# FIT ČVUT

# MI-LOM

## Lineární optimalizace a metody

## *Počítání s racionálními čísly v turingovském modelu: složitost Gaussovy eliminace, maticové inverze a výpočtu determinantu*


*Evropský sociální fond*
*Praha & EU: Investujeme do vaší budoucnosti*

Michal Černý, 2011

# Počítání s racionálními čísly v turingovském modelu: složitost Gaussovy eliminace, maticové inverze a výpočtu determinantu


*Evropský sociální fond*
*Praha & EU: Investujeme do vaší budoucnosti*

## Eukleidův algoritmus

Eukleidův algoritmus je dobře znám ze školy: slouží k nalezení největšího společného dělitele daných dvou přirozených čísel $a$ a $b$.

Eukleidův algoritmus pracuje podle následujícího schematu. Nechť platí $2 \leqslant b < a$.

*Krok* $i = 1$. Položíme

$$\boldsymbol{X}_1 := \begin{pmatrix} a & b \\ 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

*Krok* $i > 1$. Je zkonstruována matice

$$\boldsymbol{X}_{i-1} = \begin{pmatrix} a_{i-1} & b_{i-1} \\ \cdot & \cdot \\ \cdot & \cdot \end{pmatrix}.$$

Jestliže $\min\{a_{i-1}, b_{i-1}\} = 0$, skončíme; největším společným dělitelem čísel $a, b$ je

$$l := \max\{a_{i-1}, b_{i-1}\}.$$

Je-li $\min\{a_{i-1}, b_{i-1}\} > 0$, zkonstruujeme matici $\boldsymbol{X}_i$. Jestliže $i$ je sudé, získáme matici $\boldsymbol{X}_i$ z matice $\boldsymbol{X}_{i-1}$ přičtením $\mathtt{div}(a_{i-1}, b_{i-1})$-násobku druhého sloupce k prvnímu. Jestliže $i$ je liché, získáme matici $\boldsymbol{X}_i$ z matice $\boldsymbol{X}_{i-1}$ přičtením $\mathtt{div}(b_{i-1}, a_{i-1})$-násobku prvního sloupce k druhému.

**Tvrzení 1.** *(a) Eukleidův algoritmus spočte největší společný dělitel čísel $a$ a $b$.*

*(b) Počítá v polynomiálním čase.*

*(c) Pomocí algoritmu dokážeme v polynomiálním čase k daným $\nu$ a $x$, kde $\nu \geqslant 2$, $1 \leqslant x < \nu$ a $x$ a $\nu$ jsou nesoudělná, najít číslo $y$, pro něž platí $1 \leqslant y < \nu$, $y$ je nesoudělné s $\nu$ a $xy \equiv_\nu 1$.*

**Důkaz.** Algoritmus zřejmě počítá v konečném čase, protože $\min\{a_i, b_i\}$ jsou přirozená čísla a $\min\{a_i, b_i\} < \min\{a_{i-1}, b_{i-1}\}$. Nechť algoritmus skončí v kroku $n + 1$ (tj. skončili jsme s maticí $\boldsymbol{X}_n$ s nulou v prvním řádku).

Ukažme korektnost (tvrzení (a)). Snadno se vidí, že

$$(z \mid a \ \ \& \ \ z \mid b) \longrightarrow z \mid a - b.$$

To znamená, že jestliže $a_i > b_i$, pak největší společný dělitel dvojice čísel $(a_i, b_i)$ je stejný jako největší společný dělitel dvojice čísel $(a_i - b_i, b_i)$, a ten je stejný jako největší společný dělitel dvojice čísel $(a_i - 2b_i, b_i)$ etc. Tedy, největší společný dělitel dvojice čísel $(a_i, b_i)$ je stejný jako největší společný dělitel dvojice čísel $(a_i - k \cdot b_i, b_i)$, kde $k = \mathtt{div}(a_{i-1}, b_{i-1})$. (Podobně v případě

$a_i < b_i$). Tím máme zaručeno, že pro každé $i, j \leqslant n$ platí: největší společný dělitel dvojice čísel $(a_i, b_i)$ a největší společný dělitel čísel $(a_j, b_j)$ je stejný. Protože $a_1 = a, b_1 = b$ a největší společný dělitel čísel $a_n, b_n$ je $\max\{a_n, b_n\}$ (ježto jedno z čísel $a_n, b_n$ je nulové), je tvrzení (a) dokázáno.

*Důkaz (c).* Nechť v $n$-tém kroku skončil výpočet algoritmu tak, že $b_n = 0$. (Případ, kdy se skončí s $a_n = 0$, se probere stejně.) Označme

$$\boldsymbol{X}_n = \begin{pmatrix} l & 0 \\ \alpha & \beta \\ \gamma & \delta \end{pmatrix};$$

víme již z (a), že $l$ je největší společný dělitel čísel $a$ a $b$.

