování a dekódování.

Lineární kódy. Speciálním typem kódů jsou lineární kódy, mezi něž patří i Hammingův kód. Zde abeceda S je konečné těleso (hlavní příklad:

$S = \mathrm{GF}(2)$), a pak S^n je vektorový prostor nad S. Každý vektorový podprostor S^n se nazývá *lineární kód.*

Pozorování: Pro lineární kód C platí

$$d(C) = \min\{d(0, \mathbf{w}) : \mathbf{w} \in C, \mathbf{w} \neq \mathbf{0}\}.$$

Lineární kód se nemusí zadávat výčtem všech slov. Lze jej popsat prostředky lineární algebry, dvěma základními způsoby.

1. Bází, neboli **generující maticí** G kódu. To je matice typu $k \times n$, kde $k = \dim(C)$, jejíž řádky jsou vektory nějaké báze C.

   Generující matice je užitečná pro kódování. Máme-li přenést vektor $\mathbf{v} \in S^k$, pošleme vektor $\mathbf{w} = \mathbf{v}^T G \in C$.

   Vhodnou volbou báze podprostoru C můžeme vždy dostat generující matici tvaru $G = (I_k | A)$. Potom vektor $\mathbf{w}$ má prvních k složek shodných s $\mathbf{v}$, tedy při kódování se k původnímu vektoru připíše $n-k$ „kontrolních složek“. Takový způsob kódování, kdy zakódované slovo sestává ze slova původního a nějakých znaků navíc, se nazývá *systematický.*

   Hammingův kód je systematický lineární kód délky 7 nad GF(2) a má generující matici

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

2. Lineární kód C se dá zadat také jako množina všech řešení soustavy $P\mathbf{w} = \mathbf{0}$, kde P je tzv. **matice kontroly parity** kódu C. To je užitečné pro dekódování, viz dále. Je-li $G = (I_k | A)$, pak můžeme vzít $P = (-A^T | I_{n-k})$ (ověřte, že to funguje!).

Příklad: Zobecněný Hammingův kód. Hammingův kód má matici kontroly parity

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

Všimněme si, že sloupce jsou právě všechny možné nenulové vektory z $\mathrm{GF}(2)^3$. Tato konstrukce se dá zobecnit: Zvolíme parametr $\ell \geq 2$, a

definujeme *zobecněný Hammingův kód* pomocí matice kontroly parity P. Ta má ℓ řádek a $n = 2^\ell - 1$ sloupců, a sloupce jsou všechny nenulové vektory z $GF(2)^\ell$. Tedy $k = 2^\ell - \ell - 1$ a $n = 2^\ell - 1$.

Tvrzení: Zobecněný Hammingův kód C má $d(C) = 3$, tedy opravuje 1 chybu.

Důkaz: Stačí ověřit, že žádný $\mathbf{w} \in GF(2)^n$ s jednou nebo dvěma jedničkami nesplňuje $P\mathbf{w} = \mathbf{0}$. Pro $\mathbf{w}$ s jednou jedničkou by to znamenalo, že P má nulový sloupec, a pro $\mathbf{w}$ se dvěma jedničkami bychom dostali, že dva sloupce P se rovnají. Ani jedna možnost tudíž nenastává a důkaz je hotov.

Poznamenejme, že (zobecněný) Hammingův kód je optimální v následujícím smyslu: Žádný kód $C \subseteq GF(2)^{2^\ell - 1}$ s $d(C) \geq 3$ nemá víc slov než zobecněný Hammingův kód. Důkaz ponecháváme jako (těžší) cvičení.

Dekódování zobecněného Hammingova kódu. Někdo nám poslal slovo $\mathbf{w}$ zobecněného Hammingova kódu a přijali jsme $\mathbf{w}'$. Pokud došlo k nejvýš jedné chybě, máme $\mathbf{w}' = \mathbf{w}$ nebo $\mathbf{w}' = \mathbf{w} + \mathbf{e}_i$ pro nějaké $i \in \{1, 2, \ldots, n\}$, kde $\mathbf{e}_i$ má jedničku na místě i a jinde nuly.

Zda došlo k chybě při přenosu a kde se okamžitě pozná podle součinu $P\mathbf{w}'$. Pokud totiž $\mathbf{w}' = \mathbf{w}$, pak $P\mathbf{w}' = \mathbf{0}$, zatímco pro $\mathbf{w}' = \mathbf{w} + \mathbf{e}_i$ je $P\mathbf{w}' = P\mathbf{w} + P\mathbf{e}_i = P\mathbf{e}_i = \mathbf{p}_i$, což je i-tý sloupec matice P. Protože sloupce P jsou nenulové a navzájem různé, chybná pozice $\mathbf{w}'$ se dá snadno identifikovat.

Můžeme dokonce přerovnat sloupce matice P tak, aby $\mathbf{p}_i$ byl binární zápis čísla i, a pak vektor $P\mathbf{w}'$ přímo „ukazuje“ polohu chyby. Nesmíme ovšem zapomenout správně přerovnat i sloupce matice G.

6 Kontrola násobení matic

Násobení matic je veledůležitá operace. Přímočarý algoritmus na násobení dvou matic typu $n \times n$ vyžaduje řádově n^3 aritmetických operací. Překvapivě byly ale objeveny algoritmy s lepší asymptotickou složitostí a nejlepšímu z nich stačí řádově jen $O(n^{2.376})$ operací. Nicméně konstanta úměrnosti je zatím tak astronomická, že tento algoritmus je zajímavý pouze teoreticky. Matice, pro něž by se jeho lepší asymptotická efektivita projevila, se nemohou vejít do žádného současného a asi ani budoucího počítače.

Pokrok ale nejde zastavit, a brzy může nějaká firma začít prodávat program MATRIX WIZARD, o němž tvrdí, že nevídaným novým algoritmem násobí matice opravdu bleskově. Vám by se takový program hodil, ale nesprávně spočtený součin matic by pro vás mohl mít nedozírné následky. Potřebovali byste nějaký jednoduchý program, který by vždycky zkontroloval, jestli výsledná matice C je opravdu součinem zadaných matic A a B. Nemá samozřejmě smysl matice A a B vynásobit a porovnat výsledek s C, protože neumíte násobit matice ani zdaleka tak rychle jako MATRIX WIZARD. Když se ale připustí maličká pravděpodobnost chyby, správnost maticového násobení se opravdu dá kontrolovat velmi efektivně. Pro jednoduchost předpokládejme, že prvky matic jsou racionální čísla, i když následující metoda funguje pro matice nad jakýmkoliv tělesem.

Kontrolní algoritmus dostane matice A, B, C typu $n \times n$ jako vstup. Zvolí si pomocí generátoru náhodných čísel náhodný n-složkový vektor $\mathbf{x}$ z nul a jedniček. Přesněji, každý vektor z $\{0,1\}^n$ se objeví se stejnou pravděpodobností, rovnou 2^{-n}. Algoritmus spočítá součin $C\mathbf{x}$ (pomocí řádově n^2 operací) a součin $AB\mathbf{x}$ (zase pomocí řádově n^2 operací – správné uzávorkování je samozřejmě $A(B\mathbf{x})$). Pokud se výsledky shodují, odpoví algoritmus ANO (C je součinem A a B), a jinak NE.

Pokud platí $C = AB$, odpoví algoritmus vždy ANO, a tedy správně. Pokud ale $C \neq AB$, může odpovědět jako NE, tak ANO. Tvrdíme ale, že (nesprávná) odpověď ANO má pravděpodobnost nejvýš $\frac{1}{2}$, a tedy algoritmus odhalí chybné maticové násobení s pravděpodobností aspoň $\frac{1}{2}$.

Položme $D = C - AB$. Teď stačí ukázat, že je-li D libovolná nenulová matice typu $n \times n$ a $\mathbf{x}$ je náhodný vektor $\{0,1\}^n$, potom vektor $\mathbf{y} = D\mathbf{x}$ je nenulový s pravděpodobností aspoň $\frac{1}{2}$. Buď $d_{ij} \neq 0$. Ověříme, že pak $y_i \neq 0$ s pravděpodobností nejméně $\frac{1}{2}$. Platí

$$y_i = d_{i1}x_1 + d_{i2}x_2 + \cdots + d_{in}x_n = d_{ij}x_j + S,$$

kde

$$S = \sum_{\substack{k=1,2,\ldots,n \\ k \neq j}} d_{ik}x_k.$$

Představme si, že volíme složky vektoru $\mathbf{x}$ jednu po druhé, řekněme podle výsledků n hodů mincí, a že x_j se volí jako poslední. Před tímto posledním hodem mincí je hodnota S, která na x_j nezávisí, už zafixována. Po posledním hodu buď necháme S beze změny (když vyjde $x_j = 0$), nebo k němu přičteme nenulové číslo d_{ij} (pokud $x_j = 1$). V aspoň jednom z těchto případů dostaneme nenulový výsledek, a tudíž $D\mathbf{x} \neq \mathbf{0}$ má pravděpodobnost přinejmenším $\frac{1}{2}$, jak jsme tvrdili.

Dosud popsaný algoritmus kontroly maticového násobení je rychlý, ale zatím vypadá značně nespolehlivý. Ukázali jsme pouze, že odhalí

chybu aspoň v polovině případů. Když ho ale zopakujeme pro jeden vstup A, B, C třeba padesátkrát, unikne mu chyba s pravděpodobností nejvýš $2^{-50} < 10^{-15}$, a tato pravděpodobnost je pro praktické účely zanedbatelná.

