Algebraické metody v teoretické informatice

Nestandardní reprezentace čísel

Zuzana Masáková, Edita Pelantová a Milena Svobodová

Katedra matematiky FJFI, ČVUT v Praze

Červenec 2023

Obsah

Kapitola 1

K čemu slouží exotické zápisy čísel

Abychom mohli s čísly pracovat, musíme je umět zapsat a také ze zápisu jednoznačně odvodit, které číslo ním bylo zapsáno. Ještě do pozdního středověku Evropa zapisovala čísla tak, jak se to dělávalo ve starém Římě, tedy pomocí symbolů I, V, X, L, C, D, M. Tento způsob zápisu má zřejmé nevýhody: problémy při zápisu velkých čísel nebo neceločíselných hodnot a komplikovanost algoritmů pro běžné operace. (Jak násobit 38×57 v zápisu $XXXVIII \times LVII$?). Postupně se v praxi prosadila decimální soustava, kterou používáme v běžném životě dodnes.

I když je převážná část textu věnována pozičním zápisům čísel, které jsou určeny jednou pevnou bází a konečnou sadou znaků, obvykle nazývaných cifry, v této úvodní části se zmíníme o jiných typech zápisu čísel a jejich významu. Mezi takové patří zápis reálného čísla x ve tvaru tzv. řetězového zlomku $x = [a_0, a_1, a_2, \ldots]$, který zachycuje rovnost

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ldots}}}$$

Řetězové zlomky hrají důležitou roli při nejlepších racionálních aproximacích reálných čísel, a proto je studiu řetězových zlomků věnována velká pozornost v každé učebnici teorie čísel. Není tedy důvod se jim věnovat na tomto místě.

1.1 Cantorovy rozvoje

Georg Cantor zavedl zobecnění pozičních soustav na zápisy v (dnes nazývané) Cantorově bázi na základě následující věty. Cantor využíval tento typ zápisu při důkazech iracionality některých čísel.

Věta 1.1. *Nechť $(q_n)_{n=1}^{\infty}$ je posloupnost přirozených čísel splňující $q_n \geq 2$ pro každý index $n \in \mathbb{N}$. Pak ke každému číslu $x \in [0,1)$ existuje právě jedna posloupnost nezáporných celých čísel $(a_n)_{n=1}^{\infty}$ taková, že*

$$x = \sum_{n=1}^{\infty} \frac{a_n}{q_1 q_2 \cdots q_n}$$

a pro každé $n \in \mathbb{N}$ platí

1. $0 \leq a_n < q_n$
2. $a_n a_{n+1} a_{n+2} \ldots \neq (q_n - 1)(q_{n+1} - 1)(q_{n+2} - 1) \ldots .$

Důkaz. Uvědomme si, že pro každý člen uvedené nekonečné řady platí

$$0 \leq \frac{a_n}{q_1 \cdots q_n} \leq \frac{1}{q_1 \cdots q_{n-1}} \leq \frac{1}{2^{n-1}},$$

a tedy řada je konvergentní. Součet této řady je zřejmě kladný a menší než 1, protože

$$\sum_{n=1}^{\infty} \frac{a_n}{q_1 \cdots q_n} < \sum_{n=1}^{\infty} \frac{q_n - 1}{q_1 \cdots q_n} = \sum_{n=1}^{\infty} \frac{1}{q_1 \cdots q_{n-1}} - \sum_{n=1}^{\infty} \frac{1}{q_1 \cdots q_n} = 1. \tag{1.1}$$

Nerovnost je ostrá díky podmínce (2). Pokud by číslo $x \in [0,1)$ mělo být vyjádřené ve tvaru $x = \frac{a_1}{q_1} + \frac{a_2}{q_1 q_2} + \frac{a_3}{q_1 q_2 q_3} + \ldots$, pak

$$q_1 x = a_1 + \underbrace{\frac{a_2}{q_2} + \frac{a_3}{q_2 q_3} + \ldots}_{\in [0,1)} \quad \text{a odtud nutně jediným kandidátem je} \quad a_1 = \lfloor q_1 x \rfloor < q_1.$$

Fakt, že číslo označené svorkou padne do intervalu $[0,1)$, plyne z aplikace diskuse provedené v (1.1) na Cantorovou bázi $(q_{n+1})_{n=1}^{\infty}$. V této nové bázi máme najít vyjádření čísla $x_{new} = q_1 x - a_1 \in [0,1)$. Zřejmě, $x = \frac{a_1}{q_1} + \frac{x_{new}}{q_1}$. Celý postup opakujeme. Vytváříme tak rekurentně zadanou posloupnost (x_n) a posloupnost cifer (a_n) takto

$$x_1 = x \quad \text{a pro každé } n \in \mathbb{N}, n \geq 1, \text{ klademe} \quad a_n = \lfloor q_n x_n \rfloor \quad \text{a} \quad x_{n+1} = q_n x_n - a_n.$$

Matematickou indukcí snadno dokážeme, že v N-tém kroku platí rovnost

$$x = \sum_{n=1}^{N} \frac{a_n}{q_1 q_2 \ldots q_n} + \frac{x_{N+1}}{q_1 q_2 \ldots q_N}.$$

Jelikož $x_{N+1} \in [0,1)$ a $\lim_{N \to \infty} q_1 q_2 \ldots q_N = +\infty$, je x součtem nekonečné řady, jak tvrdí věta. □

Poznámka 1.2. Pokud je posloupnost $(q_n)_{n=1}^{\infty}$ konstantní, tj. $q_n = q > 1$ pro každé $n \in \mathbb{N}$, je zápis čísla x v předchozí větě rozvojem čísla v q-ární soustavě. V tomto smyslu Cantorova věta zobecňuje klasické numerační systémy.

Příklad 1.3. Známou rovnost $e = \sum_{n=0}^{\infty} \frac{1}{n!}$ lze interpretovat jako zápis čísla $e-2 = \sum_{n=1}^{\infty} \frac{1}{(n+1)!}$ v Cantorově bázi, kde $q_n = n+1$ pro každé $n \in \mathbb{N}, n \geq 1$.

Věta 1.4. *Mějme $(q_n)_{n=1}^{\infty}$ jako ve větě 1.1, $x \in [0,1)$. Nechť pro každé prvočíslo p existuje nekonečně mnoho indexů $n \in \mathbb{N}$ takových, že q_n je dělitelné číslem p. Pak x je iracionální právě tehdy, když Cantorův zápis čísla x nekončí na řetězec ze samých 0.*

Důkaz. Implikace ($\Rightarrow$) je jasná, dokažme ($\Leftarrow$). Postupujme sporem. Nechť Cantorův zápis čísla x nekončí na řetězec ze samých 0 a nechť x je racionální, tedy pro nějaká kladná $P, Q \in \mathbb{N}$ platí

$$x = \sum_{n=1}^{\infty} \frac{a_n}{q_1 q_2 \cdots q_n} = \frac{P}{Q}.$$

Najdeme $N \in \mathbb{N}$ takové, že $q_1 q_2 \cdots q_N \frac{1}{Q} \in \mathbb{Z}$. Takové N existuje díky předpokladu, že každé prvočíslo dělí nekonečně mnoho q_n. Pak

$$0 < \frac{P}{Q} - \sum_{n=1}^{N} \frac{a_n}{q_1 q_2 \cdots q_n} = \sum_{n=N+1}^{\infty} \frac{a_n}{q_1 q_2 \cdots q_n} = \frac{1}{q_1 q_2 \cdots q_N} \underbrace{\sum_{n=N+1}^{\infty} \frac{a_n}{q_{N+1} q_{N+2} \cdots q_n}}_{<1}.$$

První nerovnost je ostrá, protože x má v dané Cantorově báze nekonečný rozvoj. Odhad $\sum_{n=N+1}^{\infty} \frac{a_n}{q_{N+1} q_{N+2} \cdots q_n} < 1$ platí ze stejných důvodů jako (1.1) v důkazu věty 1.1. Po vynásobení $q_1 q_2 \cdots q_N$ dostáváme

$$0 < \underbrace{\frac{q_1 q_2 \cdots q_N}{Q} P - \sum_{n=1} a_n q_{n+1} \cdots q_N}_{\in \mathbb{N}} < 1,$$

a to je spor. □

1.2 Binární rozvoje pro algoritmy typu Shift and Add

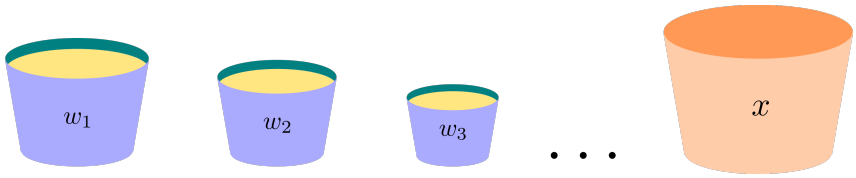
V této podkapitole představíme binární rovoje, které umožňují rýchle vyhodnocovat hodnoty elementárných funkcí jako jsou exponenciála, logaritmus, sinus a kosinus. Čerpáme z knihy Jeana-Michela Mullera [20].

Věta 1.5. *Nechť $(w_n)_{n=1}^{\infty}$ je ostře klesající posloupnost kladných čísel taková, že řada $\sum_{n=1}^{\infty} w_n$ konverguje a pro každé $N \in \mathbb{N}$ platí $w_N \leq \sum_{n=N+1}^{\infty} w_n$. Označme $\sum_{n=1}^{\infty} w_n = w$. Potom*

1. *Pro každé* $x \in [0, w]$ *existuje posloupnost* $(d_n)_{n=1}^{\infty}$ *taková, že* $d_n \in \{0, 1\}$ *pro každé kladné* $n \in \mathbb{N}$ *a*
$$x = \sum_{n=1}^{\infty} d_n w_n.$$

2. *Pro každé* $x \in [-w, w]$ *existuje posloupnost* $(d_n)_{n=1}^{\infty}$ *taková, že* $d_n \in \{-1, 1\}$ *pro každé kladné* $n \in \mathbb{N}$ *a*
$$x = \sum_{n=1}^{\infty} d_n w_n.$$

Důkaz. Ukažme bod 1.



Obrázek 1.1: Ilustrace k důkazu věty 1.1

Nádobu o objemu x chceme vyplnit pískem z kbelíků s obsahem $w_1, w_2, \ldots$. Bereme postupně $w_1, w_2, \ldots$ a pokaždé, kdy je v nádobě ještě dost místa, přisypeme obsah w_n do x.

Nejdříve dokažme bod (1). Pro zadané $x \in [0, w]$, položíme $x_0 = x$ a definujme rekurentně posloupnost $(x_n)_{n=0}^{\infty}$ a posloupnost $(d_n)_{n=1}^{\infty}$ následujícím **hladovým** způsobem.

$$x_n = x_{n-1} - d_n w_n, \quad \text{kde} \quad d_n = \begin{cases} 1, & \text{pokud } x_{n-1} \leq w_n, \\ 0, & \text{jinak.} \end{cases}$$

Jelikož $x_{n-1} - x_n = d_n w_n$, platí

$$x_0 = \sum_{i=1}^{N} (x_{i-1} - x_i) + x_N = \sum_{i=1}^{N} d_i w_i + x_N$$

K důkazu 1. tvrzení stačí ukázat, že $\lim_{N\to\infty} x_N = 0$. Nejdříve odvodíme matematickou indukcí, že $x_N \leq \sum_{n=N+1}^{\infty} w_n$.

Pro $N = 0$ tvrzení platí, protože $x_0 = x \in [0, w]$. Předpokládejme, že tvrzení platí pro $N \in \mathbb{N}$.

- Pokud $x_N \geq w_{N+1}$, pak $x_{N+1} = x_N - w_{N+1} \overset{IP}{\leq} \sum_{n=N+2}^{\infty} w_n$.
- Pokud $x_N < w_{N+1}$, pak $x_{N+1} = x_N < w_{N+1} \leq \sum_{n=N+2}^{\infty} w_n$, kde poslední nerovnost platí díky vlastnostem posloupnosti $(w_n)_{n=1}^{\infty}$.

Celkově, $x_N \leq N$-tý zbytek konvergentní řady, a proto $\lim_{N\to\infty} x_N = 0$.

Druhá část věty plyne z první části. Pro dané $x \in [-w, w]$ položíme $y = \frac{1}{2}(x+w) \in [0, w]$ a podle bodu 1 najdeme $\tilde{d}_n \in \{0, 1\}$ taková, že $y = \sum_{n=1}^{\infty} \tilde{d}_n w_n$. Protože $w = \sum_{n=1}^{\infty} w_n$, dostaneme $x = 2y - w = \sum_{n=1}^{\infty} (2\tilde{d}_n - 1) w_n$. Stačí tedy položit $d_n = 2\tilde{d}_n - 1 \in \{-1, 1\}$. □

Povšimněme si, jak výpočetně nenáročné je v hladovém algoritmu nalezení členů posloupnosti (d_n) pro $n = 1, 2, \ldots, N$. Předpokládáme, že v počítači máme uloženy hodnoty $w_1, w_2, \ldots, w_N$. Každý krok vyžaduje porovnání dvou čísel (konkrétně x_{n-1} a w_n) a v případě, že $d_n = 1$, také odečítání (konkrétně $x_{n-1} - w_n$).

Příklad 1.6. Uvedeme tři příklady posloupnosti $(w_n)_{n=1}^{\infty}$, které vyhovují předpokladům věty.

- $w_n = \frac{1}{2^n}$. Součet geometrické řady $\frac{1}{2^N} = \sum_{n=N+1}^{\infty} \frac{1}{2^n}$ potvrzuje platnost nerovnosti požadované na posloupnosti (w_n) (zde se nerovnost mění v rovnost). Protože $w = 1$, věta říká, že každé číslo z $[0, 1]$ lze zapsat v klasické binární soustavě. Věta netvrdí nic o jednoznačnosti, ale hladový algoritmus využitý v důkazu věty zaručuje, že pro $x \in [0, 1)$ posloupnost cifer (d_n) nekončí řetězcem ze samých jedniček.

- $w_n = \ln(1 + 2^{-n})$. Tuto posloupnost využijme k výpočtu hodnot funkce e^x na intervalu $[0, \ln 2]$. K ověření, že $w_N \le \sum_{n=N+1}^{\infty} w_n$ a $\ln 2 \le \sum_{n=1}^{\infty} w_n$ stačí využít nerovnosti

$$x - \frac{x^2}{2} \le \ln(1+x) \le x - \frac{x^2}{2} + \frac{x^3}{3} \quad \text{pro } 0 < x < 1$$

  vyplývající z Taylorova rozvoje funkce $\ln(1+x)$. Ten má tvar $x - \frac{x^2}{2} + \frac{x^3}{3} + \cdots$
  Pro $x = 2^{-N}$ dostáváme odhady

$$\ln(1 + 2^{-N}) < \frac{1}{2^N} - \frac{1}{2}\frac{1}{4^N} + \frac{1}{3}\frac{1}{8^N} =: \alpha$$
$$\sum_{n=N+1}^{\infty} \ln(1 + 2^{-n}) \ge \sum_{n=N+1}^{\infty} \left(\frac{1}{2^n} - \frac{1}{2}\frac{1}{4^n} \right) = \frac{1}{2^N} - \frac{1}{6}\frac{1}{4^N} := \beta,$$

  Protože $\alpha < \beta$, nerovnost $w_N \le \sum_{n=N+1}^{\infty} w_n$ platí.

  Spodní nerovnost pro $N = 0$ dává $w = \sum_{n=1}^{\infty} \ln(1 + 2^{-n}) \ge 1 - \frac{1}{6} > \ln 2$.

- $w_n = \operatorname{arctg} 2^{-n}$. Tuto posloupnost využijeme k výpočtům hodnot funkcí sin a cos pro argument $x \in [0, \frac{\pi}{4}]$. Derivováním funkce arctg odvodíme její Taylorův rozvoj.

$$\frac{1}{1+x^2} = 1 - x^2 + x^4 - x^6 + \cdots \quad \text{a odtud} \quad \operatorname{arctg} x = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \cdots$$

Čtenář snadno ověří, že w_n splňuje předpoklady věty 1.5 a také, že $\sum_{n=1}^{\infty} \operatorname{arctg} 2^{-n} > \frac{\pi}{4}$. Stačí využít nerovnosti

$$x - \frac{x^3}{3} < \operatorname{arctg} x < x - \frac{x^3}{6} \qquad \text{platné pro } x \in [0, \tfrac{1}{2}].$$

1.3 Výpočet hodnot funkcí exp, sin a cos

I když chceme počítat hodnoty e^x, $\sin x$ a $\cos x$ pro libovolně zadané reálné x, stačí mít k dispozici algoritmus, který počítá hodnoty těchto funkcí na jistém omezeném intervalu. Kvůli periodičnosti funkcí $\sin x$ a $\cos x$ a symetrii $\sin x = \cos(x - \frac{\pi}{2})$, stačí uvažovat $x \in [0, \frac{\pi}{4}]$.

Ukažme, že také u funkce exp stačí uvažovat omezený interval, jmenovitě interval $[0, \ln 2]$. Vskutku, pro $y \in \mathbb{R}$ existuje $k \in \mathbb{Z}$ tak, že $y = x + k \ln 2$, kde $x \in [0, \ln 2]$. Potom $e^y = e^{x+k\ln 2} = e^x (e^{\ln 2})^k = 2^k e^x$. Algoritmem spočítáme hodnotu e^x, a protože výpočty v počítači probíhají v soustavě se základem 2, představuje násobení číslem 2^k jenom posun zlomkové tečky o k míst.

Převodu reálného argumentu x na argument vyžadovaný zvoleným algoritmem, se říká v anglické literatuře "range reduction".

Výpočet exponenciální funkce

V počítači jsou uschovány hodnoty $w_n = \ln(1 + 2^{-n})$ pro několik počátečních hodnot $n = 1, 2, 3, \ldots$ podle požadované přesnosti výpočtu, viz diskusi níže. V příkladě 1.6 jsme ověřili, že můžeme použít větu 1.5 a její pomocí vyjádřit zadané $x \in [0, \ln 2]$ ve formě

$$x = \sum_{n=1}^{\infty} d_n \ln(1 + 2^{-n}). \tag{1.2}$$

Jelikož d_n jsou buď 0 nebo 1, platí $d_n \ln(1 + 2^{-n}) = \ln(1 + d_n 2^{-n})$. Můžeme tedy upravovat

$$E := e^x = \prod_{n=1}^{\infty} e^{d_n \ln(1+2^{-n})} = \prod_{n=1}^{\infty} e^{\ln(1+d_n 2^{-n})} = \prod_{n=1}^{\infty} (1 + d_n 2^{-n}).$$

Definujme posloupnost (E_N) předpisem $E_N = \prod_{n=1}^{N} (1 + d_n 2^{-n})$. Zřejmě $E = \lim_{N\to\infty} E_N$,

$$E_0 = 1 \quad \text{a} \quad E_N = E_{N-1}(1 + d_N 2^{-N}) = E_{N-1} + d_N E_{N-1} 2^{-N}.$$

Tedy při výpočtu E_N z už napočítané hodnoty E_{N-1} pouze posuneme binární tečku a sčítáme dvě čísla. Proto se algoritmu tohoto typu říká *shift and add*.

Odhad chyby po N-tém kroku

$$\frac{E_N}{E} = \frac{1}{\prod_{n=N+1}^{\infty}(1+d_n 2^{-n})} \geq \frac{1}{\prod_{n=N+1}^{\infty}(1+2^{-n})} \overset{(\alpha)}{\geq} \frac{1}{1+2^{-N}+2^{-2N}}$$

V nerovnosti označené $\overset{(\alpha)}{\geq}$ jsme využili odhad

$$\prod_{n=N+1}^{\infty}(1+2^{-n}) = \exp\Big(\sum_{n=N+1}^{\infty}\ln(1+2^{-n})\Big) \overset{(\beta)}{\leq} \exp\Big(\sum_{n=N+1}^{\infty}2^{-n}\Big) = \exp(2^{-N}) \overset{(\gamma)}{\leq} 1+2^{-N}+2^{-2N},$$

kde jsme v nerovnostech označených jako $\overset{(\beta)}{\leq}$ a $\overset{(\gamma)}{\leq}$ využili odhady $\ln(1+x) < x$ resp. $e^x \leq 1+x+x^2$, oba platné pro $x \in [0, \frac{1}{2}]$. Celkově pro chybu po N-tém kroku platí

$$0 \leq \underbrace{E}_{e^x} - E_N = E\left(1-\frac{E_N}{E}\right) \leq e^x\left(1-\frac{E_N}{E}\right) < 2\left(1-\frac{1}{1+2^{-N}+2^{-2N}}\right) \leq \frac{1}{2^{N-1}}.$$

Algoritmus výpočtu e^x pro dané $x \in [0, \ln 2]$

(obsahuje v sobě i určení koeficientů d_n pro zápis ve tvaru (1.2))
Polož $E = 1$. Pro $i = 1, 2, 3, \ldots$ dělej

- pokud $x \geq \ln(1+2^{-i})$, pak $E := E + 2^{-i}E$ a $x := x - \ln(1+2^{-i})$,
- jinak nedělej nic.

Příklad 1.7. Najdeme $e^{1/2}$. Máme $x = \frac{1}{2} \in [0, \ln 2]$, označíme $E_0 = 1$. Prvních deset kroků algoritmu:

$\boldsymbol{i=1}$: $\frac{1}{2} = x_0 \overset{?}{\geq} \ln\left(\frac{3}{2}\right) \approx 0,405\ldots$ nerovnost platí, $d_1 = 1$

$E_1 = E_0 + \frac{1}{2}E_0 = \frac{3}{2}$

$x_1 = x_0 - \ln\left(\frac{3}{2}\right) \approx 0,0945\ldots$

$\boldsymbol{i=2}$: $x_1 \overset{?}{\geq} \ln\left(\frac{5}{4}\right) \approx 0,22314\ldots$ nerovnost neplatí, $d_2 = 0$

$E_2 = E_1$

$x_2 = x_1$

$\boldsymbol{i=3}$: $x_2 \overset{?}{\geq} \ln\left(\frac{9}{8}\right) \approx 0,11778\ldots$ nerovnost neplatí, $d_3 = 0$

$E_3 = E_2$

$x_3 = x_2$

$\boldsymbol{i=4}$: $x_3 \overset{?}{\geq} \ln\left(\frac{17}{16}\right) \approx 0,06062\ldots$ nerovnost platí, $d_4 = 1$

$$E_4 = E_3 + \frac{1}{16}E_3 = \frac{51}{32} \approx 1,59375\ldots$$

$$x_4 = x_3 - \ln\left(\frac{17}{16}\right) \approx 0,0339\ldots$$

$\boldsymbol{i = 5}$: $x_4 \overset{?}{\geq} \ln\left(\frac{33}{32}\right) \approx 0,03077\ldots$ nerovnost platí, $d_5 = 1$

$$E_5 = E_4 + \frac{1}{32}E_4 = \frac{1683}{1024} \approx 1,64355\ldots\ldots$$

$$x_5 = x_4 - \ln\left(\frac{33}{32}\right) \approx 0031386\ldots$$

$\boldsymbol{i = 6}$: $x_5 \overset{?}{\geq} \ln\left(\frac{65}{64}\right) \approx 0,01550\ldots$ nerovnost neplatí, $d_6 = 0$

$$E_6 = E_5$$

$$x_6 = x_5$$

$\boldsymbol{i = 7}$: $x_6 \overset{?}{\geq} \ln\left(\frac{129}{128}\right) \approx 0,0077821\ldots$ nerovnost neplatí, $d_7 = 0$

$$E_7 = E_6$$

$$x_7 = x_6$$

$\boldsymbol{i = 8}$: $x_7 \overset{?}{\geq} \ln\left(\frac{257}{256}\right) \approx 0,00388986\ldots$ nerovnost neplatí, $d_8 = 0$

$$E_8 = E_7$$

$$x_8 = x_7$$

$\boldsymbol{i = 9}$: $x_8 \overset{?}{\geq} \ln\left(\frac{513}{512}\right) \approx 0,00195122\ldots$ nerovnost platí, $d_9 = 1$

$$E_9 = E_8 + \frac{1}{512}E_8 = \frac{863379}{524288} \approx 1,64676\ldots$$

$$x_9 = x_8 - \ln\left(\frac{513}{512}\right) \approx 0,00118739\ldots$$

$\boldsymbol{i = 10}$: $x_9 \overset{?}{\geq} \ln\left(\frac{1025}{1024}\right) \approx 0,000976\ldots$ nerovnost platí, $d_{10} = 1$

$$E_{10} = E_9 + \frac{1}{1024}E_9 = \frac{863379}{524288} \cdot \frac{1025}{1024} \approx 1,6483729\ldots$$

$$x_{10} = x_9 - \ln\left(\frac{1025}{1024}\right) \approx 0,00118739\ldots$$

Po prvních deseti krocích algoritmu je chyba na čtvrté pozici v zápise v desátkové soustavě, a tedy menší, než $\frac{1}{2^9} = \frac{1}{512}$.

Výpočet funkcí kosinus a sinus

V počítači jsou uschovány hodnoty $w_n = \operatorname{arctg} 2^{-n}$ pro několik počátečních hodnot $n = 1, 2, 3, \ldots$. Nyní budeme používat vyjádření úhlu $\Theta \in [0, \frac{\pi}{4}]$ ve tvaru

$$\Theta = \sum_{n=1}^{\infty} d_n \operatorname{arctg} 2^{-n}, \qquad \text{kde } d_n \in \{-1, 1\}. \tag{1.3}$$

Abychom odůvodnili níže uvedený algoritmus, který je znám pod zkratkou CORDIC, zkoumejme vztah hodnot cos a sin u sousedních členů posloupnosti zadané předpisem $\Theta_N = \sum_{n=1}^{N} d_n w_n$.

$$\begin{pmatrix} \cos\Theta_N \\ \sin\Theta_N \end{pmatrix} = \begin{pmatrix} \cos(\Theta_{N-1} + d_N w_N) \\ \sin(\Theta_{N-1} + d_N w_N) \end{pmatrix} = \begin{pmatrix} \cos\Theta_{N-1}\cos(d_N w_N) - \sin\Theta_{N-1}\sin(d_N w_N) \\ \sin\Theta_{N-1}\cos(d_N w_N) + \cos\Theta_{N-1}\sin(d_N w_N) \end{pmatrix} =$$

$$= \begin{pmatrix} \cos w_N & -d_N \sin w_N \\ d_N \sin w_N & \cos w_N \end{pmatrix} \cdot \begin{pmatrix} \cos\Theta_{N-1} \\ \sin\Theta_{N-1} \end{pmatrix} = \cos w_N \begin{pmatrix} 1 & -d_N 2^{-N} \\ d_N 2^{-N} & 1 \end{pmatrix} \begin{pmatrix} \cos\Theta_{N-1} \\ \sin\Theta_{N-1} \end{pmatrix}$$

Poslední rovnost plyne ze vztahu

$$\frac{\sin w_N}{\cos w_N} = \operatorname{tg} w_N = \operatorname{tg}\bigl(\operatorname{arctg} 2^{-N}\bigr) = 2^{-N}.$$

V každém kroku násobíme vektor skalárem $\cos w_N$, který nezávisí na koeficientech d_N ve vyjádření úhlu Θ. Proto celkový součin, označme jej K, těchto koeficientů je uložený v počítači předem a startovací složky vektoru $\cos\Theta_0 = \cos 0 = 1$ a $\sin\Theta_0 = \sin 0 = 0$, rovnou vynásobíme číslem K. Jelikož $\cos\alpha = \frac{1}{\sqrt{1+\operatorname{tg}^2\alpha}}$, dostaneme $\cos w_n = \frac{1}{\sqrt{1+2^{-2N}}}$ a odtud

$$K = \prod_{n=1}^{\infty} \cos w_n = \prod_{n=1}^{\infty} \frac{1}{\sqrt{1+2^{-2n}}} = 0,828159360960215627076198 32\ldots$$

Algoritmus výpočtu $\cos\Theta$ **a** $\sin\Theta$ **pro dané** $\Theta \in [0, \frac{\pi}{4}]$

(obsahuje v sobě i určení koeficientů d_n v zápisu (1.3))

Polož $x := K$ a $y := 0$.

Pro $i = 1, 2, 3, \ldots$ dělej

- pokud $\Theta > 0$, pak $\Theta := \Theta - \operatorname{arctg} 2^{-i}$ a $\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 1 & -2^{-i} \\ 2^{-i} & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$
- jinak $\Theta := \Theta + \operatorname{arctg} 2^{-i}$ a $\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 1 & 2^{-i} \\ -2^{-i} & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$

Zdůrazněme, že se opět jedná o algoritmus typu "shift and add".

Kapitola 2

Reprezentace s převahou nulových cifer

Při klasickém násobení čísel zapsaných v soustavě s bází b a množinou cifer $\mathcal{D}$ jako $x = x_k x_{k-1} \cdots x_0$ a $y = y_n y_{n-1} \cdots y_0$ násobíme celý řetězec $x_k x_{k-1} \cdots x_0$ každou z cifer y_i. Pokud je samotná množina $\mathcal{D}$ uzavřená na násobení, pak výsledek násobení cifrou y_i je řetězec $(x_k y_i)(x_{k-1} y_i) \cdots (x_0 y_i)$. Protože nedochází k přenosu cifry na sousední pozici, lze při souběžném použití k výpočetních jednotek získat výsledek násobení cifrou y_i v jednom kroku. A celkový výsledek $x \times y$ získáme sčítáním maximálně n řádků. Počet nutných sčítaní klesá s počtem nulových cifer v zápisu čísla y. Tyto vlastnosti násobení vedly k vytvoření tzv. NAF-reprezentací celých čísel [26], které se uplatňují při algoritmech vyžadujících násobení velkých čísel, jako je např. metoda RSA určena k šifrování s veřejně přístupným klíčem.

2.1 NAF-reprezentace

Klasická binární soustava sice má abecedu $\mathcal{D} = \{0, 1\}$ uzavřenou na násobení, ale zápis v této soustavě je jednoznačný, tj. nelze ovlivnit počet nul v zápisu čísla. Stejné pozorování platí i o soustavě s bází $b = 3$ a abecedou $\mathcal{D} = \{-1, 0, 1\}$. Uvažujme proto

$$\text{soustavu s bází } b = 2 \text{ a abecedou } \mathcal{D} = \{\bar{1}, 0, 1\}, \quad \text{kde } \bar{1} \text{ značí -1.}$$

Pozorování

- Každé $x \in \mathbb{Z}$ lze zapsat ve tvaru

$$x = \sum_{k=0}^{n} a_k 2^k, \qquad \text{kde } a_k \in \{\bar{1}, 0, 1\} \quad \text{pro každé } k = 0, 1, \ldots, n. \tag{2.1}$$

- Pokud $a_n = 1$, pak $x > 0$. Vskutku

$$x = 2^n + a_{n-1} 2^{n-1} + \cdots + a_1 2 + a_0 \geq 2^n - 2^{n-1} - \cdots - 2 - 1 = 1,$$

tedy znaménko u vedoucí mocniny určuje znaménko samotného čísla x.

- Číslo x může mít více zápisů, např. číslo s decimálním zápisem 15 lze v této soustavě zapsat jako 1111, nebo $1000\bar{1}$, nebo jako $100\bar{1}1$.

Věta 2.1. *Každé $x \in \mathbb{Z}$ lze zapsat v bázi $b = 2$ a abecedě $\mathcal{D} = \{\bar{1}, 0, 1\}$ tak, že žádné dvě nenulové cifry v zápise čísla nejsou na sousedních pozicích. Tento zápis je jednoznačný, pokud je koeficient u vedoucí mocniny nenulový.*

Poznámka 2.2. Zápis čísla z věty nazýváme *non-adjacent form*, zkráceně *NAF*.

Důkaz. Zapišme $x \in \mathbb{Z}$ ve tvaru (2.1). Abychom upravili zápis čísla x do tvaru bez sousedících nenulových koeficientů, využijeme přepisovací pravidla založená na jednoduchém pozorování: pro všechny $j \in \mathbb{N}$ platí

$$1 \cdot 2^j + \bar{1} \cdot 2^{j-1} = 1 \cdot 2^{j-1}$$
$$1 \cdot 2^j + 1 \cdot 2^{j-1} = 1 \cdot 2^{j+1} + \bar{1} \cdot 2^{j-1}.$$

Proto v řetězci $a_n a_{n-1} \cdots a_0$ můžeme přepisovat dvojice resp. trojice sousedících cifer následujícími způsoby

$$1\bar{1} \longrightarrow 01 \qquad\qquad 011 \longrightarrow 10\bar{1} \tag{2.2}$$
$$\bar{1}1 \longrightarrow 0\bar{1} \qquad\qquad 0\bar{1}\bar{1} \longrightarrow \bar{1}01, \tag{2.3}$$

aniž bychom změnili hodnotu reprezentovaného čísla. Například na klasické binární reprezentaci 11011 čísla 27 provedeme tyto úpravy

$$11011 \longrightarrow 10\bar{1}10\bar{1} \longrightarrow 100\bar{1}0\bar{1}.$$

Kombinací přepisovacích pravidel (2.2) a (2.3) vyrobíme obecnější pravidlo pro $k \in \mathbb{N}, k \geq 2$

$$0\underbrace{11\cdots1}_{k\ \times} \longrightarrow 1\underbrace{00\cdots0}_{(k-1)\times}\bar{1} \qquad \text{a} \qquad 0\underbrace{\bar{1}\bar{1}\cdots\bar{1}}_{k\ \times} \longrightarrow \bar{1}\underbrace{00\cdots0}_{(k-1)\times}1$$

Je zřejmé, že pokud se v řetězci vyskytuje dvojice sousedících nenul, lze aplikovat některé z přepisovacích pravidel. Pokud řetězec reprezentující číslo x není NAF, označme M minimální index i takový, že na pozicích $i+1$ a i jsou sousedící nenulové cifry a označme P počet nenulových cifer na pozicích M, $M-1, \ldots, 1, 0$. Tento kus řetězce je již NAF. Na jeden z podřetězců, jejíchž pravý konec je na pozici M, můžeme aplikovat přepisovací pravidlo. Tvar přepisovacích pravidel zaručuje, že nově vzniklý řetězec bude mít hodnotu $M_{new} \geq M + 2$ a $P_{new} \geq P + 1$.

Každé z přepisovacích pravidel má vlastnost, že počet nenul v celém novém řetězci není větší než počet nenul v celém starém řetězci. Přitom počet nenulových cifer v sufixu, který je NAF roste. To znamená, že po konečném počtu (maximálně o jedničku menším, než je počet nenul ve startovacím řetězci), získáme NAF-reprezentaci čísla x.

Ukažme jednoznačnost zápisu NAF. Nejprve ukážeme, že 1 nemá dva různé zápisy. Postupujme sporem. Nechť existuje zápis jedničky jiný než $1 = 1$:

$$1 = a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \cdots + a_1 \cdot 2 + a_0, \quad \text{kde } a_k \neq 0 \text{ a } k \neq 0\,.$$

Koeficient u vedoucí mocniny je nutně kladný, tj. $a_k = 1$. Kvůli paritě je $a_0 \neq 0$. Kvůli *NAF* podmínce je $a_{k-1} = 0$, a tedy $k \geq 2$. Potom ale

$$1 \geq 2^k - \sum_{i=0}^{k-2} 2^i = 2^k - 2^{k-1} + 1 = 2^{k-1} + 1 > 1 \quad \text{– spor.}$$

Nyní předpokládejme, že existují celá čísla se dvěma různými zápisy NAF. Bez újmy na obecnosti, zvolme mezi nimi nejmenší možné kladné x. Zřejmě $x > 1$ a pro dva různé řetězce $a_k a_{k-1} \ldots a_1 a_0$ a $b_{l-1} \ldots b_1 b_0$ cifer platí následující rovnost

$$x = a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \cdots + a_1 \cdot 2 + a_0 = b_l \cdot 2^l + b_{l-1} \cdot 2^{l-1} + \cdots + b_1 \cdot 2 + b_0.$$

Kdyby $a_0 = b_0$, pak $\frac{x-a_0}{2} \in \mathbb{N}$ má dva různé zápisy

$$\frac{x - a_0}{2} = a_k \cdot 2^{k-1} + a_{k-1} \cdot 2^{k-2} + \cdots + a_1 = b_l \cdot 2^{l-1} + b_{l-1} \cdot 2^{l-2} + \cdots + b_1.$$

Jelikož pro $x > 1$ platí

$$0 < \frac{x - a_0}{2} \leq \frac{x - 1}{2} < x,$$

dostáváme spor s tím, že x bylo v nejmenší kladné číslo se dvěma zápisy. Tím jsme ukázali, že minimální kladné číslo x s více NAF zápisy má poslední cifry u různých zápisů různé. Kvůli rovnosti $\mod 2$ nutně $a_0, b_0 \neq 0$. Tedy například $a_0 = 1$, $b_0 = \bar{1}$. Z podmínky *NAF* zápisu plyne $a_1 = b_1 = 0$. To vynucuje $x = a_0 \mod 4$ a $x = b_0 \mod 4$, což je spor, protože $1 \neq \bar{1} \mod 4$. □

Důsledek 2.3. *NAF zápis čísla $x \in \mathbb{Z}$ má nejmenší počet nenul mezi všemi zápisy čísla $x = \sum_{k=0}^{n} a_k 2^k$, kde $a_k \in \{\bar{1}, 0, 1\}$.*

Důkaz. Z každého zápisu čísla x umíme přepisovacími pravidly vyrobit NAF zápis, aniž bychom zvětšili počet nenulových cifer. □

Poznámka 2.4. V důkazu existence NAF zápisu celého čísla jsme uvedli, že počet kroků (aplikací přepisovacích pravidel) potřebných k převodu z klasického binárního zápisu do NAF zápisu je omezen počtem cifer 1 v klasickém zápisu zmenšeným o jedničku. Této meze se nabývá při převodu čísla z_N binárně zapsaného $\underbrace{1010\cdots10}_{(N-1)\times}11$, které má v klasickém binárním zápisu $N+1$ cifer 1. Jeho NAF zápis je $1\underbrace{0\bar{1}0\bar{1}0\cdots0\bar{1}}_{N\times}$ a má stejný počet nenulových cifer. Protože při použití přepisovacích pravidel se počet nenulových cifer nezvětšuje, musela mít reprezentace čísla z_N v každém kroku stejný počet nenul jako jeho NAF reprezentace. Tím jsme ilustrovali fakt, že i jiné reprezentace čísla mohou vystačit se stejným počtem nenulových cifer jako NAF. Takovým reprezentacím se říká minimální. Počet minimálních reprezentací lze odhadnout shora pomocí členů Fibonacciho posloupnosti (F_n). V [15] je odvozeno, že počet minimálních reprezentací libovolného čísla $z \in \mathbb{N}$ nepřevýší $F_{\lfloor \log_4 z \rfloor}$.

Poznámka 2.5. Radixové uspořádání $\preceq$ na NAF reprezentacích odpovídá uspořádání celých čísel, tj. pokud je $x, y \in \mathbb{Z}$ a $x < y$, pak NAF reprezentace x je radixově menší než NAF reprezentace y. Abychom nahlédli tuto vlastnost, stačí ukázat, že číslo α_N reprezentované řetězcem $10(\bar{1}0)^N$ je větší než číslo β_N reprezentované řetězcem $1(01)^N$. Zdůrazněme, že $10(\bar{1}0)^N \succ 1(01)^N$ a žádný NAF řetězec už v radixovém uspořádání mezi ně nelze vložit.

Poznámka 2.6. V kapitole 4 ukážeme, že NAF zápisem lze reprezentovat také všechna reálná čísla.

2.2 Průměrné počty nenulových cifer u NAF zápisů

Rozšíření množiny cifer v binární soustavě o $\bar{1}$ umožňuje některá čísla zapsat úsporněji, např. zápis čísla $x = 2^n - 1$ v klasické binární soustavě používá n jedniček, zatímco jeho NAF zápis $1\underbrace{00\cdots0}_{(n-1)\times}\bar{1}$ potřebuje pouze dvě nenuly. Na druhé straně číslo $y = 2^n$ potřebuje pouze jednu nenulu v obou zápisech. Naším cílem je ukázat, že průměrný počet nenulových cifer je při NAF zápisech menší. Budeme předpokládat, že k uložení celého čísla používáme N pozic a že všechna čísla, která lze zapsat v NAF zápise na N pozicích, se vyskytují stejně často. Označme množinu těchto čísel $\mathcal{M}_N$. Ptáme se, jaká je průměrná hodnota obsazenosti jedné pozice nenulovou cifrou, tj. na poměr

$$\Phi_N = \frac{1}{N \cdot \#\mathcal{M}_N} \cdot \sum_{x \in \mathcal{M}_N} \text{počet nenul v NAF zápise čísla } x$$

Příklad 2.7. Určeme Φ_4. Vypišme všechna čísla, k jejímž NAF zápisům stačí 4 pozice. Jsou to

0001	$000\bar{1}$	$10\bar{1}0$
0010	$00\bar{1}0$	$100\bar{1}$

0100	$0\bar{1}00$	$010\bar{1}$
1000	$\bar{1}000$	$\bar{1}010$
1010	$\bar{1}0\bar{1}0$	$\bar{1}001$
1001	$\bar{1}00\bar{1}$	$0\bar{1}01$
0101	$0\bar{1}0\bar{1}$	0000

Zapsáno je 21 čísel, použito 32 nenulových cifer. Proto

$$\Phi_4 = \frac{32}{4 \cdot 21} = \frac{8}{21}$$

Dokážeme, že průměrný počet nenulových cifer při *NAF* zápisech je pro dostatečně velké N blízký $\frac{1}{3}$. Při klasických binárních zápisech je to $\frac{1}{2}$.

Věta 2.8. *Platí* $\lim_{N\to\infty} \Phi_N = \frac{1}{3}$.

Důkaz. Zvolme pevně ale libovolně celé $k \geq 0$ a spočítejme, kolik je čísel $x \in \mathcal{M}_N$, které v *NAF* zápise mají přesně k nenul. Reprezentaci každého čísla $x \in \mathcal{M}_N$ doplníme vhodným počtem 0 na zápis délky $N+1$ (tedy zápis každého x začíná cifrou 0). Takový zápis lze poskládat ze tří druhů kostek $\boxed{0}\boxed{1}$, $\boxed{0}\boxed{\bar{1}}$ a $\boxed{0}$. Musíme přitom využít k kostek typu $\boxed{0}\boxed{1}$ nebo $\boxed{0}\boxed{\bar{1}}$. Ty obsadí $2k$ míst. Zbylých $N+1-2k$ míst obsadí kostičky $\boxed{0}$. Celkově použijeme $k+N+1-2k = N+1-k$ kostiček. Při uspořádání těchto $N+1-k$ kostiček máme $\binom{N+1-k}{N+1-2k} = \binom{N+1-k}{k}$ voleb pro umístnění kostičky $\boxed{0}$. Zbylá místa lze obsadit libovolně jednou z kostiček $\boxed{0}\boxed{1}$ nebo $\boxed{0}\boxed{\bar{1}}$. Odvodili jsme tedy, že počet čísel $x \in \mathcal{M}_N$, jejichž zápis má právě k nenulových cifer, je roven $\binom{N+1-k}{k}2^k$.

Zřejmě

$$\begin{aligned} B_N &:= \sum_{k\geq 0} k\binom{N+1-k}{k}2^k \quad = \sum_{x\in\mathcal{M}_N} \text{počet nenul v NAF zápise čísla } x \\ A_N &:= \sum_{k\geq 0} \binom{N+1-k}{k}2^k \quad = \#\mathcal{M}_N. \end{aligned}$$

Abychom explicitně určili A_N a B_N, všimneme si, že vyhovují lineárním rekurentním vztahům.

$$\begin{aligned} A_{N+1} - A_N &= \sum_{k\geq 0}\binom{N+2-k}{k}2^k - \sum_{k\geq 0}\binom{N+1-k}{k}2^k = \\ &= \sum_{k\geq 1}\binom{N+1-k}{k-1}2^k = \sum_{k\geq 0}\binom{N-k}{k}2^{k+1} = 2A_{N-1} \end{aligned}$$

Řešíme tedy rekurentní rovnici

$$A_{N+1} - A_N - 2A_{N-1} = 0.$$

Její charakteristická rovnice je $x^2 - x - 2 = (x-2)(x+1) = 0$, proto A_N je ve tvaru

$$A_N = a \cdot 2^N + b \cdot (-1)^N,$$

pro nějaká $a, b \in \mathbb{R}$, zřejmě $a > 0$. Konstanty a, b lze nalézt explicitně z počátečních hodnot $A_1 = 3$ a $A_2 = 5$, nebo lze určit A_N přímo, viz Poznámka 2.9. Na hodnotu limity posloupnosti (Φ_N), o kterou se zajímáme, však konstanty a, b nemají vliv.