Označme dále $\boldsymbol{X}_i^{[j]}$ matici, která vznikne z matice $\boldsymbol{X}_i$ vypuštěním $j$-tého řádku. S maticemi $\boldsymbol{X}_i^{[1]}, \boldsymbol{X}_i^{[2]}$ a $\boldsymbol{X}_i^{[3]}$ jsme dělali jen úpravy, které nemění determinant (přičítání násobku jednoho sloupce k druhému), a tak platí

$$\det \boldsymbol{X}_n^{[1]} = \det \boldsymbol{X}_1^{[1]}, \quad \det \boldsymbol{X}_n^{[2]} = \det \boldsymbol{X}_1^{[2]}, \quad \det \boldsymbol{X}_n^{[3]} = \det \boldsymbol{X}_1^{[3]}.$$

To je, jinými slovy,

$$\alpha\delta - \beta\gamma = 1,$$
$$l\delta = a,$$
$$l\beta = -b.$$

Vyjádřením $\delta$ a $\beta$ z druhé a třetí rovnice a dosazením do první obdržíme

$$\alpha a + \gamma b = l,$$

a protože $\alpha, \gamma$ jsou celá čísla, našli jsme vyjádření $l$ v podobě celočíselné lineární kombinace čísel $a, b$. Jestliže $a, b$ jsou nesoudělná, je $l = 1$. Odtud

$$\alpha a + \gamma b = 1.$$

Položíme-li $b := x$, $a := \nu$, obdržíme

$$\alpha\nu + \gamma x = 1.$$

Jest $\texttt{mod}(\gamma, \nu)$ hledané číslo $y$. Je jasné, že $\gamma$, a tudíž i $y$, je nesoudělné s $\nu$. Kdyby totiž pro některé prvočíslo $p \geqslant 2$ bylo $p \mid \nu$ a $p \mid \gamma$, pak $p \mid (\alpha\nu + \gamma x)$, a tedy $p \mid 1$ — spor.

*Důkaz (b).* K důkazu polynomiality algoritmu je třeba nahlédnout, že počítá v čase $poly(N)$, kde $N := \log_2 a + \log_2 b$.

V sudém kroku $i$ měníme v prvním řádku matice číslo $a_{i-1}$ na číslo $a_i$; přitom platí $a_i \leqslant \frac{1}{2} a_{i-1}$. Podobně, v lichých krocích platí $b_i \leqslant \frac{1}{2} b_{i-1}$, takže algoritmus skončí nanejvýš po

$$n := \text{konst.} + \lceil \log_2 a \rceil + \lceil \log_2 b \rceil = O(N)$$

iteracích.

Pak je třeba nahlédnout, že výpočetní čas uvnitř jedné iterace je omezen polynomem v $N$. Děláme jen výpočetně jednoduché operace (celočíselné dělení, přičítání sloupců v matici) s celými čísly, které jistě lze realisovat v polynomiálním čase v délce zápisu operandů; stačí tedy ukázat, že délka zápisu čísel v každé z matic $\boldsymbol{X}_i$ je omezena polynomem v $N$.

Označme

$$\boldsymbol{X}_i = \begin{pmatrix} a_i & b_i \\ \alpha_i & \beta_i \\ \gamma_i & \delta_i \end{pmatrix}.$$

Připomeňme, že v celé kapitole předpokládáme, že $2 \leqslant b < a$. Pro každé $i = 1, 2, \ldots, n$ platí

$$\mathtt{div}(a_i, b_i) \leqslant a - 1,$$

je-li $a_i > b_i$, a

$$\mathtt{div}(b_i, a_i) \leqslant a - 1,$$

je-li $a_i < b_i$. Indukcí ukážeme, že pro každé $i$ platí

$$|\alpha_i| \leqslant a^i, \quad |\beta_i| \leqslant a^i, \quad |\gamma_i| \leqslant a^i, \quad |\delta_i| \leqslant a^i.$$

Pro $i = 1$ je to zřejmé. Ukažme indukční krok např. pro $\alpha_i$; pro $\beta_i$ etc. je to stejné. Nechť v $i$-tém kroku přičítáme k $\alpha_i$ číslo $\mathtt{div}(b_{i-1}, a_{i-1}) \cdot \beta_{i-1}$. Pak jest

$$|\alpha_i| \leqslant \underbrace{|\alpha_{i-1}|}_{\substack{\text{i.p.} \\ \leqslant a^{i-1}}} + \underbrace{|\mathtt{div}(b_{i-1}, a_{i-1})|}_{\leqslant a-1} \cdot \underbrace{|\beta_{i-1}|}_{\substack{\text{i.p.} \\ \leqslant a^{i-1}}} \leqslant a^i$$

(i.p. značí indukční předpoklad). K zápisu každého z čísel $\alpha_i$ potřebujeme nanejvýš

$$\mathit{konst.} + \log_2 a^i \leqslant \mathit{konst.} + \log_2 a^n = \mathit{konst.} + n \log_2 a = O(N^2)$$

bitů; z předchozího totiž víme, že $n = O(N)$ a $\log_2 a = O(N)$. □

**Zobecněný Eukleidův algoritmus.** Popišme versi algoritmu, která dokáže najít největší společný dělitel souboru přirozených čísel $a_1, \ldots, a_n$. Položme $a_1^{[1]} := a_1, \ldots, a_n^{[1]} := a_n$. Jestliže máme z $(i-1)$-tého kroku k disposici čísla $a_1^{[i-1]}, \ldots, a_n^{[i-1]}$, najdeme libovolné dva indexy $j \neq k$ takové, že $0 < a_j^{[i-1]} \leqslant a_k^{[i-1]}$ a položíme

$$a_k^{[i]} := \mathtt{mod}(a_k^{[i-1]}, a_j^{[i-1]}), \quad a_j^{[i]} := a_j^{[i-1]} \quad \text{pro } j \neq k.$$

(Můžeme také říci: v $i$-tém kroku přičítáme $(-\lfloor \frac{a_k^{[i-1]}}{a_j^{[i-1]}} \rfloor)$-násobek čísla $a_j^{[i-1]}$ k číslu $a_k^{[i-1]}$; ostatní čísla se nemění.) Skončíme v kroku $N$, jakmile soubor čísel $a_1^{[N]}, \ldots, a_n^{[N]}$ obsahuje jediné nenulové číslo; toto nenulové číslo je hledaný největší společný dělitel.