Poznámka. Myšlenka *pravděpodobnostní kontroly výpočtů*, kterou jsme zde viděli v jednoduché formě, se ukázala neobyčejně plodnou. Takzvaná PCP věta v teorii výpočetní složitosti ukázala, že pro každou efektivně řešitelnou výpočetní úlohu se řešení dá velmi rychle pravděpodobnostně zkontrolovat. Populárně řečeno, pomalý osobní počítač může v principu kontrolovat výpočty po nejvýkonnějších superpočítačích. Navíc se objevily překvapivé souvislosti těchto výsledků s aproximačními algoritmy.

7 Pokrývání úplnými bipartitními grafy

Věta. *Je-li množina $E(K_n)$, tj. množiny hran úplného grafu na n vrcholech, vyjádřena jako disjunktní sjednocení množin hran m úplných bipartitních podgrafů, pak $m \geq n-1$.* (Vyjádření s $m = n - 1$ je snadné najít.)

Důkaz. Předpokládejme, že úplné bipartitní grafy $B_1, \ldots, B_m$ disjunktně pokrývají všechny hrany K_n, a nechť (X_k, Y_k) je rozklad množiny vrcholů B_k na dvě části takové, že hrany B_k jdou jen mezi nimi. (Množina $V(B_k) = X_k \cup Y_k$ nemusí být celé $V(K_n)$.)

Každému grafu B_k přiřadíme $n \times n$ matici A_k, jejíž prvek v i-tém řádku a j-tém sloupci je

$$a_{ij}^{(k)} = \begin{cases} 1 & \text{pokud } i \in X_k \text{ a } j \in Y_k \\ 0 & \text{jinak.} \end{cases}$$

Každá A_k má hodnost 1, poněvadž všechny nenulové řádky jsou rovny témuž vektoru, totiž vektoru s jedničkami v pozicích, jejichž indexy náležejí Y_k, a s nulami všude jinde.

Uvažme matici $A = A_1 + A_2 + \cdots + A_m$. Hodnost součtu dvou matic je nejvýš rovna součtu jejich hodností (proč?), a tudíž hodnost A je nejvýš m. Stačí tedy dokázat, že tato hodnost je aspoň $n-1$.

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 $a_{ij} = 0$, $a_{ji} = 1$ (přitom a_{ii}=0). Odtud $A + A^T = J_n - I_n$, kde J_n je $n \times n$ matice samých jedniček.

Předpokládejme, pro spor, že hodnost A je nejvýš $n-2$. Připíšeme-li k matici A ještě jeden řádek ze samých jedniček, má vzniklá $(n + 1) \times n$ matice pořád hodnost nejvýš $n - 1$, a tedy existuje netriviální lineární kombinace jejích sloupců rovná $\mathbf{0}$. Jinými slovy, existuje nenulový (sloupcový) vektor $\mathbf{x} \in \mathbb{R}^n$ takový, že $A\mathbf{x} = \mathbf{0}$ a zároveň $\sum_{i=1}^n x_i = 0$.

Z posledně uvedeného vztahu plyne $J_n\mathbf{x} = \mathbf{0}$. Spočítáme

$$\begin{aligned}\mathbf{x}^T\left(A + A^T\right)\mathbf{x} &= \mathbf{x}^T(J_n - I_n)\mathbf{x} = \mathbf{x}^T(J_n\mathbf{x}) - \mathbf{x}^T(I_n\mathbf{x}) = \\ &= 0 - \mathbf{x}^T\mathbf{x} = -\sum_{i=1}^n x_i^2 < 0.\end{aligned}$$

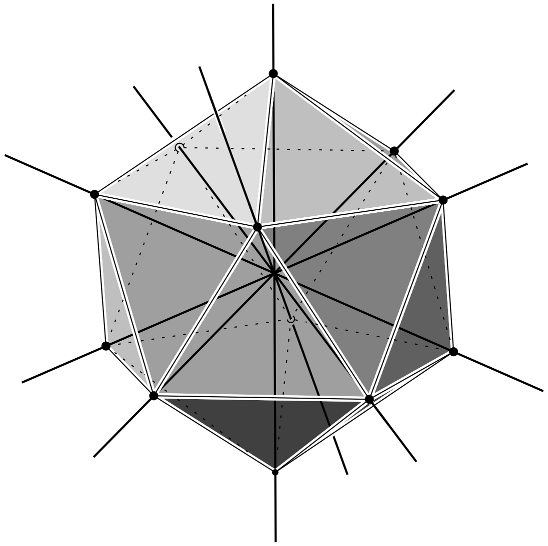
Na druhé straně ale

$$\mathbf{x}^T\left(A^T + A\right)\mathbf{x} = \left(\mathbf{x}^T A^T\right)\mathbf{x} + \mathbf{x}^T(A\mathbf{x}) = \mathbf{0}^T\mathbf{x} + \mathbf{x}^T\mathbf{0} = 0$$

a to je spor.

8 Stejné úhly

Jaký je největší počet přímek v $\mathbb{R}^3$, z nichž každé dvě svírají stejný úhel? Zatímco každý ví, že v $\mathbb{R}^3$ neexistuje víc navzájem kolmých přímek než 3, pro jiné úhly než pravé je situace složitější. Například ze 6 nejdelších úhlopříček pravidelného dvacetistěnu (spojujících dvojice protilehlých vrcholů) svírají každé dvě týž úhel:



Více přímek ale už nenajdeme:

Věta. *Největší počet přímek v $\mathbb{R}^3$, z nichž každé dvě svírají stejný úhel, je 6, a obecně v $\mathbb{R}^d$ neexistuje víc než $\binom{d+1}{2}$ takových přímek.*

Důkaz. Mějme konfiguraci n přímek, z nichž každé dvě svírají týž úhel $\vartheta \in (0, \frac{\pi}{2})$. Buď $\mathbf{v}_i$ jednotkový vektor ve směru i-té přímky (ze dvou možností pro $\mathbf{v}_i$ vybereme jednu libovolně). Podmínka s úhly přímek je ekvivalentní podmínce

$$|\langle \mathbf{v}_i \,|\, \mathbf{v}_j \rangle| = \cos\vartheta \quad \text{pro } i \neq j.$$

Považujme $\mathbf{v}_i$ za sloupcový vektor, neboli matici $d\times 1$. Potom $\mathbf{v}_i^T\mathbf{v}_j$ je skalární součin $\langle \mathbf{v}_i \,|\, \mathbf{v}_j \rangle$, nebo přesněji řečeno matice typu 1×1, jejímž jediným prvkem je $\langle \mathbf{v}_i \,|\, \mathbf{v}_j \rangle$. Naproti tomu $\mathbf{v}_i\mathbf{v}_j^T$ je matice typu $d\times d$.

Ukážeme, že matice $\mathbf{v}_i\mathbf{v}_i^T$, $i = 1, 2, \ldots, n$, jsou lineárně nezávislé. Jelikož jsou to prvky vektorového prostoru všech reálných symetrických matic typu $d\times d$, který má dimenzi $\binom{d+1}{2}$, dostaneme tím $n \le \binom{d+1}{2}$, jak jsme chtěli.

Uvažme lineární kombinaci

$$\sum_{i=1}^n a_i\mathbf{v}_i\mathbf{v}_i^T = 0.$$

Vynásobíme-li obě strany této rovnosti zleva $\mathbf{v}_j^T$ a zprava $\mathbf{v}_j$ a využijeme-li asociativity maticového násobení, dostaneme

$$0 = \sum_{i=1}^n a_i\mathbf{v}_j^T(\mathbf{v}_i\mathbf{v}_i^T)\mathbf{v}_j = \sum_{i=1}^n a_i\langle \mathbf{v}_i \,|\, \mathbf{v}_j \rangle^2 = a_j + \sum_{i\neq j} a_i\cos^2\vartheta.$$

Jinými slovy, odvodili jsme $M\mathbf{a} = \mathbf{0}$, kde $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ a $M = (1 - \cos^2\vartheta)I_n + (\cos^2\vartheta)J_n$. Zde I_n značí jednotkovou matici a J_n matici samých jedniček. Je snadné se přesvědčit, že matice M je regulární (s využitím $\cos\vartheta \neq 1$), a proto $\mathbf{a} = \mathbf{0}$. Tudíž matice $\mathbf{v}_i\mathbf{v}_i^T$ jsou lineárně nezávislé a věta je dokázána.

Poznámka. Zatímco pro $d = 3$ je horní odhad z této věty nejlepší možný, pro větší d se někdy dá zlepšit jinými metodami, a nejlepší možná hodnota obecně není známa. Nejlepší známý dolní odhad (z roku 2000) je $\frac{2}{9}(d+1)^2$, platný pro všechna čísla d tvaru $3 \cdot 2^{2t-1} - 1$, kde t je číslo přirozené.

9 Liché vzdálenosti

Věta. *Nelze najít 4 body v rovině tak, aby vzdálenost každých dvou byla liché celé číslo.*

Důkaz. (Používá determinantu a skalárního součinu.) Pro spor předpokládejme, že 4 body se všemi vzdálenostmi lichými existují. Můžeme předpokládat, že jeden z nich je $\mathbf{0}$, a zbývající tři označíme $\mathbf{a}, \mathbf{b}, \mathbf{c}$. Tedy $\|a\|$, $\|b\|$, $\|c\|$, $\|a-b\|$, $\|b-c\|$ a $\|c-a\|$ jsou lichá celá čísla.

