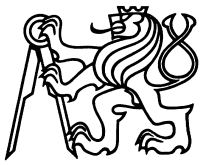
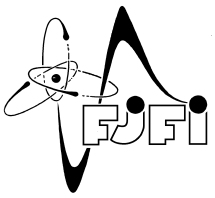


České vysoké učení technické v Praze
Fakulta jaderná a fyzikálně inženýrská



Poziční reprezentace vektorů

Positional Representations of Vectors

Bakalářská práce

Autor: **Stefan Hajduk**

Vedoucí práce: **Ing. Milena Svobodová, Ph.D.**

Konzultant: **Ing. Tomáš Vávra, Ph.D.**

Akademický rok: 2019/2020

České vysoké učení technické v Praze, Fakulta jaderná a fyzikálně inženýrská

Katedra: matematiky

Akademický rok: 2019/2020

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Student:	Stefan Hajduk
Studijní program:	Aplikace přírodních věd
Obor:	Matematická informatika
Název práce (česky):	Poziční reprezentace vektorů
Název práce (anglicky):	Positional Representations of Vectors

Pokyny pro vypracování:

1. Nastudujte známé výsledky o pozičních numeračních systémech, ve kterých prvky z množiny $\mathbb{Z}^d$ mají jednoznačné reprezentace.
2. Navrhněte a implementujte algoritmus, který rozhodne, zda zadaná expandující matice a množina cifer $\mathcal{D} \subset \mathbb{Z}^d$ tvoří takový numerační systém.
3. Systém pro reprezentaci množiny $\mathbb{Z}^2$ interpretujte jako numerační systém pro kvadratické těleso; zkoumejte případy reálné i komplexní (speciálně systémy Penneyho a Eisensteinův).
4. Seznamte se s matematickým aparátem a technikami používanými při tvorbě algoritmů pro paralelní sčítání v redundantních numeračních systémech (v tělese reálném i komplexním).
5. Pokuste se zobecnit metody pro paralelní sčítání i na poziční reprezentace vektorů.

Doporučená literatura:

1. A. Kovács, Radix expansion in lattices. Ph.D. thesis, Eötvös Loránd University Budapest, 2001.
2. J. Jankauskas, J. Thuswaldner, Characterization of rational matrices that admit finite digit systems. Linear Algebra and its Applications 557, 2018, 350–358.
3. M. Lothaire, Algebraic Combinatorics on Words. Encyclopedia of Mathematics and its Applications 90, Cambridge University Press, Chapter 8: Numeration Systems, 2002.
4. Ch. Frougny, E. Pelantová, and M. Svobodová, Parallel addition in non-standard numeration systems. Theor. Comput. Sci. 412, 2011, 5714–5727.

Jméno a pracoviště vedoucího bakalářské práce:

Ing. Milena Svobodová, Ph.D.
Katedra matematiky, Fakulta jaderná a fyzikálně inženýrská (FJFI), České vysoké učení technické (ČVUT), Trojanova 13, 120 00, Praha 2

Jméno a pracoviště konzultanta:

Ing. Tomáš Vávra, Ph.D.
Katedra algebry, Matematicko-fyzikální fakulta (MFF), Univerzita Karlova (UK), Sokolovská 83, 186 75, Praha 8

Datum zadání bakalářské práce: 31.10.2019

Datum odevzdání bakalářské práce: 7.7.2020

Doba platnosti zadání je dva roky od data zadání.

V Praze dne 23. října 2019

V.z. .....
garant oboru

.....
vedoucí katedry

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta jaderná a fyzikálně inženýrská
-1-

.....
děkan

Poděkování:
Chtěl bych zde poděkovat především své školitelce Mileně Svobodové za pečlivost, ochotu, vstřícnost a odborné i lidské zázemí při vedení mé bakalářské práce. Dále děkuji svému konzultantovi Tomáši Vávrovi za pomoc při programování. Následně patří velké poděkování Editě Pelantové, která mi pomohla s mnoha důkazy, které v práci uvádím.

Čestné prohlášení:
Prohlašuji, že jsem tuto práci vypracoval samostatně a uvedl jsem všechnu použitou literaturu.

V Praze dne 16. července 2020 Stefan Hajduk

Název práce:

Poziční reprezentace vektorů

Autor: Stefan Hajduk

Obor: Matematická informatika

Druh práce: Bakalářská práce

Vedoucí práce: Ing. Milena Svobodová, Ph.D., Katedra matematiky, Fakulta jaderná a fyzikálně inženýrská, České vysoké učení technické

Konzultant: Ing. Tomáš Vávra, Ph.D., Katedra algebry, Matematicko-fyzikální fakulta, Univerzita Karlova

Abstrakt: Tato práce se věnuje maticovým numeračním systémům a paralelním algoritmům na sčítání. Jsou v ní dokázané vlastnosti maticových systémů, například kolik tříd ekvivalence má kongruence modulo M, nebo jak vypadá abeceda systému, který jednoznačně reprezentuje množinu $\mathbb{Z}^d$. Následně je vyslovena a dokázána postačující podmínka pro systém, aby reprezentoval $\mathbb{Z}^d$. Dále je popsán a implementován program, který rozhoduje, zda maticový systém reprezentuje množinu $\mathbb{Z}^d$. V závěru práce jsou shrnuty poznatky o paralelním sčítání v nestandardních systémech a jsou zde uvedeny příklady paralelních algoritmů pro sčítání v maticových numeračních systémech.