**Věta 2.** *Algoritmus je správný a počítá v polynomiálním čase.*

**Důkaz.** Nechť $a_j \geqslant 1$ pro všechna $j \in J := \{1, \ldots, n\}$. Velikost vstupu je (řádově) $L := \sum_{j=1}^n \log_2 a_j$. Uvažme funkci

$$f(i) := \prod_{j' \in \{j \in J:\ a_j^{[i]} \neq 0\}} a_{j'}^{[i]}.$$

Jistě platí $\frac{f(i+1)}{f(i)} \leqslant \frac{1}{2}$ (protože v každém kroku se jedno z čísel seznamu zmenší přinejmenším na polovinu); odtud plyne, že algoritmus skončí nanejvýš po $\log_2 f(1) = \sum_{i=1}^n \log_2 a_i = L$ iteracích. Práci uvnitř jedné iterace lze jistě realisovat v polynomiálním čase. Během výpočtu se vyskytnou jen čísla $\leqslant \max\{a_1, \ldots, a_n\}$.

Je jasné, že dokud v seznamu $a_1^{[i]}, \ldots, a_n^{[i]}$ existují alespoň dvě nenulová čísla, je volba indexů $j$ a $k$ možná; algoritmus proto nemůže skončit jinak než v situaci, kdy je v seznamu $a_1^{[N]}, \ldots, a_n^{[N]}$ jediné nenulové číslo.

Pro každé $i$ platí, že největší společný dělitel systému čísel $a_1^{[i]}, \ldots, a_n^{[i]}$ je stejný jako největší společný dělitel systému čísel $a_1^{[i+1]}, \ldots, a_n^{[i+1]}$ — přičtení celočíselného násobku některého čísla

ze systému k jinému číslu ze systému totiž největší společný dělitel systému nemění. A je jasné, že největší společný dělitel systému čísel, které obsahuje jediné nenulové číslo $\delta$, je $\delta$. Odtud také plyne, že je-li více možných voleb dvojice indexů $j$ a $k$, libovolná z nich vede ke správnému výsledku. □

Při popisu Lenstrova algoritmu se bude hodit také tento výsledek.

**Důsledek 3.** *Nechť systém přirozených čísel $a_1, \ldots, a_n$ je nesoudělný.*[1] *V polynomiálním čase lze najít celočíselnou matici $\boldsymbol{U}$ rozměru $n \times n$ takovou, že její první řádek tvoří vektor $(a_1, \ldots, a_n)$ a matice $\boldsymbol{U}$ vznikne z jednotkové matice konečnou posloupností těchto operací: prohození sloupců, přičtení celočíselného násobku sloupce k jinému sloupci.*

**Důkaz.** Spusťme zobecněný Eukleidův algoritmus na systém čísel $a_1, \ldots, a_n$. Protože je nesoudělný, v posledním ($N$-tém) kroku obsahuje systém $a_1^{[N]}, \ldots, a_n^{[N]}$ jediné nenulové číslo, a je rovno jedné. Řekněme, že je to $a_z^{[N]}$.

Nechť matice $\boldsymbol{U}_1$ vznikne z jednotkové matice prohozením prvního a $z$-tého sloupce.

Nyní pro $i = 1, \ldots, N-1$: jestliže jsme v $(N-i+1)$-tém kroku Eukleidova algoritmu odečítali $\alpha_{N-i+1}$-násobek čísla $a_j^{[N-i]}$ od čísla $a_k^{[N-i]}$, vznikne matice $\boldsymbol{U}_{i+1}$ z matice $\boldsymbol{U}_i$ přičtením $\alpha_{N-i+1}$-násobku $j$-tého sloupce ke $k$-tému sloupci. Výstupem programu je $\boldsymbol{U} := \boldsymbol{U}_N$.

Snadno se vidí, že v prvním řádku matice $\boldsymbol{U}_{i+1}$ je vektor $(a_1^{[N-i]}, \ldots, a_n^{[N-i]})$, a tedy matice $\boldsymbol{U}_N$ má v prvním řádku vektor $(a_1^{[1]}, \ldots, a_n^{[1]}) = (a_1, \ldots, a_n)$. To znamená, že algoritmus počítá správně a má polynomiální počet iterací.