Podobně najdeme rekurenci pro B_N

$$\begin{aligned} B_{N+1} - B_N &= \sum_{k\geq 0} k\binom{N+2-k}{k}2^k - \sum_{k\geq 0} k\binom{N+1-k}{k}2^k = \\ &= \sum_{k\geq 1} k\binom{N+1-k}{k-1}2^k = \sum_{k\geq 0} (k+1)\binom{N-k}{k}2^{k+1} = 2B_{N-1} + 2A_{N-1}, \end{aligned}$$

tedy řešíme rovnici

$$B_{N+1} - B_N = 2B_{N-1} + 2A_{N-1}. \tag{2.4}$$

Tato rekurentní rovnice pro neznámou posloupnost (B_N) s pravou stranou $(2A_N)$ má řešení

$$B_N = \tilde{B}_N + e \cdot 2^N + f \cdot (-1)^N,$$

kde $\tilde{B}_N$ je partikulární řešení. To lze nalézt ve tvaru

$$\tilde{B}_N = Nh \cdot 2^N + Ng \cdot (-1)^N.$$

Konstanty h a g určíme tak, aby pro každé N platilo $\tilde{B}_{N+1} - \tilde{B}_N = 2\tilde{B}_{N-1} + 2A_{N-1}$. Jelikož

$$\begin{aligned} \tilde{B}_{N+1} - \tilde{B}_N - 2\tilde{B}_{N-1} &= (N+1)h \cdot 2^{N+1} + (N+1)g \cdot (-1)^{N+1} - Nh \cdot 2^N - Ng \cdot (-1)^N - \\ &\quad - 2\left((N-1)h \cdot 2^{N-1} + (N-1)g \cdot (-1)^N\right) = 3h \cdot 2^N + 3g \cdot (-1)^N \end{aligned}$$

se má rovnat $2A_{N-1} = 2a \cdot 2^{N-1} + 2b \cdot (-1)^{N-1}$, stačí zvolit $h = \frac{1}{3}a$, $g = -\frac{3}{2}b$.

Celkové řešení (2.4) je

$$B_N = \tilde{B}_N + e \cdot 2^N + f \cdot (-1)^N = \frac{1}{3}Na \cdot 2^N + \frac{3}{2}Nb \cdot (-1)^N + e \cdot 2^N + f \cdot (-1)^N.$$

Hodnota konstant a, b, f, g neovlivňuje hodnotu limity Φ_N, platí

$$\lim_{N\to\infty} \Phi_N = \lim_{N\to\infty} \frac{B_N}{NA_N} = \lim_{N\to\infty} \frac{\frac{1}{3}Na \cdot 2^N + \frac{3}{2}Nb \cdot (-1)^N + e \cdot 2^N + f \cdot (-1)^N}{N\left(a \cdot 2^N + b \cdot (-1)^N\right)} = \frac{1}{3}.$$

□

Poznámka 2.9. Určit počet čísel, které mají NAF zápisy dlouhé nanejvýš N - v předchozím důkaze jsme jej značili A_N - jsme mohli i jiným způsobem. A to tak, že nalezneme maximální číslo - označme jej x_N, pro jehož NAF zápis stačí N pozic. Evidentně NAF zápis čísla x_N je prefixem nekonečného řetězce $(10)^\omega$.

- Je-li N sudé, je $x_N = \frac{2}{3}(2^N - 1)$,
- je-li N liché, je $x_N = \frac{2}{3}(2^N - \frac{1}{2})$.

Protože radixové uspořádání na NAF reprezentacích odpovídá uspořádání celých čísel, lze každé celé číslo od nejmenšího $-x_N$ do největšího x_N reprezentovat na N pozicích. Odtud $A_N = 2x_N + 1 = \frac{1}{3}\left(2^{N+2} + (-1)^{N+1}\right)$.

Kapitola 3

Poziční numerační systémy v okruzích

Při hledání zápisů přirozených čísel ve standardních soustavách s bázi $b \in \mathbb{N}, b > 1$, používáme cifry $0, 1, \ldots, b-1$. Přirozené číslo x vyjadřujeme ve tvaru $x = a^n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0$. Jsou dva způsoby, jak najít koeficienty $a_0, a_1, \ldots, a_n$. První z nich - nazývaný hladový algoritmus - využívá existence uspořádání na $\mathbb{Z}$ a koeficienty začíná hledat v pořadí od koeficientu a_n u nejvyšší mocniny báze. Poslední koeficient, který hladový algoritmus nalezne, je a_0. Druhý z algoritmů - nazývaný Eukleidův - využívá toho, že v $\mathbb{N}$ je definováno dělení se zbytkem. Jako první je určen koeficient a_0 a jako poslední a_n.

Příklad 3.1. $b = 3$, $\mathcal{A} = \{0, 1, 2\}$, $x \in \mathbb{N}$.
Hledáme zápis $x = 47$ v bázi 3, $x = a_0 \cdot 3^0 + a_1 \cdot 3^1 + \cdots + a_n \cdot 3^n$.

Hladový algoritmus	**Eukleidův algoritmus**	
$3^3 \leq 47 < 3^4, \quad n = 3$	$x_0 = 47 = 2$	mod 3
$x_0 = 47 = 1 \cdot 3^3 + x_1$	$x_0 = 47 = 2$	mod 3
$x_1 = 20 = 2 \cdot 3^2 + x_2$	$x_1 = \dfrac{47-2}{3} = 15 = 0$	mod 3
$x_2 = 2 = 2 \cdot 3^0$	$x_2 = \dfrac{15}{3} = 5 = 2$	mod 3
	$x_3 = \dfrac{5-2}{3} = 1$	mod 3
	$x_4 = \dfrac{1-1}{3} = 0$	

$$(x)_3 = 1202$$

Tam, kde "rozumné" uspořádání není možné, jako je například těleso $\mathbb{C}$, hladový algoritmus nelze použít. V této kapitole se proto budeme věnovat analogii Eukleidova algoritmu. Najít zápis každého čísla ve tvaru kombinací mocnin báze, je jenom jedna stránka problému. Důležité je také

umět s takto zapsanými čísly pracovat, tj. provádět aritmetické operace. Tomu bude věnována poslední sekce této kapitoly.

3.1 Diskrétní okruhy s normou

V této kapitole budeme pracovat s normovanými okruhy. Od normy okruhu $(R, +, \cdot)$ budeme vyžadovat tyto vlastnosti:

$$\begin{aligned}
&\|\cdot\| : R \longrightarrow [0, +\infty);\\
&\|x\| = 0 \iff x = 0;\\
&\|x + y\| \leq \|x\| + \|y\| \qquad \text{pro každé } x, y \in R;\\
&\|x \cdot y\| = \|x\| \cdot \|y\| \qquad \text{pro každé } x, y \in R.
\end{aligned}$$

Definice 3.2. Okruh R s normou $\|\cdot\|$ nazveme diskrétním, pokud pro každé reálné $K > 0$ je množina $\{x \in R : \|x\| \leq K\}$ konečná.

Příklad 3.3. Příklady diskrétních okruhů s normou

- $\mathbb{Z}$ a absolutní hodnota
- $\mathbb{Z}[i] = \{a + ib \ : a, b \in \mathbb{Z}\}$ a absolutní hodnota na $\mathbb{C}$. Prvky tohoto okruhu se nazývají Gaussova celá čísla.
- $\mathbb{Z}[\omega] = \{a + \omega b \ : a, b \in \mathbb{Z}\}$ a absolutní hodnota na $\mathbb{C}$, kde $\omega = e^{i\frac{2\pi}{3}} = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Prvky tohoto okruhu se nazývají Eisensteinova celá čísla.

V okruzích budeme pracovat s kongruencí, která nám umožní hledat reprezentace prvků okruhu, tak jak bylo ilustrováno v úvodním příkladu, kde jsme využili v $\mathbb{Z}$ kongruenci $\mod 3$.

Definice 3.4. Nechť R je okruh, $\beta \in R$. Řekneme, že dva prvky $a, b \in R$ jsou kongruentní $\mod \beta$, pokud $a - b = \beta \cdot z$ pro nějaké $z \in R$. Zapisujeme $a \equiv_\beta b$.

Zřejmě pro libovolné $a_1, a_2, b_1, b_2, c \in R$ platí:

$$a_1 \equiv_\beta b_1 \quad \text{a} \quad a_2 \equiv_\beta b_2 \quad \text{implikuje} \quad a_1 + a_2 \equiv_\beta b_1 + b_2 \quad \text{a} \quad ca_1 \equiv_\beta cb_1.$$

R je disjunktním sjednocením tříd podle kongruence $\equiv_\beta$.

S kongruencí na $\mathbb{Z}$ se běžně setkáváme, třídy kongruencí v okruhu Gaussových celých čísel popisuje následující věta, která pochází (jak název okruhu napovídá) od Gausse. Analogická věta platí také pro Eisensteinova celá čísla.

Věta 3.5. *Nechť $\beta = a + ib \in \mathbb{Z}[i]$ takové, že $\gcd(a, b) = 1$. Pak počet tříd $\mod \beta$ je roven $a^2 + b^2$. Reprezentanti těchto tříd jsou $0, 1, \ldots, a^2 + b^2 - 1$.*

Důkaz. Důkaz provedeme ve třech krocích.

1. Nejprve ukážeme, že každé $\alpha \in \mathbb{Z}[i]$ je kongruentní nějakému $z \in \mathbb{Z}$. Z vlastnosti kongruence plyne, že to stačí ukázat pro i. Je-li totiž $i \equiv_\beta z$, kde $z \in \mathbb{Z}$, pak $\underbrace{x+iy}_{\in\mathbb{Z}[i]} \equiv_\beta \underbrace{x+zy}_{\in\mathbb{Z}}$.

   Nalezněme tedy celé číslo, kterému je kongruentní i. Podmínka $\gcd(a,b) = 1$ zaručuje existenci $c, d \in \mathbb{Z}$ takových, že $ad + bc = 1$. Potom

   $$i = i(ad+bc) = i(ad+bc) + ac - bd - (ac-bd) = \underbrace{(a+ib)}_{\beta}(c+id) - (ac-bd) \equiv_\beta ac - bd.$$

2. Nyní ukážeme, že každé $z \in \mathbb{Z}$ je kongruentní některému z čísel $0, 1, \ldots, a^2+b^2-1$. Dělíme v okruhu $\mathbb{Z}$ číslo z číslem $\beta\overline{\beta} = a^2+b^2$. Dostaneme $z = \underbrace{q}_{\in\mathbb{Z}}\underbrace{(a^2+b^2)}_{\beta\cdot\bar{\beta}} + r$, kde $r \in \{0, 1, \ldots, a^2+b^2-1\}$, tedy $z \equiv_\beta r$.

3. Nakonec ukážeme, že žádné dva prvky ze seznamu $0, 1, \ldots, a^2+b^2-1$ nejsou vzájemně kongruentní. Sporem - nechť pro nějaká $0 \le j < l \le a^2+b^2-1$ platí

   $$l - j = \beta \cdot w = (a+ib)\underbrace{(K+iL)}_{\in\mathbb{Z}[i]} = \underbrace{aK-bL}_{l-j} + i\underbrace{(bK+aL)}_{=0}.$$

   Znaménka bK a aL jsou obrácená, $K, L \neq 0$. Platí tedy $bK = -aL$, zároveň $\gcd(a,b) = 1$, to implikuje $a \mid K$ a $b \mid L$. Jinými slovy $K = ad_1$ a $L = bd_2$ pro nějaké celá čísla d_1 a d_2. Odtud $bK = abd_1, aL = abd_2$. Proto d_1 a d_2 mají různá znaménka. Celkově

   $$|l-j| = |aK - bL| = |a^2d_1 - b^2d_2| = a^2|d_1| + b^2|d_2| \ge a^2+b^2, \qquad \text{a to je spor.}$$

□

3.2 Reprezentace prvků diskrétních okruhů

Definice 3.6. Nechť R je diskrétní okruh s normou. Uvažujme bázi $\beta \in R$ s normou $\|\beta\| > 1$ a konečnou množinu cifer $\mathcal{A} \subset R$. Řekneme, že $x \in R$ má $(\beta, \mathcal{A})$-reprezentaci, pokud $x = \sum_{i=0}^{n} a_i \cdot \beta^i$ pro nějaká $a_0, a_1, \ldots, a_n \in \mathcal{A}$. Řetězec $a_n a_{n-1} \cdots a_0$ budeme označovat $(x)_{\beta,\mathcal{A}}$.

Naším cílem je rozhodnout, jaké vlastnosti páru $(\beta, \mathcal{A})$ zaručí reprezentovatelnost všech prvků z okruhu.

Lemma 3.7. *Mějme $R, \beta, \mathcal{A}$ jako v definici 3.6. Pokud každý prvek R má $(\beta, \mathcal{A})$-reprezentaci, pak $\mathcal{A}$ obsahuje z každé třídy $\equiv_\beta$ alespoň jeden prvek.*

Důkaz. Zvolme libovolnou třídu kongruence $\bmod \beta$ a nějaký její prvek x. Pro $(\beta, \mathcal{A})$-reprezentaci prvku x platí

$$x = \sum_{i=0}^{n} a^i \cdot \beta^i = a_0 + \beta\Big(\sum_{i=1}^{n} a_i \cdot \beta^{i-1}\Big) \equiv_\beta a_0.$$

Ke zvolené třídě patří cifra $a_0 \in \mathcal{A}$. □

Poznámka 3.8. Pokud Gaussovo celé číslo $\beta = a + ib$ má soudělné složky a, b, pak některé třídy kongruence nemají reprezentanta v $\mathbb{Z}$. Je to např. třída, do které patří i. Pokud bychom trvali na abecedě, která je podmnožinou $\mathbb{Z}$, nelze takové báze použít k reprezentování Gaussových čísel.

Pokud pár $(\beta, \mathcal{A})$ splňuje nutnou podmínku vyslovenou v předchozím lemmatu, tak o reprezentovatelnosti celého okruhu lze rozhodnout testováním jeho konečné podmnožiny. Následující věta pochází od Nielse a Kornerupa [21].

Věta 3.9. *Mějme $R, \beta, \mathcal{A}$ jako v definici 3.6 a nechť $\mathcal{A}$ obsahuje z každé třídy kongruence* $\bmod \beta$ *alespoň jednoho reprezentanta. Pokud každé $x \in R$ s normou*

$$\|x\| \leq \frac{\max\{\|d\| : d \in \mathcal{A}\}}{\|\beta\| - 1} =: H \tag{3.1}$$

má $(\beta, \mathcal{A})$-reprezentaci, pak i každý prvek R má $(\beta, \mathcal{A})$-reprezentaci.

Důkaz. Mějme $x \in R$. Zkonstruujeme $x_0 = x, x_1, x_2, \ldots, x_n \in R$ takové, že

- $\|x_i\| < \|x_{i-1}\|$ pro každé $i \in \{1, 2, \ldots, n\}$
- jestli x_i má $(\beta, \mathcal{A})$-reprezentaci, pak x_{i-1} má $(\beta, \mathcal{A})$-reprezentaci
- $\|x_n\| \leq H$.

Popišme slíbenou konstrukci:

Pokud $\|x\| \leq H$, jsme hotovi. Jinak, najdeme $d_0 \in \mathcal{A}$, které leží ve stejné třídě kongruence jako x, tj. existuje $x_1 \in R$ tak, že $x = x_1\beta + d_0$.

1. Má-li x_1 nějakou $(\beta, \mathcal{A})$-reprezentaci, tj. $x_1 = \sum_{j=0}^{k} a_j\beta^j$, kde $a_j \in \mathcal{A}$ pro každé j, pak $x = d_0 + \sum_{j=0}^{n} a_j\beta^{j+1}$ je $(\beta, \mathcal{A})$-reprezentace prvku x.

2. Ukážeme, že $\|x_1\|$ je menší než $\|x\|$. K tomu využijeme nejdříve vlastnosti normy.

   $$\|x_1\| \cdot \|\beta\| = \|x_1\beta\| = \|x - d_0\| \leq \|x\| + \|d_0\|, \qquad \text{a odtud} \qquad \|x_1\| \leq \frac{\|x\| + \|d_0\|}{\|\beta\|}.$$

   Na druhé straně

   $$\|x\| > H \geq \frac{\|d_0\|}{\|\beta\| - 1}, \qquad \text{a to lze přepsat jako} \qquad \frac{\|x\| + \|d_0\|}{\|\beta\|} < \|x\|.$$

Tím je nerovnost $\|x_1\| < \|x\|$ odvozena.

Pokud je $\|x_1\| \leq H$, jsem hotovi. Jinak postup zopakujeme a k x_1 nalezneme x_2 s vlastnostmi analogickými bodům 1) a 2). Protože R je diskrétní okruh, je množina $z \in R$ takových, že $\|z\| < \|x\|$ konečná, a tedy po konečném počtu kroků klesneme s normou pod H. □

Poznámka 3.10. Když jsou splněny předpoklady věty 3.9 a v abecedě $\mathcal{A}$ má každá třída právě jednoho reprezentanta, pak $(\beta, \mathcal{A})$-reprezentace každého $x \in R$ je jednoznačná. Je to důsledek důkazu předchozí věty.

Příklad 3.11. $R = \mathbb{Z}, \beta = 3, \mathcal{A} = \{-1, 0, 1\}$, norma je absolutní hodnota. Tato soustava se nazývá ternární symetrická soustava. V ní zapisovaly čísla první ruské počítače Setuň. Cifry se ukládaly jediným bitem, technicky realizovaným nábojem kladným, záporným nebo neutrálním. Abeceda obsahuje z každé třídy $\bmod 3$ jeden prvek. Pomocí předchozí věty ověříme, že v této soustavě lze jednoznačně reprezentovat libovolné celé číslo.

$$H = \frac{\max\{|-1|, |0|, |1|\}}{|3-1|} = \tfrac{1}{2}.$$

Jediný prvek okruhu $\mathbb{Z}$, který má normu $\leq \frac{1}{2}$, je 0 a ta je reprezentovatelená.

Příklad 3.12. $R = \mathbb{Z}, \beta = -2, \mathcal{A} = \{0, 1\}$, norma je absolutní hodnota. Tuto soustavu jako první navrhl Vittorio Grünwald v roce 1885.

$$H = \frac{\max\{0, 1\}}{|-2|-1} = 1.$$

Podle předchozí věty stačí ověřit, zda $x \in \mathbb{Z}, |x| \leq 1$ mají reprezentaci. 0 a 1 jsou reprezentace, $-1 = 1 \cdot \beta + 1 = 1 \cdot (-2) + 1$, zapisujeme $(-1)_{\beta,\mathcal{A}} = 11$.
Otázky:

- Jak porovnávat čísla pomocí jejich reprezentací?
- Jak sčítat v této soustavě?
- Jak převést čísla z klasické binární soustavy do Grünwaldovy?

3.3 Reprezentace okruhu Gaussových celých čísel

V roce 1965 Walter Penney publikoval práci [24], kde ukázal, jak pomocí dvouprvkové abecedy lze pozičně reprezentovat všechna Gaussova čísla. Také jeho výsledek můžeme odvodit pomocí věty 3.9.

Příklad 3.13. $R = \mathbb{Z}[i]$, norma je absolutní hodnota, $\beta = i - 1, \mathcal{A} = \{0, 1\}$. Podle věty 3.5 existují $\beta \cdot \bar{\beta} = 2$ třídy mod β a 0, 1 jsou jejich reprezentanti. Po dosazení do vztahu (3.1) dostaneme

$$H = \frac{1}{|\beta| - 1} = \frac{1}{\sqrt{2} - 1} = 1 + \sqrt{2}.$$

Je třeba ověřit reprezentovatelnost každého Gaussova celého čísla v kruhu s poloměrem menším nebo rovným než $\sqrt{2}+1$. Takových prvků je 21, jsou to: $\pm 1 \pm i, \pm i, \pm 1, \pm 2, \pm 2i, \pm 2 \pm i, \pm 1 \pm 2i, 0$. Rozvoje lze hledat pomocí kongruence, jak je tomu v důkazu věty 3.9, to je ale dost pracné. Jednodušší je využít tvar několika prvních mocnin báze a reprezentace z nich nakombinovat.

$$\beta^0 = 1, \quad \beta^1 = i - 1, \quad \beta^2 = -2i, \quad \beta^3 = 2 + 2i, \quad \beta^4 = -4.$$

Snadno nahlédneme, že

$$\begin{aligned}
\beta^2 + \beta^3 = 2 &\qquad (2)_{\beta,\mathcal{A}} = 1100. \\
\beta + 1 = i &\qquad (i)_{\beta,\mathcal{A}} = 11. \\
\beta^2 + \beta + 1 = -i &\qquad (-i)_{\beta,\mathcal{A}} = 111. \\
\beta^4 + \beta^3 + \beta^2 + 1 = -1 &\qquad (-1)_{\beta,\mathcal{A}} = 11101 \\
&\text{atd.} \\
\beta^7 + \beta^6 + \beta^5 + \beta^3 + \beta + 1 = -2 - i &\qquad (-2 - i)_{\beta,\mathcal{A}} = 11101011.
\end{aligned}$$

Nakonec zjistíme, že všech 21 prvků lze reprezentovat, a tedy celé $\mathbb{Z}[i]$ lze v Penneyho soustavě reprezentovat jednoznačně.

Příklad 3.14. $R = \mathbb{Z}[i], \beta = i + 1, \mathcal{A} = \{0, 1\}$. Podle věty 3.5 existují $\beta \cdot \bar{\beta} = 2$ třídy mod β a $\mathcal{A}$ obsahuje jejich zástupce. Opět máme ověřit reprezentovatelnost prvků $|z| \leq 1 + \sqrt{2}$. Zjistíme, že i nemá reprezentaci. Platí totiž, že $i \equiv_\beta 1$, protože $i - 1 = (i + 1)i = \beta \cdot i$, tedy $i = \beta \cdot i + 1$. Měli bychom vytvořit reprezenaci i pomocí reprezentace i, a tak do nekonečna.

Příklad 3.13 ukázal, že ověřovat podmínky věty 3.9 není vždy tak snadné, jako pro symetrickou ternární soustavu nebo Grünwaldovou soustavu. Někdy ověřování vyžaduje masivní nasazení výpočetní techniky. Reprezentovatelnost okruhu $\mathbb{Z}[i]$ pro všechny přípustné báze (porovnej s poznámkou 3.8) a abecedy dané větou 3.5 lze jednoduše rozhodnout pomocí následující věty. Tu dokázali Kátai a Szabó v [18].

Věta 3.15. *Nechť $\beta = a + ib$, $a, b \in \mathbb{Z}$, $\mathcal{A} = \{0, 1, \ldots, a^2 + b^2 - 1\}, \gcd(a, b) = 1$. Každé $x \in \mathbb{Z}[i]$ má $(\beta, \mathcal{A})$-reprezentaci právě tehdy, když $a \leq -1 \quad a \quad b = \pm 1$.*

Důkaz. ($\Longrightarrow$) Důkaz této implikace rozdělíme do několika drobných tvrzení:

1. Pokud by $b = 0$, pak Gaussova celá čísla s nenulovou imaginární části nemají žádnou reprezentaci.

2. Imaginární část čísla $\beta^k = (a+ib)^k$ je dělitelná číslem b pro každé $k \in \mathbb{N}$. Proto $z \in \mathbb{Z}[i]$ zapsané ve tvaru $\sum_{k=0}^{n} a_k\beta^k$ má imaginární část dělitelnou číslem b. Odtud plyne, že β, které dovoluje reprezentovat celý okruh, má $|b| = 1$.

3. Čísla β a $\overline{\beta}$ mají stejnou velikost, a proto i stejnou abecedu $\mathcal{A}$. Pokud $\left\{\sum_{k=0}^{n} a_k\beta^k : n \in \mathbb{N}, a_k \in \mathcal{A}\right\} = \mathbb{Z}[i]$, pak také $\left\{\sum_{k=0}^{n} a_k(\overline{\beta})^k : n \in \mathbb{N}, a_k \in \mathcal{A}\right\} = \mathbb{Z}[i]$. Tedy báze β dovoluje reprezentovat celý okruh právě tehdy, když to dovoluje báze $\overline{\beta}$.

4. Proto bez újmy na obecnosti dále uvažujeme $\beta = a + i$, kde $a \in \mathbb{Z}$ a abeceda $\mathcal{A} = \{0, 1, \ldots, a^2\}$. Požadavek $|\beta| > 1$, vynucuje $a \neq 0$. Pro dokončení důkazu implikace zbývá odvodit, že $a < 0$.

   Při platnosti nerovnosti $a > 0$ ukážeme, že Gaussovo číslo $z = (1-a) + i$ nemá žádnou $(\beta, \mathcal{A})$-reprezentaci. Pro spor předpokládejme, že $z = \sum_{k=0}^{n} a_k\beta^k$. Zřejmě, $z \equiv_\beta a_0$. Snadno ověříme, že pro naše z platí, $z = \beta z + (a-1)^2 + 1$. Jelikož je $a > 0$, je $(a-1)^2 + 1 \in \mathcal{A}$. Podle věty 3.5 je v abecedě $\mathcal{A}$ z každé třídy kongruence právě jeden prvek, a tedy nutně $a_0 = (a-1)^2+1$. Ze vztahu $z = \beta z + a_0$ plyne, že $\sum_{k=1}^{n} a_k\beta^{k-1}$ je také $(\beta, \mathcal{A})$-reprezentací čísla z - a to je podle poznámky 3.10 spor.

($\Longleftarrow$) Označme $c = -a \in \mathbb{Z}$. Tedy $\beta = i - c$, kde $c > 0$. Abeceda je $\mathcal{A} = \{0, 1, \ldots, c^2\}$. Toto β je kořenem kvadratické rovnice $(X-\beta)(X-\overline{\beta}) = 0$ a kubické rovnice $(X-1)(X-\beta)(X-\overline{\beta}) = 0$. Po roznásobení a dosazení β dostaneme dvě rovnosti, které při hledání reprezentací prvků okruhu budeme využívat.

$$\beta^2 + 2c\beta + c^2 + 1 = 0 \qquad \text{a} \qquad \beta^3 + (2c-1)\beta^2 + (c-1)^2\beta - (c^2+1) = 0. \tag{3.2}$$

Speciálně si všimněme, že rovnost vlevo má koeficienty u β^0, β^1 a β^2 kladné. Druhá rovnost má koeficient u β^0 záporný, koeficienty u β^1, β^2 a β^3 jsou nezáporné. Součet všech čtyř koeficientů dohromady je roven nule.

Nechť $z = A + iB \in \mathbb{Z}[i]$. Nejdříve vyjádříme z ve tvaru $z = s_2\beta^2 + s_1\beta + s_0$, kde $s_2, s_1, s_0 \in \mathbb{N}$. Toho docílíme tak, že vyjádříme z ve tvaru $z = A + iB = B\beta^1 + (A + cB)\beta^0$ a k tomuto vyjádření přičteme 0 ve formě D násobku první rovnice z (3.2). Dostaneme

$$z = z + D\underbrace{(\beta^2 + 2c\beta + c^2 + 1)}_{=0} = D\beta^2 + (B + 2cD)\beta^1 + \big(A + cB + D(c^2+1)\big)\beta^0 =: s_2\beta^2 + s_1\beta + s_0.$$

Pro dostatečně velké $D \in \mathbb{N}$ jsou všechny koeficienty s_2, s_1, s_0 nezáporné. Označme $K = s_2 + s_1 + s_0$. Pokud jsou všechny tyto koeficienty $\leq c^2$, tj. jsou z abecedy $\mathcal{A}$, máme kýženou reprezentaci čísla z. Jinak budeme k $s_2\beta^2 + s_1\beta + s_0$ přičítat 0 ve tvaru β^j násobku druhé z rovností (3.2) a

tento postup budeme opakovat tak dlouho, až koeficienty u všech mocnin β^k, které se ve vyjádření z vyskytují, budou z abecedy $\mathcal{A}$.

Obecně, označme reprezentaci čísla z, kterou máme v ℓ-tém kroku, jako $z = \sum_{k=0}^{n_\ell} s_k^{(\ell)} \beta^k$, kde všechny $s_k^{(\ell)}$ jsou nezáporné. Pokud některý z koeficientů je příliš velký, tj. $s_k^{(\ell)} \geq c^2 + 1$, označíme M_ℓ minimální koeficient s touto vlastností. Definujeme $P_\ell = \sum_{k=0}^{M_\ell - 1} s_k^{(\ell)}$. Tedy P_ℓ představuje sumu všech koeficientu u mocnin β ostře menších než M_ℓ. Další, tedy $(\ell+1)$-ní reprezentaci čísla z vytvoříme tak, že k ℓ-té reprezentaci přičteme 0 ve tvaru $D\beta^{M_\ell}\left(\beta^3 + (2c-1)\beta^2 + (c-1)^2\beta - (c^2+1)\right)$. Číslo $D \in \mathbb{N}$ volíme tak, aby $s_{M_\ell}^{(\ell)} - D(c^2+1) \in \mathcal{A}$.

Nová reprezentace čísla $z = \sum_{k=0}^{n_{\ell+1}} s_k^{(\ell+1)} \beta^k$ má

- $s_k^{(\ell+1)} = s_k^{(\ell)}$ pro $k = 0, 1, \ldots, M_{\ell-1}$;
- $s_{M_\ell}^{(\ell+1)} = s_{M_\ell}^{(\ell)} - D(c^2+1) \in \mathcal{A}$;
- $M_{\ell+1} > M_\ell$;
- $P_{\ell+1} = P_\ell + s_{M_\ell}^{(\ell+1)} \geq P_\ell$.

Přitom suma všech koeficientů u nové reprezentace čísla z zůstala stejná, a to K jako u startovací reprezentace. Přičítaný výraz má totiž součet koeficientů u mocnin β roven 0. Pokud po konečném počtu kroků dostaneme reprezentaci čísla z, u které jsou všechny koeficienty z abecedy $\mathcal{A}$, jsme hotovi a máme $(\beta, \mathcal{A})$ reprezentaci čísla z.

Předpokládejme proto, že pro každé $\ell \in \mathbb{N}$ zápis čísla $z = \sum_{k=0}^{n_\ell} s_k^{(\ell)} \beta^k$ obsahuje koeficient, který není z abecedy $\mathcal{A}$. Navíc P_ℓ je neklesající posloupnost omezena shora číslem K. Od jistého indexu $\widetilde{\ell}$, je posloupnost P_ℓ konstantní. To znamená, že pro každé $\ell > \widetilde{\ell}$ a pro každé $k = M_{\widetilde{\ell}} + 1, \ldots, M_\ell - 2, M_\ell - 1$ je $s_k^{(\ell)} = 0$. ℓ-té vyjádření čísla z má tedy tvar

$$z = \underbrace{\sum_{k=0}^{M_{\widetilde{\ell}}} s_k^{(\ell)} \beta^k}_{=:\widetilde{z}} + \underbrace{\sum_{k=M_\ell}^{n_\ell} s_k^{(\ell)} \beta^k}_{y_\ell . \beta^{M_\ell}}$$

Číslo $\widetilde{z}$ je stejné pro každé $\ell > \widetilde{\ell}$ a $y_\ell \in \mathbb{Z}[i]$. Kdyby $y_\ell \neq 0$, pak $|y_\ell| \geq 1$. Proto $|z - \widetilde{z}| = |y_\ell . \beta^{M_\ell}| \geq |\beta|^{M_\ell}$. To dává pro dostatečně velké ℓ spor. Tedy nutně, $y_\ell = 0$ a $z = \widetilde{z}$ je $(\beta, \mathcal{A})$ reprezentace čísla z. □

Kapitola 4

Poziční reprezentace reálných a komplexních čísel

Pokud chceme pozičně reprezentovat množinu všech reálných nebo komplexních čísel, které jsou nespočetné, budeme k reprezentaci většiny čísel potřebovat nekonečné řetězce cifer. Proto nelze využít metodu založenou na dělitelnosti v diskrétních okruzích, kterou jsme představili v kapitole 3. Tato metoda umožňuje hledat jenom konečné řetězce cifer. Generování nekonečných řetězců vyžaduje iterativní proces. Myšlenka iterativního procesu ve vícerozměrném vektorovém prostoru nad tělesem $\mathbb{R}$ se prvně objevila v práci [30], která se zabývá dlážděním prostoru. My uvedeme její variantu pro těleso $\mathbb{C}$, které lze chápat jako vektorový prostor dimenze dva nad $\mathbb{R}$.

Věta 4.1. *Nechť je dána báze $\beta \in \mathbb{C}$, $|\beta| > 1$ a konečná abeceda $\mathcal{A} \subset \mathbb{C}$. Pokud existuje množina $V \subset \mathbb{C}$ s vlastnostmi*

1. *V je omezená,*
2. *0 leží ve vnitřku V, tj. $0 \in V^\circ$,*
3. *$\beta V \subset \bigcup_{a \in \mathcal{A}} (V + a)$,*

pak každé $z \in \mathbb{C}$ lze zapsat ve tvaru

$$z = \sum_{k=-\infty}^{n} b_k \beta^k,$$

kde $n \in \mathbb{Z}$ a pro všechna $k \in \mathbb{Z}, k \leq n$, je $b_k \in \mathcal{A}$.

Důkaz. Nejdříve dokážeme tvrzení, že každé $z \in V$ lze zapsat ve tvaru

$$z = \sum_{k=1}^{\infty} a_k \beta^{-k}, \quad \text{kde } a_k \in \mathcal{A} \text{ pro všechna } k \in \mathbb{N}.$$

Nechť tedy $z \in V$. Jelikož $\beta z \in \beta V$, existuje $a_1 \in \mathcal{A}$ tak, že $\beta z = a_1 + z^{(1)}$, kde $z^{(1)} \in V$. Tedy

$$z = \frac{a_1}{\beta} + \frac{z^{(1)}}{\beta}.$$

Opakujeme $\beta z^{(1)} \in \beta V$, proto existuje $a_2 \in \mathcal{A}$ tak, že $\beta z^{(1)} = a_2 + z^{(2)}$, kde $z^{(2)} \in V$. Odtud

$$z = \frac{a_1}{\beta} + \frac{a_2}{\beta^2} + \frac{z^{(2)}}{\beta^2}.$$

V n-tém kroku

$$z = \frac{a_1}{\beta} + \frac{a_2}{\beta^2} + \cdots + \frac{a_n}{\beta^n} + \frac{z^{(n)}}{\beta^n},$$

kde $z^{(n)} \in V$. Protože V je omezená platí $\frac{z^{(n)}}{\beta^n} \longrightarrow 0$.

Nyní uvažujme libovolné $z \notin V$. Z faktu, že $0 \in V^\circ$, plyne existence čísla $n \in \mathbb{N}$, pro které $\frac{1}{\beta^{n+1}} z \in V$. Podle už dokázaného tvrzení $\frac{1}{\beta^{n+1}} z$ lze vyjádřit ve tvaru $\sum_{k=1}^{\infty} a_k \beta^{-k}$, a tedy $z = \sum_{k=1}^{\infty} a_k \beta^{n+1-k} = \sum_{k=-\infty}^{n} a_{n+1-k} \beta^k$, což dokazuje větu. □

Poznámka 4.2. Důkaz Thurstonovy věty v sobě zahrnuje iterativní proces založený na transformaci $T : V \mapsto V$, když prvku $z^{(i)} \in V$ přiřazujeme $z^{(i+1)} \in V$. Aby algoritmus z Thurstonovy věty byl realizovatelný v počítači, musí existovat algoritmus, který rozhodne, zda $\beta z^{(i)} \in V + a$.

Poznámka 4.3. Pro reálné těleso platí analogie Thurstonovy věty a její důkaz je identický.

4.1 Poziční reprezentace reálných čísel - příklady

Otázku, kdy k zadané bázi a abecedě existuje množina V s požadovanými vlastnostmi, není obecně jednoduché zodpovědět. V případě, že báze i abeceda jsou reálné, se odpověď hledá snadněji, jak předvedeme na příkladech reprezentací v Grünwaldově soustavě a NAF reprezentací.

Příklad 4.4. Uvažujme Grünwaldovu soustavu $\beta = -2$ a $A = \{0, 1\}$. Množina $V = \left[-\frac{2}{3}, \frac{1}{3}\right]$ má požadované vlastnosti

$$-2\left[-\frac{2}{3}, \frac{1}{3}\right] = \left[-\frac{2}{3}, \frac{4}{3}\right] = \left[-\frac{2}{3}, \frac{1}{3}\right] \cup \left(1 + \left[-\frac{2}{3}, \frac{1}{3}\right]\right) \tag{4.1}$$

Ilustrujme hledání rozvoje Eulerova čísla $e = 2,71828\ldots$ v této soustavě.

$$\begin{aligned} z &:= \frac{e}{(-2)^3} = -0.339785228\ldots && \in \left[-\frac{2}{3}, \frac{1}{3}\right] \\ \beta z &= 0.679570456\ldots && \in 1 + \left[-\frac{2}{3}, \frac{1}{3}\right] \implies a_1 = 1 \\ z^{(1)} &= \beta z - 1 = -0.320429554\ldots \end{aligned}$$

$$\begin{aligned}
\beta z^{(1)} &= 0.640859088\ldots && \in 1+\left[-\frac{2}{3},\frac{1}{3}\right] \implies a_2 = 1\\
z^{(2)} &= \beta z^{(1)} - 1 = -0.359140912\ldots\\
\beta z^{(2)} &= 0.718281824\ldots && \in 1+\left[-\frac{2}{3},\frac{1}{3}\right] \implies a_3 = 1\\
z^{(3)} &= \beta z^{(2)} - 1 = -0.281718176\ldots\\
\beta z^{(3)} &= 0.563436352\ldots && \in 1+\left[-\frac{2}{3},\frac{1}{3}\right] \implies a_4 = 1\\
z^{(4)} &= \beta z^{(3)} - 1 = -0.436563648\ldots\\
\beta z^{(4)} &= 0.873127296\ldots && \in \left[-\frac{2}{3},\frac{1}{3}\right] \implies a_5 = 1\\
z^{(5)} &= -0.126872704\ldots\\
\beta z^{(5)} &= 0,253745408\cdots \implies a_6 = 0, a_7 = 0, a_8 = 1\ldots
\end{aligned}$$

$$(e)_{\beta,\mathcal{A}} = 111\cdot 11001\cdots = 4-2+1-\frac{1}{2}+\frac{1}{4}-\frac{1}{32}+\cdots$$

Všimněme si, že množina V ve vztahu (4.1) má vlastnost $\beta V = V \cup (V+1)$ a průnik množin V a $V+1$ obsahuje jediný bod, totiž $\frac{1}{3}$. To znamená, že při určení cifry a podle toho, kam padne $\beta z \in \beta V$, máme na výběr pouze v případě, kdy $\beta z = \frac{1}{3}$. Číslo $\frac{1}{3}$ lze v Grünwaldově soustavě reprezentovat dvěma způsoby $\left(\frac{1}{3}\right)_{\beta,\mathcal{A}} = 1\cdot(10)^\omega = 0\cdot(01)^\omega$. Podobný jev známe i z klasické desítkové soustavy, kdy $1.0^\omega = 0.9^\omega$.

Pokud zvětšíme abecedu, přijdeme o jednoznačnost rozvoje pro většinu čísel. Zato si mezi rozvoji můžeme vybírat ty, které mají vlastnost vhodnou pro nějaké speciální účely.

Příklad 4.5. Je dána báze $\beta = 2$ a abeceda $\mathcal{A} = \{\bar{1}, 0, 1\}$. Pokud

$$V = \left[-\frac{2}{3},\frac{2}{3}\right), \quad \text{pak} \quad 2V = \left[-\frac{4}{3},\frac{4}{3}\right) \subset (V-1)\cup V\cup(V+1) = \left[-\frac{5}{3},\frac{5}{3}\right).$$

Průnik $V \cap (V+1) = \left[\frac{1}{3},\frac{2}{3}\right)$ a symetricky pro $V \cap (V-1)$. Tedy pro volbu cifer máme více volnosti. Dokonce tolik, že vhodnou volbou dostáváme NAF reprezentace čísel. Fakticky jsme hranice intervalu pro V volili jako maximální číslo zapsané v NAF "za binární tečkou"

$$\frac{a_1}{2}+\frac{a_2}{2^2}+\frac{a_3}{2^3}+\cdots \le \frac{1}{2}+\frac{1}{2^3}+\frac{1}{2^5}+\cdots = \frac{2}{3}$$

a minimální číslo $-\frac{2}{3}$. Při odvození algoritmu pro hledání NAF rozvoju využijeme toho, že maximální (minimální) číslo zapsatelné v NAF ve tvaru

$$-\frac{1}{3} \le \frac{0}{2}+\frac{a_2}{2^2}+\frac{a_3}{2^3}+\cdots \le \frac{1}{3}$$

Algoritmus pro hledání *NAF* rozvoje pro $x \in \left[-\frac{2}{3}, \frac{2}{3}\right)$

- Pokud $x \in \left[-\frac{1}{3}, \frac{1}{3}\right)$ polož $a = 0$ a $x_{new} = 2x$.
- Pokud $x \in \left[\frac{1}{3}, \frac{2}{3}\right)$ polož $a = 1$ a $x_{new} = 2x - 1$.
- Pokud $x \in \left[-\frac{2}{3}, -\frac{1}{3}\right)$ polož $a = -1$ a $x_{new} = 2x + 1$.

Platí pokud $a \neq 0$, pak $x_{new} \in \left[-\frac{1}{3}, \frac{1}{3}\right)$, tedy po nenulové cifře následuje cifra 0. Navíc

$$x = \frac{a}{2} + \frac{1}{2}x_{new}.$$

Proto po N krocích

$$x = \frac{a_1}{2} + \frac{a_2}{2^2} + \cdots + \frac{a_N}{2^N} + \underbrace{\frac{1}{2^N}x_{N+1}}_{\xrightarrow{N\to\infty}0}$$

Algoritmus pro hledání *NAF* reprezentací pro $x \in \mathbb{R}$

Každé reálné x lze zapsat ve tvaru $x = N + \alpha$, kde $N \in \mathbb{Z}$ a $\alpha \in [-\frac{1}{3}, \frac{2}{3})$.

- Pokud $\alpha \in [-\frac{1}{3}, \frac{1}{3})$, pak NAF-reprezentace α je tvaru $\alpha = \frac{0}{2} + \frac{a_2}{2^2} + \ldots$. Proto spojení NAF-reprezentace čísla $N = \sum_{k=0}^{n} b_k 2^k$ s NAF-reprezentací čísla α nebude obsahovat sousedící nenulové cifry.
- Pokud $\alpha \in [\frac{1}{3}, \frac{2}{3})$ a číslo N je sudé, pak NAF-reprezentace čísla N končí na cifru $b_0 = 0$ a opět spojením NAF-reprezentací dostaneme NAF-reprezentaci.
- Pokud $\alpha \in [\frac{1}{3}, \frac{2}{3})$ a číslo N je liché, pak využijeme toho, že $x = N + 1 + \alpha - 1$, kde $N + 1$ je sudé a $\alpha - 1 \in [-\frac{2}{3}, -\frac{1}{3})$. Spojovat budeme NAF-reprezentaci sudého celého čísla $N + 1$ s NAF-reprezentaci čísla $\alpha - 1$.

Příklad 4.6. Najdeme několik míst NAF reprezentace čísla π. Nejprve najdeme zápis $\pi - 3 = 0,141592653598\ldots$

$$\begin{aligned}
x_0 &\approx 0,141592\ldots && \in \left[-\frac{1}{3}, \frac{1}{3}\right) && a_1 = 0\\
x_1 = 2x_0 &\approx 0,283185\ldots && \in \left[-\frac{1}{3}, \frac{1}{3}\right) && a_2 = 0\\
x_2 = 2x_1 &\approx 0,566370\ldots && \in \left[\frac{1}{3}, \frac{2}{3}\right) && a_3 = 1\\
x_3 = 2x_2 - 1 &\approx 0,132741\cdots && \in \left[-\frac{1}{3}, \frac{1}{3}\right) && a_4 = 0\\
x_4 = 2x_3 &\approx 0,265482\ldots && \in \left[-\frac{1}{3}, \frac{1}{3}\right) && a_5 = 0\\
x_5 = 2x_4 &\approx 0,5309649\ldots && \in \left[\frac{1}{3}, \frac{2}{3}\right) && a_6 = 1
\end{aligned}$$

$$
\begin{aligned}
x_6 &= 2x_5 - 1 \approx 0,061929\ldots && \in \left[-\frac{1}{3}, \frac{1}{3}\right) && a_7 = 0\\
x_7 &= 2x_6 \approx 0,123859\ldots && \in \left[-\frac{1}{3}, \frac{1}{3}\right) && a_8 = 0\\
x_8 &= 2x_7 \approx 0,247719\ldots && \in \left[-\frac{1}{3}, \frac{1}{3}\right) && a_9 = 0\\
x_9 &= 2x_8 \approx 0,4954386\ldots && \in \left[\frac{1}{3}, \frac{2}{3}\right) && a_{10} = 1\\
x_{10} &= 2x_9 - 1 \approx -0,009122\ldots && \in \left[-\frac{1}{3}, \frac{1}{3}\right) && a_{11} = 0
\end{aligned}
$$

Po deseti krocích algoritmu máme $0,14159265359878323\ldots$ aproximované jako

$$\frac{0}{2} + \frac{0}{4} + \frac{1}{8} + \frac{0}{16} + \frac{0}{32} + \frac{1}{64} + \frac{0}{128} + \frac{0}{256} + \frac{1}{512} = \frac{73}{512} \approx 0,142578125.$$

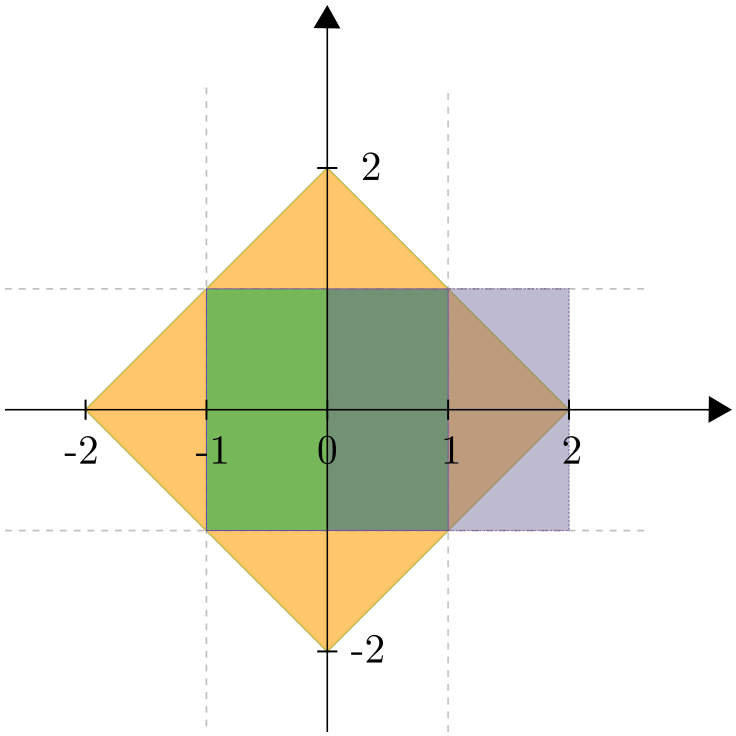
Celkově má číslo π NAF reprezentaci

$$10\bar{1} \cdot 0010010010\ldots$$

4.2 Poziční reprezentace komplexních čísel s bázi $\beta = i - 1$

Pro komplexní případ je nelezení V těžké, pokud hledáme V pro malou abecedu. Je-li abeceda větší, hledá se V snadněji - tím se však vzdáváme jednoznačnosti reprezentací.