Pozorování: je-li m liché celé číslo, pak m^2 dává zbytek 1 modulo 8. Proto druhé mocniny uvažovaných vzdáleností dávají zbytek 1 modulo 8. Z kosinové věty pak dostaneme, že i $2\langle \mathbf{a} \,|\, \mathbf{b}\rangle = \|\mathbf{a}\|^2 + \|\mathbf{b}\|^2 - \|\mathbf{a}-\mathbf{b}\|^2$ dává zbytek 1 modulo 8, a podobně pro $2\langle \mathbf{a} \,|\, \mathbf{c}\rangle$ a $2\langle \mathbf{b} \,|\, \mathbf{c}\rangle$. Je-li B matice

$$\begin{pmatrix} \langle \mathbf{a} \,|\, \mathbf{a}\rangle & \langle \mathbf{a} \,|\, \mathbf{b}\rangle & \langle \mathbf{a} \,|\, \mathbf{c}\rangle \\ \langle \mathbf{b} \,|\, \mathbf{a}\rangle & \langle \mathbf{b} \,|\, \mathbf{b}\rangle & \langle \mathbf{b} \,|\, \mathbf{c}\rangle \\ \langle \mathbf{c} \,|\, \mathbf{a}\rangle & \langle \mathbf{c} \,|\, \mathbf{b}\rangle & \langle \mathbf{c} \,|\, \mathbf{c}\rangle \end{pmatrix},$$

pak $2B$ je kongruentní matici

$$Z = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$$

modulo 8, a proto $\det(B) \neq 0$. (Podrobněji: Každý člen v definujícím výrazu pro determinant matice $2B$ dává stejný zbytek modulo 8 jako odpovídající člen v determinantu matice Z, a tedy $\det(2B)$ je kongruentní $\det(Z)$ modulo 8. Přitom $\det(Z)$ dává nenulový zbytek, a tudíž i $\det(2B) \neq 0$.) Hodnost matice B je tedy 3. Na druhé straně $B = A^T A$, kde

$$A = \begin{pmatrix} a_1 & b_1 & c_1 \\ a_1 & b_2 & c_2 \end{pmatrix}.$$

Matice A má hodnost nejvýš 2, a jak známo, hodnost součinu matic je nejvýš rovna hodnosti každého z činitelů. Tudíž B má hodnost nejvýš 2 – spor.

10 Jen dvě vzdálenosti

Mějme množinu bodů $\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_n$ v rovině. Nejdříve předpokládejme, že každé dva z nich mají tutéž vzdálenost. Potom musí tvořit vrcholy rovnostranného trojúhelníka, a tudíž $n \leq 3$. Co když připustíme, že vzdálenosti mezi nimi mohou být dvě různá čísla (ale ne víc)? Snadno se najde čtyřbodová konfigurace jen se dvěma vzdálenostmi, třeba vrcholy čtverce, a další zamyšlení odhalí i pětibodovou konfiguraci, totiž vrcholy pravidelného pětiúhelníka. Ale jak ukázat, že nemůžeme najít konfiguraci mnohem větší?

Podobně se můžeme ptát ve vyšší dimenzi, tj. v prostoru $\mathbb{R}^d$, $d \geq 3$: Jaké je maximální číslo $n = n(d)$ takové, že v $\mathbb{R}^d$ existuje n-tice bodů jen se dvěma vzdálenostmi? Následující elegantní metoda dává poměrně dobrý horní odhad pro $n(d)$, i když výsledek pro rovinu není úplně ohromující (dostane se horní odhad 9).

Věta. $n(d) \leq \frac{1}{2}(d^2 + 5d + 4)$.

Důkaz. Nechť $\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_n$ jsou body v $\mathbb{R}^d$. Označme $D(\mathbf{p}_i, \mathbf{p}_j)$ vzdálenost $\mathbf{p}_i$ od $\mathbf{p}_j$. Máme

$$D(\mathbf{p}_i, \mathbf{p}_j)^2 = (p_{i1} - p_{j1})^2 + (p_{i2} - p_{j2})^2 + \cdots (p_{id} - p_{jd})^2,$$

kde p_{ij} značí j-tou souřadnici bodu $\mathbf{p}_i$. Předpokládejme, že $D(\mathbf{p}_i, \mathbf{p}_j) \in \{a, b\}$ pro každé $i \neq j$.

Definujeme funkce $f_1, f_2, \ldots, f_n \colon \mathbb{R}^d \to \mathbb{R}$ takto (to je základní trik důkazu):

$$f_i(\mathbf{x}) = \left(D(\mathbf{x}, \mathbf{p}_i)^2 - a^2\right) \left(D(\mathbf{x}, \mathbf{p}_i)^2 - b^2\right),$$

kde $\mathbf{x} = (x_1, x_2, \ldots, x_d) \in \mathbb{R}^d$. Z předpokladu o dvou vzdálenostech dostaneme

$$f_i(\mathbf{p}_j) = \begin{cases} 0 & \text{pro } i \neq j, \\ a^2 b^2 \neq 0 & \text{pro } i = j. \end{cases} \tag{1}$$

Uvažme vektorový prostor všech reálných funkcí $\mathbb{R}^d \to \mathbb{R}$, a jeho podprostor V generovaný funkcemi $f_1, f_2, \ldots, f_n$. Nejdříve tvrdíme, že $f_1, f_2, \ldots, f_n$ jsou lineárně nezávislé. Předpokládejme, že lineární kombinace $f = \alpha_1 f_1 + \alpha_2 f_2 + \cdots + \alpha_n f_n$ je rovna 0, tj. je to funkce $\mathbb{R}^d \to \mathbb{R}$ dávající hodnotu 0 ve všech bodech $\mathbb{R}^d$. Speciálně dává 0 i v každém z bodů $\mathbf{p}_i$ a z toho podle (1) dostaneme $0 = f(\mathbf{p}_i) = \alpha_i a^2 b^2$, takže $\alpha_i = 0$ pro všechna i. Tedy $\dim V = n$.

Nyní najdeme pokud možno malý systém generátorů. Přesněji řečeno, najdeme malý počet funkcí $\mathbb{R}^d \to \mathbb{R}$ takových, že každou f_i lze vyjádřit jako jejich lineární kombinací; přitom tyto funkce nemusejí ležet ve V.

Každá f_i je mnohočlen v proměnných $x_1, x_2, \ldots, x_d$ stupně nejvýš 4, a proto ji lze vyjádřit jako lineární kombinaci všech jednočlenů v $x_1, x_2, \ldots, x_d$ stupně nejvýš 4. Těch je, jak se dá spočítat, $\binom{d+4}{4}$, a tak máme horní odhad $n = \dim V \leq \binom{d+4}{4}$. Najdeme ale ještě úspornější systém generátorů.

Vyjádříme $D(\mathbf{x},\mathbf{p}_i)^2 = \sum_{j=1}^d (x_j - p_{ij})^2 = X - \sum_{j=1}^d 2x_jp_{ij} + P_i$, kde jsme položili $X = \sum_{j=1}^d x_j^2$ a $P_i = \sum_{j=1}^d p_{ij}^2$. Dále máme

$$\begin{aligned} f_i(\mathbf{x}) &= \left(D(\mathbf{x},\mathbf{p}_i)^2 - a^2\right)\left(D(\mathbf{x},\mathbf{p}_i)^2 - b^2\right) = \\ &= \left(X - \sum_{j=1}^d 2x_jp_{ij} + A_i\right)\left(X - \sum_{j=1}^d 2x_jp_{ij} + B_i\right), \end{aligned}$$

kde píšeme $A_i = P_i - a^2$ a $B_i = P_i - b^2$. Další úpravou dostáváme

$$\begin{aligned} f_i(\mathbf{x}) &= X^2 - 4X\sum_{j=1}^d p_{ij}x_j + \left(\sum_{j=1}^d 2p_{ij}x_j\right)^2 + \\ &\quad + (A_i + B_i)\left(X - \sum_{j=1}^d 2p_{ij}x_j\right) + A_iB_i. \end{aligned}$$

Odtud už je vidět, že každá f_i je lineární kombinací následujících funkcí:

$$\begin{array}{ll} X^2, & \\ x_jX, & j = 1,2,\ldots,d, \\ x_j^2, & j = 1,2,\ldots,d, \\ x_ix_j, & 1 \le i < j \le d, \\ x_j, & j = 1,2,\ldots,d \text{ a} \\ 1. & \end{array}$$

(Poznamenejme, že X samo je lineární kombinací x_j^2.) To je celkem $1 + d + d + \binom{d}{2} + d + 1 = \frac{1}{2}(d^2 + 5d + 4)$ funkcí. Tím je věta dokázána.

Poznámka. Příklad konfigurace $\binom{d}{2}$ bodů v $\mathbb{R}^d$ pouze se dvěma vzdálenostmi dávají body se dvěma souřadnicemi 1 a ostatními 0. Tato konfigurace leží v nadrovině $\sum_{i=1}^d x_i = 2$, takže ji můžeme umístit i v $\mathbb{R}^{d-1}$, což dává dolní odhad $n(d) \ge \binom{d+1}{2} = \frac{1}{2}(d^2 + d)$. Dokázaný horní odhad tedy není pro velké dimenze daleko od pravdy.

11 Pokrývání krychle bez jednoho vrcholu

Tvrzení: Nechť $h_1, h_2, \ldots, h_m$ jsou nadroviny v $\mathbb{R}^d$ neprocházející počátkem, které pokrývají všechny body množiny $\{0,1\}^d$ až na počátek. Pak $m \ge d$.

Důkaz (polynomiální metoda). Nechť h_i má rovnici $a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{id}x_d = 1$. Uvážíme mnohočlen

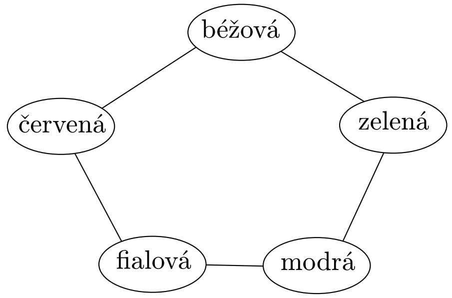
$$f(x_1, x_2, \ldots, x_d) = \prod_{i=1}^m \left(1 - \sum_{j=1}^d a_{ij}x_j\right) - \prod_{j=1}^d (1 - x_j).$$

Podle předpokladu je hodnota f rovna 0 ve všech bodech $\{0,1\}^d$. Kdyby platilo $m < d$, potom by f měl stupeň d, a jediný jednočlen stupně d by byl $x_1x_2\cdots x_d$ s nenulovým koeficientem. Zbývá ukázat, že tento jednočlen není lineární kombinací jednočlenů nižšího stupně, uvažujeme-li tyto jednočleny jako reálné funkce na $\{0,1\}^d$.