Zbývá ukázat, že během výpočtu se vyskytnou jen krátká čísla. Matice $\boldsymbol{U}_i$ jsou zřejmě nezáporné. Pro každé $i$ platí $1 \leqslant \alpha_i \leqslant M-1$, kde $M := \max\{a_1, \ldots, a_n\}$. Indukcí ukážeme, že pro každé číslo $u$ v matici $\boldsymbol{U}_{i+1}$ platí $u \leqslant M^{i+1}$. Pro $i = 0$ je to zřejmé. Je-li to pravda pro $i$, víme, že každé číslo $v_{lk}$ ($l = 1, \ldots, n$, $k = 1, \ldots, n$) v matici $\boldsymbol{U}_i$ splňuje $v_{lk} \leqslant M^i$. Číslo $u_{lk}$ v matici $\boldsymbol{U}_{i+1}$ vzniklo jako $v_{lk} + \alpha_{N-i+1} \cdot v_{lj}$ pro některé $j \neq k$. Odtud

$$u_{lk} = v_{lk} + \alpha_{N-i+1} \cdot v_{lj} \leqslant M^i + (M-1)M^i = M^{i+1}.$$

Tedy, libovolné číslo, které se během výpočtu vyskytne, lze zapsat řádově pomocí $\log_2 M^i \leqslant \log_2 M^N = N \cdot \log_2 M \leqslant L^2$ bitů (užíváme $\log_2 M \leqslant L$, $N \leqslant L$). □

## Velikost zápisu racionálních čísel, vektorů a matic

Na chvíli si představme, že máme k disposici abecedu $\{0, 1, \#, @\}$ (namísto tradiční abecedy $\{0, 1\}$); symboly 0 a 1 budeme užívat k dvojkovému zápisu čísel a symboly $\#, @$ jako oddělovače. Počet symbolů, kterých je třeba k zápisu čísel, vektorů a matic v této abecedě, budeme značit $\sigma(\cdot)$. Je-li $n \geqslant 1$ přirozené číslo, klademe

$$\sigma_{\mathbb{N}}(n) := \lceil \log_2(n+1) \rceil;$$

definujme ještě $\sigma_{\mathbb{N}}(0) = 1$. Pro celé číslo $z$ položíme

$$\sigma_{\mathbb{Z}}(z) := \sigma_{\mathbb{N}}(|z|) + 1,$$

protože potřebujeme bit na znaménko. Nenulové racionální číslo $q = \frac{a}{b}$, kde $a$ je celé a $b$ přirozené číslo ($a$, $b$ nesoudělná), zapíšeme jako $a \frown \# \frown b$. Potřebujeme tedy

$$\sigma_{\mathbb{Q}}(q) := \sigma_{\mathbb{Z}}(a) + 1 + \sigma_{\mathbb{N}}(b) \tag{1}$$

[1] To znamená: největší společný dělitel systému čísel $a_1, \ldots, a_n$ je 1.

symbolů; racionální nulu budeme zapisovat jako $+\frac{0}{1}$.

Racionální matici zapíšeme tak, že čísla v řádku budeme oddělovat symbolem # a konec řádku oddělíme @. Pak na zápis matice $\boldsymbol{A}$ rozměru $m \times n$ potřebujeme

$$\sigma_{\mathbb{Q}}(\boldsymbol{A}) := mn + \sum_{i,j} \sigma_{\mathbb{Q}}((\boldsymbol{A})_{i,j}) \tag{2}$$

symbolů. Vektor je speciálním případem matice. Analogicky bychom definovali $\sigma_{\mathbb{Z}}$ velikost zápisu celočíselné matice a celočíselného vektoru.

Nadále u symbolu $\sigma$ nebudeme psát dolní index $_{\mathbb{N},\mathbb{Z},\mathbb{Q}}$, je-li z kontextu patrné, o jaký typ čísel se jedná.

Není příliš důležité, že pracujeme v abecedě $\{0,1,\#,@\}$; tradičním způsobem můžeme pomocí přiřazení $0 \mapsto 00$, $1 \mapsto 01$, $\# \mapsto 10$, $@ \mapsto 11$ přejít ke standardní abecedě $\{0,1\}$. Tím se počet symbolů zdvojnásobí; pro naše účely však prodloužení vstupu na dvojnásobek nemá vliv. Budeme-li nadále hovořit o čísle $\sigma(x)$, budeme často říkat, že se jedná o *počet bitů* k zápisu čísla (vektoru, matice) $x$; je to vyjádření nepřesné, leč pro naše účely přijatelné.

Chceme-li prokázat, že algoritmus, který pracuje (řekněme) s racionální maticí $\boldsymbol{A}$, počítá v polynomiálním čase, je třeba ukázat, že jeho čas je omezen polynomem v proměnné $\sigma(\boldsymbol{A})$. Tradičně se pro $\sigma(\boldsymbol{A})$ používá též symbol $L$.

Při počítání s racionálními čísly budeme pracovat v racionální aritmetice. To znamená, že racionální číslo representujeme jako dvojici [čitatel: celé číslo, jmenovatel: kladné celé číslo]; aritmetické operace se zlomky jsou definovány přirozeně, např. $[a,b]+[c,d] = [\frac{ad+bc}{g}, \frac{bd}{g}]$, kde $g$ je největší společný dělitel čísel $ad+bc$ a $bd$. Eukleidův algoritmus zajistí, že takto definovanou aritmetickou operaci lze realisovat v polynomiálním výpočetním čase. To je důležité pozorování, protože Eukleidův algoritmus nám dovolí udržovat během výpočtu zlomky *v úsporném tvaru*, a to dokonce v nejúspornějším možném (co do počtu bitů k zápisu čitatele a jmenovatele). *Ukážeme-li tedy, že některé racionální číslo lze zapsat pomocí omezeného počtu bitů, pak tohoto zápisu se dosáhne užitím Eukleidova algoritmu.* Naivní implementace algoritmů pracujících s racionálními čísly bez Eukleidova algoritmu může snadno vést do situace, kdy velikosti zápisů čísel vyskytujících se během výpočtu exponenciálně narůstají. Ačkoliv to nadále nebudeme zdůrazňovat, počítáme s tím, že Eukleidův algoritmus je nedílnou součástí procedur pro aritmetické operace.