Příklad 4.7. Obrázek 4.1 ilustruje, že k bázi $\beta = i - 1$ a abecedě $\mathcal{A} = \{\pm 1, \pm i, 0\}$ je vhodnou volbou množina $V = \{z \in \mathbb{C} : |\mathrm{Re}\, z| \leq 1, |\mathrm{Im}\, z| \leq 1\}$.



Obrázek 4.1: Zelená množina V, oranžová množina βV, modrá množina $V + 1$

Abecedu jsme však zvětšili ze dvou cifer 0 a 1, které stačí k jednoznačné reprezentaci gaussovských celých čísel v soustavě se stejnou bázi, na abecedu o pěti cifrách.

Zkusme pro bázi $\beta = i - 1$ hledat množinu V k abecedě $\mathcal{A} = \{0, 1\}$. Nutně

$$\beta V \subset V \cup (V + 1). \tag{4.2}$$

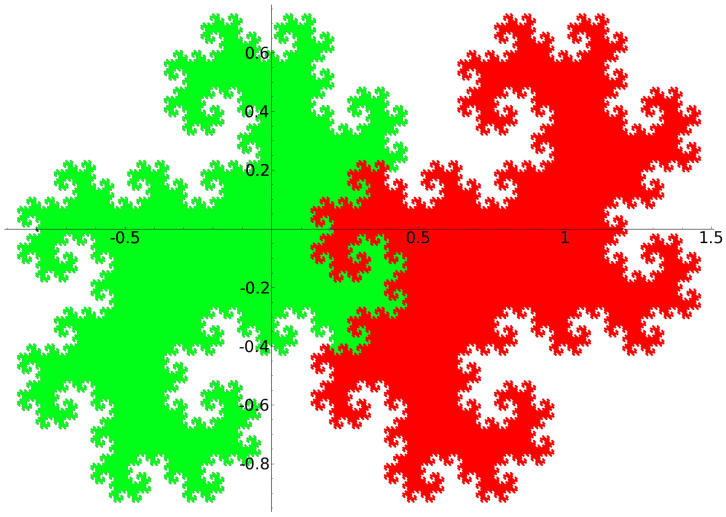
Kdyby V bylo měřitelné, pak $V^\circ \neq 0$ implikuje, že míra $\mu(V)$ množiny V je kladná a

$$\mu(\beta V) = |\beta|^2 \mu(V) = 2\mu(V)$$

Aby platila inkluze (4.2), tak až na množinu míry nula, musí platit $\beta V = V \cup (V+1)$ a sjednocení by až na množinu míry 0 mělo být disjunktní. Takovou množinu lze popsat explicitně.

$$V = \left\{ \sum_{k=1}^{\infty} \frac{a_k}{\beta^k} : a_k \in \{0, 1\} \right\} = \left\{ \frac{a_1}{\beta} + \frac{a_2}{\beta^2} + \frac{a_3}{\beta^3} + \cdots : a_k \in \{0, 1\} \right\} \quad \text{a}$$

$$\beta V = \left\{ a_1 + \sum_{k=1}^{\infty} \frac{a_{k+1}}{\beta^k} : a_k \in \{0, 1\} \right\} = V \cup (1 + V).$$



Obrázek 4.2: Zelená množina V, červená množina $V + 1$, jejich sjednocení je βV.

Množina V je vykreslena na obrázku 4.2. Lze ukázat, že V má fraktální hranici. To ale znamená, že se musíme vzdát naděje hledat efektivně reprezentaci komplexních čísel v bázi $\beta = i - 1$ a abecedě $\mathcal{A} = \{0, 1\}$ pomocí věty 4.1. Neznamená to však, že v Penneyově soustavě nelze reprezentovat všechna komplexní čísla.

Definice 4.8. Řekneme, že M je relativně hustá v $\mathbb{C}$, pokud existuje poloměr $r > 0$ takový, že pro každé $z \in \mathbb{C}$ je $B(z, r) \cap M \neq \emptyset$, tj. v kouli o poloměru r s libovolným středem leží alespoň jeden prvek z M.

K důkazu existence $(\beta, \mathcal{A})$ reprezentací komplexních čísel využijeme množinu

$$\mathrm{Fin}_{\mathcal{A}}(\beta) = \left\{ \sum_{k \in I} a_k \beta^k : I \subset \mathbb{Z}, I \text{ konečná }, a_k \in \mathcal{A} \text{ pro každé } k \in I \right\}.$$

Příklad 4.9. $\mathbb{Z}[i]$ je relativně hustá v $\mathbb{C}$. Navíc víme, že pro bázi $\beta = i - 1$ a $\mathcal{A} = \{0, 1\}$ je $\mathbb{Z}[i] = \{\sum_{k=0}^{n} a_k \beta^k : n \in \mathbb{N}_0, a_0, a_1, \ldots, a_n \in \mathcal{A}\}$. Proto

$$\mathrm{Fin}_{\mathcal{A}}(\beta) = \mathbb{Z}[i] \cup \frac{1}{\beta}\mathbb{Z}[i] \cup \frac{1}{\beta^2}\mathbb{Z}[i] \cup \cdots = \bigcup_{n \in \mathbb{N}_0} \frac{1}{\beta^n}\mathbb{Z}[i]$$

je hustá v $\mathbb{C}$. Proto pro každé $z \in \mathbb{C}$ existuje posloupnost $z^{(n)} \in \mathrm{Fin}_{\mathcal{A}}(\beta)$ taková, že $z^{(n)} \longrightarrow z$. Zbývá vyřešit otázku, jakým řetězcem reprezentovat z.

Věta 4.10. *Nechť R je diskrétní a relativně hustý okruh v $\mathbb{C}$. Uvažujme bázi $\beta \in R$, $|\beta| > 1$ a abecedu $\mathcal{A} \subset R$, $0 \in \mathcal{A}$. Pokud $R = \{\sum_{k=0}^{n} a_k \beta^k : n \in \mathbb{N}_0, a_0, a_1, \ldots, a_n \in \mathcal{A}\}$, pak každé $z \in \mathbb{C}$*

lze zapsat ve tvaru

$$z = \sum_{k=-\infty}^{n} a_k \beta^k, \qquad \textit{kde } n \in \mathbb{Z} \;\; \textit{a} \;\; \textit{pro každé celé} \;\; k \leq n \;\; \textit{je} \;\; a_k \in \mathcal{A}.$$

Důkaz. Protože R je relativně hustý v $\mathbb{C}$, je množina $\mathrm{Fin}_{\mathcal{A}}(\beta)$ hustá v $\mathbb{C}$, a tedy libovolné $z \in \mathbb{C}$ je limitou posloupnosti prvků množiny $\mathrm{Fin}_{\mathcal{A}}(\beta)$. Nechť

$$z = \lim_{n\to\infty} z^{(n)}, \quad \text{kde} \;\; z^{(n)} = \sum_{k=D_n}^{H_n} a_k^{(n)} \beta^k.$$

Označme $M := \max\{|a| : a \in \mathcal{A}\}$ a definujme "celou" a "zlomkovou" část čísla $z^{(n)}$ takto

$$z^{(n)} = \underbrace{\sum_{k=0}^{H_n} a_k^{(n)} \beta^k}_{:=x^{(n)} \in R} + \underbrace{\sum_{k=D_n}^{-1} a_k^{(n)} \beta^k}_{:=r_n}.$$

Jelikož $|r_n| \leq \sum_{k=-\infty}^{-1} M|\beta|^k = \frac{M}{|\beta|-1}$, je posloupnost (r_n) omezená. Konvergentní posloupnost $(z^{(n)})$ je omezená také, a tedy $x^{(n)} = z^{(n)} - r_n \in R$ je omezená. Okruh R je diskrétní, a proto posloupnost $x^{(n)}$ nabývá pouze konečně mnoho hodnot. Bez újmy na obecnosti předpokládejme, že stejné celé části $x^{(n)}$ jsou jako prvky R reprezentovány stejně. Tedy H_n nabývá konečně mnoho hodnot, maximální hodnotu označme H. Bez újmy na obecnosti

$$z^{(n)} = \sum_{k=D_n}^{H} a_k^{(n)} \beta^k \longrightarrow z.$$

Vybereme posloupnost $z^{(k_n)}$ takovou, že pro každé $n, m \in \mathbb{N}, n < m$ se n prvních cifer v zápisu $z^{(k_n)}$ a $z^{(k_m)}$ shoduje. Definujeme cifry $a_H, a_{H-1}, a_{H-2}, \cdots \in \{0, 1\}$

$$\begin{aligned}
a_H = a \text{ tak, aby } M_1 &= \{z^{(n)} : z_H^{(n)} = a\} \text{ byla nekonečná,} \\
a_{H-1} = a \text{ tak, aby } M_2 &= \{z^{(n)} : z_H^{(n)} z_{H-1}^{(n)} = a_H a\} \text{ byla nekonečná,} \\
a_{H-2} = a \text{ tak, aby } M_3 &= \{z^{(n)} : z_H^{(n)} z_{H-1}^{(n)} z_{H-2}^{(n)} = a_H a_{H-1} a\} \text{ byla nekonečná,} \\
&\vdots
\end{aligned}$$

Zřejmě

$$\sum_{k=-n}^{H} a_k \beta^k \longrightarrow z.$$

$z^{(k_1)}$ vybereme libovolně z M_1, $z^{(k_2)}$ vybereme z M_2, ... □

Poznamenejme, že předchozí důkaz s malou modifikací je převzat z knihy [19].

Důsledek 4.11. *Každé komplexní číslo má reprezentaci v Penneyho soustavě.*

Kapitola 5

Číselné soustavy s jednoznačným zápisem

5.1 Rényiho f-rozvoje

V článku [25], Alfréd Rényi zavedl reprezentace reálného čísla x pomocí iterací pozitivní monotonní funkce $f : [0, T) \to [0, +\infty)$ ve tvaru tzv. f-rozvoje

$$x = \varepsilon_0 + f(\varepsilon_1 + f(\varepsilon_2 + f(\varepsilon_3 + \cdots) \cdots) \,. \tag{5.1}$$

'Cifry' $\varepsilon_n = \varepsilon_n(x)$, $n \in \mathbb{N}_0$, a 'zbytky'

$$r_n(x) = f(\varepsilon_{n+1} + f(\varepsilon_{n+2} + f(\varepsilon_{n+3} + \cdots) \cdots) \,, \quad n \in \mathbb{N}_0 \,,$$

v zápisu (5.1) jsou definované rekurzivně

$$\begin{aligned} \varepsilon_0(x) &= \lfloor x \rfloor \,, & r_0(x) &= \{x\} \,, \\ \varepsilon_{n+1}(x) &= \lfloor \varphi(r_n(x)) \rfloor \,, & r_{n+1}(x) &= \big\{\varphi(r_n(x))\big\} \,, \quad n \in \mathbb{N}_0 \,, \end{aligned}$$

kde φ je funkce inverzní k funkci f. Symbol $\{z\} = z - \lfloor z \rfloor$ pak označuje zlomkovou část čísla z.

Rényi dokázal postačující podmínku na fukci f, aby reprezentace (5.1) existovala pro každé reálné číslo x. Tato podmínka je formulována zvlášť pro dva případy, podle toho, zda je funkce f rostoucí nebo klesající.

Nechť $f : [1, +\infty) \to [0, 1]$ je klesající: Předpokládejme, že f navíc splňuje

- $f(1) = 1$;
- $f(t)$ je spojitá a ostře klesající funkce na $[1, T]$, kladná pro $t < T$ a nulová pro $t \geq T$, kde $2 < T \leq +\infty$;

- $|f(t_2) - f(t_1)| \leq |t_2 - t_1|$ pro $1 \leq t_1 < t_2$, a navíc existuje $\lambda \in (0,1)$ taková, že $|f(t_2) - f(t_1)| \leq \lambda |t_2 - t_1|$ pro $1 + f(2) < t_1 < t_2$.

Označíme-li $\varphi : [0,1] \to [1,T]$ inverzní k f, pak f-rozvoj (5.1) existuje ke každému reálnému číslu x. V závislosti na parametru T mohou cifry ε_n, $n \geq 1$, v f-rozvoji nabývat různých hodnot.

- Je-li $T = +\infty$, pak $\varepsilon_n(x)$ mohou nabývat libovolnou přirozenou hodnotu, $\varepsilon_n(x) \in \mathbb{N}$;
- je-li $T \in \mathbb{N}$, $2 < T < +\infty$, pak pro $n \geq 1$ je $\varepsilon_n(x) \in \{1, 2, 3, \cdots, T-1\}$;
- pokud $T \notin \mathbb{Z}$, $2 < T < +\infty$, pak $\varepsilon_n(x)$, $n \geq 1$, nabývá pouze hodnot $\varepsilon_n(x) \in \{1, 2, 3, \cdots, \lfloor T \rfloor\}$.

Nechť $f : [0, +\infty) \to [0,1]$ je rostoucí: Předpokládejme, že f navíc splňuje

- $f(0) = 0$;
- $f(t)$ je spojitá, ostře rostoucí funkce na $[0,T]$, a $f(t) = 1$ pro $t \geq T$, kde $1 < T \leq +\infty$;
- $|f(t_2) - f(t_1)| < |t_2 - t_1|$ pro $0 \leq t_1 < t_2$.

Označíme-li $\varphi : [0,1] \to [0,T]$ inverzní k f, pak f-rozvoj (5.1) existuje ke každému reálnému číslu x. Parametr T opět rozhoduje o tom, jakých hodnot mohou nabývat cifry f-rozvoje.

- Je-li $T = +\infty$, pak $\varepsilon_n(x)$ mohou nabývat libovolného nezáporného celého čísla, $\varepsilon_n(x) \in \mathbb{N}$;
- je-li $T \in \mathbb{N}$, $1 < T < +\infty$, pak $\varepsilon_n(x) \in \{0, 1, 2, 3, \cdots, T-1\}$ pro $n \geq 1$;
- je-li $T \notin \mathbb{Z}$, $1 < T < +\infty$, pak $\varepsilon_n(x) \in \{0, 1, 2, 3, \cdots, [T]\}$ pro $n \geq 1$.

Obecný obecný rámec f-rozvojů zahrnuje známé reprezentace reálných čísel pomocí řetězových zlomků, obvyklé soustavy se základem $q \in \mathbb{Z}$, $q \geq 2$, ale i méně známé způsoby zápisu čísel. To si předvedeme na několika příkladech.

Příklad 5.1. Reprezentace reálného z ve tvaru řetězového zlomku lze získat pomocí Rényiho algoritmu, pokud za f zvolíme klesající funkci

$$f(x) = \frac{1}{x}\,, \qquad \text{pro } x \geq 1\,.$$

Každé reálné číslo z má reprezentaci ve tvaru

$$z = \varepsilon_0 + \cfrac{1}{\varepsilon_1 + \cfrac{1}{\varepsilon_2 + \cfrac{1}{\varepsilon_3 + \cdots}}}\,.$$

Protože inverzní funkce je $\varphi(y) = \frac{1}{y}$, cifry ε_n, $n \in \mathbb{N}_0$, lze získat

$$\begin{array}{rclcrcl} \varepsilon_0 &=& \lfloor z \rfloor\,, & & r_0 &=& \{z\}\,, \\ \varepsilon_1 &=& \lfloor \varphi(r_0) \rfloor = \lfloor \frac{1}{\{z\}} \rfloor\,, & & r_1 &=& \left\{ \frac{1}{\{z\}} \right\}\,, \\ & \vdots & & & & \vdots & \end{array}$$

což je odpovídá klasickému algoritmu pro výpočet koeficientů řetězového zlomku čísla z. Není složité ověřit, že funkce $f(x) = \frac{1}{x}$ splňuje postačující podmínky (pro případ klesající funkce), parametr $T = +\infty$, a proto cifry ε_n, $n \in \mathbb{N}$, nabývají hodnot libovolného přirozeného čísla.

Příklad 5.2. Uvažujme funkci $f(x) = \sqrt[m]{1+x} - 1$ pro $0 \le x \le 2^m - 1$, $m \in \mathbb{N}$, $m \ge 2$. Podmínky pro rostoucí funkci jsou splněny s parametrem $T = 2^m - 1$, takže každé reálné číslo x lze vyjádřit ve tvaru

$$x = \varepsilon_0 - 1 + \sqrt[m]{\varepsilon_1 + \sqrt[m]{\varepsilon_2 + \sqrt[m]{\varepsilon_3 + \cdots}}}$$

a cifry ε_n získané předpisem

$$\begin{array}{rclcrcl} \varepsilon_0 &=& \lfloor z \rfloor\,, & & r_0 &=& \{z\}\,, \\ \varepsilon_1 &=& \lfloor \varphi(r_0) \rfloor = \lfloor (1+r_0)^m - 1 \rfloor\,, & & r_1 &=& \{(1+r_0)^m - 1\}\,, \\ & \vdots & & & & \vdots & \end{array}$$

nabývají hodnot v množině $\{0, 1, \ldots, 2^m - 2\}$. Tyto rozvoje (pro $m = 2$) použil už v roce 1832 W. Bolyai k aproximaci kořenů některých rovnic [5].

Příklad 5.3. Nechť q je celé číslo $q \ge 2$. Položme

$$f(x) = \begin{cases} \dfrac{x}{q}\,, & \text{pro } 0 \le x \le q\,, \\ \\ 1\,, & \text{for } q < x\,. \end{cases} \tag{5.2}$$

Každé reálné z má reprezentaci tvaru

$$z = \varepsilon_0 + \frac{\varepsilon_1}{q} + \frac{\varepsilon_2}{q^2} + \frac{\varepsilon_3}{q^3} + \cdots\,, \tag{5.3}$$

kde cifry ε_n, $n \in \mathbb{N}_0$, jsou získány s pomocí inverzní funkce $\varphi(y) = qy$ předpisem

$$\begin{array}{rclcrcl} \varepsilon_0 &=& \lfloor z \rfloor\,, & & r_0 &=& \{z\}\,, \\ \varepsilon_1 &=& \lfloor q\{z\} \rfloor\,, & & r_1 &=& \big\{q\{z\}\big\}\,. \\ & \vdots & & & & \vdots & \end{array}$$

V tomto postupu může čtenář rozeznat hladový algoritmus pro rozvoj v soustavě se základem q. Funkce f splňuje podmínky pro rostoucí funkce s parametrem $T = q < +\infty$. Cifry nabývají hodnot $\varepsilon_n \in \{0, 1, 2, \ldots, q-1\}$.

Všimněme si, že vyjádření čísla z pro $0 \leq z < q$ ve tvaru (5.3) odpovídá klasickému zápisu čísla z v soustavě s celočíselným základem q. Pokud bychom chtěli získat q-ární rozvoj pro libovolné nezáporné z, musí se Rényiův algoritmus lehce modifikovat.

5.2 β-rozvoje

Příklady v předchozí kapitole ilustrovaly Rényiho konstrukci f-rozvojů pro funkce f, v nichž parametr T byl buď nekonečný nebo celočíselný. Podle Rényiho výsledku v těchto případech (tj. když T není neceločíselné reálné číslo) každá konečná posloupnost přípustných cifer $\varepsilon_0, \varepsilon_1, \varepsilon_2, \cdots$ odpovídá f-rozvoji nějakého reálného čísla x. Pokud ale $T < +\infty$ a zároveň $T \notin \mathbb{Z}$, pak toto není pravda. Tento jev můžeme pozorovat u tzv. β-rozvojů, které získáme Rényiho algoritmem při použití funkce f z příkladu 5.3, kde celočíselné q nahradíme libovolným reálným $\beta > 1$. Obvykle u β-rozvojů používáme algoritmus modifikovaný, tak aby se pro $\beta \in \mathbb{N}$ shodoval s klasickými soustavami v celočíselné bázi.

Pro každou reálnou bázi $\beta > 1$ najdeme reprezentaci každého kladného reálného čísla $x > 0$ v bázi β s nezápornými celými ciframi, tedy ve tvaru

$$x = \sum_{i=-\infty}^{k} x_i \beta^i, \quad x_i \in \mathbb{N}_0. \tag{5.4}$$

Takovou reprezentaci pak zapíšeme posloupností cifer, přičemž oddělujeme cifry u nezáporných mocnin zlomkovou tečkou,

$$x = x_k x_{k-1} \cdots x_1 x_0 \cdot x_{-1} x_{-2} \cdots$$

Narozdíl od Rényiova vyjádření používáme obvyklejší indexování tak, aby indexy klesaly s klesající mocninou základu β.

Reprezentaci čísla x ve tvaru (5.4) lze najít například hladovým algoritmem:

Najdi $k \in \mathbb{N}_0$ tak, že $\beta^k \leq x < \beta^{k+1}$; polož $i = k$.

Dokud $x > 0$, prováděj: $x_i := \lfloor \frac{x}{\beta^i} \rfloor$; $x := x - x_i \beta^i$; $i := i - 1$.

Je zřejmé, že cifry x_i nabývají hodnot v množině $\{0, 1, \ldots, \lceil \beta \rceil - 1\}$ pro $i \leq k$, přičemž $x_k \geq 1$, a navíc vzniklá posloupnost cifer splňuje (5.4).

Příklad 5.4. Rozvineme číslo 2 v bázi $\tau = \frac{1}{2}(1+\sqrt{5}) \approx 1.618$, což je kořen polynomu $x^2 - x - 1$. Platí $\tau^1 < 2 < \tau^2 = \tau + 1$, takže $k = 1$, $x_1 = \lfloor 2/\tau \rfloor = 1$. V dalším kroku $x := 2 - \tau \approx 0.382$.

Proto

$$x_0 = \left\lfloor \frac{x}{\tau^0} \right\rfloor = 0, \quad x := 2 - \tau \approx 0.382$$
$$x_{-1} = \left\lfloor \frac{x}{\tau^{-1}} \right\rfloor = 0 \quad x := 2 - \tau \approx 0.382$$

Nyní porovnáváme $x = 2 - \tau$ s τ^{-2}. Máme

$$2 - \tau = 2 - (1 + \frac{1}{\tau}) = 1 - \frac{1}{\tau} = \frac{1}{\tau^2},$$

což znamená $x_{-2} = \lfloor x/\tau^{-2} \rfloor = 1$ a nově $x := 0$. Celkově $2 = 1 \cdot \tau + 1 \cdot \tau^{-2} = 10 \cdot 01$.

Často je vhodné na číselnou soustavu nahlížet jako na dynamický systém, tedy prostor vybavený transformací. V našem případě to bude tzv. β-transformace na intervalu $[0, 1)$.

Definice 5.5. Nechť $\beta > 1$, definujeme tzv. β-transformaci $T_\beta : [0, 1) \to [0, 1)$ na intervalu $[0, 1)$ předpisem

$$T_\beta(x) = \beta x - \lfloor \beta x \rfloor.$$

Položme

$$d_\beta(x) := x_1 x_2 x_3 \cdots, \qquad x_i = \lfloor \beta T_\beta^{i-1}(x) \rfloor. \tag{5.5}$$

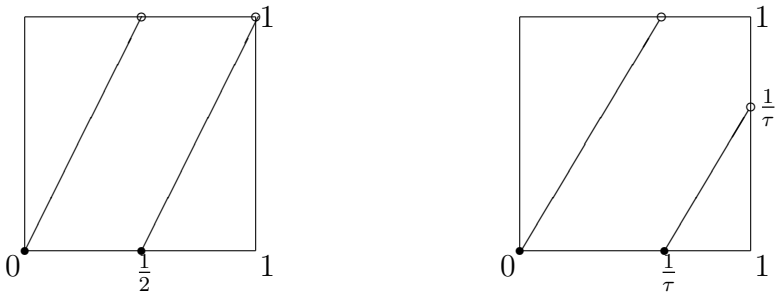
Snadno ověříme, že posloupnost $d_\beta(x) := x_1 x_2 x_3 \cdots$ opravdu reprezentuje číslo x. Splňuje totiž

$$x = \frac{x_1}{\beta} + \frac{x_2}{\beta^2} + \frac{x_3}{\beta^3} + \cdots$$

Navíc pro iterace čísla x platí, že

$$d_\beta(T^j(x)) = x_{j+1} x_{j+2} x_{j+3} \cdots .$$

Příklad 5.6. Graf transformace T_β pro $\beta = 2$ (vlevo) a pro $\beta = \frac{1}{2}(1 + \sqrt{5})$ (vpravo).



Uvažujme nejprve $\beta = 2$. Padne-li $(i-1)$. iterace bodu x do intervalu $[0, 1/2)$, je i. cifra v rozvoji x rovna $x_i = 0$. Je-li $T^{i-1}(x)$ v intervalu $[1/2, 1)$, pak $x_i = 1$. Protože $T\big([0, 1/2)\big) = [0, 1)$, může v rozvoji za cifrou 0 následovat cifra 0 i 1. Stejně tak platí $T\big([1/2, 1)\big) = [0, 1)$, takže i za cifrou 1 mohou následovat 0 i 1.

Nyní položme $\beta = \tau$. Zde platí, že $T^{i-1}(x) \in [0, 1/\tau)$, implikuje $x_i = 0$ a je-li $T^{i-1}(x) \in [1/\tau, 1)$, pak $x_i = 1$. Máme $T\big([0, 1/\tau)\big) = [0, 1)$, takže za cifrou 0 může následovat cifra 0 i 1. Ale $T\big([1/\tau, 1)\big) = [0, 1/\tau)$, takže za cifrou 1 nutně následuje cifra 0.

Je tedy vidět, že obecně ne každá posloupnost vhodných cifer je rozvojem nějakého čísla. Přípustné posloupnosti budou popsány dále v této kapitole.

Tvrzení 5.7. *Nechť $x \in [0, 1)$. Pak $d_\beta(x)$ je lexikograficky největší řetězec nezáporných celých čísel, který reprezentuje x. Přesněji, pokud $d_\beta(x) = x_1x_2x_3\cdots$ a pro $y_1y_2y_3\cdots \in \mathbb{N}_0^{\mathbb{N}}$ platí*

$$x = \sum_{i=1}^{\infty} \frac{x_i}{\beta^i} = \sum_{i=1}^{\infty} \frac{y_i}{\beta^i}, \tag{5.6}$$

pak $y_i = x_i$ pro všechna $i \geq 1$ nebo $y_j < x_j$, kde j je nejmenší z indexů $i \geq 1$, pro který $x_i \neq y_i$.

Důkaz. Nechť řetězec $\mathbf{y} = y_1y_2y_3\cdots$ reprezentuje číslo $x \in [0, 1)$, tj. platí (5.6), a přitom $\mathbf{y} \succ \mathbf{d}_\beta(x)$. Označme j minimální index takový, že $y_j > x_j$. Pak

$$y_j + \frac{y_{j+1}}{\beta} + \frac{y_{j+2}}{\beta^2} + \cdots = x_j + \frac{x_{j+1}}{\beta} + \frac{x_{j+2}}{\beta^2} + \cdots$$

Odtud

$$1 \leq y_j - x_j = \underbrace{\Big(\frac{x_{j+1}}{\beta} + \frac{x_{j+2}}{\beta^2} + \cdots\Big)}_{=T_\beta^j(x)\in[0,1)} - \underbrace{\Big(\frac{y_{j+1}}{\beta} + \frac{y_{j+2}}{\beta^2} + \cdots\Big)}_{\geq 0} < 1$$

což je spor. □

Tvrzení 5.8. *Nechť $x, y \in [0, 1)$. Pak $d_\beta(x) \prec d_\beta(y)$, právě když $x < y$.*

Důkaz. Předpokládejme, že $d_\beta(x) = x_1x_2x_3\cdots \prec d_\beta(y) = y_1y_2y_3\cdots$, tzn. existuje $j \geq 1$ tak, že $x_i = y_i$ pro $i = 1, \ldots, j-1$ a $x_j < y_j$. Bez újmy na obecnosti lze uvažovat $j = 1$. Máme

$$x_1 = \lfloor \beta x \rfloor < \lfloor \beta y \rfloor = y_1,$$

a tedy nutně $x < y$.

Naopak nechť $x = \sum_{i=1}^{\infty} \frac{x_i}{\beta^i} < \sum_{i=1}^{\infty} \frac{y_i}{\beta^i} = y$. Označme j index ≥ 1 takový, že $x_i = y_i$ pro $i = 1, \ldots, j-1$ a $x_j \neq y_j$. Pak

$$x_j + \underbrace{\frac{x_{j+1}}{\beta} + \frac{x_{j+2}}{\beta^2} + \cdots}_{=T_\beta^j(x)\in[0,1)} < y_j + \underbrace{\frac{y_{j+1}}{\beta} + \frac{y_{j+2}}{\beta^2} + \cdots}_{=T_\beta^j(y)\in[0,1)}.$$

Odtud $x_j < y_j + 1$, což dále díky celočíselnosti cifer znamená $x_j \leq y_j$. Ale z předpokladu $x_j \neq y_j$, takže $x_j < y_j$, což jsme měli dokázat. □

Dusledek 5.9. *Zobrazení* $d_\beta : [0,1) \to \mathbb{N}_0^{\mathbb{N}}$ *je ostře rostoucí vůči lexikografickému uspořádání. Proto existuje limita*

$$d_\beta^*(1) := \lim_{\varepsilon \to 1-} d_\beta(1-\varepsilon)$$

a pro každé $x \in [0,1)$ *platí* $d_\beta(x) \prec d_\beta^*(1)$.

Poznamenejme, že limitu v předchozím tvrzení definujeme pomocí metriky na prostoru nekonečných posloupností nad konečnou abecedou. Pro dvě posloupnosti $u = u_1u_2u_3\cdots$, $v = v_1v_2v_3\cdots$ definujeme

$$\varrho(u,v) = \begin{cases} 2^{-\min\{j : u_j \neq v_j\}} \text{ pro } u \neq v, \\ 0 \text{ pro } u = v. \end{cases}$$

Dvě nekonečná slova jsou si tedy tím bližší, čím mají delší společný prefix.

Řetězec $d_\beta^*(1)$ využijeme pro zjištění, která posloupnost cifer je rozvojem nějakého čísla x z intervalu $[0,1)$.

Definice 5.10. Nechť $\beta > 1$. Řekneme, že řetězec cifer $x_1x_2x_3\cdots \in \mathbb{N}_0^{\mathbb{N}}$ je přípustný, jestliže existuje $x \in [0,1)$ tak, že $d_\beta(x) = x_1x_2x_3\cdots$.

Věta 5.11 ([23])**.** *Nechť* $\beta > 1$. *Řetězec cifer* $x_1x_2x_3\cdots \in \mathbb{N}_0^{\mathbb{N}}$ *je přípustný, právě když každý jeho sufix* $x_ix_{i+1}x_{i+2}\cdots$ *je lexikograficky ostře menší než* $d_\beta^*(1)$.

Aby Parryho věta byla prakticky použitelná, musíme umět zjistit tvar řetězce $d_\beta^*(1)$.

Definice 5.12. Nechť $\beta > 1$. Definujeme tzv. Rényiův rozvoj jedničky $d_\beta(1) = t_1t_2t_3\cdots$ předpisem

$$t_1 = \lfloor \beta \rfloor, \quad t_2t_3t_4\cdots = d_\beta\big(\beta - \lfloor \beta \rfloor\big).$$

Tvrzení 5.13. *Nechť* $\beta > 1$. *Pak*

$$d_\beta^*(1) = \begin{cases} (t_1\cdots t_{m-1}(t_m-1))^\omega, & \textit{pokud } d_\beta(1) = t_1t_2\cdots t_m0^\omega, \textit{ kde } t_m \neq 0, \\ d_\beta(1), & \textit{pokud } d_\beta(1) \textit{ obsahuje nekonečně mnoho nenulových cifer.} \end{cases}$$

Příklad 5.14. Zjistíme Rényiův rozvoj jedničky pro bázi $\beta = q \in \mathbb{N}$. Máme

$$t_1 = \lfloor q \rfloor = q, \quad d_q(q-q) = d_q(0) = 0^\omega \quad \Rightarrow \quad d_q(1) = q0^\omega.$$

Podle předchozího tvrzení je $d_q^*(1) = (q-1)^\omega$. Parryho podmínka nám potom říká, že přípustné jako rozvoje v bázi q jsou řetězce cifer, v nichž každý sufix je lexikograficky ostře menší než $d_q^*(1) = (q-1)^\omega$. Každý řetězec $x_1x_2x_3\cdots$ s ciframi $x_i \in \{0,1,\ldots,q-1\}$ je tedy přípustný, pokud nekončí na sufix $(q-1)^\omega$. Speciálně každý konečný řetězec (se sufixem 0^ω) je přípustný.

Příklad 5.15. Zjistíme Rényiův rozvoj jedničky pro bázi $\tau = \frac{1}{2}(1+\sqrt{5})$. Máme

$$t_1 = \lfloor \tau \rfloor = 1, \quad d_\tau(\tau - 1) = d_\tau\big(\tfrac{1}{\tau}\big)\big) = 10^\omega \quad \Rightarrow \quad d_\tau(1) = 110^\omega.$$

Odtud odvodíme $d^*_\tau(1) = (10)^\omega$. Podle Parryho podmínky zjistíme, které řetězce cifer jsou přípustné jako rozvoje v bázi τ. Jsou to posloupnosti, v nichž každý sufix je lexikograficky ostře menší než $d^*_\tau(1) = (10)^\omega$. Takový řetězec $x_1x_2x_3\cdots$ tedy musí mít cifry $x_i \in \{0,1\}$, nesmí obsahovat faktor 11 a nesmí končit na sufix $(10)^\omega$.

Příklad 5.16. Zjistíme Rényiův rozvoj jedničky pro bázi $\beta = \tau^2 = \frac{1}{2}(3+\sqrt{5})$, což je kořen polynomu $x^2 - 3x + 1$. Máme $t_1 = \lfloor \beta \rfloor = 2$, potom $\beta - 2 = 1 - \beta^{-1}$. Zjistíme, že $d_\beta(\beta - 2) = 1^\omega$. Odtud $d_\beta(1) = 21^\omega$. Protože Rényiův rozvoj jedničky je nekonečný, platí $d^*_\beta(1) = d_\beta(1) = 21^\omega$. Přípustné posloupnosti jsou tedy nad abecedou $\{0,1,2\}$ a neobsahují žádný z faktorů 21^j2, $j \geq 0$, ani 21^ω.

5.3 Parryho čísla

Z věty 5.11 lze soudit, že důležitou roli v číselných soustavách hrají ty základy, jejichž Rényiův rozvoj jedničky je pravidelný.

Definice 5.17. Řekneme, že číslo $\beta > 1$ je Parryho číslo, pokud jeho Rényiho rozvoj jedničky $d_\beta(1)$ je posloupnost posléze periodická. Jestliže je dokonce konečná (tedy posléze periodická s periodou 0^ω), pak β nazýváme jednoduché Parryho číslo.

Napříště budeme uvažovat Rényiho rozvoj jedničky v následujícím tvaru:

$$d_\beta(1) = \begin{cases} t_1t_2\cdots t_m, \\ t_1\cdots t_m(t_{m+1}\cdots t_{m+p})^\omega, \end{cases} \tag{5.7}$$

přičemž předpokládáme, že $m, p \in \mathbb{N}$ jsou minimální, aby $d_\beta(1)$ šlo zapsat v tomto tvaru.

Význam Parryho čísel spočívá v tom, že přípustné řetězce lze popsat pomocí množiny zakázaných faktorů, která je dokonce konečná, pokud je báze jednoduché Parryho číslo. Jazyk reprezentací reálných čísel lze pak rozpoznávat pomocí konečného automatu.

Postupně budeme zkoumat algebraické vlastnosti Parryho čísel.

Tvrzení 5.18. *Nechť β je Parryho číslo. Potom β je algebraické celé číslo.*

Důkaz. Nechť β je jednoduché Parryho číslo, tedy $d_\beta(1) = t_1t_2\cdots t_m$. To znamená, že

$$1 = \frac{t_1}{\beta} + \frac{t_2}{\beta^2} + \cdots + \frac{t_m}{\beta^m}.$$

Číslo β je tedy kořenem polynomu

$$P(x) = x^m - t_1 x^{m-1} - \cdots - t_{m-1}x - t_m\,. \tag{5.8}$$

Polynom P je monický s celočíselnými koeficienty, β je proto algebraické celé číslo.

Nechť je nyní β nejednoduché Parryho číslo, tedy $d_\beta(1) = t_1 t_2 \cdots t_m (t_{m+1} \cdots t_{m+p})^\omega$. To znamená, že

$$\begin{aligned} 1 &= \frac{t_1}{\beta} + \cdots + \frac{t_m}{\beta^m} + \frac{t_{m+1}\beta^{p-1} + t_{m+2}\beta^{p-1} + \cdots + t_{m+p}}{\beta^{m+p}}\Big(1 + \frac{1}{\beta^p} + \frac{1}{\beta^{2p}} + \cdots\Big) = \\ &= \frac{t_1}{\beta} + \cdots + \frac{t_m}{\beta^m} + \frac{t_{m+1}\beta^{p-1} + t_{m+2}\beta^{p-1} + \cdots + t_{m+p}}{\beta^m\big(\beta^p - 1\big)}. \end{aligned}$$

Po úpravě zjistíme, že číslo β je kořenem polynomu

$$P(x) = x^{m+p} - t_1 x^{m+p-1} - \cdots - t_{m+p-1}x - t_{m+p} - \big(x^m - t_1 x^{m-1} - \cdots - t_{m-1}x - t_m\big)\,. \tag{5.9}$$

Opět vidíme, že polynom P je monický s celočíselnými koeficienty a nejednoduché Parryho číslo je také algebraické celé číslo. □

Definice 5.19. Nechť $\beta > 1$ je Parryho číslo ve tvaru (5.7). Polynom (5.8), respektive (5.9) se nazývá Parryho polynom čísla β.

Poznamenejme, že Parryho polynom nemusí být nutně ireducibilní nad $\mathbb{Q}$. Příkladem je Parryho polynom čísla $\beta \approx 2.1479$ s minimálním polynomem $x^3 - x^2 - 2x - 1$. Rényiův rozvoj jedničky je v tomto případě $d_\beta(1) = 20011$, Parryho polynom je roven

$$P(x) = x^5 - 2x^4 - x - 1 = (x^3 - x^2 - 2x - 1)(x^2 - x + 1).$$

Pro uvedení dalšího tvrzení budeme potřebovat známou Perronovu-Frobeniovu větu pro nezáporné nerozložitelné matice. S jejím důkazem se čtenář mohl seznámit v kurzu Teorie matic, jinak odkazujeme na [10].

Věta 5.20. *Nechť $M \in \mathbb{R}^{n\times n}$ je nezáporná nerozložitelná matice se spektrálním poloměrem $\rho(M) = \lambda$. Potom platí*

1. *Číslo λ je kladné a je vlastním číslem matice M.*
2. *Vlastní podprostor matice M příslušný k vlastnímu číslu λ je jednodimenzionální.*
3. *Vlastní vektor matice M příslušný k vlastnímu číslu λ lze volit kladný.*
4. *Žádné vlastní číslo matice M kromě λ nemá kladný vlastní vektor.*

Poznamenejme, že mluvíme o nezáporné matici, jestliže všechny její složky jsou nezáporné, podobně je matice kladná, jsou-li všechny její složky kladné. Čtvercová matice je nerozložitelná, pokud ji nelze simultánními permutacemi řádků a sloupců převést na blokově horní trojuhelníkový tvar. Ekvivalentně lze uvést popis nerozložitelných matic pomocí grafů. K nezáporné matici M uvažujme matici A, která má stejný rozměr jako M, přičemž $A_{ij} = 0$, když $M_{ij} = 0$ a $A_{ij} = 1$ jinak. Taková matice je adjacenční matice orientovan0ho grafu na n vrcholech $\{1, 2, \ldots, n\}$, ve kterém vede hrana z vrcholu i do vrcholu j, právě když $A_{ij} = 1$. Lze ukázat, že matice M je nerozložitelná tehdy a jen tehdy, když graf s příslušnou adjacenční maticí je silně souvislý, totiž pro každé dva vrcholy i, j v něm existuje cesta z vrcholu i do vrcholu j.

Tvrzení 5.21. *Nechť β je Parryho číslo. Pak β je dominantním kořenem svého Parryho polynomu.*

Důkaz. V případě jednoduchého Parryho čísla je Parryho polynom (5.8) charakteristickým polynomem své matice společnice

$$M_P = \begin{pmatrix} 0 & 1 & \ldots & 0 & 0 \\ 0 & 0 & \ddots & & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ t_m & t_{m-1} & \cdots & t_2 & t_1 \end{pmatrix}$$

Protože $t_m \neq 0$, je tato matice je nezáporná a nerozložitelná. Tento fakt se snadno ověří zakreslením grafu příslušné adjacenční matice. Číslo β je jejím vlastním číslem ke kladnému vlastnímu vektoru $(1, \beta, \beta^2, \ldots, \beta^{m-1})$. Podle Perronovy-Frobeniovy věty je β ostře větší než absolutní hodnoty všech ostatních vlastních čísel.

V případě nejednoduchého Parryho čísla nelze ke stejnému argumentu použít matici společnici Parryho polynomu (5.9), protože ta nemá nezáporné koeficienty. Parryho polynom je ale charakteristickým polynomem jiné matice, a to

$$\begin{pmatrix} 0 & 1 & \ldots & 0 & 0 \\ 0 & 0 & \ddots & & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ t_{m+p} & t_{m+p-1} & \cdots & t_2 & t_1 \end{pmatrix} + N,$$

kde $N_{p(p+1)} = 1$ a $N_{ij} = 0$ jinak. Lze opět ukázat, že rovněž tato matice je nezáporná a nerozložitelná a β je jejím dominantním vlastním číslem. □

Dusledek 5.22. *Parryho čísla patří mezi tzv. Perronova čísla, tj. algebraická celá čísla $\beta > 1$, jejichž sdružené kořeny jsou v absolutní hodnotě ostře menší než β.*

Ukázali jsme, že kořeny Parryho polynomu čísla β jsou v absolutní hodnotě ostře menší než β. Lze ale ukázat daleko přesnější odhad.

Tvrzení 5.23. *Nechť β je Parryho číslo. Pak ostatní kořeny Parryho polynomu čísla β jsou v absolutní hodnotě menší než 2.*

Důkaz. Rozebereme případ jednoduchého Parryho čísla, jehož Parryho polynom je tvaru $P(x) = x^m - t_1x^{m-1} - \cdots - t_{m-1}x - t_m$. Do tohoto polynomu dosadíme za koeficienty t_i jejich vyjádření pomocí iterací transformace T_β. Máme totiž $T_\beta^j(1) = \beta T_\beta^{j-1}(1) - t_j$. Pro přehlednost použijeme zkrácené značení $T_\beta^j(1) = T^j$. Po dosazení vidíme

$$P(x) = x^m - (\beta - T^1)x^{m-1} - (\beta T^1 - T^2)x^{m-2} - \cdots - (\beta T^{m-2} - T^{m-1})x - (\beta T^{m-1} - T^m).$$

Když si uvědomíme, že $T^m = T_\beta^m(1) = 0$, což plyne z faktu, že poslední nenulový koeficient v $d_\beta(1)$ je t_m, lze z polynomu P vytknout faktor $(x - \beta)$ takto

$$P(x) = (x - \beta)\underbrace{(x^{m-1} + T^1x^{m-2} + \cdots + T^{m-2}x + T^{m-1})}_{Q(x)}.$$

Polynom $Q(x)$ má tedy kromě vedoucího koeficientu všechny koeficienty v intervalu $[0, 1)$. Navíc každý kořen γ polynomu P, $\gamma \neq \beta$, je kořenem polynomu Q. Využijeme $Q(\gamma) = 0$, tedy

$$\gamma^{m-1} = -(T^1\gamma^{m-2} + \cdots + T^{m-2}\gamma + T^{m-1}).$$

Pomocí trojúhelníkové nerovnosti získáme odhad

$$|\gamma|^{m-1} = \Big|\sum_{j=0}^{m-2} T^{m-1-j}\gamma^j\Big| < \sum_{j=0}^{m-2} |\gamma|^j = \frac{|\gamma|^{m-1} - 1}{|\gamma| - 1}.$$

Po zkrácení vyjde požadovaná nerovnost $|\gamma| < 2$.