Nejprve si všimneme, že na $\{0,1\}^d$ platí $x_i = x_i^2$, a tudíž každý mnohočlen je ekvivalentní lineární kombinaci jednočlenů tvaru $x_I = \prod_{i\in I} x_i$, kde $I \subseteq \{1,2,\ldots,d\}$. Stačí tedy ukázat, že taková x_I jsou lineárně nezávislá. Mějme lineární kombinaci $\sum_{I\subseteq\{1,2,\ldots,d\}} \alpha_I x_I = 0$. Předpokládejme, že existuje $\alpha_I \ne 0$, a vezměme minimální takové I ($\alpha_J = 0$ kdykoli $J \subset I$). Dosazením $x_i = 1$ pro $i \in I$ a $x_i = 0$ pro $i \notin I$ dostaneme $\alpha_I = 0$, spor.

12 Agent a paraplíčko

Tajný vládní agent v pouštním výcvikovém táboře podvratné organizace nemá mnoho možností, jak bezpečně předávat zprávy. Má pět šátků, červený, béžový, zelený, modrý a fialový, a každý den si vezme k uniformě jeden z nich. Analytici na ústředí pak barvu jeho šátku vyhodnocují na družicovém snímku, ale protože šátky nejsou nejčistší, ukázalo se, že se některé barvy nedají spolehlivě odlišit. Možné záměny jsou znázorněny na obrázku,



například fialová se nepozná spolehlivě od modré ani od červené, ale není nebezpečí, že by se zaměnila se zelenou nebo béžovou. Pro spolehlivé předávání zpráv může agent používat například jen modrý a červený šátek, čímž každý den vyšle jednu ze dvou možností, neboli informaticky řečeno, jeden bit. Za k dnů tedy může sdělit jednu z 2^k možných zpráv.

Mohlo by se zdát, že v této situaci agent víc než jeden bit zprávy denně poslat nemůže, protože mezi každými třemi z jeho šátků jsou aspoň dva záměnné. Ale lepší možnost existuje! Během dvou dnů po sobě může poslat jednu z pěti zpráv, například takto:

	první den	druhý den
zpráva 1	červený	červený
zpráva 2	béžový	zelený
zpráva 3	zelený	fialový
zpráva 4	modrý	béžový
zpráva 5	fialový	modrý

Skutečně, u žádných dvou z těchto dvoudenních kombinací nehrozí záměna, jak se může čtenář sám přesvědčit. Tímto způsobem lze za k dnů, pro sudé k, poslat jednu z $5^{k/2} = \sqrt{5}^k$ možných zpráv. Efektivita na den uvedeným trikem vzrostla ze 2 na $\sqrt{5}$.

Otázka nyní je, jestli efektivitu lze dál zvýšit, například kombinacemi třídenními nebo desetidenními. To je těžký matematický problém. Odpověď zní, že efektivitu již zvýšit nejde, a následující mistrovský kousek je jediný známý důkaz.

Nejprve problém formulujeme matematicky (a obecněji). Uvažujeme nějakou *abecedu* S, v našem případě S sestává z pěti možných barev šátků. U některých dvojic prvků z S je nebezpečí záměny, což vyjádříme grafem $G = (S, E)$, kde zaměnitelné symboly z S jsou spojené hranou. Pro popsanou situaci s agentem jsme graf G uvedli na obrázku a je to kružnice délky 5, čili C_5.

Uvažme dvě zprávy délky k, $a_1 a_2 \cdots a_k$ a $b_1 b_2 \cdots b_k$ (v terminologii teorie kódů jsou to slova délky k nad abecedou S, viz sekci 5). Ty jsou zaměnitelné, právě když pro každé $i = 1, 2, \ldots, k$ je a_k zaměnitelné s b_k, neboli platí $a_i = b_i$ nebo $\{a_i, b_i\} \in E$. Nechť $\alpha_k(G)$ označuje maximální velikost množiny zpráv délky k, z nichž žádné dvě nejsou zaměnitelné. Speciálně $\alpha_1(G)$ je maximální velikost *nezávislé množiny* v grafu G, tj. množiny vrcholů, z nichž žádné dva nejsou spojené hranou. Tato velikost se obvykle označuje $\alpha(G)$. Pro náš příklad zjevně $\alpha_1(C_5) = \alpha(C_5) = 2$. Uvedená tabulka dokazuje, že $\alpha_2(C_5) \geq 5$, a ve skutečnosti platí rovnost – nerovnost $\alpha_2(C_5) \leq 5$ bude velmi speciální případ výsledku, který dokážeme.

Shannonova kapacita grafu G je definována takto:

$$\Theta(G) := \sup \left\{ \alpha_k(G)^{1/k} : k = 1, 2, \ldots \right\}.$$

Vyjadřuje maximální možnou efektivitu bezchybného posílání zpráv, vztaženou na jeden symbol. Pro dost velké k může agent za k dní poslat jednu z přibližně $\Theta(C_5)^k$ možných zpráv, a víc poslat nemůže. Dokážeme následující:

Věta. $\Theta(C_5) = \sqrt{5}$.

Nejdříve si všimneme, že $\alpha_k(G)$ můžeme vyjádřit jako maximální možnou velikost nezávislé množiny ve vhodném grafu. Množina vrcholů tohoto grafu je S^k, tedy vrcholy jsou všechny možné zprávy (slova) délky k, a dva vrcholy $a_1 a_2 \cdots a_k$ a $b_1 b_2 \cdots b_k$ jsou spojené hranou, právě když jsou záměnné. Tento graf budeme značit G^k. Je to takzvaný **silný součin** k exemplářů grafu G. Pro dva obecné grafy H a H' se silný součin $H \cdot H'$ definuje takto:

$$\begin{aligned} V(H \cdot H') &= V(H) \times V(H'), \\ E(H \cdot H') &= \{\{(u, u'), (v, v')\} : (u = v \text{ nebo } \{u, v\} \in E(H)) \\ &\qquad \text{a zároveň } (u' = v' \text{ nebo } \{u', v'\} \in E(H'))\}. \end{aligned}$$

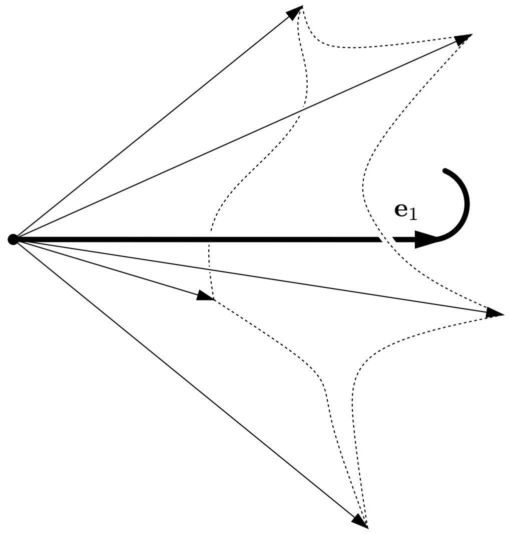
Náš úkol je tedy shora omezit velikost nezávislé množiny v grafech C_5^k.

Pokračujeme obecnou úvahou, která dává do souvislosti nezávislé množiny v grafu s jistými systémy vektorů. Buď $H = (V, E)$ libovolný graf. **Ortogonální reprezentace** grafu H je zobrazení $\rho\colon V \to \mathbb{R}^n$ pro nějaké n, splňující následující podmínky:

- $\|\rho(v)\| = 1$ pro každé $v \in V$, tj. vrcholům se přiřazují *jednotkové* vektory.

- Jestliže $\{u, v\} \notin E$, pak $\langle \rho(u) \,|\, \rho(v) \rangle = 0$, tj. vrcholům *nespojeným* hranou jsou vždy přiřazeny kolmé vektory (v této sekci značí $\langle . \,|\, . \rangle$ standardní skalární součin v $\mathbb{R}^n$).

Pro důkaz hlavní věty budeme potřebovat zajímavou ortogonální reprezentaci ρ_{Lp} grafu C_5 v $\mathbb{R}^3$, „Lovászovo paraplíčko“. Představíme si složený deštník s pěti dráty, jehož rukojeť je vektor $\mathbf{e}_1 = (1, 0, 0)$, a pomalu ho rozevíráme až do okamžiku, kdy jsou každé dva nesousední dráty kolmé:



V této chvíli dráty definují jednotkové vektory $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_5$, a přiřadíme-li i-tému vrcholu grafu C_5 vektor $\mathbf{v}_i$, dostaneme ortogonální reprezentaci ρ_{Lp}. Není těžké spočítat potřebný úhel rozevření deštníku: vyjde $\langle \mathbf{v}_i \,|\, \mathbf{e}_1 \rangle = 5^{-1/4}$, což budeme za chvíli potřebovat.