Všimněme si, že během výpočtu, který běží v polynomiálním čase, *mohou celá čísla růst exponenciálně*, ale nesmí exponenciálně růst jejich logaritmy. U zlomků bývá obvykle třeba zvlášť ošetřit velikost zápisu čitatele a zvlášť velikost zápisu jmenovatele; mohlo by se totiž stát, že délka zápisu racionálního čísla je velká proto, že samo číslo je velké, anebo také proto, že racionální číslo je (například) velmi blízko nuly.

**Lemma 4.** *Budiž $\boldsymbol{A}$ celočíselná matice rozměru $n \times n$. Pak*

$$\sigma(\det \boldsymbol{A}) < \sigma(\boldsymbol{A}).$$

**Důkaz.** Případ s $n = 1$ je jasný, buď $n \geqslant 2$. Mějme dánu matici $\boldsymbol{A} = (a_{ij})$. Z definice determinantu je

$$|\det \boldsymbol{A}| \leqslant \sum_{\pi} |a_{1,\pi(1)}| \cdot |a_{2,\pi(2)}| \cdots |a_{n,\pi(n)}|, \tag{3}$$

kde se sčítá přes permutace $\pi$ množiny $\{1,2,\ldots,n\}$. Platí

$$|\det \boldsymbol{A}| \leqslant \prod_{i,j=1}^{n} (|a_{ij}|+1),$$

protože roznásobíme-li závorky ve výrazu $\prod_{i,j=1}^{n}(|a_{ij}|+1)$, obdržíme dlouhý součet, ve kterém se vyskytují i všechny $n$-členné součiny čísel $|a_{ij}|$, které se vyskytují v sumě (3), a ještě toho hodně zbyde. Proto

$$\sigma(\det \boldsymbol{A}) = 1 + \lceil \log_2(1 + |\det \boldsymbol{A}|)\rceil \leqslant 1 + \lceil \log_2(1 + \prod_{i,j=1}^{n}(|a_{ij}|+1))\rceil$$
$$\leqslant 1 + \lceil \log_2(2 \cdot \prod_{i,j=1}^{n}(|a_{ij}|+1))\rceil = 2 + \lceil \sum_{i,j=1}^{n} \underbrace{\log_2(|a_{ij}|+1)}_{\leqslant \sigma(a_{ij})}\rceil < n^2 + \sum_{i,j=1}^{n}\sigma(a_{ij}) = \sigma(\boldsymbol{A}).$$

□

## Gaussova eliminace

Zavedeme následující označení: k dané matici $\boldsymbol{Q}$ rozměru $m \times n$ a množinám $I \subseteq \{1,2,\ldots,m\}$, $J \subseteq \{1,2,\ldots,n\}$ buď $\boldsymbol{Q}[I,J]$ matice, která z $\boldsymbol{Q}$ vznikne vypuštěním všech řádků s indexy $i \notin I$ a všech sloupců s indexy $j \notin J$.

Gaussova eliminace je tento algoritmus. Mějme dánu celočíselnou matici $\boldsymbol{A}$ rozměru $m \times n$ a celočíselný vektor $\boldsymbol{b}$ rozměru $m \times 1$. Začneme s $\boldsymbol{X}_0 := (\boldsymbol{A}\ \boldsymbol{b})$ a konstruujeme posloupnost matic

$$\boldsymbol{X}_k = \begin{pmatrix} \boldsymbol{E}_k & \boldsymbol{F}_k \\ \boldsymbol{0} & \boldsymbol{G}_k \end{pmatrix},$$

kde $\boldsymbol{E}_k$ je *regulární* horní trojúhelníková matice rozměru $k \times k$, nulová matice je rozměru $(m-k) \times k$, $\boldsymbol{F}_k$ je rozměru $k \times (n+1-k)$ a $\boldsymbol{G}_k$ je rozměru $(m-k) \times (n+1-k)$.

Skončíme po dokončení $K$-té iterace, je-li $\boldsymbol{G}_K$ matice s jediným sloupcem nebo je-li $\boldsymbol{G}_K$ matice obsahující mimo poslední sloupec samé nuly. Se znalostí $\boldsymbol{X}_K$ již snadno dokážeme rozhodnout, zdali soustava $\boldsymbol{Ax} = \boldsymbol{b}$ má řešení, a pokud ano, některé řešení v polynomiálním čase najít.

Při konstrukci $\boldsymbol{X}_k$ z $\boldsymbol{X}_{k-1}$ postupujeme tak, že

(a) mezi prvními $n-k+1$ sloupci matice $\boldsymbol{G}_{k-1}$ najdeme sloupec, řekněme $i$-tý, který obsahuje alespoň jedno nenulové číslo (pokud takový neexistuje, končíme);

(b) v matici $\boldsymbol{X}_{k-1}$ prohodíme $k$-tý s $(k+i)$-tým sloupcem.