V případě nejednoduchého Parryho čísla s Parryho polynomem $P(x) = x^{m+p} - t_1x^{m+p-1} - \cdots + t_{m+p-1}x - t_{m+p} - \big(x^m - t_1x^{m-1} - \cdots - t_{m-1}x - t_m\big)$ postupujeme obdobně. Nejdříve dosazením za koeficienty $t_j = T^j - \beta T^{j-1}$ a využitím periodicity (tj. $T^{m+p} = T^m$) odvodíme

$$P(x) = (x - \beta)\underbrace{(x^{m+p-1} + T^1x^{m+p-2} + \cdots + T^{m+p-1} - (x^{p-1} + T^1x^{p-2} + \cdots + T^{p-1})}_{Q(x)}.$$

Po dosazení kořene $\gamma \neq \beta$ do polynomu $Q(x)$ máme $Q(\gamma) = 0$, tedy po úpravě

$$\gamma^{m+p-1} - \gamma^{p-1} + T^1(\gamma^{m+p-2} - \gamma^{p-2}) + \cdots + T^{p-1}(\gamma^m - 1) + T^p\gamma^{m-1} + \cdots + T^{m+p-2}\gamma + T^{m+p-1}.$$

Proto

$$(\gamma^{m-1} - 1)(\gamma^{p-1} + T^1\gamma^{p-2} + \cdots + T^{p-1}) = -T^p\gamma^{m-1} - \cdots - T^{m+p-2}\gamma - T^{m+p-1}.$$

Pro $|\gamma| > 1$ platí $|\gamma^m - 1| \geq |\gamma|^m - 1$, a tedy pomocí trojúhelníkové nerovnosti získáme odhad

$$(|\gamma|^{m-1} - 1)|\gamma^{p-1} + T^1\gamma^{p-2} + \cdots + T^{p-1}| = \Big|\sum_{j=0}^{m-1} T^{m+p-1-j}\gamma^j\Big| < \sum_{i=0}^{m-2} |\gamma|^j = \frac{|\gamma|^{m-1} - 1}{|\gamma| - 1}.$$

Po zkrácení vyjde nerovnost

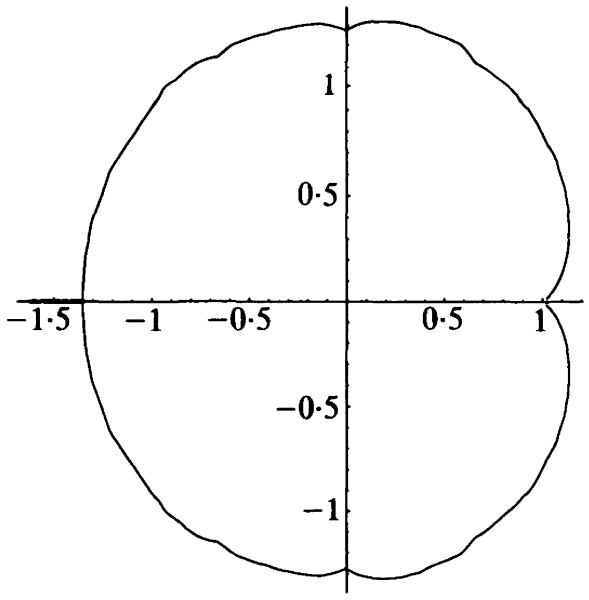
$$|\gamma^{p-1} + T^1\gamma^{p-2} + \cdots + T^{p-1}| < \frac{1}{|\gamma| - 1}.$$

Opět využijeme, že absolutní hodnota rozdílu je větší než rozdíl absolutních hodnot, takže

$$|\gamma^{p-1}| < \frac{1}{|\gamma| - 1} + |\gamma^{p-1} + T^1\gamma^{p-2} + \cdots + T^{p-1}| < \frac{1}{|\gamma| - 1} + \frac{|\gamma^{p-1}| - 1}{|\gamma| - 1} = \frac{|\gamma^{p-1}|}{|\gamma| - 1},$$

což opět vede na nerovnost $|\gamma| < 2$. □

Přesnější popis oblasti komplexní roviny, ve které leží sdružené kořeny Parryho čísel podal Solomyak [28], viz obrázek 5.1.



Obrázek 5.1: Oblast, ve které se nacházejí sdružené kořeny Parryho čísel

5.4 Pisotova čísla, Salemova čísla

Mezi Parryho čísly jsou významné dvě třídy, a to tzv. Pisotova a Salemova čísla.

Definice 5.24. Algebraické celé číslo $\beta > 1$ se nazývá Pisotovo, pokud všechna čísla s ním algebraicky sdružená leží uvnitř jednotkového kruhu, tj. jsou v absolutní hodnotě ostře menší než 1. Algebraické celé číslo $\beta > 1$ se nazývá Salemovo, pokud všechna čísla s ním algebraicky sdružená leží v jednotkovém kruhu a alespoň jedno z nich leží na jednotkové kružnici.

Příklad 5.25. Mezi Pisotova čísla patří triviálně všechna přirozená čísla ≥ 2. Nejjednodušším netriviálním příkladem je již zmíněný zlatý řez $\tau = \frac{1}{2}(1+\sqrt{5})$ s minimálním polynomem x^2-x-1. Algebraicky sdruženým číslem je $\tau' = \frac{1}{2}(1-\sqrt{5}) = 1-\tau \approx -0.618$.

Popišme všechna kvadratická Pisotova čísla.

Tvrzení 5.26. *Kvadratická Pisotova čísla jsou právě dominantní kořeny polynomů*

$$x^2 - ax - b, \quad a \geq b \geq 1, \qquad x^2 - ax + b, \quad a \geq b+2 \geq 3.$$

Důkaz. Polynom $f(x) = x^2 - ax - b$ má vhodně rozložené kořeny $\beta > 1$ a $\beta' \in (-1, 1)$, právě když má hodnoty

$$f(1) = 1 - a - b < 0, \quad f(-1) = 1 + a - b > 0.$$

Protože a, b jsou celá čísla, lze požadavek na koeficienty zapsat $a \geq \max\{b, -b+2\}$. Případ $b = 0$ odpovídá reducibilnímu polynomu $f(x) = x^2 - ax = x(x-a)$, jehož kořenem jsou racionální Pisotova čísla. Pro $b \geq 1$, vychází $a \geq b$. Pro $b \leq -1$ pak $a \geq 2 - b$. □

Popis Pisotových čísel stupně 3 a 4 lze najít v [1]. Popsat obecně minimální polynomy Pisotových čísel libovolného stupně není jednoduché. Existují ale postačující podmínky na koeficienty polynomu, aby byl minimálním polynomem Pisotova čísla.

Tvrzení 5.27 ([11],[17])**.** *Nechť $f(x) = x^d - a_1x^{d-1} - a_2x^{d-2} - \cdots - a_{d-1}x - a_d \in \mathbb{Z}[x]$. Jestliže koeficienty splňují $a_1 \geq a_2 \geq \cdots \geq a_d$ nebo $a_1 > \sum_{i=2}^{d} a_i$, pak f je minimálním polynomem Pisotova čísla.*

Podívejme se na algebraické vlastnosti Salemových čísel.

Tvrzení 5.28. *Nechť β je Salemovo číslo a $f \in \mathbb{Z}[x]$ je jeho minimální polynom. Pak f je sudého stupně a má právě dva reálné kořeny β, β^{-1}. Všechny ostatní kořeny f leží na jednotkové kružnici.*

Důkaz. Nechť $f(x) = x^d + \sum_{i=1}^{d-1} c_i x^i + c_0$, $c_i \in \mathbb{Z}$, je minimální polynom Salemova čísla β. Označme α sdružený kořen k β, který leží na jednotkové kružnici. Polynom f je reálný, a proto s kořenem α má i kořen $\overline{\alpha}$. Přitom $|\alpha|^2 = \alpha\overline{\alpha} = 1$, a proto $\alpha^{-1} = \overline{\alpha}$.

Jestliže α má minimální polynom f, pak α^{-1} má minimální polynom reciproký k f, tj.

$$g(x) = x^d + \sum_{i=1}^{d-1} c_{d-i} c_0^{-1} x^i + c_0^{-1}.$$

Protože minimální polynom algebraického čísla je určen jednoznačně, platí $f = g$, takže polynom f je reciproký a s každým kořenem γ má i kořen γ^{-1}. Proto je stupeň f sudý. Protože jediný kořen polynomu f vně jednotkové kružnice je β, je jediný kořen uvnitř jednotkové kružnice β^{-1}. Ostatní kořeny f leží na jednotkové kružnici. □

Příklad 5.29. Z tvrzení 5.28 je zřejmé, že Salemova čísla jsou algebraické jednotky nejméně čtvrtého stupně.

Pro ilustraci předvedeme, jak nalézt minimální polynomy všech Salemových čísel stupně 4, viz např. [6]. Jejich minimální polynom je reciproký, tedy tvaru $f(x) = x^4 - ax^3 + bx^2 - ax + 1$. Tento polynom má kořeny β, β^{-1} a dále pár komplexně sdružených kořenů γ, $\gamma^{-1} = \overline{\gamma}$ na jednotkové kružnici. Polynom f lze také zapsat $f(x) = x^2 A(x + x^{-1})$, kde $A(t) = t^2 - at + (b-2)$ má za kořeny $\beta + \beta^{-1}$ a $\gamma + \overline{\gamma}$. Tyto kořeny splňují nerovnosti

$$-2 < \gamma + \overline{\gamma} < 2 < \beta + \beta^{-1}.$$

Naopak předpokládejme, že polynom A má dva reálné kořeny, řekněme δ, η splňující nerovnosti

$$-2 < \delta < 2 < \eta.$$

Rovnice

$$\gamma^2 - \delta\gamma - 1 \quad \text{a} \quad \beta^2 - \eta\gamma - 1$$

pak definují čísla γ a β (jednoznačně, pokud položíme požadavek $\Re(\gamma) > 0$, $\beta > 1$). V případě, že δ není celé číslo ($\delta \neq -1, 0, 1$), je β Salemovo číslo stupně 4 se sdruženými kořeny β^{-1}, γ, $\overline{\gamma}$.

Dokázali jsme tedy, že kořen $\beta > 1$ celočíselného polynomu $f(x) = x^4 - ax^3 + bx^2 - ax + 1$ je Salemovo číslo stupně 4, právě když polynom $A(t) = t^2 - at + (b-2)$ má dva reálné kořeny $\delta \neq 0, \pm 1$, η splňující nerovnosti $-2 < \delta < 2 < \eta$. Snadno si uvědomíme, že to nastane tehdy a jen tehdy, když

$$A(-2) > 0 > A(2) \quad \text{a} \quad A(-1) \neq 0,\ A(0) \neq 0,\ A(1) \neq 0.$$

Dosazením získáme úplný popis Salemových čísel stupně 4.

Tvrzení 5.30. *Salemova čísla stupně 4 jsou právě kořeny $\beta > 1$ polynomů $f(x) = x^4 - ax^3 + bx^2 - ax + 1$, $a, b \in \mathbb{Z}$, kde*

$$-2a - 2 < b < 2a - 2, \quad b \neq \pm a - 1, \quad b \neq 2.$$

Kapitola 6

Aritmetika v β-rozvojích

V předchozí kapitole jsme předvedli, jak reprezentovat v soustavě se základem β číslo x ze základního intervalu $[0, 1)$, viz rovnost (5.5). Velmi přirozeně definujeme rozvoj v soustavě se základem β pro libovolné nezáporné číslo.

Definice 6.1. Nechť $\beta > 1$. Pro každé $x \geq 0$ najdeme $k \in \mathbb{Z}$ tak, že $x\beta^{-k} \in [0, 1)$, a označíme $d_\beta(x\beta^{-k}) = x_1x_2x_3\cdots$. Pak definujeme tzv. β-rozvoj čísla x

$$(x)_\beta = \begin{cases} x_1x_2\cdots x_{k-1}x_k \cdot x_{k+1}x_{k+2}\cdots, & \text{když } k \geq 1 \\ 0 \cdot 0^{|k|}x_1x_2x_3\cdots, & \text{pro } k \leq 0. \end{cases}$$

Pro $x < 0$ definujeme β-rozvoj pomocí znaménka $(x)_\beta = -(|x|)_\beta$.

Poznamenejme, že β-rozvoj přesně odpovídá reprezentaci, kterou bychom našli hladovým algoritmem. Pro další výklad označme

$$\begin{aligned} \mathrm{Per}(\beta) &= \{x \in \mathbb{R} : (|x|)_\beta \text{ je posléze periodická posloupnost}\}, \\ \mathrm{Fin}(\beta) &= \{x \in \mathbb{R} : (|x|)_\beta \text{ je konečná posloupnost}\}, \\ \mathbb{Z}_\beta &= \{x \in \mathbb{R} : (|x|)_\beta \text{ nemá nenulové cifry u záporných mocnin báze}\}. \end{aligned}$$

V následujícím textu se zaměříme na aritmetické vlastnosti β-rozvojů.

6.1 Periodické rozvoje

U klasických číselných systémů s přirozenou bází víme, že periodické rozvoje mají právě racionální čísla. Formálně $\mathrm{Per}(\beta) = \mathbb{Q} = \mathbb{Q}(\beta)$. V obecném případě lze snadno usoudit, že $\mathrm{Per}(\beta) \subseteq \mathbb{Q}(\beta)$. Můžeme se ptát, zda pro některé neceločíselné báze platí rovnost. Tuto otázku téměř úplně zodpovídá následující věta. Ukazuje, že v tomto smyslu jsou přímým zobecněním přirozených bází Pisotovy báze. Nejdříve si ukážeme, že rovnost nastává pouze pro Parryho čísla.

Tvrzení 6.2. *Jestliže pro $\beta > 1$ platí $\mathrm{Per}(\beta) = \mathbb{Q}(\beta)$, pak β je Parryho číslo, tedy specielně algebraické celé číslo.*

Důkaz. Předpokládejme, že platí $\mathrm{Per}(\beta) = \mathbb{Q}(\beta)$. Protože $\beta - \lfloor\beta\rfloor \in \mathbb{Q}(\beta)$, z předpokladu tvrzení je jeho rozvoj posléze periodický. Proto i posloupnost $d_\beta(1)$ z definice 5.12 je posléze periodická, a proto β je z definice Parryho číslo. □

Věta 6.3 ([27])**.** *Nechť $\beta > 1$. Potom platí následující implikace. Je-li β Pisotovo číslo, pak $\mathrm{Per}(\beta) = \mathbb{Q}(\beta)$. Je-li $\mathrm{Per}(\beta) = \mathbb{Q}(\beta)$, pak β je Pisotovo nebo Salemovo číslo.*

Lemma 6.4. *Nechť K je číselné těleso stupně $[K : Q] = d$. Nechť $(y_n)_{n\in\mathbb{N}}$ je posloupnost algebraických celých čísel z tělesa K taková, že pro všechny $\mathbb{Q}$-izomorfizmy σ, je $\big(\sigma(y_n)\big)_{n\in\mathbb{N}}$ omezená. Pak y_n nabývá pouze konečně mnoha hodnot.*

Důkaz. Nechť α je algebraické číslo takové, že $K = \mathbb{Q}(\alpha)$. Zvolíme α tak, aby okruh $\mathcal{O}_K$ algebraických celých čísel tělesa K byl obsažen v množině

$$\mathbb{Z}[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} : a_0, \ldots, a_{d-1} \in \mathbb{Z}\}.$$

Označme $\alpha = \alpha^{(1)}, \ldots, \alpha^{(d)}$ sdružené kořeny k číslu α. Pak obraz prvku $y = a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} \in K$, $a_i \in \mathbb{Z}$ při působení $\mathbb{Q}$-izomorfizmů $\sigma_1, \ldots, \sigma_d$ je

$$\sigma_i(y) = a_0 + a_1\alpha^{(i)} + \cdots + a_{d-1}(\alpha^{(i)})^{d-1}, \quad i = 1, \ldots, d.$$

Nerovnost $|\sigma_i(y)| < K$ vytyčuje v prostoru $\mathbb{R}^d$ koeficientů $a_0, \ldots, a_{d-1}$ vrstvu ohraničenou dvěma rovnoběžnými nadrovinami s normálou $\big(1, \alpha^{(i)}), \ldots, (\alpha^{(i)})^{d-1}\big)$. Pokud taková nerovnost platí pro každé i, koeficienty $a_0, \ldots, a_{d-1}$ nutně leží v ohraničé oblasti.

Mějme posloupnost $(y_n = a_0^{(n)} + a_1^{(n)}\alpha + \cdots + a_{d-1}^{(n)}\alpha^{d-1})_{n\in\mathbb{N}} \in \mathcal{O}_K$ takovou, že pro všechna i je $\big(\sigma(y_n)\big)_{n\in\mathbb{N}}$ omezená. Jelikož koeficienty $a_j^{(n)}$ jsou celočíselné a leží v omezené oblasti, nabývá posloupnost y_n pouze konečně mnoha hodnot. □

Důkaz věty 6.3. Zvolme $x \in \mathbb{Q}(\beta)$, bez újmy na obecnosti v intervalu $[0, 1)$. Ukážeme, že jeho β-rozvoj $x = \sum_{i=1}^{\infty} x_i\beta^{-i}$ je posléze periodický. Když β je stupně D, pak číslo x lze také zapsat ve tvaru

$$x = \frac{1}{q}\big(c_0 + c_1\beta + \cdots + c_{d-1}x^{d-1}\big),$$

kde $q \in \mathbb{N}$ je minimální a $c_0, \ldots, c_{d-1} \in \mathbb{Z}$. Snadno si rozmyslíme, že při aplikaci transformace T_β na číslo x získáme opět čísla v obdobném tvaru,

$$T_\beta^{(n)}(x) = \frac{1}{q}\big(c_0^{(n)} + c_1^{(n)}\beta + \cdots + c_{d-1}^{(n)}x^{d-1}\big),$$

kde $c_i^{(n)} \in \mathbb{Z}$. Zároveň tyto iterace lze vyjádřit jako

$$T_\beta^{(n)}(x) = \sum_{i=n+1}^{\infty} x_i \beta^{n-i} = \beta^n \Big(x - \sum_{i=1}^{n} x_i \beta^{-i} \Big).$$

Zjevně $T_\beta^{(n)}(x) \in [0,1)$ pro všechna n. Zvolme libovolný sdružený kořen k β, označme ho γ. Aplikací tělesového izomorfizmu $\sigma : \mathbb{Q}(\beta) \to \mathbb{Q}(\gamma)$ zjistíme, že

$$\sigma\big(T^{(n)}(x)\big) = \gamma^n \sigma(x) - \sum_{i=1}^{n} x_i \gamma^{n-i}.$$

Protože β je z předpokladu Pisotovo číslo, je $|\gamma| < 1$, a proto je $\sigma\big(T^{(n)}(x)\big)$ omezená v n.

Máme tedy posloupnost algebraických celých čísel $\big(qT^{(n)}(x)\big)_{n\in\mathbb{N}}$, která splňuje předpoklady lemmatu. Proto $T_\beta^{(n)}(x)$ nabývá pouze konečně mnoha hodnot. Jestliže $l < k$ jsou takové indexy, že $T_\beta^{(l)}(x) = T_\beta^{(k)}(x)$, pak β-rozvoj čísla x je periodický s periodou $k - l$.

Dokažme nyní opačnou implikaci. Předpokládejme, že platí $\mathrm{Per}(\beta) = \mathbb{Q}(\beta)$. Specielně to znamená, že každé racionální číslo r má posléze periodický rozvoj. Ke každému $m \in \mathbb{N}$ lze jistě zvolit racionální číslo $r^{(m)} = r$, jehož β-rozvoj je tvaru

$$r = \beta^{-1} + \sum_{j=m+1}^{\infty} x_j \beta^{-j}. \tag{6.1}$$

Stačí volit libovolné racionální číslo v intervalu $(\beta^{-1}, \beta^{-1} + \beta^{-m})$. Podle tvrzení 6.2 je β algebraické celé číslo. Je-li γ jeho sdružený kořen, pak aplikací příslušného $\mathbb{Q}$-izomorfizmu získáme

$$\sigma(r) = r = \gamma^{-1} + \sum_{j=m+1}^{\infty} x_j \gamma^{-j}. \tag{6.2}$$

V této rovnosti jsme využili, že rozvoj r je periodický, a tedy izomorfizmus na sumu lze aplikovat. Porovnáním (6.1) a (6.2) dostaneme

$$\beta^{-1} - \gamma^{-1} = \sum_{j=m+1}^{\infty} x_j (\gamma^{-j} - \beta^{-j}).$$

Můžeme odhadnout

$$|\beta^{-1} - \gamma^{-1}| \le \sum_{j=m+1}^{\infty} x_j |\gamma^{-j} - \beta^{-j}| \le 2\lfloor \beta \rfloor \sum_{j=m+1}^{\infty} \eta^j,$$

kde $\eta = \max\{|\beta|^{-1}, |\gamma|^{-1}\}$. Pokud $|\gamma| > 1$, vede tento odhad pro dostatečně velké m ke sporu. Proto nutně každý sdružený kořen γ je v absolutní hodnotě $|\gamma| \leq 1$ a β je Pisotovo nebo Salemovo číslo. □

Poznamenejme, že se dosud nepodařilo vyřešit otázku periodicity rozvojů prvků tělesa $\mathbb{Q}(\beta)$, byť jen u jediné Salemovy báze β.

Dusledek 6.5. *Pisotova čísla jsou Parryho.*

Důkaz. Stačí kombinovat tvrzení 6.2 a větu 6.3. □

Příklad 6.6. V předchozím důsledku nelze implikaci obrátit. Existují totiž Parryho čísla, která nejsou Pisotova. Například dominantní kořen polynomu $x^7 - x^6 - 1$ je Parryho číslo, protože $d_\beta(1) = 1000001$. Ale β má sdružený kořen $\alpha \approx 0.78 + 0.70i$.

Dokázali jsme, že Pisotova čísla β splňují $\mathrm{Per}(\beta) = \mathbb{Q}(\beta)$, a tudíž jsou Parryho. Není rozhodnuto, zda analogie k tomuto tvrzení lze formulovat pro Salemova čísla. O platnosti $\mathrm{Per}(\beta) = \mathbb{Q}(\beta)$ není rozhodnuto pro žádný případ Salemova čísla. Pro Salemova čísla čtvrtého stupně je ovšem dokázáno slabší tvrzení, totiž že jsou to Parryho čísla.

6.2 Konečné rozvoje a vlastnost (F)

Ze soustav s celočíselnou bází jsme zvyklí, že při sčítání dvou čísel se zápisem, ve kterém jsou nenulové koeficienty pouze u nezáporných mocnin základu, vznikne opět číslo stejného typu. Je to tím, že pro $\beta \in \mathbb{N}$ odpovídají β-celá čísla číslům celým, tedy množina $\mathbb{Z}_\beta$ je rovna okruhu $\mathbb{Z}$. Pokud za základ soustavy zvolíme číslo, které není celé, toto už neplatí.

Tvrzení 6.7. *Nechť $\beta > 1$. Potom $\mathbb{Z}_\beta$ je okruh, právě když $\beta \in \mathbb{Z}$.*

Důkaz. Je-li $\beta \in \mathbb{Z}$, pak lze snadno ukázat, že každé přirozené číslo lze napsat ve tvaru $\sum_{i=0}^{k} a_i \beta^i$, kde $a_i \in \{0, 1, \ldots, \beta - 1\}$. Poznamenejme, že takový zápis je dokonce jednoznačný, pokud $a_k \neq 0$. Navíc je tento zápis i přípustný, jak je zřejmé z příkladu 5.14. Je tedy $\mathbb{Z} \subset \mathbb{Z}_\beta$ Naopak každé číslo výše uvedeného tvaru je zjevně celé, takže $\mathbb{Z}_\beta = \mathbb{Z}$, což je okruh.

Uvažujme číslo $x = \lfloor \beta \rfloor + 1$, které vznikne součtem dvou β-celých čísel $\lfloor \beta \rfloor$ a 1. Najdeme k takové, že $\beta^k < x < \beta^k + 1$. (Poznamenejme, že k může být větší než 1 pro β blízko 1.) Pak β-rozvoj čísla x je ve tvaru

$$(x)_\beta = 10^k \cdot x_{-1} x_{-2} \cdots ,$$

kde aspoň jedna z cifer x_j, $j \leq -1$ je nenulová. Proto $x \notin \mathbb{Z}_\beta$, takže $\mathbb{Z}_\beta$ není okruh. □

Výsledkem aritmetických operací s β-celými čísly může být číslo, které má nenulovou zlomkovou část, tj. jeho β-rozvoj má nenulové cifry u záporných mocnin báze β. Jak uvidíme na příkladech, může se dokonce stát, že zlomková část je nekonečná.

Příklad 6.8. Nechť nejprve $\beta = \tau$. Rozdílem $\tau - 1$ dostaneme číslo $\frac{1}{\tau}$. Zapsáno v rozvojích, máme

$$10 \cdot \quad - \quad 1 \cdot \; = \; 0 \cdot 1$$

Uvažujme nyní bázi $\beta = \tau^2 = (3+\sqrt{5})/2$. Připomeňme příklad 5.16, kde je ukázáno, že $d_\beta(1) = 21^\omega$. Odtud lze snadno odvodit, že rozdílem $\beta - 1$ dostaneme číslo s nekonečným β-rozvojem $1 \cdot 1^\omega$. To znamená, že v případě této báze není ani množina $\mathrm{Fin}(\beta)$ uzavřená na aritmetické operace.

Vidíme tedy, že bude nutné rozlišovat báze soustav, ve kterých je množina konečných rozvojů uzavřená na aritmetické operace, a ve kterých tomu tak není. K tomu slouží tzv. vlastnost (F)[1].

Definice 6.9. Řekneme, že reálné číslo $\beta > 1$ má vlastnost (F), jestliže platí

$$(F) \qquad\qquad \mathrm{Fin}(\beta) = \mathbb{Z}[\beta^{-1}].$$

Tvrzení 6.10. *Reálné číslo $\beta > 1$ má vlastnost (F), právě když* $\mathrm{Fin}(\beta)$ *je okruh.*

Důkaz. Implikace zleva doprava je zřejmá. Předpokládejme proto, že $\mathrm{Fin}(\beta)$ je okruh. Zjevně $\mathrm{Fin}(\beta) \subset \mathbb{Z}[\beta, \beta^{-1}]$. Uzavřenost množiny konečných rozvojů vůči sčítání a odčítání lze formulovat tak, že platí i opačná inkluze, tedy

$$\mathbb{Z}[\beta, \beta^{-1}] = \mathrm{Fin}(\beta). \tag{6.3}$$

Speciálně také $\mathbb{Z} \subset \mathrm{Fin}(\beta)$. To implikuje, že číslo $\lfloor\beta\rfloor + 1$ má konečný rozvoj. Podobně jako v důkazu tvrzení 6.7 zjistíme, že tento rozvoj je tvaru

$$(\lfloor\beta\rfloor + 1)_\beta = 10^k \cdot a_{-1}a_{-2}\cdots a_{-j}.$$

Vyčíslením zjistíme, že β je kořenem monického polynomu s celočíselnými koeficienty,

$$X^{k+j} - (\lfloor\beta\rfloor + 1)X^j + a_{-j}X^{j-1} + \cdots + a_{-j}.$$

Tím jsme dokázali, že β je algebraické celé číslo. Pak ale platí $\mathbb{Z}[\beta, \beta^{-1}] = \mathbb{Z}[\beta^{-1}]$, takže rovnost (6.3) přechází přímo v definici vlastnosti (F). □

[1] F jako finiteness, tedy konečnost

Úplný algebraický popis bází, které splňují vlastnost (F) dosud nebyl podán. Uvedeme nicméně některé třídy čísel s touto vlastností. Čerpáme především z práce Ch. Frougny a B. Solomyaka [11]. Nejprve jednu podmínku nutnou.

Věta 6.11. *Nechť číslo $\beta > 1$ splňuje vlastnost (F). Potom β je Pisotovo číslo, jehož žádný sdružený kořen není kladný.*

Důkaz. Fakt, že β je algebraické celé číslo, už jsme ukázali v rámci důkazu tvrzení 6.10. Dokažme nejprve, že β nemůže mít sdružený kořen γ takový, že $|\gamma| > 1$. Kdyby β takový srdužený kořen mělo, jistě by bylo možné volit exponent $m \in \mathbb{N}$ takový, aby hodnota $|\beta^m - \gamma^m|$ byla libovolně velká. Označme $\nu = \max\{|\beta|^{-1}, |\gamma|^{-1}\}$. Zvolíme m takové, že

$$|\beta^m - \gamma^m| > C := 2\lfloor\beta\rfloor\nu(1-\nu)^{-1}. \tag{6.4}$$

Nyní uvažujme β-rozvoj přirozeného čísla $\lfloor\beta^m\rfloor + 1$. Protože β má vlastnost (F), je tento rozvoj konečný. S využitím nerovnosti $\beta^m < \lfloor\beta^m\rfloor + 1 < \beta^m + 1$ dostaneme rozvoj $(\lfloor\beta^m\rfloor + 1)_\beta = a_m 0^m \cdot a_{-1} \cdots a_{-j}$. Vyčísleno máme

$$\lfloor\beta^m\rfloor + 1 = a_m\beta^m + a_{-1}\beta^{-1} + \cdots + a_{-j}\beta^{-j}.$$

Na tuto rovnici aplikujeme izomorfizmus $\sigma : \mathbb{Q}(\beta) \to \mathbb{Q}(\gamma)$, který číslu β přiřazuje jeho sdružený kořen γ, tj. $\sigma(\beta) = \gamma$. Dostaneme

$$\lfloor\beta^m\rfloor + 1 = a_m\gamma^m + a_{-1}\gamma^{-1} + \cdots + a_{-j}\gamma^{-j},$$

kde jsme využili, že izomorfizmus σ je identický na tělese racionálních čísel. Odečtením těchto dvou rovnic od sebe vyjde

$$\beta^m - \gamma^m = a_{-1}(\gamma^{-1} - \beta^{-1}) + \cdots + a_{-j}(\gamma^{-j} - \beta^{-j}).$$

Toto číslo odhadneme v absolutní hodnotě

$$\left|\beta^m - \gamma^m\right| \le \sum_{i=1}^{j} a_{-i}(|\beta|^{-j} + |\gamma|^{-j}) < 2\lfloor\beta\rfloor \sum_{i=1}^{+\infty} \nu^j = C.$$

To je ovšem spor s volbou exponentu $m \in \mathbb{N}$, viz (6.4).

Z výše uvedeného vyplývá, že β je algebraické celé číslo bez sdruženého kořene velikosti > 1. Jinými slovy, β je Pisotovo nebo Salemovo číslo. Jelikož podle tvrzení 5.28 má každé Salemovo číslo α sdružený kořen α^{-1}, stačí k vyloučení Salemových čísel ukázat, že β nemá kladný sdružený kořen. K tomu využijeme β-rozvoj čísla $\beta - \lfloor\beta\rfloor \in [0, 1)$, tedy $(\beta - \lfloor\beta\rfloor)_\beta = 0 \cdot a_{-1}a_{-2}\cdots a_{-j}$. Po

vyčíslení

$$\beta - \lfloor \beta \rfloor = a_{-1}\beta^{-1} + \cdots + a_{-j}\beta^{-j}.$$

Předpokládejme existenci sdruženého kořene $\gamma > 0$. Aplikací izomorfizmu $\sigma : \beta \mapsto \gamma$ dostaneme

$$\gamma - \lfloor \beta \rfloor = a_{-1}\gamma^{-1} + \cdots + a_{-j}\gamma^{-j}.$$

To je ovšem spor, protože na levé straně této rovnosti je číslo záporné a na pravé straně číslo kladné. □

Poznámka 6.12. V důkazu věty jsme pro odvození faktu, že β nemá sdružené kořeny vně jednotkové kružnice, použili pouze to, že kladná celá čísla mají konečný rozvoj.

Následující příklad ukazuje, že implikace ve výše uvedené větě nelze obrátit. Existují totiž Pisotova čísla bez kladných sdružených kořenů, která nemají vlastnost (F).

Příklad 6.13. Nechť β je dominantní kořen polynomu $X^4 - 2X^3 - X - 1$, takže $\beta \approx 2.277$ a jeho sdružené kořeny jsou $\gamma \approx -0.557$ a $\delta_{1,2} \approx 0,139 \pm 0.876i$. Platí $d_\beta(1) = 20110^\omega$. Rozvoj čísla 3 je nekonečný, $(3)_\beta = 10.111(00012)^\omega$.

6.3 Vlastnost (PF)

Množina $\mathrm{Fin}(\beta)$ obsahuje kladná i záporná čísla. Při zkoumání uzavřenosti na sčítání se ovšem můžeme omezit na sčítání kladných čísel, jak ukazuje následující tvrzení.

Věta 6.14. *Nechť $\beta > 1$ a nechť $d_\beta(1)$ je příslušný Rényiův rozvoj jedničky.*

(i) Je-li $d_\beta(1)$ nekonečný, pak β nesplňuje vlastnost (F).

(ii) Je-li $d_\beta(1)$ konečný, pak β splňuje vlastnost (F), právě když je $\mathrm{Fin}(\beta)$ uzavřená na sčítání kladných prvků.

Důkaz. (i) Podle definice Rényiova rozvoje jedničky (5.12) je $d_\beta(\beta - \lfloor \beta \rfloor) = t_2 t_3 \cdots$. Číslo $\beta - \lfloor \beta \rfloor$ tedy nepatří do $\mathrm{Fin}(\beta)$. Tudíž β nesplňuje vlastnost (F).

(ii) Nechť $d_\beta(1) = t_1 t_2 \cdots t_m$. To znamená, že

$$1 = \frac{t_1}{\beta} + \frac{t_2}{\beta^2} + \cdots + \frac{t_m}{\beta^m}\,. \tag{6.5}$$

Předpokládejme, že $\mathrm{Fin}(\beta)$ je uzavřené na sčítání kladných prvků. Uvažujme libovolné $x \in \mathrm{Fin}(\beta)$ a libovolné $\ell \in \mathbb{Z}$ takové, že $x > \beta^\ell$. β-rozvoj čísla x je tvaru $x = \sum_{i=-N}^{n} x_i \beta^i$, pro nějaké $n \geq \ell$.

Opakovaným použitím (6.5) lze získat reprezentaci x ve tvaru $x = \sum_{i=-M}^{\ell} \tilde{x}_i \beta^i$ takovou, že $\tilde{x}_\ell \geq 1$. Potom

$$(\tilde{x}_\ell - 1)\beta^\ell + \sum_{i=-M}^{\ell-1} \tilde{x}_i \beta^i$$

je konečná β-reprezentace čísla $x - \beta^\ell$. Tu lze interpretovat jako součet konečného počtu kladných prvků z množiny $\mathrm{Fin}(\beta)$. Proto je i $x - \beta^\ell \in \mathrm{Fin}(\beta)$.

Zbývá uvědomit si, že rozdíl $x - y$ libovolných čísel $x, y \in \mathrm{Fin}(\beta)$, $x > y > 0$ je jen konečný počet odečítání jednotlivých mocnin β. Proto uzavřenost $\mathrm{Fin}(\beta)$ na sčítání kladných prvků implikuje uzavřenost na sčítání libovolných $x, y \in \mathrm{Fin}(\beta)$.

Násobení čísel $x, y \in \mathrm{Fin}(\beta)$ je podle distributivního zákone jen sčítáním konečného počtu sčítanců z množiny $\mathrm{Fin}(\beta)$. Tím je věta dokázána. □

Motivováni předchozí větou, zavedeme tzv. vlastnost (PF)[2].

Definice 6.15. Řekneme, že reálné číslo $\beta > 1$ má vlastnost (PF), jestliže platí

$$(PF) \qquad\qquad \mathrm{Fin}(\beta) \subset \mathbb{Z}^+[\beta^{-1}].$$

Podle poznámky 6.12 můžeme říct, že vlastnost (PF) implikuje, že daná báze je Pisotovo nebo Salemovo číslo.

Následující úvahy byly předvedeny v článku [4]. Od této chvíle se tedy soustředíme na sčítání $x + y$ svou čísel $x, y \in \mathrm{Fin}(\beta)$, $x, y \geq 0$. Bez újmy na obecnosti stačí uvažovat čísla $x, y \in \mathbb{Z}_\beta$. Ať tedy čísla $x, y \in \mathbb{Z}_\beta$, $x, y \geq 0$ mají β-rozvoje $x = \sum_{k=0}^{n} a_k \beta^k$, $y = \sum_{k=0}^{n} b_k \beta^k$. Pak $\sum_{k=0}^{n} (a_k + b_k)\beta^k$ je β-reprezentace čísla $x + y$. Jestliže posloupnost cifer $(a_n + b_n)(a_{n-1} + b_{n-1}) \cdots (a_0 + b_0)$ splňuje Parryho podmínku přípustnosti (věta 5.11), získali jsme přímo β-rozvoj čísla $x + y$. V opačném případě posloupnost cifer musí obsahovat zakázaný řetězec.

Definice 6.16. Nechť $\beta > 1$. Zakázaný řetězec $u_k u_{k-1} \cdots u_0$ nezáporných celých čísel se nazývá minimální, jestliže

(i) řetězce $u_{k-1} \cdots u_0$ a $u_k \cdots u_1$ jsou přípustné a

(ii) $u_i \geq 1$ implikuje, že $u_k \cdots u_{i+1}(u_i - 1)u_{i-1} \cdots u_0$ is přípustný řetězec pro všechna $i = 0, 1, \ldots, k$.

Minimální zakázaný řetězec $u_k u_{k-1} \cdots u_0$ obsahuje alespoň jednu nenulovou cifru, označme ji $u_i \geq 1$. Pak $u_k u_{k-1} \cdots u_0$ s cifrou $u_i \geq 1$ je β-reprezentací součtu dvou čísel $w = u_k \beta^k + \cdots + u_{i+1}\beta^{i+1} + (u_i - 1)\beta^i + u_{i-1}\beta^{i-1} + \cdots + u_0$ a $\tilde{w} = \beta^i$, která jsou β-celá podle definice

[2] PF jako positive finiteness, tedy kladná konečnost

minimálního zakázaného řetězce. Protože β-rozvoj daného čísla je lexikograficky největší mezi všemi jeho β-reprezentacemi, musí platit, že součet $w + \tilde{w} \in \mathrm{Fin}(\beta)$ má konečnou β-reprezentaci lexikograficky ostře větší než $u_k u_{k-1} \cdots u_0$. Tím jsme odvodili nutnou podmínku na β, aby mělo vlastnost (PF). Pro přesnou formulaci (tvrzení 6.18) uvedeme nejprve definici.

Definice 6.17. Nechť $k, p \in \mathbb{Z}$, $k \geq p$ a $z = z_k\beta^k + z_{k-1}\beta^{k-1} + \cdots + z_p\beta^p$, kde $z_i \in \mathbb{N}_0$, $p \leq i \leq k$. Konečná β-reprezentace čísla z tvaru $v_n\beta^n + v_{n-1}\beta^{n-1} + \cdots + v_\ell\beta^\ell$, $\ell \leq n$, se nazývá *transkripce* reprezentace $z_k\beta^k + z_{k-1}\beta^{k-1} + \cdots + z_p\beta^p$, pokud

$$k \leq n \qquad \text{a} \qquad v_n v_{n-1} \cdots v_\ell \succ \underbrace{00\cdots0}_{(n-k)\text{ times}}\ z_k \cdots z_p\,.$$

Věta 6.18 (Vlastnost T)**.** *Jestliže $\beta > 1$ splňuje vlastnost (PF), pak má i vlastnost T:*

Ke každému minimálnímu zakázanému řetězci $u_k u_{k-1} \cdots u_0$ existuje transkripce $u_k\beta^k + u_{k-1}\beta^{k-1} + \cdots + u_1\beta + u_0$.

Pokud je vlastnost T splněna, transkripci β-reprezentace čísla z lze dostat následovně. Každou β-reprezentace z obsahující zakázaný řetězec můžeme chápat jako součet minimálního zakázaného řetězce $\beta^j(u_k\beta^k + \cdots + u_1\beta + u_0)$ a β-reprezentace nějakého čísla $\tilde{z}$. Transkripci β-reprezentace z dostaneme součtem po cifrách transkripce $\beta^j(v_n\beta^n + \cdots + v_\ell\beta^\ell)$ minimálního zakázaného řetězce (z vlastnosti T) a β-representation of $\tilde{z}$.

Příklad 6.19. V soustavě se základem $\tau = \frac{1}{2}(1 + \sqrt{5})$ jsou přípustné všechny konečné τ-reprezentace $x_k \cdots x_\ell$ s ciframi $x_i \in \{0, 1\}$ takové, že $x_i x_{i-1} = 0$ pro $\ell < i \leq k$. Podle definice jsou minimálními zakázanými řetězci 2 a 11. Zlatý řez τ splňuje vlastnost T, protože lze přepsat $2 = \tau + \tau^{-2}$ a $\tau + 1 = \tau^2$, přičemž $02 \prec 1001$ and $011 \prec 100$. Tato pravidla mohou být použita k přepisu každého zakázaného řetězce na τ-rozvoj reprezentující stejné číslo. Například

$$3 = 1 + 2 = 1 + \tau + \frac{1}{\tau^2} = \tau^2 + \frac{1}{\tau^2}\,.$$

τ-reprezentace $\tau + 1 + \tau^{-2}$ a $\tau^2 + \tau^{-2}$ jsou transkripce čísla 3. Z těchto transkripcí je $100 \bullet 01$ přímo τ-rozvojem čísla 3.

Nechť $z_k\beta^k + z_{k-1}\beta^{k-1} + \cdots + z_p\beta^p$ je β-reprezentace čísla z taková, že řetězec cifer $z_k z_{k-1} \cdots z_p$ není přípustný. Opakováním předchozího postupu dostaneme lexikograficky rostoucí posloupnost transkripcí. Obecně se může stát, že tato posloupnost bude nekonečná, tedy nebude možné získat β-rozvoj čísla z. Následující věta dává postačující podmínku, aby tato nepříznivá situace nenastala.

Věta 6.20. *Nechť $\beta > 1$. Předpokládejme, že ke každému minimálnímu zakázanému řetězci $u_k u_{k-1} \cdots u_0$ existuje transkripce $v_n\beta^n + v_{n-1}\beta^{n-1} + \cdots + v_\ell\beta^\ell$ reprezentace $u_k\beta^k + u_{k-1}\beta^{k-1} +$*

$\cdots + u_1\beta + u_0$ *taková, že*

$$v_n + v_{n-1} + \cdots + v_\ell \le u_k + u_{k-1} + \cdots + u_0\,.$$

Potom β splňuje vlastnost (PF). Speciálně β-rozvoj součtu $x + y$ pro libovolné $x, y \in \mathrm{Fin}(\beta)$ lze získat z libovolné β-reprezentace $x + y$ pomocí konečného počtu transkripcí.

Abychom ověřili, zda číslo β splňuje vlastnost T, musíme znát příslušné minimální zakázané řetězce. V případě, kdy je Rényiův rozvoj jedničky konečný, tj. $d_\beta(1) = t_1 t_2 \cdots t_m$, pak tyto řetězce musí být mezi

$$(t_1 + 1), \quad t_1(t_2 + 1), \quad t_1 t_2 (t_3 + 1), \quad \ldots, \quad t_1 t_2 \cdots t_{m-2}(t_{m-1} + 1), \quad t_1 t_2 \cdots t_{m-1} t_m.$$

Všimněte si, že ne všechny výše uvedené zakázané řetězce musí být minimální. Například když $d_\beta(1) = 111$, tak tento seznam je složený z 2, 12, 111. Nicméně 12 není minimální zakázaný řetězec.

Jako důsledék předchozí věty dostáváme jednu zajímavou třídu Pisotových čísel β takových, že $\mathrm{Fin}(\beta)$ je okruh. Poznamenejme, že důkaz, že tato třída splňuje vlastnost (F) už byl uveden v [11].

Dusledek 6.21. *Nechť $\beta > 1$ je takové, že $d_\beta(1) = t_1 \cdots t_m$, $t_1 \ge t_2 \ge \cdots \ge t_m \ge 1$. Potom β splňuje vlastnost (F).*

Důkaz. Protože Rényiův rozvoj jedničky je konečný, podle věty 6.14 stačí dokázat platnost vlastnosti (PF). To provedeme ověřením platnosti předpokladů věty 6.20. Uvažujme zakázaný řetězec $t_1 t_2 \cdots t_{i-1}(t_i + 1)$, $1 \le i \le m - 1$. Zjevně platí

$$t_1\beta^{i-1} + \cdots + t_{i-2}\beta^2 + t_{i-1}\beta + (t_i + 1) =$$
$$= \beta^i + (t_1 - t_{i+1})\beta^{-1} + \cdots + (t_{m-i} - t_m)\beta^{-m+i} + t_{m-i+1}\beta^{-m+i-1} + \cdots + t_m\beta^{-m}.$$

Z předpokladu plyne, že cifry na pravé straně rovnosti jsou nezáporné. Ciferný součet je stejný na obou stranách. Proto je

$$1\underbrace{0\,0\cdots 0}_{i \text{ times}}\,(t_1 - t_{i+1})\,(t_2 - t_{i+2})\cdots(t_{m-i} - t_m)$$

žádaným řetězcem lexikograficky ostře větším než $0\,t_1 t_2 \cdots t_{i-1}(t_i + 1)$.