Pomocí každé ortogonální reprezentace můžeme shora omezit maximální velikost nezávislé množiny:

Lemma. *Je-li H graf a ρ nějaká jeho ortogonální reprezentace, pak $\alpha(H) \le \vartheta(H,\rho)$, kde*

$$\vartheta(H,\rho) = \max_{v \in V(H)} \frac{1}{\langle \rho(v) \,|\, \mathbf{e}_1 \rangle^2}.$$

Důkaz. Vyrobit ortogonální reprezentaci ρ s co nejmenší hodnotou $\vartheta(H,\rho)$ geometricky znamená naskládat všechny vektory $\rho(v)$ do co nejmenšího kužele kolem vektoru $\mathbf{e}_1$. Přitom nezávislá množina v H odpovídá systému ortonormálních vektorů a pro systém ortonormálních vektorů můžeme vypočítat nejmenší možný úhel kužele, který jej obsahuje – z toho vyjde tvrzení lemmatu.

K formálnímu důkazu potřebujeme vědět, že je-li $(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m)$ jakýkoli ortonormální systém vektorů v nějakém $\mathbb{R}^n$ a $\mathbf{u}$ je libovolný další vektor, pak

$$\sum_{i=1}^{m} \langle \mathbf{b}_i \,|\, \mathbf{u} \rangle^2 \le \|\mathbf{u}\|^2.$$

Můžeme totiž daný systém $(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m)$ přidáním dalších $n-m$ vhodných vektorů rozšířit na ortonormální bázi $(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$. Potom i-tá souřadnice vektoru $\mathbf{u}$ vzhledem k této bázi je $\langle \mathbf{b}_i \,|\, \mathbf{u} \rangle$ a pro délku vektoru $\mathbf{u}$ máme z Pythagorovy věty rovnost $\|\mathbf{u}\|^2 = \sum_{i=1}^{n} \langle \mathbf{b}_i \,|\, \mathbf{u} \rangle^2$. Požadovaná nerovnost se dostane vynecháním posledních $n-m$ členů na pravé straně.

Je-li nyní $I \subseteq V(H)$ nezávislá množina vrcholů v grafu H, pak $(\rho(v) : v \in I)$ tvoří ortonormální systém, a tudíž $\sum_{v \in I} \langle \rho(v) \,|\, \mathbf{e}_1 \rangle^2 \le \|\mathbf{e}_1\|^2 = 1$. Proto existuje $v \in I$, pro nějž $\langle \rho(v) \,|\, \mathbf{e}_1 \rangle^2 \le \frac{1}{|I|}$, a tedy $\vartheta(H,\rho) \ge |I|$. □

Pro graf C_5 dává uvedené lemma a Lovászovo paraplíčko

$$\alpha(C_5) \le \vartheta(C_5, \rho_{\mathrm{Lp}}) = \sqrt{5}.$$

Dokazovaná věta pak plyne z následujícího lemmatu o chování ortogonálních reprezentací vzhledem k silnému součinu.

Lemma. *Nechť H_1, H_2 jsou grafy, a nechť ρ_i je nějaká ortogonální reprezentace H_i, $i = 1, 2$. Potom existuje ortogonální reprezentace ρ silného součinu $H_1 \cdot H_2$, pro niž platí $\vartheta(H_1 \cdot H_2, \rho) = \vartheta(H_1, \rho_1) \cdot \vartheta(H_2, \rho_2)$.*

Aplikujeme-li toto lemma (indukcí) na silný součin k exemplářů C_5, dostáváme

$$\alpha(C_5^k) \le \vartheta(C_5, \rho_{\mathrm{LP}})^k = \sqrt{5}^k,$$

což dokazuje $\Theta(C_5) \le \sqrt{5}$.

Zbývá dokázat lemma. K tomu potřebujeme operaci **tenzorového součinu**[1]. Tenzorový součin dvou vektorů $\mathbf{x} \in \mathbb{R}^m$ a $\mathbf{y} \in \mathbb{R}^n$ je vektor v $\mathbb{R}^{mn}$, jehož složky jsou všechny součiny $x_i y_j$ pro $i = 1, 2, \ldots, m$ a $j = 1, 2, \ldots, n$. Budeme jej označovat zápisem $\mathbf{x} \otimes \mathbf{y}$. Například pro $\mathbf{x} = (x_1, x_2, x_3)$ a $\mathbf{y} = (y_1, y_2)$ máme

$$\mathbf{x} \otimes \mathbf{y} = (x_1y_1, x_2y_1, x_3y_1, x_1y_2, x_2y_2, x_3y_2) \in \mathbb{R}^6.$$

Čtenáři přenecháme snadné ověření následujícího faktu:

$$\langle \mathbf{x} \otimes \mathbf{y} \,|\, \mathbf{x}' \otimes \mathbf{y}' \rangle = \langle \mathbf{x} \,|\, \mathbf{x}' \rangle \cdot \langle \mathbf{y} \,|\, \mathbf{y}' \rangle$$

pro libovolná $\mathbf{x}, \mathbf{x}' \in \mathbb{R}^m$, $\mathbf{y}, \mathbf{y}' \in \mathbb{R}^n$.

Teď už můžeme definovat ortogonální reprezentaci ρ silného součinu $H_1 \cdot H_2$ jako v lemmatu. Vrcholy $H_1 \cdot H_2$ jsou dvojice (v_1, v_2), $v_1 \in H_1$, $v_2 \in H_2$. Položíme

$$\rho((v_1, v_2)) = \rho_1(v_1) \otimes \rho_2(v_2).$$

[1] V lineární algebře se tenzorový součin definuje obecněji, pro dva libovolné vektorové prostory. Definici uvedenou zde můžeme považovat za „standardní“ tenzorový součin.

Ze zmíněného faktu o skalárním součinu tenzorových součinů je snadné zkontrolovat jak to, že ρ bude opravdu ortogonální reprezentace $H_1 \cdot H_2$, tak rovnost $\vartheta(H_1 \cdot H_2, \rho) = \vartheta(H_1, \rho_1) \cdot \vartheta(H_2, \rho_2)$. Tím je důkaz věty ukončen. $\square$

Poznámky. Veličina

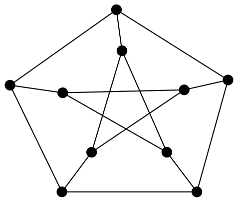
$$\vartheta(G) = \inf\{\vartheta(G, \rho) : \rho \text{ ortogonální reprezentace grafu } G\}$$

se nazývá **Lovászova theta-funkce** grafu G. Jak jsme viděli, dává horní odhad na $\alpha(G)$ (nezávislost grafu). Také není těžké ukázat, že zdola odhaduje barevnost doplňku grafu G, neboli minimální počet úplných podgrafů potřebných k pokrytí G. Zatímco vypočítat nezávislost či barevnost daného grafu jsou algoritmicky obtížné (NP-úplné) úlohy, $\vartheta(G)$ se kupodivu dá vypočítat v polynomiálním čase (tedy přesněji řečeno aproximovat s libovolnou předepsanou přesností). Tím, a řadou dalších podivuhodných vlastností, je Lovászova funkce velmi užitečná.

Shannonova kapacita grafu je mnohem těžší oříšek. Pro její výpočet či aproximaci není znám *vůbec žádný* obecný algoritmus (ani polynomiální, ani nepolynomiální). A pro nevyřešený případ nemusíme chodit daleko – $\Theta(C_7)$ není známo! Kdyby měl agent sedm šátků, nikdo mu zatím neporadí, jak nejlépe vysílat.

13 Tři Petersenovy grafy nestačí

Známý Petersenův graf



má 10 vrcholů stupně 3. Tři kopie Petersenova grafu mají dohromady přesně stejně hran jako úplný graf K_{10}. Přesto jimi nelze všechny hrany K_{10} pokrýt. Přesněji řečeno:

Věta. *Neexistují tři podgrafy K_{10}, každý z nich isomorfní Petersenovu grafu, které by dohromady pokrývaly všechny hrany K_{10}.*

Větu je samozřejmě možné dokázat rozborem mnoha případů. Následující elegantní důkaz je malou ukázkou poměrně rozsáhlé části teorie grafů – vlastnosti a použití vlastních čísel matice sousednosti grafu.

Důkaz. Matice sousednosti grafu G na množině vrcholů $\{1, 2, \ldots, n\}$ je definována jako matice A typu $n \times n$, kde

$$a_{ij} = \begin{cases} 1 & \text{pokud } i \neq j \text{ a } \{i, j\} \in E(G), \\ 0 & \text{jinak.} \end{cases}$$

Tedy matice sousednosti grafu K_{10} je $J_{10} - I_{10}$, kde J_n je $n \times n$ matice samých jedniček a I_n je jednotková matice.

Předpokládejme, že existuje pokrytí hran K_{10} podgrafy P, Q a R, z nichž každý je isomorfní Petersenovu grafu. Značí-li A_P matici sousednosti grafu P, a podobně pro A_Q a A_R, musí platit $A_P + A_Q + A_R = J_{10} - I_{10}$.

Je snadné ověřit, že jsou-li dva grafy isomorfní, mají jejich matice sousednosti stejný soubor vlastních čísel, a taky stejné dimenze vlastních podprostorů příslušných k jednotlivým vlastním číslům.