Dostaneme tak matici $\boldsymbol{X}'$. Tím se nám změnila matice $\boldsymbol{G}_{k-1}$ na jistou matici $\boldsymbol{G}'$ (prohodil se její první a $i$-tý sloupec), jež má v prvním sloupci alespoň jedno nenulové číslo. Nechť je (některé) nenulové číslo v $j$-tém řádku $\boldsymbol{G}'$.

(c) V matici $\boldsymbol{X}'$ prohodíme $(k+j-1)$-tý řádek s $k$-tým řádkem.

Dostaneme tak matici $\boldsymbol{X}''$, která má na posici $(k,k)$ nenulové číslo. Pak

(d) pro každé $i = k+1, k+2, \ldots, m$, provedeme s $\boldsymbol{X}''$ následující: přičteme $\left(-\frac{(\boldsymbol{X}'')_{ik}}{(\boldsymbol{X}'')_{kk}}\right)$-násobek $k$-tého řádku $\boldsymbol{X}''$ k $i$-tému řádku $\boldsymbol{X}''$.

Výsledná matice je $\boldsymbol{X}_k$. Je vidět, že jsme řádky a sloupce přeházeli tak, že matice

$$\boldsymbol{E}_k = \boldsymbol{X}_k[\{1,\ldots,k\},\{1,\ldots,k\}]$$

je regulární.

**Příklad.** Uvažme

$$\boldsymbol{A} = \begin{pmatrix} 0 & 0 & 2 & 1 & 1 \\ 0 & 4 & 2 & 2 & 4 \\ 0 & 6 & 3 & 3 & 2 \\ 0 & 2 & 1 & 1 & 4 \end{pmatrix}, \quad \boldsymbol{b} = \begin{pmatrix} 1 \\ 3 \\ 5 \\ 1 \end{pmatrix};$$

Gaussovou eliminací rozhodneme o existenci reálného řešení systému $\boldsymbol{Ax} = \boldsymbol{b}$. Čarami je v maticích $\boldsymbol{X}_k$ naznačeno rozdělení $\left(\begin{array}{c|c} \boldsymbol{E}_k & \boldsymbol{F}_k \\ \hline \boldsymbol{0} & \boldsymbol{G}_k \end{array}\right)$.

$$\boldsymbol{X}_0 = \left(\begin{array}{cccccc} x_1 & x_2 & x_3 & x_4 & x_5 & \boldsymbol{b} \\ \hline 0 & 0 & 2 & 1 & 1 & 1 \\ 0 & 4 & 2 & 2 & 4 & 3 \\ 0 & 6 & 3 & 3 & 2 & 5 \\ 0 & 2 & 1 & 1 & 0 & 1 \end{array}\right) \xrightarrow{\text{(a), (b) s } i=2} \begin{pmatrix} x_2 & x_1 & x_3 & x_4 & x_5 & \boldsymbol{b} \\ 0 & 0 & 2 & 1 & 1 & 1 \\ 4 & 0 & 2 & 2 & 4 & 3 \\ 6 & 0 & 3 & 3 & 2 & 5 \\ 2 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{\text{(c) s } j=4} \begin{pmatrix} x_2 & x_1 & x_3 & x_4 & x_5 & \boldsymbol{b} \\ 2 & 0 & 1 & 1 & 0 & 1 \\ 4 & 0 & 2 & 2 & 4 & 3 \\ 6 & 0 & 3 & 3 & 2 & 5 \\ 0 & 0 & 2 & 1 & 1 & 1 \end{pmatrix} \xrightarrow{\text{(d)}} \left(\begin{array}{cccccc} x_2 & x_1 & x_3 & x_4 & x_5 & \boldsymbol{b} \\ \hline 2 & 0 & 1 & 1 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 & 4 & 1 \\ 0 & 0 & 0 & 0 & 2 & 2 \\ 0 & 0 & 2 & 1 & 1 & 1 \end{array}\right) = \boldsymbol{X}_1$$

$$\xrightarrow{\text{(a),(b) s } i=2} \begin{pmatrix} x_2 & x_3 & x_1 & x_4 & x_5 & \boldsymbol{b} \\ 2 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 4 & 1 \\ 0 & 0 & 0 & 0 & 2 & 2 \\ 0 & 2 & 0 & 1 & 1 & 1 \end{pmatrix} \xrightarrow{\text{(c) s } j=3} \begin{pmatrix} x_2 & x_3 & x_1 & x_4 & x_5 & \boldsymbol{b} \\ 2 & 1 & 0 & 1 & 0 & 1 \\ 0 & 2 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 4 & 1 \end{pmatrix}$$

$$\xrightarrow{\text{(d)}} \left(\begin{array}{cccccc} x_2 & x_3 & x_1 & x_4 & x_5 & \boldsymbol{b} \\ \hline 2 & 1 & 0 & 1 & 0 & 1 \\ 0 & 2 & 0 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 4 & 1 \end{array}\right) = \boldsymbol{X}_2 \xrightarrow{\text{(a),(b) s } i=3} \begin{pmatrix} x_2 & x_3 & x_5 & x_4 & x_1 & \boldsymbol{b} \\ 2 & 1 & 0 & 1 & 0 & 1 \\ 0 & 2 & 1 & 1 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 & 2 \\ 0 & 0 & 4 & 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{\text{(d)}} \left(\begin{array}{cccccc} x_2 & x_3 & x_5 & x_4 & x_1 & \boldsymbol{b} \\ \hline 2 & 1 & 0 & 1 & 0 & 1 \\ 0 & 2 & 1 & 1 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 & 2 \\ \hline 0 & 0 & 0 & 0 & 0 & -3 \end{array}\right) = \boldsymbol{X}_3.$$