Zbývající řetězec $t_1 t_2 \cdots t_{m-1} t_m$ lze přepsat na lexikograficky větší $1\underbrace{0\,0\cdots 0}_{m \text{ times}}$. □

Podmínky věty 6.20 jsou splněny i pro báze, které nepatří do třídy popsané v Důsledku 6.21.

Příklad 6.22. Uvažujme dominantní kořen polynomu $X^3 - X - 1$. Je dokázáno, že takové β je nejmenší ze všech Pisotových čísel. Rényiův rozvoj jedničky je v tomto případě $d_\beta(1) = 10001$. Číslo β splňuje

$$\beta^3 = \beta + 1 \qquad \text{and} \qquad \beta^5 = \beta^4 + 1\,.$$

Minimální zakázané řetězce jsou 2, 11, 101, 1001 a 10001. Jejich transkripce pro vlastnost T pak máme:

$$\begin{aligned} 2 &= \beta^2 + \beta^{-5} \\ \beta + 1 &= \beta^3 \\ \beta^2 + 1 &= \beta^3 + \beta^{-3} \\ \beta^3 + 1 &= \beta^4 + \beta^{-5} \\ \beta^4 + 1 &= \beta^5 \end{aligned}$$

Ciferný součet u každé transkripce je menší nebo roven cifernému součtu příslušného minimálního zakázaného řetězce. Podle věty 6.20 má minimální Pisotovo číslo vlastnost (PF) a díky větě 6.14 i vlastnost (F). Poznamenejme, že vlastnost (F) minimálního Pisotova čísla plyne už z výsledku Akiyamy [2].

Poznámka 6.23. Implikaci ve větě 6.20 není možné obrátit. Například β kořen polynomu $x^3 - 2x^2 - 1$ splňuje $d_\beta(1) = 201$ a jeho minimální zakázaný řetězec 3 má β-rozvoj

$$3 = \beta + \frac{1}{\beta} + \frac{1}{\beta^2} + \frac{1}{\beta^3} + \frac{1}{\beta^4}\,.$$

Ciferný součet této transkripce je 5. Kdyby existovala jiná transkripce řetězce 3 s ciferným součtem 3, musela by být lexikograficky ostře větší než 03 a ostře menší než 101111. Lze snadno ukázat, že taková transkripce neexistuje. Přesto má tato báze β vlastnost (PF). Má totiž vlastnost (F), viz [2].

Na druhou stranu vlastnost T bez podmínky na ciferný součet transkripcí nestačí pro vlastnost (PF). Jako příklad můžeme vzít bázi β s Rényiovým rozvojem jedničky $d_\beta(1) = 100001$. Taková báze je kořenem polynomu $X^6 - X^5 - 1$. Mezi sdruženými kořeny β je pár komplexně sdružených čísel vně jednotkové kružnice. Proto β není Pisotovo a podle poznámky 6.12 nemá vlastnost (PF). Nicméně všechny minimální zakázané řetězce mají transkripce:

$$\begin{aligned} 2 &= \beta + \beta^{-6} + \beta^{-7} + \beta^{-8} + \beta^{-9} + \beta^{-10} \\ \beta + 1 &= \beta^2 + \beta^{-6} + \beta^{-7} + \beta^{-8} + \beta^{-9} \\ \beta^2 + 1 &= \beta^3 + \beta^{-6} + \beta^{-7} + \beta^{-8} \end{aligned}$$

$$\begin{aligned}
\beta^3 + 1 &= \beta^4 + \beta^{-6} + \beta^{-7} \\
\beta^4 + 1 &= \beta^5 + \beta^{-6} \\
\beta^5 + 1 &= \beta^6
\end{aligned}$$

Kapitola 7

Redundantní poziční soustavy s celočíselnou bází

Zaměříme se nyní na způsob, jakým jsou základní operace (sčítání a odčítání, násobení a dělení) realizovány z pohledu výpočetní aritmetiky. Tzv. klasické / školní způsoby počítání nemusejí být optimální co do náročnosti a rychlosti zpracování, proto si představíme i několik alternativních postupů. Pro sčítaní a odčítaní to jsou algoritmy tzv. paralelní, pro násobení a dělení pak algoritmy tzv. on-line.

Uvažujeme číselné numerační systémy $(\beta, \mathcal{A})$, kde báze $\beta \in \mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{C}$ má velikost $|\beta| > 1$, a abeceda $\mathcal{A} \subset \mathbb{Z}$, resp. $\mathcal{A} \subset \mathbb{Z}[\omega]$ pro $\omega \in \mathbb{R}, \mathbb{C}$, jejíž prvky nazýváme cifry, vždy obsahuje $0 \in \mathcal{A}$.

Reprezentaci čísla x v numeračním systému $(\beta, \mathcal{A})$ značíme jako

$$x = (x_n x_{n-1} \dots x_1 x_0 \cdot x_{-1} x_{-2} \dots)_\beta = \sum_j x_j \beta^j \qquad x_j \in \mathcal{A}\,,$$

a množinu všech konečných reprezentací čísel v $(\beta, \mathcal{A})$ jako

$$\mathrm{Fin}_{\mathcal{A}}(\beta) = \left\{ \sum_{j \in I} x_j \beta^j \mid I \subset \mathbb{Z} \text{ konečná }, x_j \in \mathcal{A} \right\} = \left\{ \sum_{j=m}^{n} x_j \beta^j \mid m, n \in \mathbb{Z}, x_j \in \mathcal{A} \right\}.$$

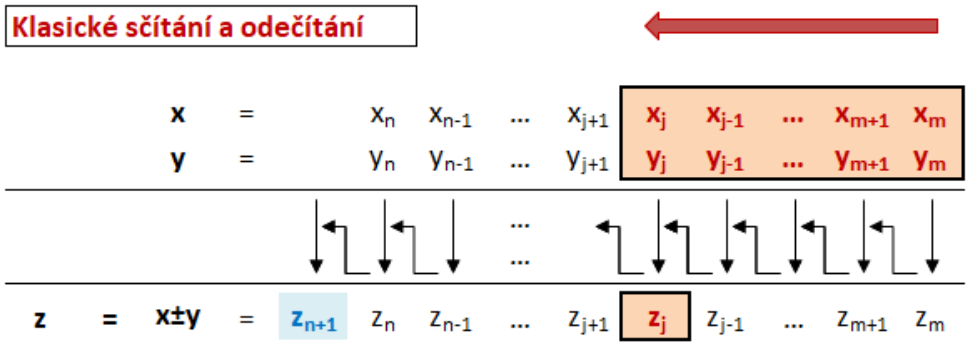
Při realizaci aritmetických operací v počítači se fakticky jedná vždy právě o reprezentace konečné, proto práce na množině $\mathrm{Fin}_{\mathcal{A}}(\beta)$ vlastně nepředstavuje žádné omezení.

7.1 Aritmetické operace v klasickém provedení

Připomeňme si, jak základní aritmetické operace fungují v klasickém provedení.

Sčítání a odčítání

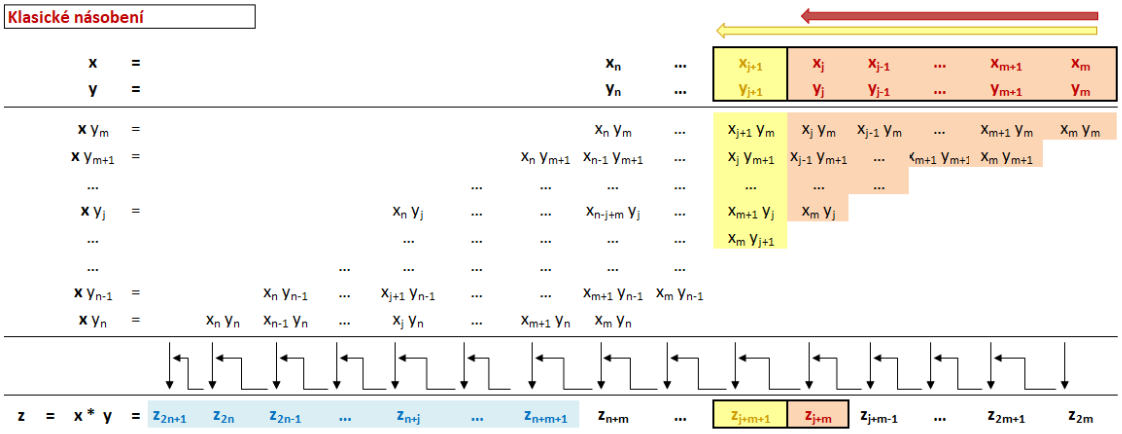
Směr zpracování je zprava doleva, tedy od nejméně významných cifer. Při výpočtu dochází k přenosu cifer max. o jednu pozici doleva.



Ze vstupních sčítanců $x = \sum_{j=m}^{n} x_j \beta^j$ a $y = \sum_{j=m}^{n} y_j \beta^j$ s ciframi $x_j, y_j \in \mathcal{A}$ po zpracování obdržíme součet (případně analogicky též rozdíl) ve tvaru $z = x \pm y = \sum_{j=m}^{n+1} z_j \beta^j$ - tedy opět s ciframi z výchozí abecedy $z_j \in \mathcal{A}$, a s (maximálně) jednou další pozicí v reprezentaci navíc (viz nově obsazený index $n+1$).

Násobení

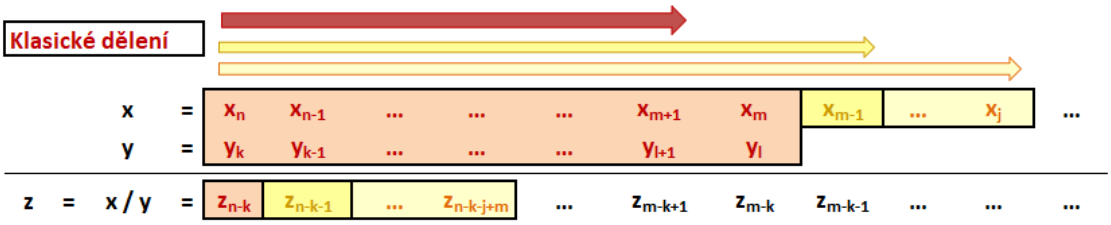
Také násobení se v klasickém režimu zpracovává směrem zprava doleva (tj. počínaje od cifer nejméně důležitých); a dochází při něm k přenosu cifer směrem doleva - ovšem v tomto případě počet přenášených cifer není pevný, ale závisí na délce vstupů.



Ze vstupních činitelů $x = \sum_{j=m}^{n} x_j \beta^j$ a $y = \sum_{j=m}^{n} y_j \beta^j$ s ciframi $x_j, y_j \in \mathcal{A}$ po zpracování dostaneme součin ve tvaru $z = x \cdot y = \sum_{j=m}^{2n} z_j \beta^j$ - tedy opět s ciframi z výchozí abecedy $z_j \in \mathcal{A}$, ale s až n pozicemi vlevo obsazenými navíc ve výstupním součinu (oproti vstupním činitelům).

Dělení

Při dělení je směr zpracování opačný - zleva doprava, tedy počínaje od nejvýznamnějších cifer. Počet cifer výsledného podílu ovšem není předem znám, a může být i nekonečný (ačkoliv při počítačové realizaci výpočtu se i takový případ omezí na konečný počet cifer, za cenu určité nepřesnosti výsledku).



Ze vstupního dělence $x = \sum_{j=m}^{n_1} x_j \beta^j$ a dělitele $y = \sum_{j=m}^{n_2} y_j \beta^j$ (který musí být nenulový) získáme podíl ve tvaru $z = x : y = \sum_{l}^{m-n_2} z_j \beta^j$, kde hodnota dolního indexu l není pevně dána.

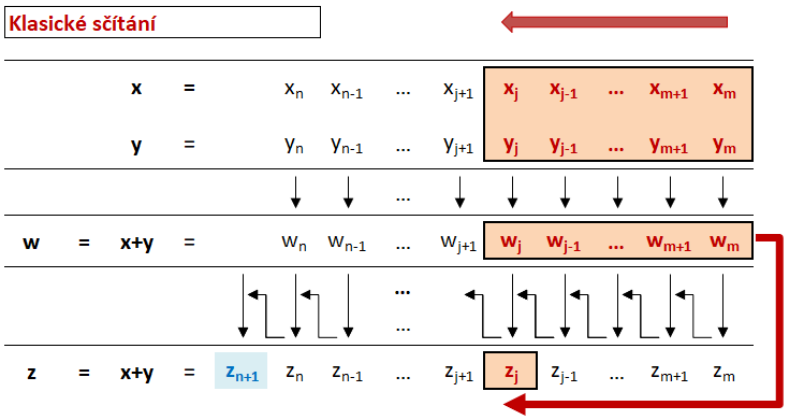
U všech těchto klasických algoritmů je vždy nutné před zahájením výpočtu znát vstupní operandy úplně celé, bez kompletní reprezentace vstupů nelze výpočet zahájit ani určit žádnou část výstupu. Je to dáno mj. tím, že klasické numerační systémy nedisponují žádnou redundancí - neboli možností vyjádřit stejné číslo pomocí více (konečných) reprezentací v $(\beta, \mathcal{A})$.

Princip redundance budeme využívat a podrobně ilustrovat v následujících kapitolách, kde představíme paralelní algoritmy pro sčítaní (resp. odčítaní) a on-line algoritmy pro násobení a dělení. Ty budou mít několik společných aspektů:

- jednak v nich není nutné znát vstupní operandy úplně celé, a přesto už lze postupně produkovat výstupní cifry (částečného) výsledku;
- můžeme postupovat od cifer nejvýznaměnjších (tj. zleva doprava) v případě on-line algoritmů, anebo dokonce počítat na všech pozicích zároveň v případě paralelních algoritmů.

7.2 Od sčítání klasického k paralelnímu

S myšlenkou paralelního sčítání v ceočíselných bázích $b \in \mathbb{N}, b > 2$ přišel jak první Avizienis v roce 1961 [3]. Jeho metodu rozšířili na systém s bázi $b = 2$ Chow a Robertson [9]. Před posunem ke sčítání paralelnímu ještě podrobněji rozepíšeme postup sčítání klasického:



Mějme numerační systém $(\beta, \mathcal{A})$, a v něm reprezentované sčítance $x = \sum_{j=m}^{n} x_j \beta^j$, $y = \sum_{j=m}^{n} y_j \beta^j$ s ciframi $x_j, y_j \in \mathcal{A}$.

Zavedeme samostatné značení také pro mezisoučet $w = x + y = \sum_{j=m}^{n} (x_j + y_j)\beta^j = \sum_{j=m}^{n} w_j \beta^j$ - tedy pro reprezentaci součtu $x + y$ v téže bázi, ale v abecedě $\mathcal{B} = \mathcal{A} + \mathcal{A} \ni w_j$.

Algoritmus pro sčítání dvou reprezentací x a y do součtové reprezentace z v numeračním systému $(\beta, \mathcal{A})$ tak vlastně převedeme na algoritmus konverze reprezentace w ze systému $(\beta, \mathcal{B} = \mathcal{A} + \mathcal{A})$ do reprezentace z v systému $(\beta, \mathcal{A})$.

Při klasickém sčítání lze (kvůli přenosům zprava) j-tou cifru z_j určit až poté, co byly určeny všechny předchozí cifry $z_{j-1}, \ldots, z_m$ vpravo, neboli

$$z_j = z_j(w_j, w_{j-1}, \ldots, w_m)\,. \tag{7.1}$$

Příklad 7.1. Klasické sčítání v numeračním systému $(\beta, \mathcal{A})$, s bází $\beta = 4$, s výchozí abecedou $\mathcal{A} = \{0, 1, 2, 3\}$, a se součtovou abecedou $\mathcal{B} = \mathcal{A} + \mathcal{A} = \{0, 1, \ldots, 5, 6\}$, ve které leží cifry mezisoučtové reprezentace $w_j \in \mathcal{A} + \mathcal{A} = \mathcal{B}$.

Postupně zprava doleva určujeme cifry z_j na základě $w_j, w_{j-1}, \ldots, w_m$ tak, aby $z_j \in \mathcal{A}$ a přitom byla zachována hodnota $z = w$. Nejprve tedy pro $j = m$, máme $z_m = z_m(w_m)$:

- je-li $w_m \in \{0, 1, 2, 3\}$, pak $z_m := w_m - 0$ a $q_m := 0$;
- je-li $w_m \in \{4, 5, 6\}$, pak $z_m := w_m - 4$ a $q_m := 1$.

Pro ostatní cifry na pozicích $j > m$ máme funkci $z_j = z_j(w_j, q_{j-1})$:

- je-li $(w_j + q_{j-1}) \in \{0, 1, 2, 3\}$, pak $z_j = w_j + q_{j-1}$ a $q_j = 0$;
- je-li $(w_j + q_{j-1}) \in \{4, 5, 6, 7\}$, pak $z_j = w_j - 4 + q_{j-1}$ a $q_j = 1$.

Výše uvedený postup lze jednotně zapsat ve tvaru

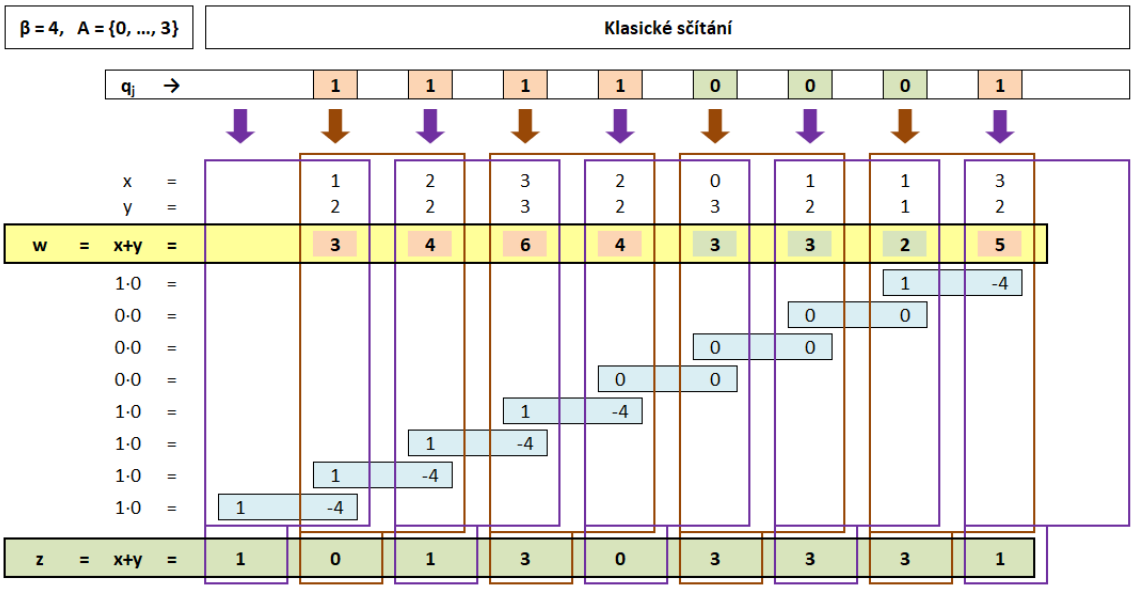
$$z_j := w_j - 4q_j + q_{j-1} = w_j - \beta q_j + q_{j-1} \in \mathcal{A}\,,$$

kde výše neurčené hodnoty q_j a w_j pro $j \notin \{n, \ldots, m\}$ jsou nulové. Takový zápis snadno ukazuje, že při této konverzi je zachována hodnota $z = w$:

$$z = \sum_j z_j \beta^j = \sum_j (w_j - \beta q_j + q_{j-1})\beta^j = \sum_j w_j \beta^j - \sum_j q_j \beta^{j+1} + \sum_j q_{j-1}\beta^j =$$
$$= w - \sum_j q_j \beta^{j+1} + \underbrace{\sum_j q_{j-1}\beta^j}_{\sum_l q_l \beta^{l+1}} = w\,;$$

tedy že $z = (z_{n+1} z_n \ldots z_m)_\beta$ skutečně je reprezentace součtu $(x + y) = w$ v numeračním systému $(\beta, \mathcal{A})$. Jsou totiž splněny všechny k tomu potřebné podmínky:

- hodnota $z = w = x + y$,
- cifry $z_j \in \mathcal{A}$ jsou ze správné abecedy,
- $z = (z_{n+1} z_n \ldots z_m)_\beta$ je konečná reprezentace.



Sčítáme-li klasicky, jsou v algoritmu tyto závislosti:

- $z_j = z_j(w_j, q_j, q_{j-1})$ a
- $q_j = q_j(w_j, q_{j-1})$, a následně
- $z_j = z_j(w_j, q_j, q_{j-1}, \ldots, q_m) = z_j(w_j, w_{j-1}, \ldots, w_m)$.

Ve sčítání paralelním, které představíme v následujícím textu, se zbavíme závislosti na dění na všech pozicích vpravo od pozice právě zpracovávané (j-té); a to při určování pomocných koeficientů q_j, čímž se závislost odstraní i z předpisu pro výsledné cifry z_j.

Původní zápis, kde řešíme sčítání dvou vstupů $x, y \in \mathrm{Fin}_{\mathcal{A}}(\beta)$, zjednodušíme - díky proveditelnosti kroku $w = \sum_j w_j \beta^j = \sum_j (x_j + y_j)\beta^j = x + y$ v konstantním čase, tj. bez ohledu na délku reprezentace sčítanců. Místo sčítání dvou reprezentací $x, y \in \mathrm{Fin}_{\mathcal{A}}(\beta)$ rovnou řešíme konverzi jediného vstupu $w \in \mathrm{Fin}_{\mathcal{A}+\mathcal{A}}(\beta)$ na $z \in \mathrm{Fin}_{\mathcal{A}}(\beta)$, resp. konverzi $w \in \mathrm{Fin}_{\mathcal{B}}(\beta)$ na $z \in \mathrm{Fin}_{\mathcal{A}}(\beta)$.

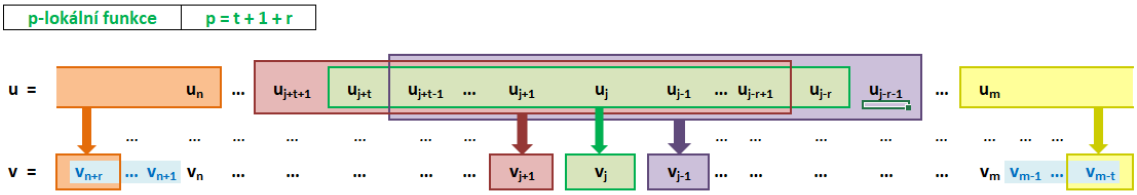
Definice 7.2. Nechť $\mathcal{A}$, $\mathcal{B}$ jsou abecedy, $\beta \in \mathbb{C}$ je báze a $\varphi : \mathcal{B}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$ je zobrazení řetězců cifer. Řekneme, že φ je p-lokální funkce konverze z $\mathcal{B}$ do $\mathcal{A}$ v bázi β, když existují $r, t \in \mathbb{N}_0$ a existuje $\phi : \mathcal{B}^p \to \mathcal{A}$ takové, že $p = r + t + 1$ a přitom

- $\varphi(u) = v = (v_j)_j \in \mathcal{A}^{\mathbb{Z}}$ splňuje $\forall u = (u_j)_j \in \mathcal{B}^{\mathbb{Z}}$ vztah

$$\sum_j u_j \beta^j = \sum_j v_j \beta^j, \text{ kde } v_j = \phi(u_{j+t}, \ldots, u_j, \ldots, u_{j-r}) \quad \forall j \in \mathbb{Z},$$

- $\varphi(\mathrm{Fin}_{\mathcal{B}}(\beta)) \subset \mathrm{Fin}_{\mathcal{A}}(\beta)$.

Přiložené schéma ilustruje působení takové p-lokální funkce - tedy jednak omezení závislosti výsledné cifry ve výstupu jen na několik (p) cifer vstupu; a také fakt, že délka výstupní reprezentace (po aplikaci p-lokální funkce) může být oproti vstupní reprezentaci širší, a to o maximálně r cifer vlevo a t cifer vpravo.



Příklad 7.3. Paralelní sčítání v numeračním systému $(\beta, \mathcal{A})$, kde báze $\beta = 4$, výchozí abeceda $\mathcal{A} = \{0, 1, \ldots, 5, 6\}$, a mezi-součtová abeceda $\mathcal{B} = \mathcal{A} + \mathcal{A} = \{0, 1, \ldots, 11, 12\}$. Hledáme p-lokální konverzi z $\mathcal{A}+\mathcal{A} = \mathcal{B}$ do $\mathcal{A}$ v bázi β. Mějme mezi-součet $w = \sum_j w_j \beta^j$ s ciframi $w_j \in \mathcal{B} = \mathcal{A}+\mathcal{A}$. Použijeme pomocné koeficienty $q_j \in Q = \{0, 1, 2, 3\}$ určené předpisem

$$q_j(w_j) = q_j := \begin{cases} 0 & \text{pokud } w_j \in \{0, 1, 2, 3\}, \\ 1 & \text{pokud } w_j \in \{4, 5, 6, 7\}, \\ 2 & \text{pokud } w_j \in \{8, 9, 10, 11\}, \\ 3 & \text{pokud } w_j \in \{12\}. \end{cases}$$

Výsledek po konverzi $z = \sum_j z_j \beta^j$ s ciframi $z_j \in \mathcal{A}$ je určen předpisem

$$z_j := \underbrace{(w_j - 4q_j)}_{\in\{0,1,2,3\}} + \underbrace{q_{j-1}}_{\in\{0,1,2,3\}} \in \{0, 1, \ldots, 5, 6\} = \mathcal{A}\Omega$$

Přitom $z_j = z_j(w_j, q_j, q_{j-1}) = z_j(w_j, q_j(w_j), q_{j-1}(w_{j-1})) = z_j(w_j, w_{j-1})$, tedy $p = r + t + 1 = 1 + 0 + 1 = 2$, a jedná se o 2-lokální konverzi.

Důležitá okolnost při paralelním sčítání je, že pro fungování p-lokální konverze se do numeračního systému musí zavést určitá míra redundance.

Definice 7.4. Redundance v numeračním systému $(\beta, \mathcal{A})$ znamená, že

$$\Big(\exists x \in \mathrm{Fin}_{\mathcal{A}}(\beta)\Big)\Big(x = \sum_{j=m}^{n} x_j\beta^j = \sum_{j=m'}^{n'} x'_j\beta^j \mid x_j, x'_j \in \mathcal{A} \text{ a přitom } (\exists j_0 \in \mathbb{Z})(x_{j_0} \neq x_{j_0})\Big).$$

Neboli existuje $x \in \mathrm{Fin}_{\mathcal{A}}(\beta)$, které má dvě různé konečné $(\beta, \mathcal{A})$ reprezentace.

Pro paralelní p-lokální sčítání je redundance numeračního systému podmínka nutná, ale ne postačující. Míra redundance pro paralelní sčítání ani není dána jednoznačně - různým mírám redundance (v numeračních systémech s toutéž bází β) odpovídají různé složitosti sčítacích algoritmů; čím vyšší míra redundance, tím jednodušší podoba algoritmu, a naopak. Viz ilustrace na příkladech 7.3 vs. 7.5.

Příklad 7.5. Paralelní sčítání v numeračním systému $(\beta, \mathcal{A})$ s bází $\beta = 4$, s výchozí abecedou $\mathcal{A} = \{0, 1, 2, 3, 4\}$, a se součtovou abecedou $\mathcal{B} = \mathcal{A} + \mathcal{A} = \{0, 1, \ldots, 7, 8\}$ pro cifry mezi-součtu $w_j \in \mathcal{B}$. Pomocné koeficienty $q_j \in Q = \{0, 1, 2\}$ mají závislost $q_j = q_j(w_j, w_{j-1})$ podle předpisu:

$$q_j := \begin{cases} 0 & \text{pokud } w_j \in \{0,1,2\} \\ 0 & \text{pokud } w_j \in \{3\} \text{ a zároveň } w_{j-1} \leq 3 \\ 1 & \text{pokud } w_j \in \{3\} \text{ a zároveň } w_{j-1} \geq 4 \\ 1 & \text{pokud } w_j \in \{4,5,6\} \\ 1 & \text{pokud } w_j \in \{7\} \text{ a zároveň } w_{j-1} \leq 3 \\ 2 & \text{pokud } w_j \in \{7\} \text{ a zároveň } w_{j-1} \geq 4 \\ 2 & \text{pokud } w_j \in \{8\} \end{cases}$$

Nakonec pro stanovení výsledných cifer z_j použijeme již známý předpis:

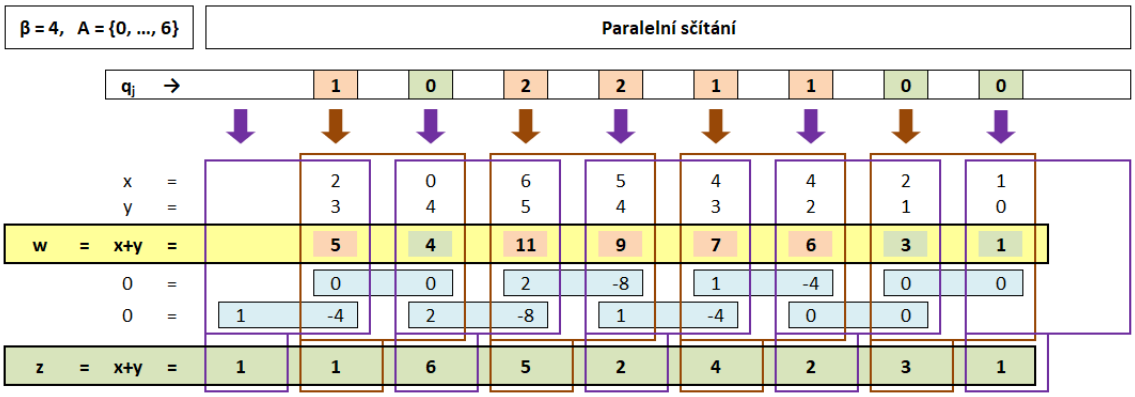
$$z_j := \underbrace{(w_j - 4q_j)}_{\in\{-1,\ldots,3\}} + \underbrace{q_{j-1}}_{\in\{0,1,2\}} \in \{0,1,2,3,4\} = \mathcal{A}$$

Přitom $z_j = z_j(w_j, q_j, q_{j-1}) = z_j(w_j, q_j(w_j, w_{j-1}), q_{j-1}(w_{j-1}, w_{j-2})) = z_j(w_j, w_{j-1}, w_{j-2})$, tedy $p = 2 + 0 + 1$, a máme zde 3-lokální konverzi.

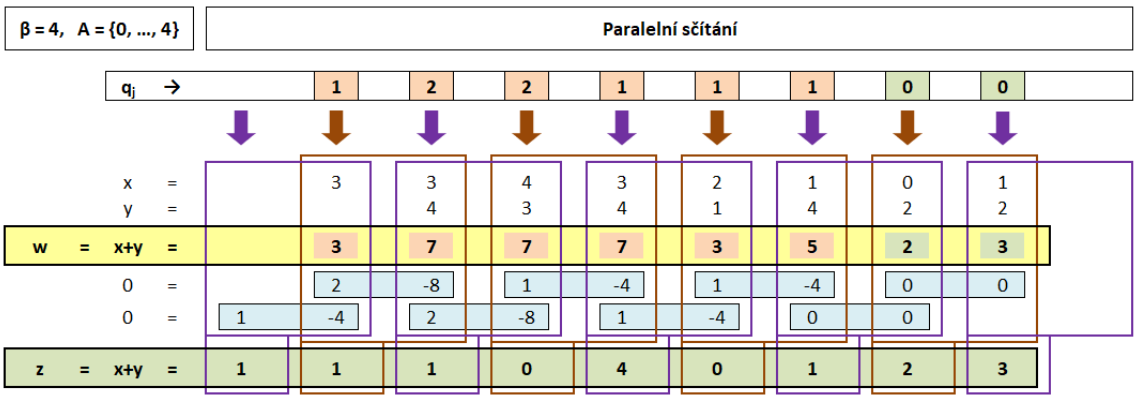
Porovnání příkladů 7.1 (klasický) vs. 7.3 a 7.5 (paralelní)

Je v ních stejná báze $\beta = 4$, ale různé abecedy s různou mírou redundance:

Příklad 7.3	**Příklad 7.5**	**Příklad 7.1**
$\mathcal{A} = \{0, 1, \ldots, 6\}$	$\mathcal{A} = \{0, 1, \ldots, 4\}$	$\mathcal{A} = \{0, 1, 2, 3\}$
$\#\mathcal{A} = 7 > \lvert\beta\rvert$	$\#\mathcal{A} = 5 > \lvert\beta\rvert$	$\#\mathcal{A} = 4 = \lvert\beta\rvert$
$p = 2$	$p = 3$	není redundantní, takže
		neexistuje p-lokální konverze



Obrázek 7.1: ad příklad 7.3 - paralelní sčítání v numeračním systému $(\beta, \mathcal{A}) = (4, \{0, \ldots, 6\})$



Obrázek 7.2: ad příklad 7.5 - paralelní sčítání v numeračním systému $(\beta, \mathcal{A}) = (4, \{0, \ldots, 4\})$

Poznámka 7.6. V příkladech 7.3 a 7.5 se pro paralelní sčítání pomocí p-lokální funkce používá sice stejný předpis pro výpočet výsledné cifry $z_j = w_j - \beta q_j + q_{j-1}$ jako v klasickém (neparalelním) příkladě 7.1, ale klíčový rozdíl je ve způsobu určení pomocných koeficientů q_j - tzv. přenosů ("carry propagation"). Pro klasické neparalelní sčítaní platí závislost $q_j = q_j(w_j, w_{j-1}, \ldots, w_m)$

- tedy na všech předchozích pozicích vpravo; zatímco pro paralelní sčítání jen omezená závislost $q_j = q_j(w_{j+t,\dots,w_j,\dots,w_{j-r+1}})$ - tedy na pevném počtu sousedních cifer (vpravo i vlevo).

Příklad 7.7. První obecné výsledky o paralelním sčítání formuloval A. Avizienis: totiž pro celočíselné báze $\beta = b \geq 3, b \in \mathbb{N}$, s abecedami ve tvaru $\mathcal{A} = \{-a, \dots, 0, \dots, a\}$, kde $\frac{b}{2} < a \leq b-1$. Vstupní sčítance značíme obvyklým způsobem: $x = \sum x_j \beta^j$, $y = \sum y_j \beta^j$ s ciframi $x_j, y_j \in \mathcal{A}$. Postup sčítání je pak následující:

- nejdřív pro všechna $j \in \mathbb{Z}$ zároveň spočítat mezi-součtové cifry w_j:

$$w_j = x_j + y_j \in \mathcal{A} + \mathcal{A} = \{-2a, \dots, 0, \dots, 2a\}\,;$$

- pak pro všechna $j \in \mathbb{Z}$ zároveň určit koeficienty $q_j \in \{-1, 0, 1\}$ s jednoduchou závislostí $q_j = q_j(w_j)$, tj. bez ohledu na sousední pozice:

$$q_j = \begin{cases} 1 & \text{pokud} \quad w_j \geq a\,, \\ 0 & \text{pokud} \quad -a < w_j < a\,, \\ -1 & \text{pokud} \quad w_j \leq -a\,; \end{cases}$$

- a nakonec, opět pro všechna $j \in \mathbb{Z}$ zároveň, dopočet výsledných cifer $z_j = w_j - \beta q_j + q_{j-1} = w_j - bq_j + q_{j-1} = z_j(w_j, q_j(w_j), q_{j-1}(w_{j-1})) = z_j(w_j, w_{j-1})$, tedy p-lokalita s $p = 2$.

Ukážeme, že tento algoritmus funguje - tedy že výsledné cifry leží ve správné abecedě $\mathcal{A} \ni z_j$:

- Pokud $-a < w_j < a$, tak

$$z_j = w_j - b \cdot 0 + q_{j-1} \in \{-a+1, \dots, a-1\} + \{-1, 0, 1\} = \{-a, \dots, a\} = \mathcal{A}.$$

- Pokud $w_j \geq a$, pak

$$z_j = w_j - b \cdot 1 + q_{j-1} \in \{a, \dots, 2a\} - b + \{-1, 0, 1\} = \{\underbrace{a-b-1}_{C}, \dots, \underbrace{2a-b+1}_{D}\}.$$

  Přitom platí

$$\frac{b}{2} < a \implies b < 2a \implies b \leq 2a - 1 \implies -b \geq -2a + 1,$$

  a odtud dostáváme

$$C = a + (-b) - 1 \geq a + (-2a + 1) - 1 = -a$$

$$D = 2a - b + 1 = a + a - b + 1 \leq (b-1) + a - b + 1 = a,$$

a tedy

$$\{a - b - 1, \ldots, 2a - b + 1\} = \{C, \ldots, D\} \subseteq \{-a, \ldots, a\} = \mathcal{A}.$$

- Pro $w_j \leq -a$ bychom ověření provedli analogickým postupem.

Příklad 7.8. Avizienisův algoritmus pro bázi $\beta = b = 4$ s co nejmenší abecedou, kterou určíme z podmínky $\frac{b}{2} < a \leq b - 1$:

$$2 = \frac{4}{2} = \frac{b}{2} < a \leq b - 1 = 4 - 1 = 3 \quad \Longrightarrow \quad a := 3\,, \text{ tedy } \mathcal{A} = \{-3, \ldots, 3\}, \quad \#\mathcal{A} = 7.$$

Dál bude paralelní sčítací algoritmus pracovat analogicky jako v příkladu 7.3, který využívá abecedu $\mathcal{A} = \{0, \ldots, 6\}$ stejné velikosti $\#\mathcal{A} = 7$ a má stejnou p-lokalitu $p = 2$.

Poznámka 7.9. Redundantní abecedu $\{-5, -4, \ldots, 4, 5\}$ pro decimální soustavu používal už Cauchy [8], který své výpočty prováděné v klasické decimální soustavě kontroloval výpočtem s redundantní abecedou. Cauchy také konstatoval, že v rozšířené abecedě je pouze malo přenosů cifry na sousední pozici.

Kapitola 8

Redundantní poziční soustavy s algebraickou bází

Zaměříme se postupně na otázky směřující k získání dalších výsledků / obecnějších algoritmů pro paralelní sčítání:

- Které báze $\beta \in \mathbb{C}$ vůbec umožňují paralelní sčítání?
- Které abecedy $\mathcal{A} \subset \mathbb{Z}$ (resp. $\mathcal{A} \subset \mathbb{Z}[\omega]$) pro danou bázi $\beta \in \mathbb{C}$ umožňují paralelní sčítání? Hledáme minimální velikost takové abecedy $\mathcal{A}$, a příslušný algoritmus paralelního sčítání.

Klíčovým nástrojem k sestrojení algoritmu paralelního sčítání je tzv. přepisovací pravidlo / reprezentace nuly pro příslušnou bázi β, kde přepisovací pravidlo obsahuje tzv. dominantní koeficient. Takové přepisovací pravidlo je vlastně jen vhodné vyjádření nuly (v bázi β), které lze při konverzi abeced přičíst či odečíst v libovolném násobku, za účelem dospění do cílové abecedy.

8.1 Paralelní sčítání využívající silné a slabé reprezentace nuly

Dosud jsme pracovali jen s přirozenými bázemi $\beta \in \mathbb{N}$ a s jediným přepisovacím pravidlem ve tvaru $[1, -\beta]$, což je zkrácený zápis pro výraz $1 \cdot \beta^{j+1} - \beta \cdot \beta^j = 0$. Nyní tento pojem zobecníme:

Definice 8.1. Buď $\beta \in \mathbb{C}$, $|\beta| > 1$. Říkáme, že β má reprezentaci nuly s dominantním koeficientem, když existují $b_k, b_{k-1}, \ldots, b_0, b_{-1}, \ldots, b_{-h+1}, b_{-h}$ takové, že platí

$$b_k\beta^k + b_{k-1}\beta^{k-1} + \cdots + b_0\beta^0 + \cdots + b_{-h}\beta^{-h} = 0$$

a navíc existuje $t \geq 1$ takové, že

$$b_0 > t \cdot \sum_{\substack{j=-h \\ j\neq 0}}^{k} |b_j|.$$

Speciálně pro $t = 1$ je reprezentace nuly takzvaně *slabá* (WRZ = Weak Representation of Zero), pro $t = 2$ hovoříme o *silné* reprezentaci (SRZ = Strong Representation of Zero).

Věta 8.2. *(SRZ-algoritmus) Nechť $\beta \in \mathbb{C}$, $|\beta| > 1$ má silnou reprezentaci nuly ve tvaru*

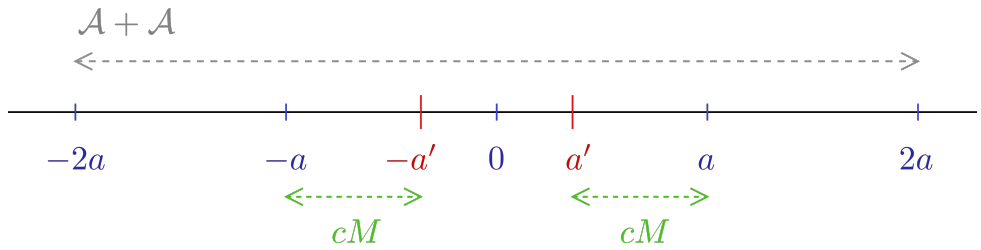
$$S(x) = b_k x^k + \cdots + b_0 x^0 + \cdots + b_{-h} x^{-h}, \qquad b_j \in \mathbb{Z},$$

kde při značení $B = b_0$, $M = \sum_{\substack{j=-h \\ j\neq 0}}^{k} |b_j|$ platí $B > 2M$. Pak existuje algoritmus paralelního sčítání v numeračním systému $(\beta, \mathcal{A})$ s abecedou $\mathcal{A} = \{-a, \ldots, a\}$ pro $a = \left\lceil \frac{B-1}{2} \right\rceil + M \left\lceil \frac{B-1}{2(B-2M)} \right\rceil$.

Důkaz. Přímo nalezneme potřebný algoritmus, pročež si označíme pomocné parametry

$$a' := \left\lceil \frac{B-1}{2} \right\rceil \qquad\qquad c := \left\lceil \frac{B-1}{2(B-2M)} \right\rceil,$$

tedy $a = a' + cM$. Dále značíme tzv. vnitřní abecedu jako $\mathcal{A}' := \{-a', \ldots, 0, \ldots, a'\}$.



Postup algoritmu je pak následující:

- Vstupy / sčítence mají tvar $x = \sum_{j=m}^{n} x_j \beta^j$ a $y = \sum_{j=m}^{n} y_j \beta^j$, kde $x_j, y_j \in \mathcal{A}$.
- Mezi-součet $w = x + y = \sum_{j=m}^{n} (x_j + y_j)\beta^j = \sum_{j=m}^{n} w_j \beta^j$, kde $w_j \in \mathcal{A} + \mathcal{A}$.
- Určení koeficientů $q_j \in \{-c, \ldots, c\} = Q$ tak, aby platilo $w_j - q_j \beta \in \mathcal{A}' = \{-a', \ldots, a'\}$.
- Cifry mezi-součtu w_j i koeficienty q_j lze získat pro všechny pozice $j \in \{m, \ldots, n\}$ paralelně; a stejně tak i cifry výsledné reprezentace z:
- Výstupní cifry se vypočtou podle vzorce

$$z_j := w_j - \sum_{l=h}^{k} q_{j-l} b_l \tag{8.1}$$

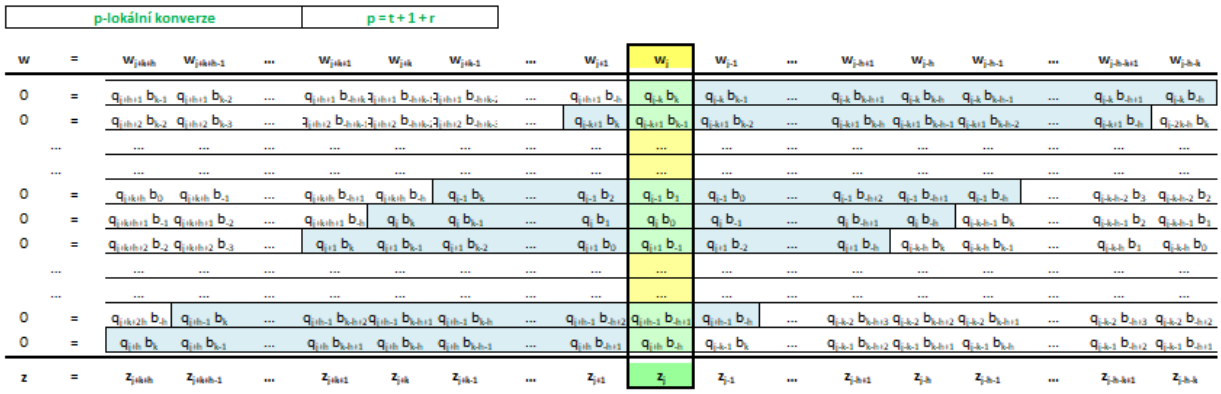
a leží v abecedě $\mathcal{A} \ni z_j$, protože platí

$$|z_j| = \left| w_j - q_j b_0 - \sum_{\substack{l=-h \\ l\neq 0}}^{k} q_{j-l} b_l \right| \leq |w_j - q_j B| + \sum_{\substack{l=-h \\ l\neq 0}}^{k} |q_{j-l}||b_l| \leq$$

$$\leq a' + c \sum_{\substack{l=-h \\ l\neq 0}}^{k} |b_l| = a' + cM = a\,.$$

Určení $q_j \in Q$ je možné díky tomu, že šířka vnitřní abecedy je $\mathcal{A}' = 2a'+1$, a tak se jistě dá do $\mathcal{A}'$ trefit alespoň jedním bodem ve tvaru $w_j - q_j B \in \mathbb{Z}$, protože $B \leq 2a'+1$ (z definice $a' = \lceil \frac{B-1}{2} \rceil$).