Gaussovou eliminací spočítáme, že pro matici sousednosti Petersenova grafu má vlastní podprostor příslušný k vlastnímu číslu 1 dimenzi 5, tj. matice $A_P - I_{10}$ má 5-dimenzionální jádro. Navíc má tato matice v každém sloupci přesně tři jedničky a jednu -1, a tedy sečteme-li všechny rovnice ze soustavy $(A_P - I_{10})\mathbf{x} = 0$, dostaneme $2x_1 + 2x_2 + \cdots + 2x_{10} = 0$. Jinými slovy, celé jádro $A_P - I_{10}$ je obsaženo v 9-dimenzionálním ortogonálním doplňku vektoru $(1, 1, \ldots, 1)$. Totéž platí pro jádro $A_Q - I_{10}$, a proto mají obě jádra společný nějaký nenulový vektor $\mathbf{x}$. Pro něj víme $J_{10}\mathbf{x} = 0$ (protože je kolmý k $(1, 1, \ldots, 1)$), a spočítáme

$$\begin{aligned} A_R\mathbf{x} &= (J_{10} - I_{10} - A_P - A_Q)\mathbf{x} = \\ &= J_{10}\mathbf{x} - I_{10}\mathbf{x} - (A_P - I_{10})\mathbf{x} - (A_Q - I_{10})\mathbf{x} - 2I_{10}\mathbf{x} = \\ &= 0 - \mathbf{x} - 0 - 0 - 2\mathbf{x} = -3\mathbf{x}. \end{aligned}$$

To znamená, že -3 musí být vlastním číslem A_R, ale matice sousednosti Petersenova grafu toto vlastní číslo nemá – spor.

14 Konec padesátníků

Internetové zasilatelství dostalo m objednávek, každá z nich požaduje několik kusů zboží různých druhů. Vtom vyšel vládní výnos rušící padesátníky a nařizující, že cena každého zboží musí být zaokrouhlena na celé koruny (nahoru nebo dolů, a pokud cena už byla v celých korunách, pak se nemění). Může zasilatelství zaokrouhlit všechny ceny tak, aby se celková cena žádné objednávky moc nezměnila? Tento zaokrouhlovací problém a jemu podobné se studují v teorii *diskrepance*. Tady uvedeme jednu větu, která se dokazuje pomocí lineární algebry.

Věta. *Jestliže od žádného druhu zboží není dohromady objednáno víc než t kusů, a jestliže žádná objednávka nepožaduje více než jeden kus zboží od každého druhu, potom lze ceny zaokrouhlit na celé koruny tak, že cena žádné objednávky se nezmění o víc než t korun. (Původní ceny dokonce mohou být zcela libovolné a nemusí být v celých padesátnících.)*

Je pozoruhodné, že odhad chyby zaokrouhlení zde vůbec nezávisí na celkovém počtu objednávek ani na počtu druhů zboží.

Matematičtější vyjádření problému. Označme druhy zboží $1, 2, \ldots, n$ a buď c_j cena jednoho kusu od j-tého druhu. Můžeme předpokládat, že každé $c_j \in (0, 1)$ (protože v problému hraje roli jen změna ceny zaokrouhlením). Poněvadž žádná objednávka nepožaduje víc než jeden kus zboží každého druhu, můžeme i-tou objednávku reprezentovat jako množinu $S_i \subseteq \{1, 2, \ldots, n\}$, $i = 1, 2, \ldots, m$. Věta nyní tvrdí, že pokud žádné j není ve víc než t množinách, existují čísla $z_1, z_2, \ldots, z_n \in \{0, 1\}$ taková, že

$$\left| \sum_{j \in S_i} c_j - \sum_{j \in S_i} z_j \right| \le t, \quad \text{pro každé } i = 1, 2, \ldots, m.$$

Důkaz. Pro každý index $j \in \{1, 2, \ldots, n\}$ zřídíme jednu reálnou proměnnou $x_j \in [0, 1]$, jíž na začátku přiřadíme hodnotu c_j, a která se bude v průběhu důkazu měnit. Nakonec bude mít každé x_j hodnotu 0 nebo 1, a tuto hodnotu použijeme jako z_j.

V každém kroku jsou některé z proměnných x_j už ustálené, zatímco ostatní jsou „kolísavé“. Na začátku jsou všechna x_j kolísavá. Ustálená x_j mají hodnoty 0 nebo 1, a ty se již nikdy nebudou měnit. Hodnoty kolísavých proměnných jsou v intervalu $(0, 1)$. V každém kroku se aspoň jedna kolísavá proměnná ustálí.

Nazývejme množinu S_i *hrozivou*, jestliže obsahuje víc než t indexů j takových, že x_j je ještě kolísavá. Ostatní množiny jsou *neškodné*. Budeme udržovat v platnosti následující podmínku:

$$\sum_{j \in S_i} x_j = \sum_{j \in S_i} c_j \text{ pro všechny hrozivé } S_i. \tag{2}$$

Označme F množinu indexů všech kolísavých proměnných, a uvažme (2) jako systém lineárních rovnic, jehož neznámé jsou kolísavé proměnné (zatímco hodnoty ustálených proměnných zde vystupují jako konstanty). Tento systém určitě má řešení, totiž momentální hodnoty kolísavých proměnných. Poněvadž předpokládáme, že každá kolísavá proměnná leží v intervalu $(0, 1)$, zmíněné řešení je vnitřním bodem $|F|$-dimenzionální krychle $[0, 1]^{|F|}$. Chceme ukázat, že existuje také řešení na hranici této krychle, tj. takové, že aspoň jedna neznámá má hodnotu 0 nebo 1.

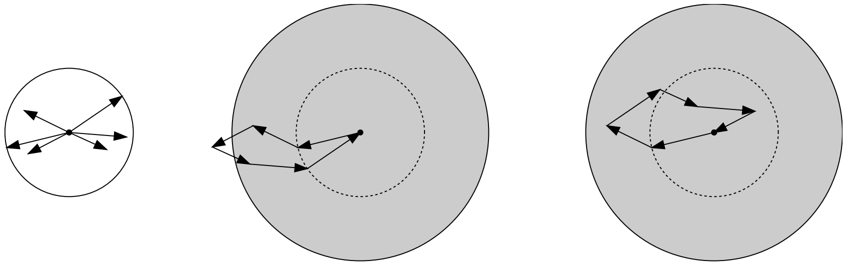
Klíčové pozorování je, že počet hrozivých množin je v každém okamžiku ostře menší než počet kolísavých proměnných (každá hrozivá množina potřebuje víc než t kolísavých proměnných, zatímco jedna kolísavá proměnná přispěje nejvýš t hrozivým množinám). Tudíž uvažovaná soustava lineárních rovnic má méně rovnic než neznámých, a proto množina řešení má dimenzi aspoň jedna. Uvažovaným řešením uvnitř krychle $[0, 1]^{|F|}$ tedy prochází nějaká přímka (jednodimenzionální afinní podprostor), jejíž všechny body jsou také řešeními. Taková přímka protíná hranici krychle v nějakém bodě $\mathbf{y}$. Souřadnice bodu $\mathbf{y}$ použijeme jako hodnoty kolísavých proměnných pro další krok. Všechny kolísavé proměnné x_j, pro něž odpovídající souřadnice bodu $\mathbf{y}$ je 0 nebo 1, budou však od následujícího kroku počínaje ustálené.

Popsaný krok opakujeme, dokud se všechny proměnné neustálí. Tvrdíme, že vezmeme-li za z_j ustálenou hodnotu x_j pro všechna j, bude splněna podmínka $\left|\sum_{j \in S_i} c_j - \sum_{j \in S_i} z_j\right| \le t$ pro každé $i = 1, 2, \ldots, m$, jak jsme chtěli. Abychom to nahlédli, uvažme nějakou množinu S_i. V okamžiku, kdy přestala být hrozivá, platilo ještě $\sum_{j \in S_i} c_j - \sum_{j \in S_i} x_j = 0$ podle podmínky (2). Tehdy S_i obsahovala indexy nejvýš t kolísavých proměnných. Hodnota každé z těchto kolísavých proměnných se ve zbytku postupu nezměnila víc než o 1 (mohla být třeba 0.001 a pak se ustálit na 1). Tím je důkaz hotov.

15 Vektory v ohrádce

Věta. *Buď M libovolná množina n vektorů v $\mathbb{R}^d$, splňující $\|\mathbf{v}\| \le 1$ pro každé $\mathbf{v} \in M$, kde $\|\mathbf{v}\|$ značí normu $\mathbf{v}$ neboli obvyklou euklidovskou délku, a dále $\sum_{\mathbf{v} \in M} \mathbf{v} = 0$. Potom se všechny vektory z M dají srovnat do posloupnosti $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ tak, že $\|\mathbf{v}_1 + \mathbf{v}_2 + \cdots + \mathbf{v}_k\| \le d$ pro každé $k = 1, 2, \ldots, n$.*

Například pro rovinu ($d = 2$) věta zaručuje takové pořadí, že vyjdemeli z počátku, popojdeme o $\mathbf{v}_1$, pak o $\mathbf{v}_2$, pak o $\mathbf{v}_3, \ldots$, a nakonec o $\mathbf{v}_n$, nikdy nevybočíme z kruhové ohrádky o poloměru 2 se středem v počátku.



množina M špatné pořadí dobré pořadí

V příkladu na obrázku lze vektory dokonce srovnat tak, že cestička nevybočí z ohrádky o poloměru 1, ale obecně to možné není (zkuste najít příklad). Pro rovinu se přesně ví nejmenší možný poloměr ohrádky $\sqrt{5}/2 \approx 1.118$, a pro obecnou dimenzi d je nejlepší známý dolní odhad řádu $\sqrt{d}$. Otázka, zda se věta dá obecně vylepšit na ohrádky s poloměrem $O(\sqrt{d}\,)$, je otevřená.

Důkaz věty. Je to trošku složitější variace metody z oddílu 14. Položíme $M_n = M$, a budeme postupně konstruovat množiny $M_{n-1}, M_{n-2}, \ldots, M_d$, přičemž M_{k-1} vznikne z M_k ubráním jednoho vektoru (takže $|M_k| = k$). Spolu s množinou M_k vyrobíme také soubor reálných koeficientů pro vektory z M_k, tj. čísla $\alpha_{k,\mathbf{v}} \in \mathbb{R}$, $\mathbf{v} \in M_k$, splňující podmínky

(i) $0 \leq \alpha_{k,\mathbf{v}} \leq 1$ pro všechna $\mathbf{v} \in M_k$,

(ii) $\sum_{\mathbf{v} \in M_k} \alpha_{k,\mathbf{v}} = k - d$,

(iii) $\sum_{\mathbf{v} \in M_k} \alpha_{k,\mathbf{v}} \mathbf{v} = 0$.