Když je zkonstruována matice $\boldsymbol{X}_3$, výpočet končí, ježto v $\boldsymbol{G}_3 = (0\ 0\ -3)$ jsou kromě posledního sloupce samé nuly. Zřejmě systém $\boldsymbol{Ax} = \boldsymbol{b}$ nemá řešení, neboť z posledního řádku $\boldsymbol{X}_3$ plyne spor $0x_2 + 0x_3 + 0x_5 + 0x_4 + 0x_1 = -3$. □

Velikost vstupu označíme

$$L := \sigma((\boldsymbol{A}\ \boldsymbol{b})).$$

**Věta 5.** *Pro celočíselnou matici $\boldsymbol{A}$ a celočíselný vektor $\boldsymbol{b}$ běží Gaussova eliminace v polynomiálním čase.*

**Důkaz.** Ukážeme, že pro $k \leqslant K$ mají všechna čísla v matici

$$\boldsymbol{G}_k = \boldsymbol{X}_k[\{k+1, \ldots, n+1\}, \{k+1, \ldots, m\}]$$

velikost zápisu omezenou $O(L)$.

Základní trik je v tomto pozorování. Pro účely následující úvahy můžeme bez újmy na obecnosti předpokládat, že jsme nepřehazovali žádné řádky ani sloupce. Pro každé $1 < k \leqslant K$, $i \in \{1, \ldots, m-k\}$ a $j \in \{1, \ldots, n+1-k\}$ je

$$(\boldsymbol{G}_k)_{i,j} = \frac{\det \boldsymbol{X}_k[\{1, \ldots, k, k+i\}, \{1, \ldots, k, k+j\}]}{\det \boldsymbol{E}_k}. \tag{4}$$

Opravdu, poslední řádek matice $\boldsymbol{X}_k[\{1,\ldots,k,k+i\},\{1,\ldots,k,k+j\}]$ obsahuje samé nuly, kromě posledního místa, kde je (obecně) nenulové číslo $(\boldsymbol{G}_k)_{i,j}$. Rozvojem

$$\det \boldsymbol{X}_k[\{1,\ldots,k,k+i\},\{1,\ldots,k,k+j\}]$$

podle posledního řádku dostaneme, že

$$\det \boldsymbol{X}_k[\{1,\ldots,k,k+i\},\{1,\ldots,k,k+j\}] = (\boldsymbol{G}_k)_{i,j} \cdot \det \boldsymbol{E}_k.$$

Tím je dokázáno (4).

Učiňme toto pozorování: *matice $\boldsymbol{E}_k$ vznikla z matice*

$$(\boldsymbol{A}\ \boldsymbol{b})[\{1,\ldots,k\},\{1,\ldots,k\}]$$

*pouze přičítáním násobků řádků k jiným řádkům.* To platí, protože v krocích $1,\ldots,k-1$ jsme přičítali k dalším řádkům pouze násobky prvních $(k-1)$ řádků v matici $(\boldsymbol{A}\ \boldsymbol{b})$. To jsou ovšem operace, které nemění determinant.

Díky pozorování platí

$$\det \boldsymbol{E}_k = \det(\boldsymbol{A}\ \boldsymbol{b})[\{1,\ldots,k\},\{1,\ldots,k\}].$$

Odtud s pomocí lemmatu 3 plyne

$$\begin{aligned}\sigma(\det \boldsymbol{E}_k) = \sigma(\det(\boldsymbol{A}\ \boldsymbol{b})[\{1,\ldots,k\},\{1,\ldots,k\}]) \leqslant \\ \leqslant \sigma((\boldsymbol{A}\ \boldsymbol{b})[\{1,\ldots,k\},\{1,\ldots,k\}]) \leqslant \sigma((\boldsymbol{A}\ \boldsymbol{b})) = L. \quad (5)\end{aligned}$$

Podobně se vidí, že matice $\boldsymbol{X}_k[\{1,\ldots,k,k+i\},\{1,\ldots,k,k+j\}]$ vznikla z matice

$$(\boldsymbol{A}\ \boldsymbol{b})[\{1,\ldots,k,k+i\},\{1,\ldots,k,k+j\}]$$

jen přičítáním násobků řádků k jiným řádkům, odkud

$$\begin{aligned}\sigma(\det \boldsymbol{X}_k[\{1,\ldots,k,k+i\},\{1,\ldots,k,k+j\}]) = \\ = \sigma(\det(\boldsymbol{A}\ \boldsymbol{b})[\{1,\ldots,k,k+i\},\{1,\ldots,k,k+j\}]) \leqslant \\ \leqslant \sigma((\boldsymbol{A}\ \boldsymbol{b})[\{1,\ldots,k,k+i\},\{1,\ldots,k,k+j\}]) \leqslant \sigma((\boldsymbol{A}\ \boldsymbol{b})) = L. \quad (6)\end{aligned}$$

Z (5) a z (6) vyplývá, že v (4) nám na zápis jak čitatele, tak i jmenovatele čísla $(\boldsymbol{G}_k)_{i,j}$ stačí $L$ bitů. Racionální číslo $(\boldsymbol{G}_k)_{i,j}$ lze tudíž zapsat pomocí $O(L)$ bitů.