Zachování hodnoty zpracovávané reprezentace, tj. $z = w$, je zajištěno díky tomu, že dochází pouze k přičítání vhodných q_j-násobků reprezentace nuly - viz ilustrace:



Anebo v podrobném zápisu sumace takto:

$$z = \sum_{j=m-h}^{n+k} z_j \beta^j = \sum_{j=m-h}^{n+k} \left(w_j - \sum_{l=-h}^{k} q_{j-l} b_l \right) \beta^j = \sum_{j=m-h}^{n+k} w_j \beta^j - \sum_{j=m-h}^{n+k} \sum_{l=-h}^{k} q_{j-l} b_l \beta^j =$$

$$= w - \sum_{j=m-h}^{n+k} \sum_{l=-h}^{k} b_l \beta^l q_{j-l} \beta^{j-l} = w - \sum_{s\in\mathbb{Z}} \underbrace{\left(\sum_{l=-h}^{k} b_l \beta^l \right)}_{=0} q_s \beta^s = w - \sum_{s\in\mathbb{Z}} 0 \cdot q_s \beta^s = w - 0 = w,$$

kde $q_s = 0$ pro $s \notin \{m-h, \ldots, n+k\}$, a $\sum_{l=-h}^{k} b_l \beta^l = 0$, protože β je kořenem SRZ.

Pro určení p-lokality funkce v algoritmu díky závislosti $q_j = q_j(w_j)$ platí

$$z_j = z_j(w_j, q_{j-k}, \ldots, q_j, \ldots, q_{j+h}) = z_j(w_j, q_{j-k}(w_{j-k}), \ldots, q_j(w_j), \ldots, q_{j+h}(w_{j+h})) =$$
$$= z_j(w_{j+h}, \ldots, w_j, \ldots, w_{j-k}) \implies p = h + 1 + k\,.$$

□

Příklad 8.3. Paralelní sčítání pomocí SRZ-algoritmu, v bázi β, která je největším kořenem polynomu $2\beta^3 - 9\beta^2 - \beta + 1$. Máme zde tedy rovnou k dispozici silnou reprezentaci nuly ve tvaru

$S(x) = -2x + 9 + x^{-1} - x^{-2}$, tedy $k = 1$, $h = 2$, a dominantní koeficient má hodnotu 9. Dále

$$B = b_0 = 9 \qquad M = \sum_{j \neq 0} |b_j| = |2| + |1| + |1| = 4$$

$$a' = \left\lceil \frac{B-1}{2} \right\rceil = \left\lceil \frac{9-1}{2} \right\rceil = 4 \qquad c = \left\lceil \frac{B-1}{2(B-2M)} \right\rceil = \left\lceil \frac{9-1}{2(9-8)} \right\rceil = 4.$$

Výchozí abeceda numeračního systému je $\mathcal{A} = \{-20, \ldots, 0, \ldots, 20\}$, pomocná vnitřní abeceda $\mathcal{A}' = \{-4, \ldots, 0, \ldots, 4\}$, a koeficienty q_j jsou z množiny $Q = \{-4, \ldots, 0, \ldots, 4\} = \{-c, \ldots, 0, \ldots, c\}$.

Algoritmus paralelního sčítaní začne od mezi-součtu $w = x + y$:

$$w = \sum_j w_j \beta^j = \sum_j (x_j + y_j)\beta^j, \quad \text{kde } w_j \in \mathcal{A} + \mathcal{A} = \{-40, \ldots, 0, \ldots, 40\}.$$

Pro všechna j paralelně určíme $q_j \in Q = \{-4, \ldots, 0, \ldots, 4\}$ takto:

$$q_j := \begin{cases} 4 & \text{pro } w_j \in \{32, \ldots, 40\} \\ 3 & \text{pro } w_j \in \{23, \ldots, 31\} \\ 2 & \text{pro } w_j \in \{14, \ldots, 22\} \\ 1 & \text{pro } w_j \in \{5, \ldots, 13\} \\ 0 & \text{pro } w_j \in \{-4, \ldots, 4\} \end{cases}$$

a symetricky pro záporná $w_j \in \{-40, \ldots, 0\}$. Tím je splněno

$$w_j - Bq_j = w_j - 9q_j \in \{-4, \ldots, 0, \ldots, 4\} = \mathcal{A}'.$$

Dále pro všechna j paralelně určíme $z_j \in \mathcal{A} = \{-20, \ldots, 0, \ldots, 20\}$ předpisem

$$\begin{aligned} z_j &:= w_j - \sum_{l=-2}^{1} q_{j-l} b_l = w_j - (q_{j+2}b_{-2} + q_{j+1}b_{-1} + q_j b_0 + q_{j-1}b_1) = \\ &= w_j - (-q_{j+2} + q_{j+1} + 9q_j - 2q_{j-1}) = \\ &= \underbrace{(w_j - 9q_j)}_{\in \mathcal{A}'} + \underbrace{(q_{j+2} - q_{j+1} + 2q_{j-1})}_{Q+Q+2Q} \in \mathcal{A}' + Q + Q + 2Q = \mathcal{A}. \end{aligned}$$

Výše uvedený SRZ-algoritmus má sice docela snadný výpočetní předpis, ale zato funguje na relativně velkých abecedách. Dále se snažíme pracovat s abecedami menší velikosti, za cenu trochu složitějšího výpočetního postupu - např. pomocí tzv. WRZ-algoritmu (který využívá slabé reprezentaci nuly).

Věta 8.4. *(WRZ-algoritmus) Nechť $\beta \in \mathbb{C}$, $|\beta| > 1$ má slabou reprezentaci nuly ve tvaru*

$$W(x) = b_k x^k + \cdots + b_0 x^0 + \cdots + b_{-h} x^h, \qquad b_j \in \mathbb{Z},$$

kde značíme $B = b_0$, $M = \sum_{\substack{j=-h \\ j\neq 0}}^{k} |b_j|$ a platí $B > M$. Pak existuje algoritmus paralelního sčítání v numeračním systému $(\beta, \mathcal{A})$ s abecedou $\mathcal{A} = \{-a, \ldots, 0, \ldots, a\}$ pro $a = \left\lceil \frac{B-1}{2} \right\rceil + M$.

Důkaz. Přímo nalezneme takový algoritmus. Označíme $a' := \left\lceil \frac{B-1}{2} \right\rceil$, takže $a = a' + M$, a opět používáme tzv. vnitřní abecedu ve tvaru $\mathcal{A}' = \{-a', \ldots, 0, \ldots, a'\}$.
Postup algoritmu je následující:

- Vstupy / sčítance mají tvar $x = \sum_{j=m}^{n} x_j \beta^j$ a $y = \sum_{j=m}^{n} y_j \beta^j$, kde $x_j, y_j \in \mathcal{A}$.
- Z nich vytvoříme (pro všechny pozice j zároveň) cifry mezi-součtu $w = x + y = \sum_{j=m}^{n} (x_j + y_j)\beta^j = \sum_{j=m}^{n} w_j \beta^j$, kde $w_j = x_j + y_j = \in \mathcal{A} + \mathcal{A}$.
- Výpočet pomocných koeficientů i výsledných cifer proběhne v s cyklech, kde $s := \left\lceil \frac{a}{B-M} \right\rceil$. Postupně pro $i = 1, \ldots, s$ provádíme dvojici kroků, a to na všech pozicích j zároveň:
  - určení $q_j \in \{-1, 0, 1\} = Q$ předpisem

$$q_j := \begin{cases} 0 & \text{pro } w_j \in \mathcal{A}' \\ \operatorname{sgn}(w_j) & \text{pro } w_j \notin \mathcal{A}' \end{cases}$$

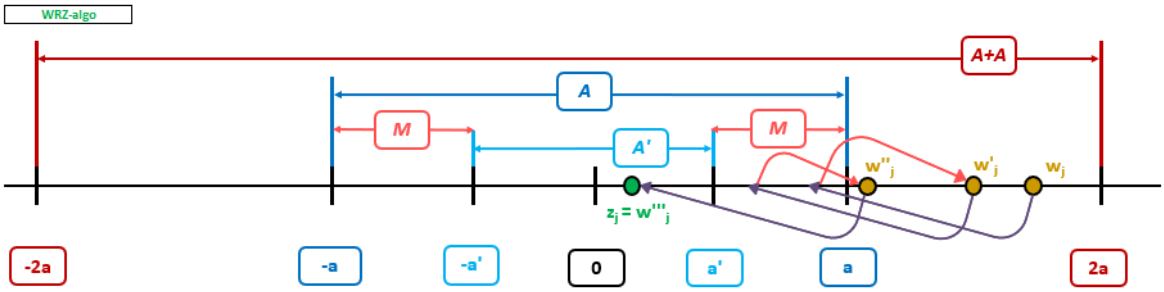
  - a dopočtem $w_j := w_j - \sum_{l=-h}^{k} q_{j-l} b_l$.
- Nakonec, po s provedeních cyklu, obdržíme konečný výsledek $z = \sum_{j=m-sh}^{n+sk} z_j \beta^j$ s ciframi $z_j \in \mathcal{A}$, kde $z_j := w_j$ z posledního s-tého cyklu.
- V každé iteraci ($i = 1, \ldots, s-1$) se maximální velikost cifer $|w_j|$ zmenší o hodnotu $(B - M) \geq 1$, díky nerovnosti:

$$\begin{aligned} |z_j| &= \left| w_j - q_j b_0 - \sum_{\substack{l=-h \\ l\neq 0}}^{k} q_{j-l} b_l \right| \leq |w_j - q_j B| + \sum_{\substack{l=-h \\ l\neq 0}}^{k} \underbrace{|q_{j-l}|}_{\in Q=\{-1,0,1\}} |b_l| \leq \\ &\leq |w_j - q_j B| + \sum_{\substack{l=-h \\ l\neq 0}}^{k} |b_l| = |w_j - q_j B| + M\,. \end{aligned}$$

  Níže uvedená ilustrace ukazuje působení jednotlivých cyklů na cifry w_j: malé cifry w_j už leží přímo v $\mathcal{A}'$, zatímco větší cifry se k $\mathcal{A}'$ přiblíží o hodnotu $(B - M)$ při každém provedení

cyklu. V poslední iteraci $i = s$ už bude $|w_j - q_j B| \leq a'$, a tedy $z_j \in \mathcal{A}$:

$$|z_j| \leq \underbrace{|w_j - q_j B|}_{\in \mathcal{A}'} + M \leq a' + M = a\,.$$



- Zachování hodnoty reprezentace $z = \sum_j z_j \beta^j = \sum_j (x_j + y_j)\beta^j = x + y$ při aplikaci WRZ-algoritmu lze ukázat analogicky jako pro algoritmus SRZ.
- Pro vyhodnocení p-lokality funkce ve WRZ-algoritmu si uvědomíme jednoduchou závislost $q_j = q_j(w_j)$. V každé iteraci, kterých je dohromady s, platí:

$$z_j = z_j(w_j, q_{j-k}(w_{j-k}), \ldots, q_{j+h}(w_{j+h})) = z_j(w_{j+h}, \ldots, w_j, \ldots, w_{j-k})\,,$$

tedy v kadém jednotlivém cyklu je dílčí $\widetilde{p} = h{+}k{+}1$, a za s cyklů pak celkové $p = s(h{+}k){+}1$.

□

Příklad 8.5. Paralelní sčítání pomocí WRZ-algoritmu, ve stejné bázi β jako v příkladu 8.3 (neboť SRZ je rovnou také WRZ) - tedy platí:

$$2\beta^3 - 9\beta^2 - \beta + 1 = 0 \qquad\qquad k = 1,\ h = 2\,.$$

Slabá (ale i silná) reprezentace nuly je $W(x) = -2x + 9 + x^{-1} - x^{-2}$. Dále platí

$$B = b_0 = 9 \qquad\qquad M = \sum_{j \neq 0} |b_j| = |2| + |1| + |1| = 4$$

$$a' = \left\lceil \frac{B-1}{2} \right\rceil = \left\lceil \frac{9-1}{2} \right\rceil = 4 \qquad\qquad s = \left\lceil \frac{a}{B-M} \right\rceil = \left\lceil \frac{8}{9-4} \right\rceil = 2$$

$$a = a' + M = 4 + 4 = 8 \qquad\qquad \mathcal{A} = \{-8, \ldots, 0, \ldots, 8\}.$$

Pro paralelní konverzi z $\mathcal{A} + \mathcal{A} = \{-16, \ldots, 0, \ldots, 16\}$ jsou potřebné $s = 2$ iterace:

- První iterace: výchozí $w_j \in \mathcal{A}+\mathcal{A} = \{-16,\dots,0,\dots,16\}$, pro všechna j zároveň určíme

$$q_j := \begin{cases} 1 & \text{pro } w_j \in \{5,\dots,16\} \\ 0 & \text{pro } w_j \in \{-4,\dots,0,\dots,4\} = \mathcal{A}' \\ -1 & \text{pro } w_j \in \{-16,\dots,-5\}\,, \end{cases}$$

$$\begin{aligned} w_j &:= (w_j - Bq_j) - (q_{j+2}b_{-2} + q_{j+1}b_{-1} + q_{j-1}b_1) = \\ &= \underbrace{(w_j - 9q_j)}_{\in\{-7,\dots,7\}} - \underbrace{(-q_{j+2} + q_{j+1} - 2q_{j-1})}_{\in\{-4,\dots,4\}} \in \{-11,\dots,0,\dots,11\}\,. \end{aligned}$$

- Druhá iterace: výchozí $w_j \in \{-11,\dots,0,\dots,11\}$, pro všechna j zároveň určíme

$$q_j := \begin{cases} 1 & \text{pro } w_j \in \{5,\dots,11\} \\ 0 & \text{pro } w_j \in \{-4,\dots,0,\dots,4\} = \mathcal{A}' \\ -1 & \text{pro } w_j \in \{-11,\dots,-5\}\,, \end{cases}$$

$$z_j := \underbrace{(w_j - 9q_j)}_{\in\{-4,\dots,4\}} - \underbrace{(-q_{j+2} + q_{j+1} - 2q_{j-1})}_{\in\{-4,\dots,4\}} \in \{-8,\dots,0,\dots,8\} = \mathcal{A}.$$

Při porovnání velikosti abeced $\mathcal{A}$ versus lokalit p pro SRZ-algoritmus a WRZ-algoritmus v téže bázi $2\beta^3 - 9\beta^2 - \beta + 1 = 0$ vidíme, že větší velikosti abecedy $\mathcal{A}$ odpovídá menší p-lokalita (tj. jednodušší výpočetní formule v algoritmu):

Příklad 8.3	**Příklad 8.5**
$p = k + 1 + h = 1 + 1 + 2 = 4$	$p = s(k+h) + 1 = 2(1+2) + 1 = 7$
$\#\mathcal{A} = 41$	$\#\mathcal{A} = 17$

Pozorování 8.6. Obecný algoritmus pro paralelní sčítání na abecedě $\mathcal{A}$ pomocí p-lokální funkce lze technicky realizovat jako vyhledávání v tabulce (tzv. Lookup Table = LuT) o velikosti

$$\#(LuT) = (\#(\mathcal{A}+\mathcal{A}))^p\,.$$

Vyhledané p-tici cifer z výchozí abecedy $\mathcal{A}+\mathcal{A}$ přiřadíme výslednou cifru $z_j \in \mathcal{A}$ z cílové abecedy:

$$(\#(\mathcal{A}+\mathcal{A}))^p \ni (w_{j+t},\dots,w_j,\dots,w_j - r) \quad \mapsto \quad z_j = z_j(w_{j+t},\dots,w_{j-r}) \in \mathcal{A}\,.$$

Pozorování 8.7. Pro realizaci algoritmu paralelního sčítání na abecedě $\mathcal{A}$ není nutno vytvořit přímo předpis pro paralelní konverzi z $(\mathcal{A}+\mathcal{A})$ do $\mathcal{A}$. Místo toho stačí zvolit množinu $\mathcal{D}$ takovou, že platí

$$\mathcal{A}+\underbrace{\mathcal{D}+\mathcal{D}+\cdots+\mathcal{D}}_{d-\text{krát}}\supset\mathcal{A}+\mathcal{A},$$

a přitom existuje paralelní konverze z $\mathcal{A}+\mathcal{D}$ do $\mathcal{A}$. Tuto paralelní konverzi (z $\mathcal{A}+\mathcal{D}$ do $\mathcal{A}$) pak použijeme d-krát, a dostaneme kýžený výsledek.

Příklad 8.8. Pro výchozí abecedu $\mathcal{A}=\{-m,\ldots,0,\ldots,M\}\subset\mathbb{Z}$ po sobě jdoucích celý čísel, kde $m,M\in\mathbb{N}$, je součtová abeceda $\mathcal{A}+\mathcal{A}=\{-2m,\ldots,0,\ldots,2M\}$. Tu lze rozložit na $\mathcal{A}+\mathcal{A}\subset\mathcal{A}+\underbrace{\mathcal{D}+\mathcal{D}+\cdots+\mathcal{D}}_{d-\text{krát}}$ s použitím $\mathcal{D}=\{-1,0,1\}$, kde $d=\max\{M,m\}$. Zde stačí mít k dispozici paralelní konverzi z $\mathcal{A}+\mathcal{D}=\{-m-1,\ldots,M+1\}$ do $\mathcal{A}$, a použít ji d-krát po sobě.

Tvrzení 8.9. *Pokud existuje algoritmus paralelního sčítání v numeračním systému $(\beta,\mathcal{A})$ s celočíselnou abecedou $\mathcal{A}\subset\mathbb{Z}$, pak báze $\beta\subset\mathbb{C}$ je algebraické číslo.*

Důkaz. Předpokládáme existenci paralelní konverze z $\mathcal{A}+\mathcal{A}$ do $\mathcal{A}$, a uvažujeme výchozí reprezentaci $w=\sum_{j=m}^{n}w_j\beta^j$ s ciframi $w_j\in\mathcal{A}+\mathcal{A}$, kde alespoň jedna cifra $w_{j_0}\in(\mathcal{A}+\mathcal{A})\setminus\mathcal{A}$. Po provedení paralelní konverze dostaneme $z=\sum_{j=m-t}^{n+r}z_j\beta^j$, kde $z_j\in\mathcal{A}$ a přitom

$$\begin{aligned}z &= \sum_{j=m-t}^{n+r}z_j\beta^j=\sum_{j=m}^{n}w_j\beta^j=w\,,\ \text{nutně tedy}\\ z-w &= \sum_{j=m-t}^{n+r}\underbrace{(z_j-w_j)}_{=:v_j}\beta^j=\sum_{j=m-t}^{n+r}v_j\beta^j=0\,,\end{aligned}$$

kde $v_{j_0}=z_{j_0}-w_{j_0}\neq 0$, protože $z_{j_0}\in\mathcal{A}$, ale $w_{j_0}\notin\mathcal{A}$, a tak $z_{j_0}\neq w_{j_0}$. Tedy β je kořenem celočíselného polynomu $\sum_{j=m-h}^{n+k}v_j\beta^j$, který není nulový, proto β je algebraické číslo. □

8.2 Báze umožňující paralelní sčítání

Vraťme se ke dříve položené otázce, které báze $\beta\in\mathbb{C}$, $|\beta|>1$ vůbec umožňují paralelní sčítaní? Přitom uvažujeme celočíselné abecedy $0\in\mathcal{A}\subset\mathbb{Z}$. Nyní už tedy víme, že báze β pro paralelní sčítání nutně musí být algebraické číslo. Dále předvedeme postup, jak pro dané algebratické číslo hledat polynomy typu SRZ nebo WRZ - a pokud to je možné, pak takové algebraické číslo je vhodná báze pro paralelní sčítání (např. pomocí SRZ- nebo WRZ-algoritmu).

Věta 8.10. *Buď $\alpha\in\mathbb{C}$, $|\alpha|>1$ algebraické číslo stupně $d\in\mathbb{N}$ se sdruženými kořeny $\alpha_1,\alpha_2,\ldots,\alpha_d$ (včetně samotného α), kde $|\alpha_j|\neq 1$ pro všechna $j=1,\ldots,d$. Pak pro libovolné*

$t \geq 1$ *existuje celočíselný polynom* $Q(x) \in \mathbb{Z}[x]$ *ve tvaru* $Q(x) = a_0x^m + a_1x^{m-1} + \cdots + a_{m-1}x + a_m$ *a index* $j_0 \in \{1, \ldots, m\}$ *tak, že* $Q(\alpha) = 0$ *a přitom* $|a_{j_0}| > t \cdot \sum_{\substack{j=0 \\ j \neq j_0}}^{m} |a_j|$.

Poznámka 8.11. Takto získané $Q(x) \in \mathbb{Z}[x]$ je reprezentace nuly pro bázi α. Při volbě $t = 1$ získáme WRZ, při volbě $t = 2$ získáme SRZ.

Důkaz. Postupujeme konstruktivně - tedy pro zvolené $\alpha \in \mathbb{C}$ a $t \geq 1$ přímo vyrobíme hledaný polynom $Q(x) \in \mathbb{Z}[x]$. Nejprve označíme minimální polynom algebraického čísla α jako

$$H(x) = \underbrace{h_0}_{\neq 0} x^d + h_1x^{d-1} + \cdots + h_{d-1}x^1 + h_dx^0 \in \mathbb{Z}[x]\,;$$

vydělíme $H(x)$ koeficientem $h_0 \in \mathbb{Z} \setminus \{0\}$, a tak získaný polynom označíme $G(x) \in \mathbb{Q}[x]$:

$$\begin{aligned} G(x) := \frac{1}{h_0}H(x) &= x^d + \frac{h_1}{h_0}x^{d-1} + \cdots + \frac{h_{d-1}}{h_0}x^1 + \frac{h_d}{h_0}x^0 = \\ &= x^d + g_1x^{d-1} + \cdots + g_{d-1}x^1 + q_dx^0 = \prod_{j=1}^{d} (x - \alpha_j)\,. \end{aligned}$$

Pro matici společnici polynomu $G(x)$, kterou označíme $\mathbb{M}$ a má tvar

$$\mathbb{M} := \begin{pmatrix} -g_1 & 1 & 0 & \ldots & 0 \\ -g_2 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -g_{d-1} & 0 & 0 & \ldots & 1 \\ -g_d & 0 & 0 & \ldots & 0 \end{pmatrix} \in \mathbb{Q}^{d \times d}$$

platí, že $G(x)$ je $(-1)^d$-násobkem charakteristického polynomu $\chi(\mathbb{M})$:

$$\chi(\mathbb{M}) = \det(\mathbb{M} - x\mathbb{I}) = \begin{vmatrix} -g_1 - x & 1 & 0 & \ldots & 0 \\ -g_2 & -x & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -g_{d-1} & 0 & 0 & \ldots & 1 \\ -g_d & 0 & 0 & \ldots & -x \end{vmatrix} =$$

$$= (-1)^{1+1}(-g_1 - x) \cdot \begin{vmatrix} -x & 1 & \ldots & 0 \\ 0 & -x & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & -x \end{vmatrix} + (-1)^{1+2} \cdot \begin{vmatrix} -g_2 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -g_{d-1} & 0 & \ldots & 1 \\ -g_d & 0 & \ldots & -x \end{vmatrix} =$$

$$= (-g_1 - x)(-x)^{d-1} - (-1)^{1+1}(-g_2) \cdot \begin{vmatrix} -x & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \\ 0 & 0 & \dots & -x \end{vmatrix} - (-1)^{1+2} \begin{vmatrix} -g_3 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -g_{d-1} & 0 & \dots & 1 \\ -g_d & 0 & \dots & -x \end{vmatrix} =$$

$$= (-1)^d x^d + (-1)^d g_1 x^{d-1} + (-1)^d g_2 x^{d-2} + \begin{vmatrix} -g_3 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -g_{d-1} & 0 & \dots & 1 \\ -g_d & 0 & \dots & -x \end{vmatrix} = \dots =$$

$$= (-1)^d \left(x^d + g_1 x^{d-1} + g_2 x^{d-2} + g_3 x^{d-3} + \dots + g_d \right) = (-1)^d \cdot G(x) \,.$$

Ze vztahu

$$\chi(\mathbb{M}) = \det(\mathbb{M} - x\mathbb{I}) = (-1)^d \cdot G(x) = (-1)^d \prod_{j=1}^{d} (x - \alpha_j)$$

víme, že všechny sdružené kořeny α_j jsou taky vlastními čísly matice-společnice $\mathbb{M}$. Odtud vyplývá, že α_j^n jsou vlastní čísla matice $\mathbb{M}^n$ pro všechna $n \in \mathbb{N}$. Označme

$$G_n(x) = \prod_{j=1}^{d} (x - \alpha_j^n) = x^d + g_1(n) x^{d-1} + \dots + g_{d-1}(n) x + g_d(n) \,, \text{ pro}$$

$$g_j(n) = (-1)^j \sum_{(i_1,\dots,i_j) \in S_j} \alpha_{i_1}^n \alpha_{i_2}^n \dots \alpha_{i_j}^n, \quad \text{kde } S_j = \{I \subset \{1,\dots,d\} \mid \#I = j\}.$$

Potom

$$\chi(\mathbb{M}) = \det(\mathbb{M}^n - x\mathbb{I}) = (-1)^d \cdot G_n(x) \in \mathbb{Q}[x].$$

Díky předpokladu $|\alpha_j| \neq 1$ pro všechna j můžeme kořeny α_j seřadit sestupně podle velikosti:

$$|\alpha_1| \geq |\alpha_2| \geq \dots \geq |\alpha_{j_H}| > 1 > |\alpha_{j_H+1}| \geq \dots \geq |\alpha_d| \,,$$

kde značíme $j_H = \max\{j \mid |\alpha_j| > 1\}$. Díky $|\alpha| > 1$ je $j_H \geq 1$, a pro každou j-tici $(i_1,\dots,i_j) \in S_j \setminus \{1,\dots,j_H\}$ platí

$$\left| \frac{\alpha_{i_j} \cdots \alpha_{i_j}}{\alpha_1 \cdots \alpha_{j_H}} \right| < 1.$$

Potom

$$\lim_{n\to\infty} \frac{\alpha_{i_1}^n \cdots \alpha_{i_j}^n}{\alpha_1^n \cdots \alpha_{j_H}^n} = \begin{cases} 0 & \text{pro všechna } (i_1,\dots,i_j) \in S_j \setminus \{1,\dots,j_H\} \\ 1 & \text{pro } (i_1,\dots,i_j) = (1,\dots,j_H). \end{cases}$$

Odtud

$$\lim_{n\to\infty}\frac{g_j(n)}{\alpha_1^n\cdots\alpha_{j_H}^n}=\lim_{n\to\infty}\frac{(-1)^j\sum_{I\in S_j}\alpha_{i_1}^n\alpha_{i_2}^n\dots\alpha_{i_j}^n}{\alpha_1^n\cdots\alpha_{j_H}^n}=\begin{cases}0 & \text{pro } j\neq j_H\\ (-1)^j & \text{pro } j=j_H\,,\end{cases}$$

kde $I=(i_1,\dots,i_j)$. Pro dané $t\geq 1$ tedy jistě nalezneme $n_0\in\mathbb{N}$ takové, že platí

$$\frac{|g_{j_H}(n_0)|}{|\alpha_1^{n_0}\cdots\alpha_{j_H}^{n_0}|}>t\cdot\sum_{\substack{j=1\\ j\neq j_H}}^{d}\frac{|g_j(n_0)|}{|\alpha_1^{n_0}\cdots\alpha_{j_H}^{n_0}|}\,,\ \text{a tedy}$$

$$|g_{j_H}(n_0)|>t\cdot\sum_{j\neq j_H}|g_j(n_0)|. \tag{8.2}$$

Tímto postupem obdržíme polynom

$$G_{n_0}(x)=\prod_{j=1}^{d}(x-\alpha_j^{n_0})=x^d+g_1(n_0)x^{d-1}+\cdots+g_d(n_0),$$

jehož kořeny jsou $\alpha_j^{n_0}$ a jehož koeficienty splňují vztah (8.2). Potom α_j jsou kořeny modifikovaného polynomu

$$G_{n_0}(y^{n_0})=\prod_{j=1}^{d}(y^{n_0}-\alpha_j^{n_0})=y^{n_0 d}+g_1(n_0)y^{n_0(d-1)}+\cdots+g_d(n_0),$$

při zavedení substituce $x=y^{n_0}$. Polynom $G_{n_0}(y^{n_0})$ má racionální koeficienty, převedeme ho do $\mathbb{Z}[y]$ vynásobením vhodným celým číslem K (které můžeme volit jako nejmenší společný násobek jmenovatelů všech $g_j(n_0)$). Potom hledaný výsledek má tvar

$$K\cdot G_{n_0}(y^{n_0})=Q(y)\in\mathbb{Z}[y]\qquad\qquad j_0:=n_0\cdot j_H\,.$$

□

Poznámka 8.12. Takto získaný polynom $Q(y)\in\mathbb{Z}[y]$ má sice stupeň $n_0 d$, ale přitom maximálně $d+1$ nenulových koeficientů. Při jeho použití v algoritmu paralelního sčítání lze fakticky pracovat v n_0 procesech nezávisle vedle sebe.

Příklad 8.13. Výše popsanou konstruktivní metodu aplikujeme na konkrétní bázi $\beta=\tau$, zlatý řez. Jeho minimální polynom a matice společnice mají tvar

$$H(x)=x^2-x-1=G(x)\quad,\quad\mathbb{M}=\begin{pmatrix}1&1\\1&0\end{pmatrix}.$$

Matici společnici $\mathbb{M}$ postupně umocňujeme

$$\mathbb{M}^2 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \qquad \mathbb{M}^3 = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix} \qquad \mathbb{M}^4 = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}.$$

a sledujeme charakteristické polynomy mocnin $\mathbb{M}^n$:

$$\begin{aligned} &\det(\mathbb{M}^2 - x\mathbb{I}) = x^2 - 3x + 1 \implies \text{WRZ pro } \tau \text{ je } W(x) = x^4 - 3x^2 + 1 \\ &\det(\mathbb{M}^3 - x\mathbb{I}) = x^2 - 4x - 1 \\ &\det(\mathbb{M}^4 - x\mathbb{I}) = x^2 - 7x + 1 \implies \text{SRZ pro } \tau \text{ je } S(x) = x^8 - 7x^4 + 1. \end{aligned}$$

Pro bázi zlatý řez jsme tedy dospěli k algoritmům paralelního sčítání WRZ a SRZ s parametry

SRZ	**WRZ**
$S(x) = x^8 - 7x^4 + 1$	$W(x) = x^4 - 3x^2 + 1$
$B = 7 > 2 \cdot 2 = 2M$	$B = 3 > 1 \cdot 2 = M$
$\mathcal{A} = \{-5, \ldots, 0, \ldots, 5\}$	$\mathcal{A} = \{-3, \ldots, 0, \ldots, 3\}$
$q_j \in Q = \{-1, 0, 1\}$	$q_j \in Q = \{-1, 0, 1\}$
$z_j = (w_j - 7q_j) + (q_{j-4} + q_{j+4})$	$z_j = (w_j - 3q_j) + (q_{j-2} + q_{j+2})$
běží v 1 iteraci	běží ve 3 iteracích
$p = k + 1 + h = 4 + 1 + 4 = 9$	$p = s(k + h) + 1 = 3(2 + 2) + 1 = 13.$

V případě SRZ se při rozdělení na 4 souběžné procesy (na pozicích $j = 4i$, $j = 4i+1$, $j = 4i+2$, $j = 4i + 3$) p-lokalita algoritmu sníží na $\tilde{p} = 1 + 1 + 1 = 3$, s vyhledávací tabulkou o velikosti $\#(LuT) = (\#(\mathcal{A}+\mathcal{A}))^{\tilde{p}} = 21^3 \approx 9,3 \cdot 10^3$. V případě WRZ se rozdělením na 2 souběžné procesy (pro pozice $j = 2i$, $j = 2i + 1$) p-lokalita algoritmu sníží na $\tilde{p} = 3(1 + 1) + 1 = 7$, a vyhledávací tabulka má (maximální) velikost $\#(LuT) = (\#(\mathcal{A} + \mathcal{A}))^{\tilde{p}} = 13^7 \approx 6,3 \cdot 10^7$.

Věta 8.10 ukazuje, že algebraické číslo, jehož všechny sdružené kořeny leží mimo jednotkovou kružnici, může být bází pro numerační systém s paralelním sčítáním. Následující tvzení adresují situaci opačnou - tedy algebraická čísla, která mají některý ze svých sdružených kořenů na jednotkové kružnici. Ukazuje se, že v takovém případě neexistuje algoritmus paralelního sčítání vůbec (bez ohledu na velikost abecedy).

Věta 8.14. *Buď $\beta \in \mathbb{C}$, $|\beta| > 1$ algebraické číslo se sdruženým kořenem $\gamma \in \mathbb{C}$, $|\gamma| = 1$. Buď $t \geq 1$ (libovolné). Pak β není kořenem žádného celočíselného polynomu $T(x) = \sum_{j=0}^{d} b_j \beta^j$ s vlastností $|b_0| > t \cdot \sum_{\substack{j=1 \\ j \neq j_0}}^{d}$ pro $j_0 \in \{0, \ldots, d\}$.*

Důkaz. Pro důkaz sporem předpokládejme, že existuje $T(x)$ s požadovanými vlastnostmi. Potom však nejen $T(\beta) = 0$, ale i $T(\gamma) = 0$, protože $T(x)$ je nutně dělitelný minimálním polynomem společným pro γ a β. Můžeme vyjádřit

$$b_{j_0}\gamma^{j_0} = -\sum_{j \neq j_0} b_j \gamma^j \,, \text{ a následně}$$

$$|b_0| = |b_{j_0}||\gamma|^{j_0} = |b_{j_0}\gamma^{j_0}| = \left| \sum_{j \neq j_0} b_j \gamma^j \right| \leq \sum_{j \neq j_0} |b_j||\gamma^j| = \sum_{j \neq j_0} |b_j| \leq t \cdot \sum_{j \neq j_0} |b_j| \,,$$

což je spor. □

Důsledek 8.15. *Buď $\beta \in \mathbb{C}$, $|\beta| > 1$ algebraické číslo. Pak β má SRZ, resp. WRZ, právě když β nemá žádný sdružený kořen γ na jednotkové kružnici.*

Poznámka 8.16. Algebraické číslo β i jeho sdružené kořeny γ mají stejné vlastnosti ohledně paralelního sčítání na celočíselné abecedě, neboť klíčovým nástrojem algoritmů paralelního sčítání jsou minimální polynom a jeho násobky v $\mathbb{Z}[x]$, což je pro β a γ společné.

Následující pomocné tvrzení (Lemma 8.17) využijeme dále k důkazu faktu, že pro algebraické číslo se sdruženým kořenem na jednotkové kružnici není paralelní sčítání vůbec možné.

Lemma 8.17. *Nechť $\gamma \in \mathbb{C}$ leží na jednotkové kružnici, tedy $|\gamma| = 1$. Pak existuje nekonečně mnoho $j \in \mathbb{N}$ takových, že $\mathrm{Re}(\gamma^j) \geq \frac{1}{2}$.*

Důkaz. Zapišme γ ako $\gamma = e^{i\varphi}$, kde $\varphi \in [-\pi, \pi]$, a označme $I = \left[-\frac{\pi}{3}, \frac{\pi}{3}\right]$. Pak

$$\mathrm{Re}\left(\gamma^j\right) \geq \frac{1}{2} \iff j\varphi \in \left[-\frac{\pi}{3}, \frac{\pi}{3}\right] + 2l\pi = I + 2l\pi \,, \text{ kde } l \in \mathbb{Z} \,.$$

Nejprve ukážeme, že pro každé $\varphi \in [-\pi, \pi]$ existuje $j \in \mathbb{N}$, $j > 1$ tak, že $j\varphi \in I + 2l\pi$ pro nějaké $l \in \mathbb{Z}$. Rozdělme interval $[-\pi, \pi]$ na části $\{0\}$, $\left(0, \frac{2\pi}{3}\right)$, $\left[\frac{2\pi}{3}, \frac{3\pi}{4}\right) = \left[\frac{8\pi}{12}, \frac{9\pi}{12}\right)$, $\left[\frac{9\pi}{12}, \frac{10\pi}{12}\right) = \left[\frac{3\pi}{4}, \frac{5\pi}{6}\right)$, $\left[\frac{5\pi}{6}, \pi\right] = \left[\frac{10\pi}{12}, \pi\right]$, $[-\pi, 0)$, a pro každou z nich nalezneme $j \in \mathbb{N} \setminus \{1\}$ splňující $j\varphi \in I + 2l\pi$.

1. Případ $\varphi = 0$ je triviální, $0 = j\varphi \in I$ pro všechna $j \in \mathbb{N}$.
2. Pro $\varphi \in \left(0, \frac{2\pi}{3}\right)$ určíme hledané $j \in \mathbb{N} \setminus \{1\}$ předpisem $j := \lceil \frac{1}{\varphi} \cdot \frac{5\pi}{3} \rceil$. Tedy j je nejmenší přirozené číslo, pro které platí $j\varphi \geq \frac{5\pi}{3}$. Určitě $j > 1$, protože $j \geq \frac{1}{\varphi} \cdot \frac{5\pi}{3} > \frac{3}{2\pi} \cdot \frac{5\pi}{3} = \frac{5}{2} > 1$. Dále víme, že $\frac{5\pi}{3} \leq j\varphi < \frac{5\pi}{3} + \varphi < \frac{5\pi}{3} + \frac{2\pi}{3} = \frac{7\pi}{3}$, a tedy $j\varphi \in I + 2\pi$.
3. Pro $\varphi \in \left[\frac{2\pi}{3}, \frac{3\pi}{4}\right) = \left[\frac{8\pi}{12}, \frac{9\pi}{12}\right)$ platí $3\varphi \in I + 2\pi$, tedy $j := 3$.

4. Pro $\varphi \in \left[\frac{3\pi}{4}, \frac{5\pi}{6}\right) = \left[\frac{9\pi}{12}, \frac{10\pi}{12}\right)$ platí $5\varphi \in I + 4\pi$, tedy $j := 5$.

5. Pro $\varphi \in \left[\frac{5\pi}{6}, \pi\right] = \left[\frac{10\pi}{12}, \pi\right]$ platí $2\varphi \in I + 2\pi$, tedy $j := 2$.

6. Pro $\varphi \in [-\pi, 0)$ označíme $\xi := -\varphi \in (0, \pi]$. Podle předchozích bodů máme pro ξ číslo $j \in \mathbb{N} \setminus \{1\}$ takové, že $j\xi \in I + 2l\pi$ pro $l \in \mathbb{Z}$. Toto j je právě také hledaným násobkem φ, jelikož platí $j\varphi = j(-\xi) \in -I - 2k\pi = I + 2(-k)\pi$, díky symetrii $I = -I$.

Dále pro $\varphi \in [-\pi, \pi]$ pomocí matematické indukce najdeme nekonečnou ostře rostoucí posloupnost přirozených čísel j_i tak, že $j_i\varphi$ leží v intervalech tvaru $I + 2l\pi$ s $l \in \mathbb{Z}$, pro všechna $i \in \mathbb{N}$.

- Pro iniciační krok $n = 1$ máme $\varphi \in [-\pi, \pi]$, a tedy z předchozího odvození víme, že existuje $j_1 \in \mathbb{N} \setminus \{1\}$ tak, že $j_1\phi \in 2l\pi$ pro nějaké $l \in \mathbb{Z}$.

- Pro indukční krok $n \to n+1$ využijeme indukčního předpokladu - tedy existence $j_n \in \mathbb{N}\setminus\{1\}$ takového, že $j_n\varphi \in I + 2k_n\pi$ pro nějaké $k_n \in \mathbb{Z}$. Označíme

$$\tilde{\varphi} := j_n\varphi - 2k_n\pi \in I.$$

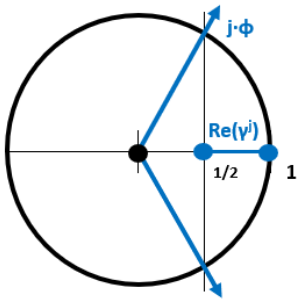
  Pomocí postupu z první části důkazu nalezneme $\tilde{j} \in \mathbb{N} \setminus \{1\}$ takové, že

$$\tilde{j}\tilde{\varphi} \in I + 2\tilde{k}\pi \quad \text{pro nějaké} \quad \tilde{k} \in \mathbb{Z}\,.$$

  Potom platí

$$\tilde{j}\tilde{\varphi} = \tilde{j}(j_n\varphi - 2k_n\pi) = (\tilde{j}j_n)\varphi - 2(\tilde{j}k_n)\ pi \in I + 2\tilde{k}\pi$$
$$(\tilde{j}j_n)\varphi \in I + 2\pi(\tilde{k} + \tilde{j}k_n)\,.$$

  Označíme-li $j_{n+1} := \tilde{j}j_n$ a $k_{n+1} := \tilde{k} + \tilde{j}k_n$, pak $j_{n+1}\varphi \in I + 2k_{n+1}\pi$ je hledaný násobek úhlu φ.



□

Věta 8.18. *Buď $\beta \in \mathbb{C}$, $|\beta| > 1$ algebraické číslo se sdruženým kořenem γ, $|\gamma| = 1$. Buď $\mathcal{A} \subset \mathbb{Z}$ abeceda, $\{0,1\} \subset \mathcal{A}$. Pak sčítání v numeračním systému $(\beta, \mathcal{A})$ nelze provádět paralelně.*

Důkaz. Abychom dospěli ke sporu, předpokládejme existenci p-lokální konverze z $(\mathcal{A}+\mathcal{A})$ do $\mathcal{A}$ v β ve tvaru

$$\phi : (\mathcal{A}+\mathcal{A})^p \to \mathcal{A}.$$

Označme

$$S := \max\left\{ \left| \sum_{j=0}^{p-1} a_j \right| : a_j \in \mathcal{A}\gamma^j \right\}.$$

Dále využijeme tělesový isomorfismus $\sigma : \mathbb{Q}(\beta) \to \mathbb{Q}(\gamma)$ splňující

$$\sigma(y) = \sigma\left(\sum_j q_j \beta^j\right) = \sum_j q_j \gamma^j = y'.$$

Díky vlastnosti $|\gamma| = 1$ z lemmatu 8.17 existuje nekonečně mnoho $j \in \mathbb{N} \setminus \{1\}$ takových, že $\mathrm{Re}(\gamma^j) \geq \frac{1}{2}$. Lze najít konstantu $N \in \mathbb{N}$, $N > p$ a posloupnost cifer $(\varepsilon_j)_{j\in\mathbb{N}_0}$, $\varepsilon_j \in \{0,1\}$, pro něž

$$\mathrm{Re}\left(\sum_{j=0}^{N-1} \varepsilon_j \gamma^j\right) > 2S.$$

Stačí volit $\varepsilon_j := 1$, pokud $\mathrm{Re}(\gamma^j) \geq \frac{1}{2}$, a $\varepsilon_j := 0$ v ostatních případech. Označme

$$T := \max\left\{ \left| \mathrm{Re}\left(\sum_{j=0}^{N-1} a_j \gamma^j\right) \right| : a_j \in \mathcal{A} \right\},$$

a nechť $x := \sum_{j=0}^{N-1} x_j \beta^j$ je vzor prvku $x' = \sigma(x)$, pro který $T = |\mathrm{Re}(x')|$. Platí vztahy

$$x' = \sum_{j=0}^{N-1} x_j \gamma^j = \sum_{j=0}^{N-1} x_j (\sigma(\beta))^j = \sigma\left(\sum_{j=0}^{N-1} x_j \beta^j\right) = \sigma(x)$$

$$|\mathrm{Re}(x')| = \left| \mathrm{Re}\left(\sum_{j=0}^{N-1} x_j \gamma^j\right) \right| \geq \left| \mathrm{Re}\left(\sum_{j=0}^{N-1} \varepsilon_j \gamma^j\right) \right| > 2S.$$

Pomocí p-lokálního algoritmu paralelního sčítání sečteme $x + x$ do reprezentace z ve tvaru

$$x + x = \sum_{j=N}^{N+p-1} z_j \beta^j + \sum_{j=0}^{N-1} z_j \beta^j + \sum_{j=-p}^{-1} z_j \beta^j, \qquad z_j \in \mathcal{A}.$$

Určíme obraz hodnoty $x + x$ v tělesovém izomorfismu σ:

$$\sigma(x+x) = x' + x' = \sum_{j=N}^{N+p-1} z_j \gamma^j + \sum_{j=0}^{N-1} z_j \gamma^j + \sum_{j=-p}^{-1} z_j \gamma^j,$$

pro který pak platí

$$2T = 2|\mathrm{Re}(x')| = |\mathrm{Re}(x'+x')| = \left|\mathrm{Re}\left(\sum_{j=N}^{N+p-1} z_j\gamma^j + \sum_{j=0}^{N-1} z_j\gamma^j + \sum_{j=-p}^{-1} z_j\gamma^j\right)\right| \leq$$

$$\leq \underbrace{|\gamma^N|}_{=1} \cdot \underbrace{\left|\mathrm{Re}\left(\sum_{l=0}^{p-1} z_{l+N}\gamma^l\right)\right|}_{\leq S} + \underbrace{\left|\mathrm{Re}\left(\sum_{j=0}^{N-1} z_j\gamma^j\right)\right|}_{\leq T} + \underbrace{|\gamma^{-p}|}_{=1} \cdot \left|\mathrm{Re}\left(\sum_{l=0}^{p-1} z_{l-p}\gamma^l\right)\right| \leq T + 2S.$$

Tedy $T \leq 2S$, ale přitom

$$2S < \mathrm{Re}\left(\sum_{j=0}^{N-1} \varepsilon_j \gamma^j\right) \leq T,$$

odtud $T \leq 2S < T$, což je hledaný spor. □

Důsledek 8.19. *Buď $\beta \in \mathbb{C}$, $|\beta| > 1$. Pak existuje abeceda $\mathcal{A} \subset \mathbb{Z}$, $\{0,1\} \subset \mathcal{A}$ taková, že v numeračním systému $(\beta, \mathcal{A})$ lze paralelně sčítat, právě když β je algebraické číslo, jehož všechny sdružené kořeny leží mimo jednotkovou kružnici.*

Nyní už tedy víme, která čísla $\beta \in \mathbb{C}$ jsou vhodná jako báze pro numerační systémy $(\beta, \mathcal{A})$ s paralelním sčítáním. Dále budeme zkoumat, které abecedy $\mathcal{A} \subset \mathbb{Z}$ lze v numeračním systému $(\beta, \mathcal{A})$ používat k paralelnímu sčítání. Sice je známo, že k tomu je nutná jistá míra redundace - ovšem jak velká redundance to musí být?