Pro $k = n$ víme, že $\sum_{\mathbf{v} \in M} \mathbf{v} = 0$, a když tedy vezmeme $\alpha_{n,\mathbf{v}} = \frac{n-d}{n}$ pro všechna $\mathbf{v} \in M_n$, budou všechny tři podmínky splněny.

Teď chceme pokročit od k ke $k-1$. Uvážíme pomocnou soustavu lineárních nerovnic a rovnic pro neznámé $x_\mathbf{v}$, $\mathbf{v} \in M_k$:

$$\begin{aligned} x_\mathbf{v} &\geq 0 \quad \text{pro všechna } \mathbf{v} \in V, && (3)\\ x_\mathbf{v} &\leq 1 \quad \text{pro všechna } \mathbf{v} \in V, && (4)\\ \sum_{\mathbf{v} \in M_k} x_\mathbf{v} &= (k-1) - d, && (5)\\ \sum_{\mathbf{v} \in M_k} x_\mathbf{v} \mathbf{v} &= 0. && (6) \end{aligned}$$

Soustava má aspoň jedno řešení, protože $x_\mathbf{v} = \frac{(k-1)-d}{k-d} \alpha_{k,\mathbf{v}}$ je podle podmínek (i)–(iii) řešením. Tvrdíme, že existuje i řešení, pro něž je některé $x_\mathbf{v} = 0$.

Nejdřív vyřídíme speciální případ: Když $k = d+1$, je pravá strana v (5) rovna 0, a proto nulový vektor je řešením.

Nyní dokazujeme tvrzení za předpokladu $k \geq d+2$ Nejdříve nahlédneme, že existuje řešení, pro něž aspoň v $k-d-1$ z nerovnic (3), (4) nastává rovnost. V soustavě máme $d+1$ rovnic (neboť (6) je rovnost dvou d-dimenzionálních vektorů), a proto množina řešení má dimenzi přinejmenším $k-d-1 \geq 1$. Vyrazíme z našeho počátečního řešení $x_\mathbf{v} = \frac{(k-1)-d}{k-d} \alpha_{k,\mathbf{v}}$ a jdeme množinou řešení po nějaké přímce, dokud nenastane v některé z nerovnic (3), (4) rovnost; geometricky, dokud nenarazíme na hranici krychle $0 \leq x_\mathbf{v} \leq 1$. Platí-li teď například rovnost $x_\mathbf{u} = 1$ pro nějaké $\mathbf{u}$, proměnnou $x_\mathbf{u}$ zafixujeme na hodnotu 1. Tím ubude jedna neznámá, a dimenze řešení naší soustavy $d+1$ rovnic klesne o 1 na $k-d-2$. Pokud tohle číslo je pořád aspoň 1, můžeme argument s přímkou a hranicí krychle zopakovat a docílit další rovnosti v jiné z nerovnic, atd. Takto dosáhneme $k-d-1$ rovností. Když aspoň jedna z těchto rovností je $x_\mathbf{v} = 0$, máme co jsme chtěli. Kdybychom měli $k-d-1$ rovností $x_\mathbf{v} = 1$, pak musí být nulová všechna ostatní $x_\mathbf{v}$ díky rovnici (5), a tvrzení platí také.

Podle tohoto tvrzení zvolíme nějaké řešení $\bar{\mathbf{x}} = (\bar{x}_\mathbf{v} : \mathbf{v} \in M_k)$ naší soustavy s aspoň jednou nulovou složkou, a vektor $\mathbf{v} \in M_k$, pro nějž $\bar{x}_\mathbf{v} = 0$, pojmenujeme $\mathbf{v}_k$ (má-li $\bar{\mathbf{x}}$ více nulových složek, vybereme z nich libovolně). To bude $\mathbf{v}_k$ jako ve větě, jak za chvíli nahlédneme. Definujeme $M_{k-1} = M_k \setminus \{\mathbf{v}_k\}$. Samozřejmě je vše přichystáno tak, že když položíme $\alpha_{k-1,\mathbf{v}} = \bar{x}_\mathbf{v}$ pro $\mathbf{v} \in M_{k-1}$, platí podmínky (i)–(iii) a indukční krok je hotov.

Teď máme definováno $\mathbf{v}_n, \mathbf{v}_{n-1}, \ldots, \mathbf{v}_{d+1}$. V M_d zbývá d neočíslovaných vektorů, a ty očíslujeme $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_d$ úplně libovolně. Nyní můžeme psát i $M_k = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$.

Odhadněme délku vektoru $\mathbf{v}_1 + \mathbf{v}_2 + \cdots + \mathbf{v}_k$. Pro $k \leq d$ jistě není víc než d, poněvadž sčítáme k vektorů délky nejvýš 1. Pro $k > d$ je hlavní trik odečíst od uvažovaného součtu výraz $\sum_{i=1}^{k} \alpha_{k,\mathbf{v}} \mathbf{v}$, rovný 0 podle (iii):

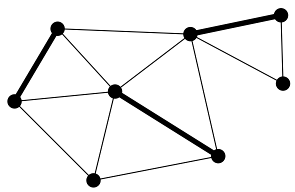
$$\begin{aligned} \|\mathbf{v}_1 + \cdots + \mathbf{v}_k\| &= \|(1-\alpha_{k,\mathbf{v}_1})\mathbf{v}_1 + \cdots + (1-\alpha_{k,\mathbf{v}_k})\mathbf{v}_k\| \leq \\ &\leq (1-\alpha_{k,\mathbf{v}_1})\|\mathbf{v}_1\| + \cdots + (1-\alpha_{k,\mathbf{v}_k})\|\mathbf{v}_k\| \leq \\ &\leq (1-\alpha_{k,\mathbf{v}_1}) + \cdots + (1-\alpha_{k,\mathbf{v}_k}) = \\ &= k - (\alpha_{k,\mathbf{v}_1} + \cdots + \alpha_{k,\mathbf{v}_k}) = k - (k-d) = d. \end{aligned}$$

Tím je důkaz věty hotov.

Poznámka. Z uvedeného důkazu ve skutečnosti plyne obecnější tvrzení, pro libovolnou konvexní ohrádku, nejen pro kruhovou: Je-li $B \subset \mathbb{R}^d$ omezená konvexní množina obsahující počátek, a je-li množina n vektorů splňující $\mathbf{v} \in B$ pro všechna $\mathbf{v} \in M$ a $\sum_{\mathbf{v}\in M} v = 0$, potom existuje pořadí $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ vektorů z M, pro něž $\mathbf{v}_1 + \mathbf{v}_2 + \cdots + \mathbf{v}_k \in dB$ pro $k = 1, 2, \ldots, n$, kde $dB = \{d\mathbf{x} : \mathbf{x} \in B\}$. Je zajímavé, že tady už je konstanta „nafouknutí“ d nejlepší možná (například v rovině to ukazuje B zvolené jako rovnostranný trojúhelník se středem v počátku).

16 Perfektní párování a determinanty

Párování v grafu G je podmnožina hran $F \subseteq E(G)$ taková, že žádný vrchol G není obsažen ve víc než jedné hraně F.



Perfektní párování je párování pokrývající všechny vrcholy. Najděte nějaké v grafu na obrázku!

Vysvětlíme poměrně jednoduchý algoritmus pro testování, zda má daný graf perfektní párování. Základní přístup je podobný jako u testování maticového násobení v oddílu 6. Probereme pouze bipartitní případ, který je jednodušší.

Uvažme bipartitní graf G. Vrcholy jsou rozděleny do dvou tříd $\{u_1, u_2, \ldots, u_n\}$ a $\{v_1, v_2, \ldots, v_n\}$ a hrany jdou jen mezi třídami, nikdy uvnitř jedné třídy. Třídy jsou přirozeně stejně velké, protože jinak bipartitní graf perfektní párování nemá. Počet hran G označme m.

Nechť S_n označuje množinu všech permutací množiny $\{1, 2, \ldots, n\}$. Každé perfektní párování v G odpovídá jednoznačně permutaci $\pi \in S_n$. Můžeme jej totiž zapsat ve tvaru $\{\{u_1, v_{\pi(1)}\}, \{u_2, v_{\pi(2)}\}, \ldots, \{u_n, v_{\pi(n)}\}\}$.