Pro čísla v maticích $\boldsymbol{E}_k$ a $\boldsymbol{F}_k$ platí, že v některém z předchozích kroků figurovala v některé z matic $\boldsymbol{G}_j$ s $j < k$; nadále se tato čísla již nemění. Tak nám (z indukce) k jejich zápisu též stačí $O(L)$ bitů.

Abychom při implementaci Gaussovy eliminace opravdu dosáhli toho, že čísla budou representována „úsporně“ (ukázali jsme, že to lze), je třeba vždy při provedení aritmetické operace spustit Eukleidův algoritmus, kterým se zlomky zkrátí, aby čitatel a jmenovatel tvořila nesoudělná čísla.

Celkem provádíme $poly(L)$ aritmetických operací (jednoduchých, jistě v racionální aritmetice implementovatelných v polynomiálním čase) na čísla velikosti $poly(L)$, přičemž $poly(L)$-krát spouštíme Eukleidův algoritmus, který pracuje v polynomiálním čase. □

Je-li zadaný systém racionální, lze každý řádek $a_1x_1+\cdots+a_nx_n = b$ soustavy rovnic $\boldsymbol{Ax} = \boldsymbol{b}$ přenásobit součinem jmenovatelů čísel $a_1,\ldots,a_n,b$. Tím dostaneme ekvivalentní celočíselnou soustavu rovnic $\boldsymbol{A'x} = \boldsymbol{b'}$, jejíž velikost zápisu je $O(L^2)$, a můžeme užít právě dokázanou větu. Proto:

**Důsledek 6.** *Pro racionální matici $\boldsymbol{A}$ a racionální vektor $\boldsymbol{b}$ běží Gaussova eliminace v polynomiálním čase.*

Fakt, že Gaussova eliminace běží v polynomiálním čase, má některé důležité důsledky. Slovem matice myslíme matici racionálních čísel.

**Důsledek 7.** *Následující úlohy lze řešit v polynomiálním čase:*

*(a) rozhodnout, zdali daná matice je regulární;*

*(b) zjistit hodnost matice;*

*(c) najít basi řádkového prostoru a sloupcového prostoru matice;*

*(d) najít některé řešení systému $\boldsymbol{Ax} = \boldsymbol{b}$ nebo konstatovat neexistenci řešení;*

*(e) k dané regulární matici najít inversi;*

*(f) spočítat determinant dané matice.* □

Pomocí Gaussovy eliminace je jistě možné testovat regularitu, zjistit hodnost matice a basi řádkového a sloupcového prostoru. K výpočtu determinantu se využije toho, že (i) prohození dvou různých řádků nebo dvou různých sloupců v matici mění znaménko determinantu, (ii) přičtením násobku řádku k jinému řádku se hodnota determinantu nemění, (iii) determinant horní trojúhelníkové matice je roven součinu diagonálních prvků.

*Důkaz (d).* Nechť existuje řešení celočíselného systému $\boldsymbol{Ax} = \boldsymbol{b}$. Gaussova eliminace nalezne regulární matici $\boldsymbol{E} := \boldsymbol{E}_K$ rozměru $K \times K$ a matici $\boldsymbol{F}_K$. Označme $\boldsymbol{b}'$ poslední sloupec matice $\boldsymbol{F}_K$. Bez újmy na obecnosti nechť je systém rovnic $\boldsymbol{Ex}' = \boldsymbol{b}'$ celočíselný (lze toho dosáhnout přenásobením rovnic společným násobkem jmenovatelů) a nechť jsme, bez újmy na obecnosti, během Gaussovy eliminace nepřehazovali sloupce. Pak podle Cramerova pravidla je vektor

$$\boldsymbol{x} := \left( \frac{\det \boldsymbol{E}^{[1]}}{\det \boldsymbol{E}}, \frac{\det \boldsymbol{E}^{[2]}}{\det \boldsymbol{E}}, \ldots, \frac{\det \boldsymbol{E}^{[K]}}{\det \boldsymbol{E}}, 0, \ldots, 0 \right)^{\mathrm{T}},$$

kde $\boldsymbol{E}^{[i]}$ je matice, jež z matice $\boldsymbol{E}$ vznikla nahrazením $i$-tého sloupce vektorem $\boldsymbol{b}'$, řešením systému $\boldsymbol{Ax} = \boldsymbol{b}$; vektor $\boldsymbol{x}$ má podle lemmatu 4 polynomiální velikost zápisu a lze jej vyčíslit v polynomiálním čase. (Upozorněme, že soustava $\boldsymbol{Ax} = \boldsymbol{b}$ může mít mnoho řešení, z nichž některé nelze spočítat v polynomiálním čase.)

*Důkaz (e).* Inversní matici k dané regulární matici $\boldsymbol{A}$ lze spočítat jako řešení soustavy lineárních rovnic $\boldsymbol{A} \cdot \boldsymbol{A}^{-1} = \boldsymbol{I}$, kde $\boldsymbol{A}^{-1}$ je matice neznámých.