Příklad 8.20. Pro $\beta = 4$ je abeceda $\mathcal{C} = \{0,1,2,3\}$ neredundantní. V příkladě 7.5 jsme ukázali algoritmus paralelního sčítání v systému $(\beta, \mathcal{A})$ pro abecedu $\mathcal{A} = \{0,1,2,3,4\}$, která je redundantní. Zde tedy stačí velikost abecedy $\#\mathcal{A} = 5 = 4 + 1 = \#\mathcal{C} + 1$, neboli rozšíření základní abecedy $\mathcal{C}$ pouze o jeden prvek, a tím už je paralelní sčítání umožněno.

Analogicky to funguje pro všechna $\beta = \pm b$, kde $b \in \mathbb{N} \setminus \{1\}$ - tedy k paralelnímu sčítání v těcho bázích postačují abecedy ve tvaru $\{0, 1, \ldots, b-1, b\}$, tedy $\#\mathcal{A} = b+1 = \#\mathcal{C}+1$. Tento výsledek pro kladné celočíselné báze jako první odvodil B. Parhami [22].

Příklad 8.21. Pro bázi $\beta = \tau$ - zlatý řez (kořen minimálního polynomu $\tau^2 - \tau - 1$) jsme v příkladu 8.13 ukázali algoritmy paralelního sčítání s použitím abeced o velikosti $\#\mathcal{A} = 11$ (pro SRZ-algoritmus), resp. $\#\mathcal{A} = 7$ (pro WRZ-algoritmus). Nyní ovšem představíme ještě třetí algoritmus paralelního sčítání pro tuto bázi, s abecedou o velikosti pouze $\#\mathcal{A} = 3 = \#\mathcal{C} + 1$, kde $\mathcal{C} = \{0,1\}$ je základní abeceda (se kterou lze v bázi τ reprezentovat celé $\mathbb{R}$).

Uvažujeme abecedu $\mathcal{A} = \{0,1,2\}$ jakožto cílovou (po paralelní konverzi) a abecedu $\mathcal{B} = \{0,1,2,3\}$ jakožto zdrojovou; hledáme tedy paralelní konverzi $\mathcal{B} \xrightarrow{\beta} \mathcal{A}$. Její vzor značíme $w = \sum_j w_j \beta^j$ s ciframi $w_j \in \mathcal{B}$, a obraz s ciframi $z_j \in \mathcal{A}$ je $z = \sum_j z_j \beta^j$. Použijeme sice stejnou reprezantaci nuly jako ve WRZ-algoritmu: $[-1,0,3,0,-1]$, ovšem rozdíl je ve způsobu určení pomocných koeficientů $q_j \in \{0,1\} = Q$:

- určení q_j (pro všechna j zároveň):

$$q_j := \begin{cases} 1 & \text{pro } (w_j = 3) \\ 1 & \text{pro } (w_j = 2) \wedge (w_{j-2} \geq 2 \vee (w_{j+2}) \geq 2) \\ 1 & \text{pro } (w_j = 1) \wedge V \\ 0 & \text{pro } (w_j = 2) \wedge (w_{j-2} \leq 1 \wedge w_{j+2} \leq 1) \\ 0 & \text{pro } (w_j = 1) \wedge (\neg V) \\ 0 & \text{pro } (w_j = 0), \end{cases}$$

  kde podmínka V má tvar

$$[(w_{j-2} = 3) \wedge (w_{j+2} = 3)] \ \vee \ [(w_{j-2} = 3) \wedge (w_{j+2} = 2 \wedge w_{j+4} \geq 2)] \ \vee$$
$$\vee \ [(w_{j-2} = 2 \wedge w_{j-4} \geq 2) \wedge (w_{j+2} = 3)] \ \vee [(w_{j-2} = 2 \wedge w_{j-4} \geq 2) \wedge (w_{j+2} = 2 \wedge w_{j+4} \geq 2)]\,;$$

  tedy $q_j = q_j(w_{j+4}, w_{j+2}, w_j, w_{j-2}, w_{j-4}) \in \{0,1\} = Q$;

- a pak (opět pro všechna j zároveň) dopočteme výsledné cifry $z_j := (w_j - 3q_j) + (q_{j-2} + q_{j+2})$.

Správnou funkčnost algoritmu dokážeme rozborem všech variant / kombinací vstupních hodnot w_j a sousedů $w_{j\pm2}$, resp. $w_{j\pm4}$:

- Pro $w_j = 2$ se přiřadí $q_j := 1$, jen když je zaručeno, že alespoň od jednoho souseda přijde $q_{j-2} = 1$ nebo $q_{j+2} = 1 \implies$ pak $z_j \in (2-3) + (\{1\} + \{0,1\}) = \{0,1\} \subset \mathcal{A}$; v opačném případě je $q_j := 0$, a výsledné $z_j \in (2-0) + (\{0\} + \{0\}) = \{2\} \subset \mathcal{A}$.

- Pro $w_j = 1$ se určí $q_j := 1$, jen když je jisté, že od obou sousedů přijde $q_{j-2} = q_{j+2} = 1 \implies$ pak $z_j = (1-3) + (1+1) = 0 \in \mathcal{A}$; v opačném případě je $q_j := 0$, a výsledné $z_j \in (1-0) + (\{0\} + \{0,1\}) = \{1,2\} \subset \mathcal{A}$.

- Pro $w_j = 3$ zcela jasně $q_j := 1 \implies$ výsledek $z_j = \in (3-3) + (\{0,1\} + \{0,1\}) = \{0,1,2\} = \mathcal{A}$.

- A pro $w_j = 0$ opět jednoznačně $\implies z_j \in (0-0) + (\{0,1\} + \{0,1\}) = \{0,1,2\} = \mathcal{A}$.

Vidíme tedy, že rozšířená abeceda $\mathcal{A} = \{0,1,2\}$ o velikosti $\#\mathcal{A} = 3$ je dostatečně redundantní, aby umožňovala paralelní sčítání. Ovšem základní abeceda $\mathcal{C} = \{0,1,\}$ o velikosti $\#\mathcal{C} = 2$ byla

redundantní také, díky reprezentaci nuly $[-1,1,1]$ - tj. přímo ve tvaru minimálního polynomu. Můžeme totiž tvořit různé končené reprezentace téhož čísla:

$$(x_n \dots x_m 011 x_{m-4} \dots x_l)_\tau = x = (x_n \dots x_m 100 x_{m-4} \dots x_l)_\tau \,.$$

Bylo tedy opravdu nutné rozšiřovat základní abecedu $\mathcal{C}$ o jeden prvek navíc?

Příklad 8.22. Existují i numerační systémy $(\beta, \mathcal{A}) = (\beta, \mathcal{C})$, kde už základní abeceda $\mathcal{C}$ je dostatečně redundantní pro algoritmus paralelního sčítaní: například pro bázi s minimálním polynomem $\beta^2 = 5\beta - 1$ a reprezentací nuly $[1,-5,1]$. Kladný kořen $\beta = \frac{5+\sqrt{5^2-4}}{2} = \frac{5+\sqrt{21}}{2} \approx 4,79$ má velikost z intervalu $(4,5) \ni |\beta|$, a základní abeceda $\mathcal{C} = \{0,1,2,3,4\}$ stačí k reprezentování všech $x \in \mathbb{R}^+$ pomocí hladového algoritmu:

- Pro dané $x \in \mathbb{R}^+$ najdeme $n \in \mathbb{Z}$ tak, aby $x \in [\beta^n, \beta^{n+1}) \implies$ pak

$$x_n = \left\lfloor \frac{x}{\beta^n} \right\rfloor \in \left\{ \left\lfloor \frac{\beta^n}{\beta^n} \right\rfloor, \left\lfloor \frac{\beta^{n+1}}{\beta^n} \right\rfloor \right\} = \{1, \lfloor \beta \rfloor\} = \{1,2,3,4\} \subset \mathcal{C} \,.$$

- Dále $\quad x' := x - x_n \beta^n \in [\beta^n, \beta^{n+1}) - \beta^n \cdot \lfloor \frac{x}{\beta^n} \rfloor \subset [0, \underbrace{\beta^{n+1} - 4\beta^n}_{<\beta^n}) \subset [0, \beta^n),$

$$\text{protože} \;\; \beta^{n+1} = 5\beta^n - \beta^{n-1} \implies \beta^{n+1} - 4\beta^n = \beta^n - \beta^{n-1} < \beta^n \,.$$

- V dalším kroku postupujeme analogicky: $x_{n-1} := \lfloor \frac{x'}{\beta^{n-1}} \rfloor \in \{0, \dots, \lfloor \beta \rfloor\} = \{0, \dots, 4\} = \mathcal{C}$, a dále takto cyklus pokračuje pro nižší cifry / pozice $n-2, n-3, \dots$.

Přitom $\mathcal{C}$ je redundantní, protože pomocí odvozené reprezentace nuly $[1,-4,-4,1]$ lze tvořit různé konečné $(\beta, \mathcal{C})$-reprezentace stejných čísel (pro $a, b \in \{0,1,2,3\}$) ve tvaru

$$(x_L \; a44b \; x_R) = x = (x_L \; (a+1)00(b+1) \; x_R) \,.$$

Abecedu $\mathcal{A} = \mathcal{C} = \{0, \dots, 4\}$ použijeme pro paralelní sčítání, respektive pro paralelní konverzi z výchozí abecedy $\mathcal{B} = \{0, \dots, 5\}$ do cílové abecedy $\mathcal{A} = \{0, \dots, 4\}$ pomocí následujícího algoritmu:

- vstupní reprezentace $w = \sum_j w_j \beta^j$ s ciframi $w_j \in \mathcal{B} = \{0, \ldots, 5\}$ určuje pomocné koeficienty $q_j := q_j(w_{j+2}, w_{j+1}, w_j, w_{j-1}, w_{j-2}) \in \{-1, 0, 1\} = Q$ předpisem

$$q_j := \begin{cases} 1 & \text{pro } (w_j = 5) \\ 1 & \text{pro } (w_j = 4) \wedge (w_{j-1} \geq 4 \vee w_{j+1} \geq 4) \\ 1 & \text{pro } (w_j = 3) \wedge (U) \\ 0 & \text{pro } (w_j = 4) \wedge (w_{j-1} \leq 3 \wedge w_{j+1} \leq 3) \\ 0 & \text{pro } (w_j = 3) \wedge (\neg\, U) \\ 0 & \text{pro } (w_j \in \{0, 1, 2\}), \end{cases}$$

  kde U je podmínka ve tvaru

$$[(w_{j-1} = 5) \vee (w_{j-1} = 4 \wedge w_{j-2} \geq 4)] \ \wedge \ [(w_{j+1} = 4 \wedge w_{j+2} \geq 4) \vee (w_{j+1} = 5)]\,;$$

- následně, s využitím reprezentace nuly $[1, -5, 1]$, určíme výsledné cifry (na všech pozicích j zároveň) předpisem $z_j := (w_j - 5q_j) + (q_{j+1} + q_{j-1}) \in \mathcal{A}$.

Důkaz, že algoritmus funguje, se provede opět analýzou všech variant / vstupů w_j a sousedních:

- Pro $w_j \in \{0, 1, 2\}$ vždy $q_j := 0 \implies z_j \in (\{0, 1, 2\} - 0) + (\{0, 1\} + \{0, 1\}) = \{0, \ldots, 4\} = \mathcal{A}$.
- Pro $w_j = 5$ je evidentně $q_j := 1 \implies z_j \in (5 - 5) + (\{0, 1\} + \{0, 1\}) \in \{0, 1, 2\} \subset \mathcal{A}$.
- Pro $w_j = 4$ se určí $q_j := 1$, právě když od alespoň jednoho souseda přijde $q_{j+1} = 1$ nebo $q_{j-1} = 1 \implies$ pak $z_j \in (4 - 5) + (\{1\} + \{0, 1\}) = \{0, 1\} \subset \mathcal{A}$; jinak $q_j := 0$, a následně $z_j \in (4 - 0) + (0 + 0) = 4 \in \mathcal{A}$.
- Pro $w_j = 3$ se určí $q_j := 1$, právě když od obou sousedů jistě přijde $q_{j+1} = q_{j-1} = 1 \implies$ pak $z_j \in (3 - 5) + (1 + 1) = 5 \in \mathcal{A}$; jinak $q_j := 0$, a potom $z_j \in (3 - 0) + (\{0\} + \{0, 1\}) = \{3, 4\} \subset \mathcal{A}$.

Situace pro β kořen $\beta^2 = 5\beta - 1$ je jiná než pro zlatý řez τ. Základní abeceda $\mathcal{C} = \{0, \ldots, 4\}$ pro reprezentování $x \in \mathbb{R}^+$ je dostatečně redundantní i pro paralelní sčítání už sama o sobě - tedy bez přidávání dalších cifer.

Poznámka 8.23. Už dříve bylo zmíněno, že na algoritmus p-lokálního paralelního sčítání v abecedě $\mathcal{A}$ lze nahlížet jako na vyhledání (výsledné cifry) v Lookup Table o velikosti $\#LuT = (\#\mathcal{A} + \#\mathcal{A})^p$, resp. modifikovaně $\#LuT = (\#\mathcal{B})^p$ pro p-lokální konverzi z $\mathcal{B}$ do $\mathcal{A}$:

$$\mathcal{A} \ni z_j = z_j(w_{j+t}, \ldots, w_j, \ldots, w_{j-r})\,, \quad w_j \in \mathcal{B}\,, \quad t + 1 + r = p\,.$$

Je tedy potřeba v LuT vyhledávat p-tice cifer $w \in \mathcal{B}$, k nim výsledek $z \in \mathcal{A}$. Anebo alternativně můžeme sestavit Lookup Table pro vyhledávání koeficientů $q_j \in Q$:

$$Q \ni q_j = q_j(w_{j+t'}, \ldots, w_j, \ldots, w_{j-r'}), \quad w_j \in \mathcal{B}, \quad t' + 1 + r' = p' < p.$$

Tedy pracujeme s LuT' menší velikost $\#(LuT') = (\#\mathcal{B})^{p'}$, vyhledaný výsledek užijeme ve vzorci

$$z_j = w_j - \sum_{l=-h}^{k} q_{j-l} b_l,$$

kde b_l jsou koeficienty reprezentace nuly, a $p = p' + (k + h)$.

Ilustrujme si tento postup na příkladu $\beta^2 = 5\beta - 1$, pro nějž LuT' má tvar

q_j	$\leftarrow$	w_{j+2}	w_{j+1}	w_j	w_{j-1}	w_{j-2}
+1	$\leftarrow$	x	x	5	x	x
+1	$\leftarrow$	x	x	4	5	x
+1	$\leftarrow$	x	x	4	4	x
+1	$\leftarrow$	x	x	3	5	x
+1	$\leftarrow$	x	x	3	4	5
+1	$\leftarrow$	x	x	3	4	4

w_{j+2}	w_{j+1}	w_j	w_{j-1}	w_{j-2}	$\rightarrow$	q_j
x	5	4	x	x	$\rightarrow$	+1
x	4	4	x	x	$\rightarrow$	+1
x	5	3	x	x	$\rightarrow$	+1
5	4	3	x	x	$\rightarrow$	+1
4	4	3	x	x	$\rightarrow$	+1

$$q_j = q_j(w_{j+2}, w_{j+1}, w_j, w_{j-1}, w_{j-2}) \qquad \Longrightarrow \; p' = 1 + 2 + 2 = 5$$
$$z_j = (w_j - 5q_j) + (q_{j-1} + q_{j+1}) \qquad \Longrightarrow \; k = h = 1$$
$$p = p' + (k + h) = 7$$

8.3 Velikost abecedy umožňující paralelní sčítání

Vraťme se zpět k otázkám velikost abecedy $\mathcal{A}$ pro paralelní sčítání v $(\beta, \mathcal{A})$:

- Mohlo by u $\beta = \tau = \tau^2 - 1$ stačit pro paralelní sčítání taky jen $\mathcal{A} = \mathcal{C} = \{0, 1\}$?
- Bude ve všech případech stačit přidání pouze jedné cifry do základní abecedy $\mathcal{C}$ pro danou bázi β, aby vznikl numerační systém $(\beta, \mathcal{A})$ s paralelním sčítáním? (tj. $\#\mathcal{A} = \#\mathcal{C} + 1$)

Odpověď na obě otázky je NE, viz následující podmínky vymezující minimální velikosti $\#\mathcal{A}$ pro paralelní sčítání v $(\beta, \mathcal{A})$.

Značení 8.24. Pro algebraické číslo $\beta \in \mathbb{C}$ značíme

$$\mathbb{Z}[\beta] = \left\{ \sum_{j=0}^{n} x_j \beta^j : n \in \mathbb{N}_0, x_j \in \mathbb{Z} \right\}. \tag{8.3}$$

Poznámka 8.25. Pro algebraické celé číslo β stupně d platí $\mathbb{Z}[\beta] = \left\{ \sum_{j=0}^{d-1} x_j \beta^j : x_j \in \mathbb{Z} \right\}$. Algebraické celé číslo β je totiž kořenem minimálního polynomu $f(x) \in \mathbb{Z}[x]$ ve tvaru

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x^1 + a_0 x^0, \qquad a_i \in \mathbb{Z},$$

tedy $f(\beta) = 0$, a proto

$$\beta^d = -a_{d-1}\beta^{d-1} - \ldots - a_1\beta^1 - a_0\beta^0. \tag{8.4}$$

Libovolné $x \in \mathbb{Z}[\beta]$ lze upravit pomocí (8.4) a tím snížit maximální index v sumě (8.3):

$$\begin{aligned} x = \sum_{j=0}^{n} x_j\beta^j = \sum_{j=0}^{d-1} x_j\beta^j + \beta^d \cdot \sum_{j=d}^{n} x_j\beta^{j-d} = \sum_{j=0}^{d-1} x_j\beta^j + \left(-\sum_{i=0}^{d-1} a_i\beta^i\right)\left(\sum_{l=0}^{n-d} x_{l+d}\beta^l\right) = \\ = \sum_{j=0}^{d-1} x_j\beta^j - \sum_{i=0}^{d-1}\sum_{l=0}^{n-d} a_i x_{l+d}\beta^{i+l} = \sum_{j=0}^{d-1} x_j\beta^j + \sum_{j=0}^{n-1} y_j\beta^j = \sum_{j=0}^{n-1} x'_j\beta^j\,, \end{aligned}$$

... tak můžeme postupovat dál, a snížit maximální index sumy až na hodnotu $d-1$.

Věta 8.26. *Buď $\beta \in \mathbb{C}$ algebraické číslo, $\mathcal{D}$ konečná abeceda, $0 \in \mathcal{D} \subset \mathbb{Z}[\beta]$, a zobrazení $\phi : (\mathcal{D}+\mathcal{D})^p \to \mathcal{D}$ určující p-lokální funkci paralelního sčítání $\varphi : (\mathcal{D}+\mathcal{D})^{\mathbb{Z}} \to \mathcal{D}^{\mathbb{Z}}$ v numeračním systému $(\beta, \mathcal{D})$, s parametry $t+1+r = p$; $t, p \in \mathbb{N}_0$. Pak pro každé $x \in \mathcal{D}+\mathcal{D}$ platí*

$$\phi(x^p) - x \in (\beta-1)\cdot\mathbb{Z}[\beta]\,, \quad \textit{kde} \;\; \phi(\underbrace{x,\ldots,x}_{p-\textit{krát}}) =: \phi(x^p)\,.$$

Důkaz. Pro $x \in \mathcal{D}+\mathcal{D}$ označíme $\phi(x^p) = y \in \mathcal{D}$. Pro libovolné $n \in \mathbb{N}$ analyzujeme číslo S_n:

$$S_n := {}^{\omega}0\underbrace{x\ldots x}_{t-\text{krát}}\underbrace{x\ldots x}_{n-\text{krát}}\cdot\underbrace{x\ldots x}_{r-\text{krát}}0^{\omega}$$

a jeho obraz po p-lokální konverzi:

$$\phi(S_n) = {}^{\omega}0u_{p-1}\ldots u_1\underbrace{y\ldots y}_{n-\text{krát}}\cdot v_1\ldots v_{p-1}0^{\omega} \in \mathcal{D}^{\mathbb{Z}}. \tag{8.5}$$

Přitom cifry u_j ani v_j nezávisejí na volbě $n \in \mathbb{N}$: $u_j = \phi(0^j x^{p-j})$ a $v_j = \phi(x^{p-j}0^j)$, takže můžeme příslušné výrazy (konstantní v proměnné n) zapsat jako $U = \sum_{j=1}^{p-1} u_j\beta^{j-1} \in \mathbb{Z}[\beta]$ a

$V = \sum_{j=1}^{p-1} v_j \beta^{p-1-j} \in \mathbb{Z}[\beta]$. Platí

$$S_n = x \cdot \sum_{j=-r}^{n+t-1} \beta^j = U \cdot \beta^n + y \cdot \sum_{j=0}^{n-1} \beta^j + V \cdot \beta^{-p+1},$$

a to pro každé $n \in \mathbb{N}$, tedy i pro $n+1$. Rozdíl $S_{n+1} - S_n$ pak má tvar:

$$\begin{aligned} S_{n+1} - S_n = x \cdot \beta^{n+t} &= U \cdot \beta^{n+1} - U \cdot \beta^n + y \cdot \beta^n \\ x \cdot \beta^t &= U(\beta - 1) + y \\ x(\beta^t - 1) &= U \cdot (\beta - 1) + (y - x) \end{aligned}$$

Odtud obdržíme $\phi(x^p) - x = y - x = x(\beta^t - 1) + U(\beta - 1)$.

- Pro $t = 0$ to znamená $y - x = x(\beta^0 - 1) + U(\beta - 1) = U(\beta - 1) \in (\beta - 1) \cdot \mathbb{Z}[\beta]$.
- Pro $t \geq 1$ lze výraz $\phi(x^p) - x = y - x$ rozepsat jako

$$\begin{aligned} y - x &= x(\beta - 1)(\beta^{t-1} + \beta^{t-2} + \cdots + \beta + 1) + U(\beta - 1) = \\ &= (\beta - 1)[\underbrace{x}_{\in \mathbb{Z}} \underbrace{(\beta^{t-1} + \beta^{t-2} + \cdots + \beta + 1)}_{\in \mathbb{Z}[\beta]} + \underbrace{U}_{\in \mathbb{Z}[\beta]}] \in (\beta - 1) \cdot \mathbb{Z}[\beta]. \end{aligned}$$

Vždy je tedy splněno $\phi(x^p) - x \in (\beta - 1) \cdot \mathbb{Z}[\beta]$, neboli $y = \phi(x^p) \equiv_{\mathbb{Z}[\beta]} x \mod (\beta - 1)$. □

Pro algebraická celá čísla lze tento nález rozšířit ještě o následující tvrzení, která umožní odhadnout minimální velikost abecedy $\#\mathcal{A}$ pro paralelní sčítání v systému $(\beta, \mathcal{A})$ pomocí minimálního polynomu báze β.

Věta 8.27. *Buď $\beta \in \mathbb{C}$ algebraické celé číslo a $\mathcal{D}$ konečná abeceda $0 \in \mathcal{D} \subset \mathbb{Z}$. Buď $\phi : (\mathcal{D} + \mathcal{D})^p \to \mathcal{D}$ zobrazení určující p-lokální funkci paralelního sčítání v numeračním systému $(\beta, \mathcal{D})$. Pak pro každé $x \in \mathcal{D} + \mathcal{D}$ platí*

$$\phi(x^p) \equiv_{\mathbb{Z}} x \mod |f(1)|,$$

kde $f(x) \in \mathbb{Z}[x]$ je minimální polynom algebraického (celého) čísla β.

Důkaz. Navážeme na tvrzení a důkaz předchozí věty 8.26, odkud obdržíme

$$\phi(x^p) - x = y - x = (\beta - 1)z \qquad \text{pro } \ z \in \mathbb{Z}[\beta]\,.$$

Báze β je algebraické celé číslo (stupně d), jeho minimální polynom $f(x) \in \mathbb{Z}[x]$ lze zapsat ve tvaru $f(x) = x^d - a_{d-1}x^{d-1} - \ldots - a_1 x - a_0$, s koeficienty $a_j \in \mathbb{Z}$. A samozřejmě β je kořenem

$f(x)$, tedy platí $f(\beta) = 0$, neboli $\beta^d = a_{d-1}\beta^{d-1} + a_{d-2}\beta^{d-2} + \cdots + a_1\beta^1 + a_0$. Díky tomu lze prvek $z \in \mathbb{Z}[\beta]$ zapsat ve tvaru

$$z = c_0 + c_1\beta^1 + \cdots + c_{d-1}\beta^{d-1} \quad \text{s koeficienty } c_j \in \mathbb{Z}\,;$$

ten pak dosadíme do vztahu $y - x = (\beta - 1)z$, a obdržíme následující výraz:

$$\begin{aligned}
0 &= x - y + (\beta - 1)(c_0 + c_1\beta + \cdots + c_{d-1}\beta^{d-1}) = \\
&= x - y + \beta(c_0 + c_1\beta + \cdots + c_{d-2}\beta^{d-2}) + c_{d-1}\beta^d - (c_0 + c_1\beta + \cdots + c_{d-1}\beta^{d-1}) = \\
&= x - y + c_0\beta + c_1\beta^2 + \cdots + c_{d-2}\beta^{d-1} + c_{d-1}(a_0 + a_1\beta + \cdots + a_{d-1}\beta^{d-1}) - \\
&- (c_0 + c_1\beta + \cdots + c_{d-1}\beta^{d-1}) = \\
&= \beta^0(x - y + c_{d-1}a_0 - c_0) + \beta^1(c_0 + c_{d-1}a_1 - c_1) + \beta^2(c_1 + c_{d-1}a_2 - c_2) + \ldots \\
&\cdots + \beta^{d-1}(c_{d-2} + c_{d-1}a_{d-1} - c_{d-1}) =: g(\beta)\,.
\end{aligned}$$

Tedy β je kořenem polynomu $g(x) \in \mathbb{Z}[x]$ s celočíselnými koeficienty stupně maximálně $d - 1$. Pak ale, jelikož stupeň β jakožto algebraického čísla je d, musí být $g(x)$ polynom nulový, a tedy jeho (celočíselný) koeficient u každé mocniny β^j musí být nulový:

$$\begin{aligned}
&\text{koeficient u } \beta^0: && 0 = x - y + c_{d-1}a_0 - c_0 \\
&\text{koeficient u } \beta^1: && 0 = \quad c_0 + c_{d-1}a_1 - c_1 \\
&\text{koeficient u } \beta^2: && 0 = \quad c_1 + c_{d-1}a_2 - c_2 \\
&\qquad\vdots && \qquad\vdots \\
&\text{koeficient u } \beta^{d-1}: && 0 = \; c_{d-2} + c_{d-1}a_{d-1} - c_{d-1}
\end{aligned}$$

Sečtením všech těchto rovnic dostaneme rovnost

$$\begin{aligned}
0 &= x - y + c_{d-1}(a_0 + a_1 + a_2 + \cdots + a_{d-1} - 1) \\
y &= x - c_{d-1}\underbrace{(1 - a_{d-1} - a_{d-2} - \ldots - a_1 - a_0)}_{=f(1)} = x - c_{d-1}f(1)\,,
\end{aligned}$$

přitom $c_{d-1} \in \mathbb{Z}$, tedy $\phi(x^p) = y \equiv_{\mathbb{Z}} x \mod |f(1)|$. □

Důsledek 8.28. *Buď $\beta \in \mathbb{C}$ algebraické celé číslo stupně d s minimálním polynomem $f(x) \in \mathbb{Z}[x]$. Buď $\mathcal{A} \subset \mathbb{Z}$ abeceda po sobě jdoucích celých čísel, $\{0, 1\} \subset \mathcal{A}$. Pokud v numeračním systému $(\beta, \mathcal{A})$ lze sčítat paralelně, pak $\#\mathcal{A} \geq |f(1)|$.*

Důkaz. Označme $\mathcal{A} = \{-m, \ldots, 0, \ldots, M\}$, kde $m \in \mathbb{N}_0$, $M \in \mathbb{N}$, a tedy $\#\mathcal{A} = M + m + 1$. Pro případy $|f(1)| = 1$ nebo $|f(1)| = 2$ je situace triviální, jistě $\#\mathcal{A} \geq 2 \geq |f(1)|$. Dál tedy mějme

$|f(1)| \geq 3$, uvažujme cifru $M+1 \in (\mathcal{A}+\mathcal{A}) \setminus \mathcal{A}$ a p-lokální funkci paralelního sčítání ϕ. Dle předchozí věty 8.27 platí kongruence

$$\phi((M+1)^p) \equiv M+1 \mod |f(1)|\,. \tag{8.6}$$

Protože $\phi((M+1)^p \in \mathcal{A})$ a zároveň $M+1 \notin \mathcal{A}$, a také díky kongruenci (8.6) jsou splněny nerovnosti

$$-m \leq \phi((M+1)^p) < M+1 \quad \text{a} \quad -m \leq \phi((M+1)^p) \leq M+1-|f(1)|\,,$$

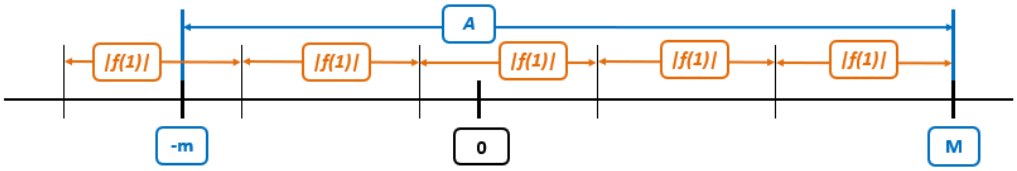
odkud již vyplývá hledaná nerovnost $|f(1)| \leq M+1+m = \#\mathcal{A}$. □

Dovětek. Pokud navíc $\beta \in \mathbb{R}$, $\beta > 1$, pak abeceda $\mathcal{A}$ pro paralelní sčítání v bázi β musí mít velikost alespoň $\#\mathcal{A} \geq |f(1)|+2$.

Důkaz. S využitím vztahů odvozených v předchozích důkazech a pomocí další série odhadů platných pro $\beta > 1$ (které zde dopodrobna neuvádíme) obdržíme následující vztahy pro krajní prvky abecedy $\mathcal{A} = \{-m, \ldots, 0, \ldots, M\} \subset \mathbb{Z}$:

$$\phi(M^p) \neq M \quad \text{a} \quad \phi(M^p) \neq -m\,.$$

Nutně tedy hodnoty $-m, M, \phi(M^p)$ jsou tři různá čísla, která všechna leží v abecedě $\mathcal{A}$, proto nutně $\#\mathcal{A} \geq 3$. Je-li $|f(1)| = 1$, pak je důkaz hotov, neboť $\#\mathcal{A} \geq 3 = 2+|f(1)| = 2+1$. Pro $|f(1)| \geq 2$ využijeme nerovnosti $-m < \phi(M^p) < M$ spolu s kongruencí $\phi(M^p) \equiv M \mod |f(1)|$.



Hodnota $\phi(M^p)$ leží v jednom z bodů ve tvaru $M - k \cdot |f(1)|$ pro $k \in \mathbb{N}$, $k > 1$. Proto platí

$$-m < \phi(M^p) \leq M-|f(1)| \quad \Longrightarrow \quad |f(1)| < M+m \quad \Longrightarrow \quad |f(1)|+2 \leq M+m+1 = \#\mathcal{A}\,,$$

neboť v těchto výrazech vystupují samá celá čísla. Dosáhli jsme tedy přísnější podmínky (vyšší hodnoty) pro minimální velikost abecedy $\#\mathcal{A}$ pro paralelní sčítání v bázi $\beta \in \mathbb{R}^+$, než je obecná podmínka odvozená v důsledku 8.28 pro $\beta \in \mathbb{C}$. □

Poznámka 8.29. Vzhledem k tomu, že algebraické číslo β a jeho sdružené kořeny mají stejné vlastnosti z pohledu paralelního sčítání na celočíselných abecedách, tak (vyšší) dolní mez na velikost abecedy $|f(1)| + 2 \leq \#\mathcal{A}$ platí i pro β, pokud některý jeho sdružený kořen je $\gamma > 1$.

Poznámka 8.30. V řadě případů skutečně existují algoritmy paralelního sčítání na numeračním systému $(\beta, \mathcal{A})$ s kladnou bází $\beta > 1$, kde velikost $\#\mathcal{A}$ nabývá dolní meze odvozené výše - tedy $\#\mathcal{A} = |f(1)| + 2$. Například pro tyto přirozené a kvadratické báze:

- $\beta = b \in \mathbb{N}$, $b \geq 2 \implies f(x) = x - b$, $\#\mathcal{A} = |f(1)| + 2 = b + 1$;
- $\beta^2 = a\beta + b$, $a, b \in \mathbb{N}$, $a \geq b \implies f(x) = x^2 - ax - b$, $\#\mathcal{A} = |f(1)| + 2 = a + b + 1$. Do této třídy patří i báze $\beta = \tau$ zlatý řez s minimálním polynomem $f(x) = x^2 - x - 1$, pro nějž jsme již odvodili algoritmus paralelního sčítání v abecedě o velikosti $\#\mathcal{A} = 3 = |f(1)| + 2$.

Avšak jsou i případy, kdy dolní mez $|f(1)| + 2$ jako velikost abecedy pro paralelní sčítání nestačí, třeba pro následující kvadratické báze:

- $\beta^2 = a\beta - b$, $a, b \in \mathbb{N}$, $a \geq b + 2 \implies f(x) = x^2 - ax + b$; přitom ale minimální abeceda pro paralelní sčítání v této bázi β má velikost $\#\mathcal{A} = a + b - 1 > a - b + 1 = |f(1)| + 2$.

Poznámka 8.31. Uveďme také příklady bází $\beta \in \mathbb{C}\backslash\mathbb{R}^+$, tedy nekladných či dokonce nereálných, kde velikost abecedy daná dolní mezí $\#\mathcal{A} = |f(1)|$ skutečně stačí pro paralelní sčítání v $(\beta, \mathcal{A})$:

- $\beta = -b$, $b \in \mathbb{N} \implies f(x) = x + b$, $\#\mathcal{A} = |f(1)| = b + 1$;
- Knuthova báze: $\beta = 2i \implies f(x) = x^2 + 4$, $\#\mathcal{A} = |f(1)| = 5$;
- Penneyho báze: $\beta = -1 + i \implies f(x) = x^2 + 2x + 2$, $\#\mathcal{A} = |f(1)| = 5$;
- Eisensteinova báze: $\beta = -1 + \exp(\frac{2\pi i}{3}) \implies f(x) = x^2 + 3x + 3$, $\#\mathcal{A} = |f(1)| = 7$.

8.4 On-line násobení a dělení

Pro operace násobení a dělení představíme tzv. on-line algoritmy. Ty byly navrženy v [29] K. Trivedim a M. Ercegovacem nejdříve pro numerační systém s bází $b \in \mathbb{N}$. Zobecnění jejich algoritmů, které zde uvádíme, funguje i pro numerační systémy s komplexní bází a lze jej nalézt v [12]. Při popisu algoritmů budeme z praktických důvodů používat obrácenou indexaci cifer v reprezentacích čísel v numeračním systému $(\beta, \mathcal{A})$:

$$u = \sum_j u_j \beta^{-j} \qquad u_j \in \mathcal{D}\,.$$

Také, bez újmy na obecnosti, pracujeme s reprezentacemi začínajícími až za zlomkovou tečkou, tedy ve tvaru

$$u = 0 \cdot u_1 u_2 u_3 \ldots u_j \ldots \qquad u_j \in \mathcal{D}\,.$$

Stejně jako u paralelních (p-lokálních) algoritmů, i v on-line algoritmech provádíme konverzi reprezentací z výchozí abecedy $\mathcal{D}$ do cílové abecedy $\mathcal{B}$, s použitím zobrazení $\varphi : \mathcal{D}^{\mathbb{Z}} \to \mathcal{B}^{\mathbb{Z}}$. Klíčový rozdíl mezi oběma metodami je v závislostních mechanismech mezi ciframi reprezentací vstupních ($u_j \in \mathcal{D}^{\mathbb{Z}}$) a výstupních ($v_j \in \mathcal{B}^{\mathbb{Z}}$):

- $v_j = \phi(u_{j+t}, \ldots, u_j, \ldots, u_{j-r})$, s parametry $p = r + t + 1$, $r, t \in \mathbb{N}$;
- $v_j = \phi(u_1, u_2, \ldots, u_j, \ldots, u_{j+\delta})$, s parametrem $\delta \in \mathbb{N}$.

V takto popsaném konceptu on-line operací násobení a dělení reprezentací v numeračním systému $(\beta, \mathcal{A})$ uvažujeme báze $\beta \in \mathbb{C}$, $|\beta| > 1$ a abecedy $\mathcal{A} \subset \mathbb{C}$, $0 \in \mathcal{A}$. Výchozí abeceda v on-line algoritmu je $\mathcal{D} = \mathcal{A} \times \mathcal{A}$, cílová abeceda je $\mathcal{B} = \mathcal{A}$, a reprezentace vstupů a výstupů mají tvar

$$\varphi_P \underbrace{(X, Y)}_{u} = \underbrace{P}_{v} \text{ pro násobení,} \qquad \varphi_Q \underbrace{(N, D)}_{u} = \underbrace{Q}_{v} \text{ pro dělení.}$$

Pro násobení jsou vstupy do on-line algoritmu činitelé X a Y ve tvaru

$$X = \sum_{j=1}^{\infty} x_j \beta^{-j} \qquad Y = \sum_{j=1}^{\infty} y_j \beta^{-j} \qquad x_j, y_j \in \mathcal{A}\,,$$

a výstupem jejich součin (produkt) P ve tvaru

$$X \cdot Y = P = \sum_{j=1}^{\infty} p_j \beta^{-j} \qquad p_j \in \mathcal{A}\,, \qquad p_j = \phi_P\left((x_1 \ldots x_{j+\delta}) \times (y_1 \ldots y_{j+\delta})\right)\,.$$

Při dělení jsou vstupy do on-line algoritmu dělenec N a dělitel D ve tvaru

$$N = \sum_{j=1}^{\infty} n_j \beta^{-j} \qquad D = \sum_{j=1}^{\infty} d_j \beta^{-j} \qquad n_j, d_j \in \mathcal{A}\,,$$

a výstupem jejich podíl (kvocient) Q ve tvaru

$$\frac{N}{D} = Q = \sum_{j=1}^{\infty} q_j \beta^{-j} \qquad q_j \in \mathcal{A}\,, \qquad q_j = \phi_Q\left((n_1 \dots n_{j+\delta}) \times (d_1 \dots d_{j+\delta})\right)\,.$$

Před přijetím vstupů do on-line algoritmu je nutné jejich před-zpracování (pre-processing). Pro činitele X, Y a pro dělenec N je třeba odsunout první nenulovou cifru o δ pozic doprava od zlomkové tečky (u on-line algoritmu se zpožděním $\delta \in \mathbb{N}$):

$$x_j := 0 \quad y_j := 0 \quad n_j := 0 \quad \forall j = 1, \dots, \delta\,.$$

Pro dělitele D jev nutno zajistit, aby nejen samotný dělitel D, ale i všechny jeho dílčí reprezentace (tj. konečné části celkové reprezentac) byly nenulové. Aneb požadujeme (pro daný numerační systém $(\beta, \mathcal{A})$) existenci konstanty $D_{min} > 0$ takové, že pro všechna $k \in \mathbb{N}$ platí

$$\left| \sum_{j=1}^{k} d_j \beta^{-j} \right| \geq D_{min}.$$

Takové před-zpracování je samostatná úloha, která také vyžaduje samostatné řešení (mimo algoritmus on-line dělení jako takový).

On-line násobení

Mějme numerační systém $(\beta, \mathcal{A})$, $|\beta| > 1$, kde vstupy / činitele zapíšeme ve tvaru

$$X = 0 \cdot 0 \dots 0 x_{\delta+1} x_{\delta+2} \dots \qquad Y = 0 \cdot 0 \dots 0 y_{\delta+1} y_{\delta+2} \dots\,,$$

a výstup / součin předpokládáme ve tvaru

$$X \cdot Y = P = 0 \cdot p_1 p_2 \dots p_{\delta+1} \cdots = 0 \cdot 0 \dots 0 p_{\delta+1} \dots\,,$$

kde cifry jsou $x_j, y_j, p_j \in \mathcal{A}$, a dílčí reprezentace značíme

$$X_k = \sum_{j=1}^{k} x_j \beta^{-j} \qquad Y_k = \sum_{j=1}^{k} y_j \beta^{-j} \qquad P_k = \sum_{j=1}^{k} p_j \beta^{-j}\,.$$

Algoritmus on-line násobení postupuje v následujících krocích:

- zavedení pomocné proměnné $W_k \in \mathbb{R}$, resp. $W_k \in \mathbb{C}$ pro reálný, resp. komplexní numerační systém;
- iniciace výchozích proměnných (s indexem $k = 0$): $W_0 = X_0 = Y_0 = P_0 = p_0 := 0$;
- iterace (pro $k = 1, 2, 3, \dots$) cyklu sestávajícího ze dvou kroků:
  - výpočet pomocné proměnné $W_k := \beta(W_{k-1} - p_{k-1}) + (x_k Y_{k-1} + y_k X_k)$,
  - a následně výběr vhodné cifry $p_k := Select_P(W_k) \in \mathcal{A}$.