Existenci perfektního párování vyjádříme pomocí determinantu. Pro každou hranu $\{u_i, v_j\} \in E(G)$ zavedeme jednu proměnnou x_{ij}, celkem tedy m proměnných, a definujeme matici A typu $n \times n$ následovně:

$$a_{ij} = \begin{cases} x_{ij} & \text{jestliže } \{u_i, v_j\} \in E(G) \\ 0 & \text{jinak.} \end{cases}$$

Determinant matice A je mnohočlen ve zmíněných m proměnných. Podle definice determinantu dostaneme

$$\begin{aligned} \det(A) &= \sum_{\pi \in S_n} \operatorname{sign}(\pi) \cdot a_{1,\pi(1)} a_{2,\pi(2)} \cdots a_{n,\pi(n)} = \\ &= \sum_{\substack{\pi \text{ určuje perfektní} \\ \text{párování v } G}} \operatorname{sign}(\pi) \cdot x_{1,\pi(1)} x_{2,\pi(2)} \cdots x_{n,\pi(n)}. \end{aligned}$$

Tudíž když G nemá žádné perfektní párování, pak $\det(A)$ je nulový mnohočlen. Obráceně, pokud nějaká permutace π určuje perfektní párování, dosadíme do $\det(A)$ za proměnné takto: $x_{i,\pi(i)} = 1$ pro všechna $i = 1, 2, \ldots, n$, a všechna ostatní x_{ij} budou 0. Potom pro tuto permutaci π máme $\operatorname{sign}(\pi) \cdot x_{1,\pi(1)} x_{2,\pi(2)} \cdots x_{n,\pi(n)} = \pm 1$. Pro každou jinou permutaci $\sigma \neq \pi$ existuje i takové, že $\sigma(i) \neq \pi(i)$, takže $x_{i,\sigma(i)} = 0$, a tedy všechny ostatní členy v $\det(A)$ jsou nulové. Pro takto zvolená x_{ij} proto máme $\det(A) = \pm 1$. Ukázali jsme, že $\det(A)$ *je nenulový mnohočlen, právě když má G perfektní párování.*

Teď bychom chtěli poznat, jestli mnohočlen $\det(A)$ je nulový nebo ne. Nemůžeme si dovolit mnohočlen explicitně spočítat, protože má tolik členů, jako je perfektních párování v G, a to může být exponenciálně mnoho. Dosadíme-li ale za všechny proměnné x_{ij} nějaká konkrétní čísla, můžeme hodnotu $\det(A)$ snadno vyčíslit, protože pak máme co činit s determinantem číselné matice a můžeme použít třeba Gaussovu eliminaci. Můžeme si tedy myslet, že máme mnohočlen v m proměnných stupně nejvýš n daný černou skříňkou, která na požádání vrátí jeho hodnotu v kterémkoli zadaném bodě.

U obecné funkce dané černou skříňkou si nikdy nemůžeme být jisti, že je identicky 0, pokud ji nenecháme spočítat ve všech možných bodech. Ale mnohočlen nevelkého stupně má podivuhodnou vlastnost: Je buď všude roven 0, anebo skoro všude nenulový. To je kvantitativně vyjádřeno následující větou.

Schwartzova-Zippelova[2] věta. *Buď $\mathbb{K}$ libovolné těleso a $S \subseteq \mathbb{K}$ jeho konečná podmnožina. Potom pro každý nenulový mnohočlen $p(x_1, \ldots, x_m)$ stupně d v m proměnných a s koeficienty z $\mathbb{K}$ je počet uspořádaných m-tic $(r_1, r_2, \ldots, r_m)$, $r_1, r_2, \ldots, r_m \in S$, pro něž $p(r_1, r_2, \ldots, r_m) = 0$, nanejvýš $d|S|^{m-1}$. Jinak řečeno, zvolíme-li náhodně a nezávisle prvky $r_1, r_2, \ldots, r_m \in S$, potom pravděpodobnost toho, že $p(r_1, r_2, \ldots, r_m) = 0$, je maximálně $\frac{d}{|S|}$.*

[2]Tenhle Schwartz je opravdu s t, narozdíl od toho z Cauchyho-Schwarzovy nerovnosti.

Než větu dokážeme, vrátíme se k bipartitnímu párování. Předpokládejme, že G má perfektní párování, a tudíž $\det(A)$ je nenulový mnohočlen. Schwartzova-Zippelova věta ukazuje, že vypočítáme-li $\det(A)$ pro hodnoty proměnných x_{ij} vybrané náhodně a nezávisle z množiny $S = \{1, 2, \ldots, 2n\}$, potom pravděpodobnost toho, že dostaneme 0, je nejvýš $\frac{1}{2}$.

Abychom zjistili, jestli determinant je po dosazení 0, musíme jej spočítat přesně, a přitom mohou vzniknout exponenciálně velké mezivýsledky (čísla s řádově n bity), a aritmetické operace s tak velkými čísly jsou časově náročné. Lepší je počítat determinanty nad konečným tělesem. Nejjednodušší je zvolit prvočíslo p mezi $2n$ a $4n$ (podle věty z teorie čísel zvané Bertrandův postulát takové určitě existuje, a není problém jej dostatečně rychle najít) a počítat v tělese zbytkových tříd modulo p. Pak jsou aritmetické operace rychlé (je ovšem potřeba si předem připravit tabulku inverzních prvků).

Použijeme-li na výpočty determinantu obvyklou Gaussovu eliminaci, dostaneme pravděpodobnostní algoritmus na testování, zda má daný bipartitní graf perfektní párování, který běží v čase $O(n^3)$ a selže s pravděpodobností nejvýš $\frac{1}{2}$. Pravděpodobnost selhání můžeme k-násobným opakováním snížit na 2^{-k}). Algoritmy na rychlá násobení matic, zmíněné v sekci 6, lze použít i na výpočet determinantu, a pak dostaneme asymptoticky nejrychlejší známý algoritmus na testování bipartitního perfektního párování, s dobou běhu $O(n^{2.376})$.

Čestně ale přiznejme, že je znám deterministický algoritmus, který (vždy) najde maximální párování v čase $O(n^{2.5})$, a ten je v praxi podstatně rychlejší. Navíc algoritmus, o němž jsme mluvili zde, sice umí poznat, jestli perfektní párování existuje, ale žádné nenajde (existují složitější varianty, které je i najdou). Na druhé straně se probraný algoritmus dá efektivně implementovat na paralelním počítači tak, že s dostatečně mnoha procesory běží ve velmi krátkém čase. Žádný jiný přístup, který by dával srovnatelně rychlé paralelní algoritmy, znám není.

Důkaz Schwartzovy-Zippelovy věty. Postupujeme indukcí podle počtu proměnných m. Případ $m = 1$ je známá věta z algebry: Mnohočlen $p(x)$ stupně d v jedné proměnné má nanejvýš d kořenů. (Dokazuje se to indukcí podle d: Je-li $p(\alpha) = 0$, potom $p(x)$ můžeme vydělit $x - \alpha$ a snížit stupeň.)

Buď $m > 1$ a předpokládejme, že se proměnná x_1 vyskytuje aspoň v jednom členu $p(x_1, \ldots, x_m)$ (když ne, proměnné vhodně přejmenujeme). Pišme $p(x_1, \ldots, x_m)$ jako mnohočlen v proměnné x_1, přičemž každý koeficient je mnohočlen v proměnných $x_2, \ldots, x_m$:

$$p(x_1, x_2, \ldots, x_m) = \sum_{i=0}^{k} x_1^i p_i(x_2, \ldots, x_m),$$

kde k je nejvyšší mocnina x_1 vyskytující se v $p(x_1, \ldots, x_n)$.

Rozdělíme m-tice $(r_1, r_2, \ldots, r_m)$ splňující $p(r_1, \ldots, r_m) = 0$ do dvou skupin. V první skupině, již označíme R_1, jsou ty, pro něž $p_k(r_2, \ldots, r_m) = 0$. Poněvadž mnohočlen $p_k(x_2, \ldots, x_m)$ je nenulový a má stupeň maximálně $d - k$, podle indukčního předpokladu máme pro $(r_2, \ldots, r_m)$ nejvýš $(d-k)|S|^{m-2}$ možností, a proto $|R_1| \leq (d-k)|S|^{m-1}$.

Ve druhé skupině R_2 jsou zbývající m-tice, pro které $p(r_1, r_2, \ldots, r_m) = 0$, ale $p_k(r_2, \ldots, r_m) \neq 0$. Jejich počet odhadneme takto: hodnoty r_2 až r_m lze zvolit nejvýš $|S|^{m-1}$ způsoby, a jsou-li $r_2, \ldots, r_m$ již zvoleny tak, že $p_k(r_2, \ldots, r_m) \neq 0$, potom r_1 musí být kořenem mnohočlenu $q(x_1) = p(x_1, r_2, \ldots, r_n)$. Tento mnohočlen v jedné proměnné má stupeň přesně k, tudíž má nejvýš k kořenů, a tedy $|R_2| \leq k|S|^{m-1}$. Velikost obou skupin dohromady tedy není větší než $d|S|^{m-1}$, a tím je Schwartzova-Zippelova věta dokázána.

Další čtení

Vynikající učebnici o lineárně algebraických metodách v kombinatorice napsali Babai a Frankl [BF92]. Dodnes oficiálně nevyšla a je (nesnadno) dostupná jako skripta chicagské university. Je v ní látka sekcí 3, 7 a 10 a mnoho dalšího materiálu v podobném duchu, jakož i pěkný výklad některých partií lineární algebry. O algebraické teorii grafů pojednávají například knížky Biggs [Big93] a Godsil a Royle [GR01]. V posledně jmenované se najdou výsledky sekcí 13 a 8. Pravděpodobnostní algoritmy v duchu oddílů 6 a 16 jsou pěkně vysvětleny v knize Motwaniho a Raghavana [MR95]. V českém textu Matoušek a Nešetřil [MN03] je aplikacím lineární algebry v kombinatorice věnována kapitola 11, a další pěkná použití jsou v sekcích 7.5 a 8.2.

Literatura

[BF92] L. Babai and P. Frankl. *Linear Algebra Methods in Combinatorics (Preliminary version 2)*. Department of Computer Science, The University of Chicago, 1992.

[Big93] N. Biggs. *Algebraic Graph Theory*. Cambridge Univ. Press, Cambridge, 1993. 2nd edition.

[GR01] C. Godsil and G. Royle. *Algebraic Graph Theory*. Springer, New York, NY 2001.

[MN03] J. Matoušek a J. Nešetřil. *Kapitoly z diskrétní matematiky*. Nakladatelství Karolinum, Praha, opravený dotisk 2. vydání, 2003.

[MR95] R. Motwani and P. Raghavan. *Randomized Algorithms*. Cambridge University Press, Cambridge, 1995.