Věta 8.32. *Proměnné W_k určené předpisem $W_k := \beta(W_{k-1} - p_{k-1}) + (x_k Y_{k-1} + y_k X_k)$ v algoritmu on-line násobení pro všechna $k \in \mathbb{N}$ splňují rovnost*

$$W_k = \beta^k (X_k Y_k - P_{k-1})\,. \tag{8.7}$$

Pokud navíc posloupnost $(W_k)_k$ je omezená, tak platí

$$X \cdot Y = \lim_{k \to +\infty} (X_k \cdot Y_k) = \lim_{k \to +\infty} (P_{k-1}) = P. \tag{8.8}$$

Důkaz. Vztah (8.7) ukážeme indukcí. Pro $k = 1$ je vidět triviálně, pouhým dosazením:

$$\begin{aligned} W_k = W_1 &:= \beta(W_0 - p_0) + (x_1 \cdot Y_0 + y_1 \cdot X_1) = \beta(0 - 0) + (x_1 \cdot 0 + y_1 \cdot X_1) = y_1 \cdot X_1 = \\ &= \beta(y_1 \beta^{-1}) X_1 = \beta(Y_1 \cdot X_1 - 0) = \beta^1 (X_1 \cdot Y_1 - P_0) = \beta^k (X_1 \cdot Y_1 - P_{k-1})\,. \end{aligned}$$

Indukční krok předpokládá platnost tvrzení pro $k - 1$, a z něj dokazuje platnost pro k:

$$\begin{aligned} W_k &:= \beta(W_{k-1} - p_{k-1}) + (x_k Y_{k-1} + y_k X_k) = \\ &= \beta(\beta^{k-1}(X_{k-1} Y_{k-1} - P_{k-2}) - p_{k-1}) + x_k Y_{k-1} + y_k X_k = \\ &= \beta^k X_{k-1} Y_{k-1} + (x_k Y_{k-1} + y_k X_k) - (\beta^k P_{k-2} + \beta p_{k-1}) = \\ &= \beta^k Y_{k-1} \left(\sum_{j=1}^{k-1} x_j \beta^{-j} + x_k \beta^{-k} \right) + y_k X^k - \beta^k \left(\sum_{j=1}^{k-2} p_j \beta^{-j} + p_{k-1} \beta^{-k+1} \right) = \\ &= \beta^k Y_{k-1} \sum_{j=1}^{k} x_j \beta^{-j} + y_k X_k - \beta^k \sum_{j=1}^{k-1} p_j \beta^{-j} = \beta^k X_k \left(\sum_{j=1}^{k-1} y_j \beta^{-j} + y_k \beta^{-k} \right) - \beta^k P_{k-1} = \\ &= \beta^k X_k Y_k - \beta^k P_{k-1} = \beta^k \left(X_k Y_k - P_{k-1} \right). \end{aligned}$$

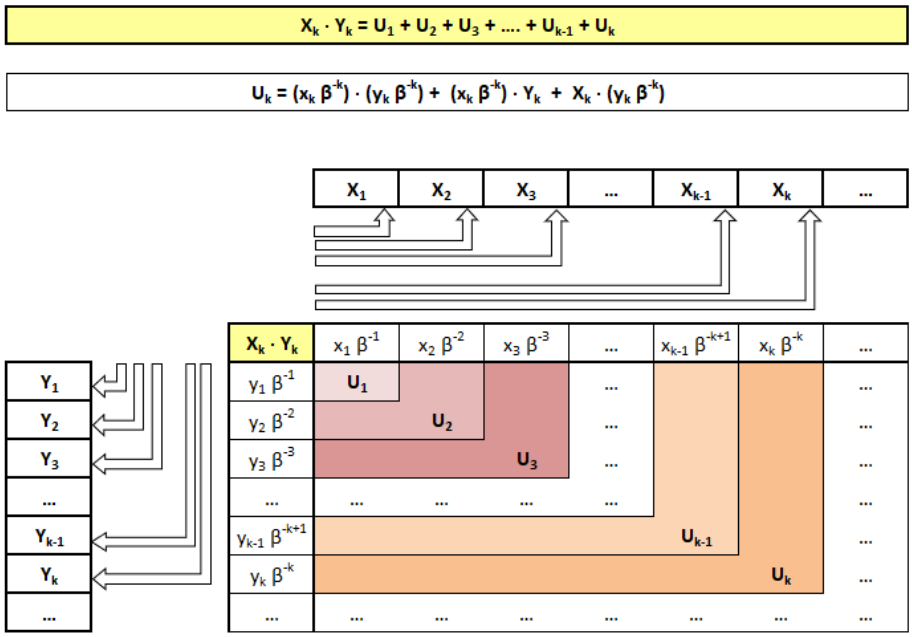
Rovnost (8.8) ukážeme pomocí vztahu $W_k = \beta^k (X_k Y_k - P_{k-1})$:

$$\beta^{-k} W_k = X_k \cdot Y_k - P_{k-1} \qquad \Longrightarrow \qquad P_{k-1} = X_k \cdot Y_k - \beta^{-k} W_k\,.$$

Díky omezenosti posloupnosti $(W_k)_k$ a velikosti $|\beta| > 1$ obdržíme potřebný výsledek:

$$P = \lim_{k \to +\infty} (P_{k-1}) = \lim_{k \to +\infty} (X_k Y_k - \beta^{-k} W_k) = X \cdot Y - 0 = X \cdot Y.$$

Postupné přijímání dalších příchozích vstupů / cifer x_j, y_j a jejich zapracovávání do pomocné proměnné W_k v jednotlivých iteracích cyklu on-line algoritmu je ilustrováno zde:



□

Klíčová úloha k nalezení on-line algoritmu násobení je určení funcke $Select_P : W \to \mathcal{A}$ tak, aby posloupnost $(W_k)_k$ byla omezená, $W_k \in W$. Ani samotný definiční obor W není jasný, je třeby ho najít (a přitom dodržet požadavek $Select_P(0) = 0$).

I tady bude nutná určitá redundance numeračního systému $(\beta, \mathcal{A})$, jinak nepřipadá v úvahu postup, ve kterém určujeme některé cifry výstupu, aniž bychom znali kompletní vstupy.

Ilustrace procesu násobení a efektu delay δ

Hledáme součin dvou vstupních činitelů ve tvaru $X_{orig} = \sum_{j=1}^{\infty} \tilde{x}_j \beta^{-j}$ a $Y_{orig} = \sum_{j=1}^{\infty} \tilde{y}_j \beta^{-j}$. Nejprve provedeme posun cifer o δ-pozic, tak že $x_j := \tilde{x}_{j-\delta}$ a $y_j := \tilde{y}_{j-\delta}$:

$$\beta^{-\delta} \cdot X_{orig} = \beta^{-\delta} \cdot 0 \cdot \tilde{x}_1 \tilde{x}_2 \cdots = 0 \cdot 0 \ldots 0 x_{\delta+1} x_{\delta+2} \cdots =: X_{new}$$
$$\beta^{-\delta} \cdot Y_{orig} = \beta^{-\delta} \cdot 0 \cdot \tilde{y}_1 \tilde{y}_2 \; dots = 0 \cdot 0 \ldots 0 y_{\delta+1} y_{\delta+2} \cdots =: Y_{new}$$

Po vynásobení $X_{new} \cdot Y_{new}$ (on-line algoritmem) tento posun zas jednoduše vrátíme zpět, použitím posunutých cifer $p_j := \tilde{p}_{j-2\delta}$:

$$P_{new} := X_{new} \cdot Y_{new} = 0 \cdot 0 \ldots 0 p_{\delta+1} p_{\delta+2} \cdots = \beta^{-2\delta}(X_{orig} \cdot Y_{orig}) = \beta^{-2\delta} \cdot P_{orig}$$

$$P_{orig} = \beta^{2\delta} P_{new} = p_{\delta+1} \ldots p_{2\delta} \cdot p_{2\delta+1} \ldots p_{3\delta} \cdots = \tilde{p}_{-\delta+1} \ldots \tilde{p}_0 \cdot \tilde{p}_1 \ldots \tilde{p}_\delta \cdots = \sum_{j=-\delta+1}^{\infty} \tilde{p}_j \beta^{-j} \,.$$

Zpoždění násobícího algoritmu o δ cifer jasně vidíme v pohledu $P_{orig} := X_{orig} \cdot Y_{orig}$, kde cifra součinu na k-té pozici je určena na základě znalosti cifer činitelů na pozicích od $k + \delta$ (včetně) směrem doleva. Nicméně algoritmus on-line násobení dále popisujeme opět v pohledu $P_{new} := X_{new} \cdot Y_{new}$, tedy jak už byl představen dříve - s nulami na prvních δ pozicích vpravo od desetinné tečky pro oba vstupy / činitele.

Ze vzorce pro určení $W_k = \beta(W_{k-1} - p_{k-1}) + (x_k Y_{k-1} + y_k X_k)$ a $Select_P(0) = 0$ a díky předpokladům $x_0 = \cdots = x_\delta = y_0 = \cdots = y_\delta = 0$ jsou jistě $W_0 = \cdots = W_\delta = 0$ i $p_0 = \cdots = p_\delta = 0$. Zde tedy k-tá cifra součinu je funkce $p_k = p_k(X_k, Y_k)$, viz schéma:

$$\begin{aligned} X_{new} = X &= 0 \cdot 0 \ldots 0 x_{\delta+1} x_{\delta+2} \ldots x_{k-1} x_k x_{k+1} \ldots \\ Y_{new} = Y &= 0 \cdot 0 \ldots 0 y_{\delta+1} y_{\delta+2} \ldots y_{k-1} y_k y_{k+1} \ldots \\ X \cdot Y = P &= 0 \cdot 0 \ldots 0 p_{\delta+1} p_{\delta+2} \ldots p_{k-1} p_k p_{k+1} \ldots \end{aligned}$$

Omezenost hodnot $W_k = \beta(W_{k-1} - p_{k-1}) + (x_k Y_{k-1} + y_k X_k)$ se snažíme zajistit zvlášť pro každou ze dvou hlavních složek výrazu W_k:

- Složka $(x_k Y_{k-1} + y_k X_k)$ je tím menší, čím větší je parametr zpoždění (delay) $\delta \in \mathbb{N}$. Označme $A := \max\{|a| : a \in \mathcal{A}\}$, tj. maximální velikost cifry z abecedy. Potom

$$|x_k Y_{k-1} + y_k X_k| \leq |x_k||Y_{k-1}| + |y_k||X_k| \leq A \cdot \left| \sum_{j=\delta+1}^{k-1} y_j \beta^{-j} \right| + A \cdot \left| \sum_{j=\delta+1}^{k} x_j \beta^{-j} \right| <$$
$$< 2A \cdot \sum_{j=\delta+1}^{\infty} A \cdot |\beta|^{-j} = 2A^2 \cdot \frac{1}{|\beta|^\delta} \cdot \frac{1}{|\beta| \left(1 - \frac{1}{|\beta|}\right)} = \frac{2A^2}{|\beta|^\delta (|\beta| - 1)},$$

  celkově tedy $|x_k Y_{k-1} + y_k X_k| < \left(\frac{1}{|\beta|}\right)^\delta \cdot \left(\frac{2A^2}{|\beta|-1}\right)$. Díky $|\beta| > 1$ se výraz $\left(\frac{1}{|\beta|}\right)^\delta$ zmenšuje (konverguje k nule) při rostoucím $\delta \in \mathbb{N}$, zatímco výraz $\left(\frac{2A^2}{|\beta|-1}\right)$ je konstanta pro daný numerační systém.

- Složku $(W_{k-1} - p_{k-1})$ směřujeme co nejblíže k nule, neboli $p_k = Select_P(W_k) :=$ nejbližší cifra z $\mathcal{A}$ k W_k.

- Dále je třeba, aby β·(okolí nuly) i s přičtením (malé) hodnoty $(x_kY_{k-1} + y_kX_k)$ leželo v okolí $\mathcal{A}$.

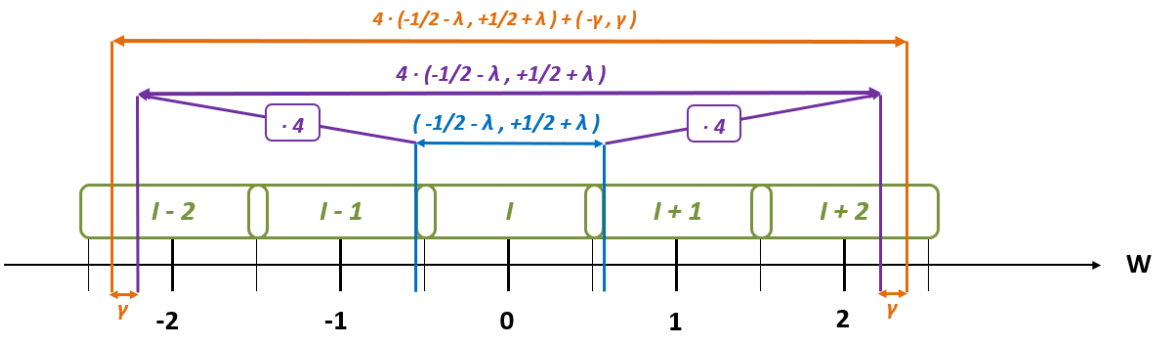
Příklad 8.33. On-line násobení v bázi $\beta = 4$ a abecedě $\mathcal{A} = \{-2, -1, 0, 1, 2\}$:
Množinu I v okolí nuly, kam směřujeme hodnoty $(W_{k-1} - p_{k-1})$, tvoří interval $\left(-\frac{1}{2} - \lambda, +\frac{1}{2} + \lambda\right)$.
V další k-té iteraci pak pracujeme s hodnotou $W_k = \beta(W_{k-1} - p_{k-1}) + (x_kY_{k-1} + y_kX_k)$, pro jejíž velikost platí nerovnost

$$|W_k| \leq |\beta| \, |W_{k-1} - p_{k-1}| + |x_kY_{k-1} + y_kX_k| \,,$$

a složky na pravé straně dále odhadneme shora:

$$|W_{k-1} - p_{k-1}| < \frac{1}{2} + \lambda \qquad \text{a} \qquad |x_kY_{k-1} + y_kX_k| < \left(\frac{1}{|\beta|}\right)^{\delta} \cdot \left(\frac{2A^2}{|\beta| - 1}\right) \leq \gamma \,.$$

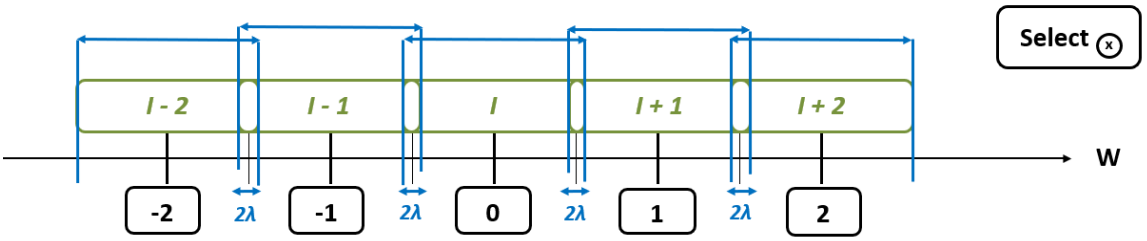
Tak sestavíme odhad celkové velikosti pro výraz W_k, totiž $|W_k| < 4\left(\frac{1}{2} + \lambda\right) = 2 + 4\lambda + \gamma$.
Přitom chceme, aby hodnota W_k ležela v okolí abecedy $\mathcal{A}$, viz ilustrace:



Odtud obdržíme požadavek, aby $2 + 4\lambda + \gamma \leq 2 + \frac{1}{2}$, resp. aby $4\lambda + \gamma \leq \frac{1}{2}$. Tu lze snadno splnit třeba tak, že prostor o velikosti $\frac{1}{2}$ rozdělíme na jednu část pro γ a druhou zbývající část pro 4λ, např. následovně:

- $\gamma := \frac{1}{4}$ je prostor pro hodnotu $|x_kY_{k-1} + y_kX_k| < \gamma \implies$ odtud odvodíme parametr δ (delay), neboť pro dost velké $\delta \in \mathbb{N}$ bude hodnota $|x_kY_{k-1} + y_kX_k|$ dostatečně malá;

- $\lambda := \frac{1}{16}$ je pak prostor pro povolenou nepřesnost při vyhodnocování velikosti W_{k-1}, resp. pro nalezení nejbližšího prvku $p_{k-1} \in \mathcal{A}$ k číslu W_{k-1} funkcí $Select_P$.


Select ⊗
l - 2
l - 1
l
l + 1
l + 2
W
-2
2λ
-1
2λ
0
2λ
1
2λ
2

On-line dělení

Mějme numerační systém $(\beta, \mathcal{A})$, $|\beta| > 1$, kde vstupy - dělence a dělitele - zapíšeme ve tvaru

$$N = 0 \cdot 0 \dots 0 n_{\delta+1} n_{\delta+2} \dots \qquad D = 0 \cdot d_1 d_2 \dots .$$

a výstup / podíl předpokládáme ve tvaru

$$\frac{N}{D} = Q = 0 \cdot q_1 q_2 \dots ,$$

kde cifry $n_j, d_j, q_j \in \mathcal{A}$, a dílčí reprezentace značíme

$$N_k = \sum_{j=1}^{k} n_j \beta^{-j} \qquad D_k = \sum_{j=1}^{k} d_j \beta^{-j} \qquad Q_k = \sum_{j=1}^{k} q_j \beta^{-j} .$$

Navíc předpokládáme, že dělitel D i všechny jeho dílčí reprezentace splňují podmínku kladné velikosti ve tvaru

$$|D_k| = \left| \sum_{j=1}^{k} d_j \beta^{-j} \right| \geq D_{min} > 0 ,$$

kde $D_{min} > 0$ je pevná konstanta pro daný numerační systém $(\beta, \mathcal{A})$.

Algoritmus on-line dělení provádíme v následujících krocích:

- zavedení pomocné proměnné $W_k \in \mathbb{R}$, resp. $W_k \in \mathbb{C}$ pro reálný, resp. komplexní numerační systém;
- iniciace výchozích proměnných (s indexem $k = 0$): $W_0 = q_0 = Q_0 := 0$;
- iterace (pro $k = 1, 2, 3, \dots$) cyklu sestávajícího ze dvou kroků:
  - výpočet pomocné proměnné $W_k := \beta(W_{k-1} - q_{k-1} D_{k-1+\delta}) + \beta^{-\delta}(n_{k+\delta} - Q_{k-1} d_{k+\delta})$,
  - a následně výběr vhodné cifry $q_k := Select_Q(W_k, D_{k+\delta}) \in \mathcal{A}$.

Věta 8.34. *Proměnné W_k určené v algoritmu on-line dělení předpisem $W_k := \beta(W_{k-1} - q_{k-1} D_{k-1+\delta}) + \beta^{-\delta}(n_{k+\delta} - Q_{k-1} d_{k+\delta})$ pro všechna $k \in \mathbb{N}$ splňují rovnost*

$$W_k = \beta^k (N_{k+\delta} - Q_{k-1} D_{k+\delta}) . \tag{8.9}$$

Pokud navíc posloupnost $(W_k)_k$ je omezená, tak platí

$$Q = \lim_{k \to +\infty} Q_{k-1} = \lim \left(\frac{N_{k+\delta}}{D_{k+\delta}} \right) = \frac{N}{D} . \tag{8.10}$$

Důkaz. Vztah (8.9) ukážeme indukcí. Pro $k = 1$ stačí pouze dosadit definiční predpisy a iniciační nulové hodnoty, a vyhodnotit výraz:

$$W_1 = \beta(W_0 - q_0 D_\delta) + \beta^{-\delta}(n_{\delta+1} - Q_0 d_{\delta+1}) = \beta(0 - 0 \cdot D_\delta) + \beta^{-\delta}(n_{\delta+1} - 0 \cdot d_{\delta+1}) =$$
$$= \beta(n_{\delta+1}\beta^{-\delta-1} - 0 \cdot D_{\delta+1}) = \beta^1(N_{\delta+1} - Q_0 \cdot D_{\delta+1}) = \beta^k(N_{\delta+k} - Q_{k-1}D_{\delta+k})\,.$$

V indukčním kroku předpokládáme platnost tvrzení pro $k-1$, a odvozujeme platnost pro k:

$$\begin{aligned} W_k &= \beta(W_{k-1} - q_{k-1}D_{k-1+\delta}) + \beta^{-\delta}(n_{k+\delta} - Q_{k-1} \cdot d_{k+\delta}) = \\ &= \beta(\beta^{k-1}(N_{k-1+\delta} - Q_{k-2}D_{k-1+\delta}) - q_{k-1}D_{k-1+\delta}) + n_{k+\delta}\beta^{-\delta} - Q_{k-1}d_{k+\delta}\beta^{-\delta} = \\ &= \beta^k(N_{k-1+\delta} + n_{k+\delta}\beta^{-k-\delta}) - \beta^k(D_{k-1+\delta}(Q_{k-2} + q_{k-1}\beta^{-k+1}) + Q_{k-1}d_{k+\delta}\beta^{-\delta-k}) = \\ &= \beta^k\left(N_{k+\delta} - Q_{k-1}(D_{k-1+\delta} + d_{k+\delta}\beta^{-k-\delta})\right) = \beta^k(N_{k+\delta} - Q_{k-1}D_{k+\delta})\,. \end{aligned}$$

Ze vztahu (8.9) pak odvodíme vztah (8.10), s využitím omezenosti posloupnosti (W_k) i omezenosti hodnot $|\frac{1}{D_{k+\delta}}|$ díky předpokladu $|D_{k+\delta}| \geq D_{min} > 0$ pro $\forall k \in \mathbb{N}$:

$$(8.9) \quad \Longrightarrow \quad \frac{1}{\beta^k}W_k = N_{k+\delta} - Q_{k-1}D_{k+\delta} \quad \Longrightarrow \quad \frac{1}{D_{k+\delta}} \cdot \frac{1}{\beta^k}W_k = \frac{N_{k+\delta}}{D_{k+\delta}} - Q_{k-1}\,,$$

$$Q = \lim_{k\to\infty}(Q_{k-1}) = \lim_{k\to\infty}\left(\frac{N_{k+\delta}}{D_{k+\delta}} - \frac{1}{D_{k+\delta}} \cdot \frac{1}{\beta^k}W_k\right) = \frac{N}{D} - 0 = \frac{N}{D}\,.$$

□

A opět i pro algoritmus on-line dělení, stejně jako u on-line násobení, je klíčovou úlohou pro sestavení algoritmu určení funkce $Select_Q : (W, \Delta) \to \mathcal{A}$. Tato funkce musí fungovat tak, aby posloupnost $(W_k)_k$ byla omezená, $W_k \in W$; přitom není předem znám definiční obor (W, Δ) funkce $Select_Q$, jen předpokládáme, že Δ neobsahuje žádné okolí nuly.

Ilustrace procesu dělení a efektu delay

Hledáme podíl dělence $N_{orig} = \sum_{j=1}^{\infty} \tilde{n}_j\beta^{-j}$ a dělitele $D_{orig} = \sum_{j=1}^{\infty} \tilde{d}_j\beta^{-j}$. Nejdřív provedeme předzpracování (aneb pre-processing):

- Pro dělenec stačí posun o δ pozic: $N_{new} := \beta^{-\delta}N_{orig} = \sum_{j=\delta+1}^{\infty} n_j\beta^j$, tedy $n_j := \tilde{n}_{j-\delta}$.
- U dělitele ovšem obecně nejde jen o pouhý posun, ale o provedení samostatné úlohy / pre-processing algoritmu, který zajistí existenci konstanty $D_{min} > 0$ takové, že pro $\forall k \in \mathbb{N}$ platí $|D_k| = \left|\sum_{j=1}^{k} d_j\beta^j\right| \geq D_{min}$: upravený tvar dělitele (po předzpracování) označíme $D_{new} := \beta^c D_{orig} = \sum_{j=1}^{\infty} d_j\beta^j$, kde však není k dispozici explicitní obecný předpis pro určení nových cifer $d_j \in \mathcal{A}$ ani pro mocninu c.

Máme tedy převodní vztahy

$$\beta^{-\delta} \cdot N_{orig} = \beta^{-\delta} \cdot 0 \cdot \tilde{n}_1 \tilde{n}_2 \cdots = 0 \cdot 0 \ldots 0 n_{\delta+1} n_{\delta+2} \ldots n_{\delta+k} n_{\delta+k+1} = N_{new}$$
$$\beta^{c} \cdot D_{orig} = \beta^{c} \cdot 0 \cdot \tilde{d}_1 \tilde{d}_2 \cdots = 0 \cdot d_1 d_2 \ldots d_{\delta+1} d_{\delta+2} \ldots d_{\delta+k} d_{\delta+k-1} = D_{new} \ .$$

Po vydělení $N_{new}/D_{new} =: Q_{new}$ on-line algoritmem, v němž k-tá cifra podílu se určí jako funkce $q_k = q_k(N_{k+\delta}, D_{k+\delta})$, zas efekty předzpracování vrátíme zpět:

$$\beta^{-\delta-c} \cdot Q_{orig} = \frac{\beta^{-\delta} \cdot N_{orig}}{\beta^{c} \cdot D_{orig}} = \frac{N_{new}}{D_{new}} = Q_{new} = 0 \cdot q_1 q_2 \ldots q_k q_{k+1} \ldots \ .$$

$$Q_{orig} = \beta^{\delta+c} Q_{new} = (q_1 q_2 \ldots q_\delta \cdot q_{\delta+1} q_{\delta+2} \ldots) \cdot \beta^{c} = (\tilde{q}_{-\delta+1} \tilde{q}_{-\delta+2} \ldots \tilde{q}_0 \cdot \tilde{q}_1 \tilde{q}_2 \ldots) \cdot \beta^{c} \, .$$

Omezenost hodnot $W_k = \beta(W_{k-1} - q_{k-1} D_{k-1+\delta}) + \beta^{-\delta}(n_{k+\delta} - Q_{k-1} d_{k+\delta})$ se snažíme zajistit zvlášť pro každou ze dvou hlavních složek výrazu W_k:

- Označíme velikost maximální cifry jako $A := \max\{|a| : a \in \mathcal{A}\}$. Parametr zpoždění δ lze použít k odhadu, resp. omezení velikosti druhé složky výrazu W_k:

$$|\beta^{-\delta}(n_{k+\delta} - Q_{k-1} d_{k+\delta})| \leq \left(\frac{1}{|\beta|}\right)^{\delta} (|n_{k+\delta}| + |Q_{k-1}| \cdot |d_{k+d}|) \leq$$
$$\leq \left(\frac{1}{|\beta|}\right)^{\delta} \left(A + \frac{A}{|\beta|-1} \cdot A\right) = \left(\frac{1}{|\beta|}\right)^{\delta} A \left(1 + \frac{A}{|\beta|-1}\right) ,$$

  kde hodnota $\left(\frac{1}{|\beta|}\right)^{\delta}$ klesá s rostoucím $\delta \in \mathbb{N}$, a hodnota $A\left(1 + \frac{A}{|\beta|-1}\right)$ je pro daný numerační systém konstantní.

- První složku odhadneme výrazem:

$$|\beta(W_{k-1} - q_{k-1} D_{k-1+\delta})| = |\beta| \cdot |D_{k-1+\delta}| \cdot \left|\frac{W_{k-1}}{D_{k-1+\delta}} - q_{k-1}\right| \leq \frac{|\beta| A}{|\beta| - 1} \cdot \left|\frac{W_{k-1}}{D_{k-1+\delta}} - q_{k-1}\right| .$$

  Složku $\left|\frac{W_{k-1}}{D_{k-1+\delta}} - q_{k-1}\right|$ směřujeme co nejblíže k nule, neboli $q_k = Select_Q(W_k, D_{k+\delta}) :=$ cifra z $\mathcal{A}$, která je nejblíž hodnotě $\frac{W_{k-1}}{D_{k-1+\delta}}$. Pak je potřeba, aby $\left(\frac{|\beta| A}{|\beta|-1}\right) \cdot$(okolí nuly) leželo v okolí $\mathcal{A}$.

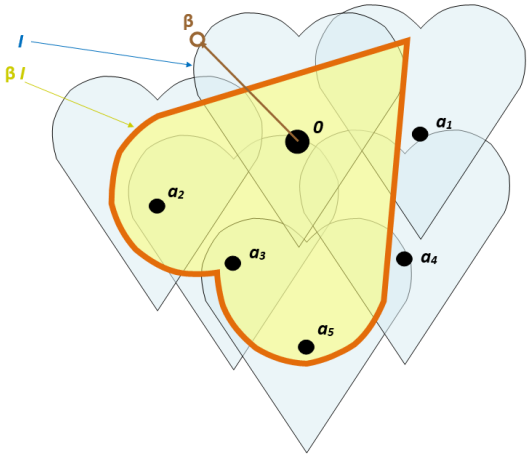
On-line vlastnost numeračního systému

Sestavení fungujících algoritmů on-line násobení a on-line dělení se jistě povede tehdy, když daný numerační systém $(\beta, \mathcal{A})$ disponuje tzv. on-line vlastností. Tato vlastnost zajistí omezenost posloupností $(W_k)_k$, resp. určení funkcí $Select_P$ a $Select_Q$.

Definice 8.35. Numerační systém $(\beta, \mathcal{A})$ má tzv. *on-line vlastnost*, neboli *OL-property*, pokud existuje konstanta $\varepsilon > 0$ a existuje omezená množina $I \subset \mathbb{C}$ splňující podmínku

$$(\forall x \in (\beta I)^{\varepsilon})\ (\exists a \in \mathcal{A})\ (B(x, \varepsilon) \subset I + a), \tag{8.11}$$

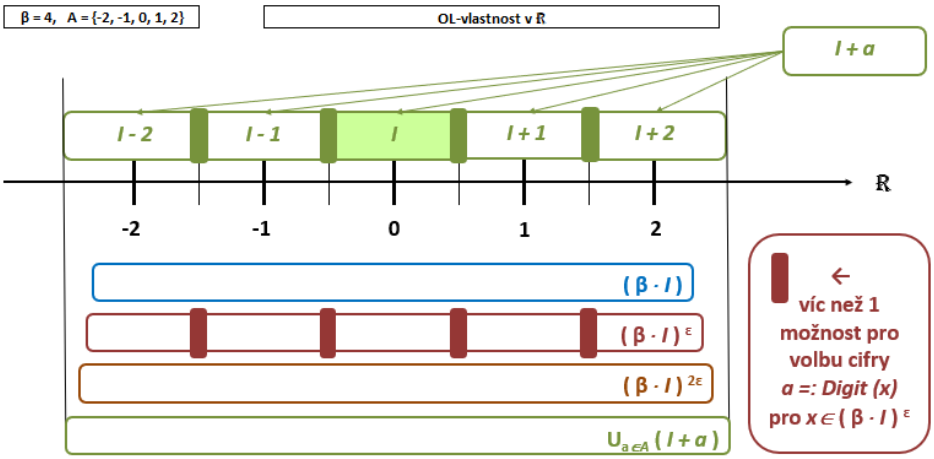
kde $B(x, \varepsilon)$ je ε-okolí bodu x.



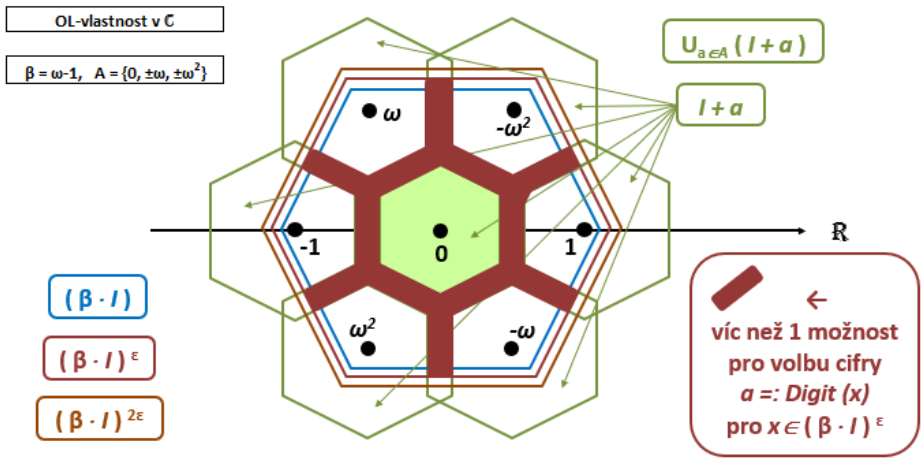
Definice 8.36. Pro numerační systém s OL-vlastností (8.11) definujeme funkci Digit : $(\beta I)^{\varepsilon} \to \mathcal{A}$ tak, že pro libovolné $x \in (\beta I)^{\varepsilon}$ platí

$$\mathrm{Digit}(x) = a \implies B(x, \varepsilon) \subset I + a\,. \tag{8.12}$$

Příklad 8.37. OL-vlastnost v $\mathbb{R}$: pro numerační systém s bází $\beta = 4$ a abecedou $\mathcal{A} = \{0, \pm 1, \pm 2\}$



Příklad 8.38. OL-vlastnost v $\mathbb{C}$: pro numerační systém s bází $\beta = -1 + \omega$ a s abecedou $\mathcal{A} = \{0, \pm 1, \pm\omega, \pm\omega^2\}$, kde $\omega = \exp\left(\frac{2}{3}i\pi\right)$:



Věta 8.39. *Nechť numerační systém $(\beta, \mathcal{A})$ má OL-vlastnost, kde omezená množina $I \subset \mathbb{C}$ a konstanta $\varepsilon > 0$ splňují podmínku $(\forall x \in (\beta I)^{\varepsilon})\ (\exists a \in \mathcal{A})\ (B(x, \varepsilon) \subset I + a)$. Je-li $0 \in I$, pak násobení i dělení jsou proveditelné pomocí on-line algoritmů (Trivedi-Ercegovac).*
Pro on-line dělení přitom navíc požadujeme i existenci algoritmu pro předzpracování dělitele.

Důkaz. Předvedeme postup pro on-line násobení. Indukcí lze ukázat, že posloupnost $(W_k)_k$ z Trivedi-Ercegovac algoritmu splňuje

$$W_k \in (\beta I)^{\frac{\varepsilon}{2}} \qquad \text{pro} \quad k = 0, 1, 2, \dots ,$$

tedy posloupnost $(W_k)_k$ je omezená, a proto on-line algoritmus funguje.

- Pro $k = 0$ stačí použít předpoklad $0 \in I$, pak platí $W_0 = 0 \in I \subset (\beta I)^{\frac{\varepsilon}{2}}$.
- Dál předpokládáme platnost tvrzení pro $k-1$, z nějž odvodíme platnost i pro k:

$$W_k = \beta \underbrace{(W_{k-1} - p_{k-1})}_{\in I} + (x_k Y_{k-1} + y_k X_k),$$

  - Při vhodné volbě (dostatečně velkého) parametru δ je pak dostatečně malá hodnota $(x_k Y_{k-1} + y_k X_k) \in B\left(0, \frac{\varepsilon}{2}\right)$.
  - Z reprezentace $W_{k-1} = (w_{-n} \dots w_0 \cdot w_1 w_2 \dots w_L w_{L+1} \dots)_\beta$ vytvoříme dílčí reprezentaci $\tilde{W}_{k-1} := (w_{-n} \dots w_0 \cdot w_1 w_2 \dots w_L 0^\omega)_\beta$. Pozice $L \in \mathbb{N}$ je přitom zvolena tak, aby platilo $|W_{k-1} - \tilde{W}_{k-1}| < \frac{\varepsilon}{2}$, což lze dosáhnout díky $|\beta| >$ a z nerovnosti / odhadu

$$|W_{k-1} - \tilde{W}_{k-1}| \le \frac{A}{|\beta|^L \cdot (|\beta| - 1)} \overset{!}{<} \frac{\varepsilon}{2} \qquad \text{neboli} \qquad |\beta|^L \overset{!}{>} \frac{2A}{\varepsilon \cdot (|\beta| - 1)} .$$

Odtud obdržíme

$$\underbrace{W_{k-1}}_{(\beta I)^{\frac{\varepsilon}{2}}} = \underbrace{(W_{k-1} - \tilde{W}_{k-1})}_{\in B\left(0,\frac{\varepsilon}{2}\right)} + \underbrace{\tilde{W}_{k-1}}_{=x} \in B\left(x, \frac{\varepsilon}{2}\right) \subset B(x,\varepsilon) \subset I + a = I + p_{k-1}\,,$$

kde $p_{k-1} = \mathrm{Digit}(x)$ a $W_{k-1} - p_{k-1} \in I$.

Pro obě složky výrazu W_k dohromady pak platí požadovaný odhad

$$W_k = \beta \underbrace{(W_{k-1} - p_{k-1})}_{\in I} + \underbrace{(x_k Y_{k-1} + y_k X_k)}_{\in B\left(0,\frac{\varepsilon}{2}\right)} \subset (\beta I)^{\frac{\varepsilon}{2}}.$$

Tím je důkaz hotov pro on-line násobení.
Pro on-line dělení je postup v zásadě analogický, avšak provedení mírně složitější. □

Časová náročnost algoritmů on-line násobení a on-line dělení

Chceme dosáhnout lineární náročnosti $\mathcal{O}(n)$ při určování prvních n cifer výsledku (produktu P nebo podílu Q). Potřebujeme proto redundanci numeračního systému $(\beta, \mathcal{A})$, a to nejen pro realizovatelnost Trivedi-Ercegovac algoritmů jako takových, ale i pro paralelní sčítání / odčítání při dílčích operacích v $(\beta, \mathcal{A})$.
Připomeňme předpisy pro výpočet pomocných proměnných W_k v obou on-line algoritmech:

- násobení: $W_k = \beta(W_{k-1} - p_{k-1}) + (x_k Y_{k-1} + y_k X_k)$
- dělení: $W_k = \beta(W_{k-1} - q_{k-1} D_{k-1-\delta}) + \beta^{-\delta}(n_{k+\delta} - Q_{k-1} d_{k+\delta})$

Jsou v nich použity následující operace:

- sčítání a odčítání: pokud možno paralelně;
- násobení $(\cdot\beta)$, resp. $(\cdot\beta^{-\delta})$ je pouhý posun cifer o několik pozic;
- násobení $(\cdot x_k)$, $(\cdot y_k)$, $(\cdot d_{k+\delta})$, $(\cdot q_{k-1})$ je násobení cifrou z abecedy $\mathcal{A}$, která je konečná.

Celkově se tedy jedná o konečný (pevně omezený) počet operací sčítání v $(\beta, \mathcal{A})$ a posunů cifer o několik pozic $(\cdot\beta)$. Úloha výpočtu proměnné W_k má tedy konstantní složitost.
Navíc k určení cifry p_k, resp. cifry q_k pomocí funkce $Select_P$, resp. $Select_Q$ nepoužijeme celou proměnnou W_k, ale jen její dílčí reprezentaci $\tilde{W}_k$ (s přesností na L pozic za zlomkovou tečkou). Analogicky i z dělitele $D_{k+\delta}$ použijeme jen dílčí reprezentaci $\tilde{D}_{k+\delta}$.

V souhrnu nakonec můžeme učinit ten závěr, že funkce $Select_P(\tilde{W}_k)$ a $Select_Q(\tilde{W}_k, \tilde{D}_{k+\delta})$ lze realizovat vlastně jako výběry z konečných seznamů (vyhledáváním v Lookup Table).

Předzpracování (pre-processing) dělitele

Jedná se o samostatnou úlohu vedoucí ke splnění podmínky pro dělitele $D = \sum_{j=1}^{\infty} d_j \beta^{-j}$ s ciframi $d_j \in \mathcal{A}$, aby byl přípustným vstupem do algoritmu on-line dělení. Musí se najít taková konstanta $D_{min} > 0$ (pevná pro daný numerační systém $(\beta, \mathcal{A})$), že pro $\forall k \in \mathbb{N}$ platí

$$|D_k| = \left| \sum_{j=1}^{k} d_j \beta^{-j} \right| \geq D_{min}.$$

Příklad 8.40. Pro bázi $\beta = 4$ s abecedou $\mathcal{A} = \{-2, -1, 0, 1, 2\}$ stačí jen provést posun zlomkové tečky k první nenulové cifře - tak aby $d_1 \neq 0$. Potom platí

$$|D_k| = \left| \sum_{j=1}^{k} d_j \beta^{-j} \right| = \left| \frac{d_1}{\beta} + \sum_{j=2}^{k} d_j \beta^{-j} \right| \geq \frac{1}{\beta} - \sum_{j=2}^{\infty} 2\beta^{-j} = \frac{1}{4} - 2\sum_{j=2}^{\infty} \left(\frac{1}{4}\right)^j = \frac{1}{4} - \frac{1}{6} = \frac{1}{12}\,.$$

Tedy $|D_k| \geq D_{min} := \frac{1}{12} > 0$ pro všechna $k \in \mathbb{N}$.

Příklad 8.41. Pro bázi $\beta = 2$ s abecedou $\mathcal{A} = \{-1, 0, 1\}$ se samozřejmě taky dělá posun zlomkové tečky k první nenulové cifře, ale to nestačí. Analogický způsob odhadu jako v předchozím případě vede jen k $|D_k| \geq \frac{1}{2} - \frac{1}{2} = 0$.

Je nutné navíc ještě použít přepisovací pravidlo $\pm[1, -2]$, kdykoliv to lze - zleva od začátku reprezentace D. Tím vyloučíme problematické řetězce $(d_1 d_2) = \pm(1, -1)$ a dostaneme lepší odhad pro upravené D:

$$|D_k| \geq \frac{1}{2} - \sum_{j=3}^{\infty} \left(\frac{1}{2}\right)^j = \frac{1}{2} - \frac{1}{4} = \frac{1}{4}\,,$$

tedy získáme $D_{min} = \frac{1}{4} > 0$, po tomto důkladnějším předzpracování.

Literatura

[1] S. Akiyama, N. Gjini, Connectedness of number theoretic tilings, Discret. Math. Theoret. Comput. Sci. 7 (2005), 269–312.

[2] S. Akiyama, *Cubic Pisot Units with finite beta expansions,* in *Algebraic Number Theory and Diophantine Analysis,* Graz 1998, Eds. F. Halter-Koch and R.F. Tichy, de Gruyter, Berlin, (2000), 11–26.

[3] A. Avizienis, Signed-digit number representations for fast parallel arithmetic, *IRE Trans. Electron. Comput.* **10** (1961), 389–400.

[4] P. Ambrož, Ch. Frougny, Z. Masáková, E. Pelantová, Arithmetics on number systems with irrational bases, Bull. Soc. Math. Belg. 10 (2003), 641–659.

[5] W. Bolyai, Tentamen iuventutem studiosam in elementa matheseos purae elementaris ac subIimioris methodo intuitiva evidentiaque huie propria introdueendi, ed. sec. (Budapest, 1897), Vol. I.

[6] D. Boyd, Salem numbers of degree four have periodic expansions, In: de Koninck, J.M., Levesque, C. (eds.) Théorie des Nombres—Number Theory, Walter de Gruyter, Berlin (1989), 57–64.

[7] A. Brauer, On algebraic equations with all but one root in the interior of the unit circle, Math. Nachr. 4 (1951), 250–257.

[8] A. Cauchy, Sur les moyens d'éviter les erreurs dans les calculs numériques, *C.R. Acad. Sc. Paris* série I **11** (1840), 789–798.

[9] C.Y. Chow, J.E. Robertson, Logical design of a redundant binary adder, in *Proc. 4th IEEE Symposium on Computer Arithmetic* (1978), 109–115.

[10] M. Fiedler, Speciální matice a jejich použití v numerické matematice, SNTL (edice Teoretická knižnice inženýra), Praha 1981.

[11] Ch. Frougny, B. Solomyak, Finite beta-expansions, Ergodic Theory Dynam. Systems, 12 (1992), 713–723.

[12] Ch. Frougny, M. Pavelka, E. Pelantová, M. Svobodová, On-line algorithms for multiplication and division in real and complex numeration systems, Discr. Math. Theor. Comput. Sci. **21**(3), (2019), #14.

[13] Ch. Frougny, E. Pelantová, M. Svobodová, Minimal digit sets for parallel addition in non-standard numeration systems, Jour. Integ. Seq. **16**(2), (2013), A13.2.17.

[14] Ch. Frougny, E. Pelantová, M. Svobodová, Parallel addition in non-standard numeration systems, Theor. Comp. Sci. **412**, (2011), 5714–5727.

[15] P.J. Grabner, C. Heuberger, On the Number of Optimal Base 2 Representations of Integers. Des Codes Crypt 40, (2006), 25–39.

[16] L.S. Guimond, Z. Masáková, E. Pelantová, Arithmetics on β-expansions, Acta Arith. 112 (2004), 23–40.

[17] M. Hollander, Linear numeration systems, finite beta expansions, and discrete spectrum of substitution dynamical systems, Ph.D. Thesis, University of Washington (1996).

[18] I. Kátai, J. Szabó, Canonical number systems in imaginary quadratic fields, Acta Sci Math 37, (1975), 255–260.

[19] M. Lothaire, Algebraic combinatorics on words, Encyclopedia of Mathematics and its Applications 90, Cambridge University Press, 2002.

[20] J.-M. Muller. Elementary Function: Algorithms and Implementation, Birkhauser, 2. ed. 2006.

[21] A. M. Nielsen, P. Kornerup, On Radix Representation of Rings, IEEE Transactions on Computers, 48, (1997), 34–43.

[22] B. Parhami, On the Implementation of Arithmetic Support Functions for Generalized Signed-Digit Number Systems, *IEEE Trans. Computers* **42** No. 3 (1993), 379–384.

[23] W. Parry, On the β-expansions of real numbers, Acta Math. Acad. Sci. Hungar., 11 (1960), 401–416.

[24] W. Penney, A "binary"system for complex numbers. *J.A.C.M.*, 12 (1965), 247–248.

[25] A. Rényi, Representations for real numbers and their ergodic properties, Acta Math. Acad. Sci. Hungar., 8 (1957), 477–493.

[26] G. Reitwiesner, Binary arithmetic, in Advances in Computers, 1, Academic Press, New York, (1960), 231–308.

[27] K. Schmidt, On periodic expansions of Pisot numbers and Salem numbers, Bull. London Math. Soc. 12 (1980), 269–278.

[28] B. Solomyak, Conjugates of Beta-Numbers and the Zero-Free Domain for a Class of Analytic Functions, Proc. London Math. Soc., 68 (1994), 477–498.

[29] K.S. Trivedi, M.D. Ercegovac, On-line algorithms for division and multiplication, IEEE Transactions on Computers **C-26**, (1977), 681–687.

[30] W. Thurston, Groups, tilings, and finite state automata, AMS Colloquium Lecture Notes, Boulder, 1989.