Klíčová slova: Eisensteinův systém, maticový systém, paralelní sčítání, Penneyho systém, poziční numerační systém

Title:

Positional Representations of Vectors

Author: Stefan Hajduk

Abstract: This work deals with matrix number systems and with parallel algorithms for addition. The properties of matrix systems are proved, for instance how many equivalence classes has kongruence modulo M or what attributes the alphabet of matrix system which uniquely represents $\mathbb{Z}^d$ has. Afterwards, sufficient condition for system to represent $\mathbb{Z}^d$ is stated and proved. Consequently, program which decides whether the matrix system represents $\mathbb{Z}^d$ is described and implemented. At the end of work, knowledge about parallel algorithms for addition in the positional numerical systems is summarized and afterwards examples of parallel algorithms for addition in the matrix systems are stated.

Key words: Eisenstein system, matrix system, parallel addition, Penney system, positional numeral system

Obsah

Seznam použitých symbolů

Symbol	Popis
$\overset{!}{=}$	rovnost, po které požadujeme, aby platila
$(a_n \dots a_0)_{(\beta,\mathcal{A})}$	reprezentace v numeračním systému s bází β a abecedou $\mathcal{A}$
$\#A$	počet prvků v množině A
A^*	množina všech konečných řetězců z prvků množiny A
$\bar{x}$	$\bar{x} := -x$, kde $x \in \mathbb{Z}$
$[x]_\sim$	třída ekvivalence obsahující prvek x podle $\sim$
$M_{\bullet j}$	j-tý sloupec matice M
$\sigma(M)$	množina všech vlastních čísel matice M, tj. spektrum matice M
$\varrho(M)$	spektrální poloměr matice M, $\varrho(M) = \max_{\lambda\in\sigma(M)} \lvert\lambda\rvert$
$\mathbb{N}$	$\mathbb{N} = \{0, 1, 2, \dots\}$
V°	vnitřek množiny V
$vol(V)$	objem množiny V

Úvod

Paralelní algoritmy pro sčítání jsou hojně využívány při manipulaci s velkými čísly, například v kryptografii, kdy umožňují snížit časovou složitost z lineární na konstantní v paralelním provedení. Jejich praktické využití je ještě umocněno faktem, že v dnešní době jsou běžné počítače s více jádry.

První základy těchto algoritmů byly položeny v roce 1961 litevským matematikem Algirdasem Avizienisem v práci [1], kde umožnil běh paralelních algoritmů pro sčítání přidáním cifer do abecedy, pomocí kterých reprezentoval čísla. Ale věnoval se pouze systémům, které měly jako bázi nezáporné celé číslo. Tento základ byl rozšířen v práci [3], kde byla uvažována jako báze také algebraická čísla v $\mathbb{C}$.

Již zmíněná báze a abeceda je základem numeračních systémů. V případě pozičního numeračního systému je báze komplexní číslo a abeceda je podmnožinou množiny komplexních čísel. Příkladem takového systému je dekadický systém, kde báze je rovna 10 a abeceda je $\{0, 1, \ldots, 9\}$. Existují taktéž méně standardní poziční numerační systémy, na ukázku můžeme jmenovat v práci hojně využívaný Penneyho systém, kde báze je rovna $\mathrm{i} - 1$ a abeceda rovna $\{0, 1\}$.

Za rozšíření pozičních numeračních systémů, kde reprezentujeme komplexní čísla, můžeme považovat maticové numerační systémy, ve kterých reprezentujeme vektory. Zde se taktéž vyskytuje báze, nyní je to matice a abecedou je množina vektorů.

Hlavní myšlenka numeračních systémů je reprezentace čísel či vektorů, proto se v práci věnujeme algoritmům, které najdou reprezentaci čísla či vektoru v daném numeračním systému. Taktéž požadujeme, aby numerační systém reprezentoval celý prostor. Proto se při zkoumání vlastností maticových systémů zaměříme na vytvoření postačující podmínky, která zaručí reprezentaci množiny $\mathbb{Z}^d$.

Dalším cíle práce je vytvořit program, který bude využívat tuto postačující podmínku, a bude schopen rozhodnout o maticovém systému, zda reprezentuje celou množinu $\mathbb{Z}^d$. V tomto programu budeme moci využívat i jiné vlastnosti maticových systémů, které nám umožní rychlejší rozhodnutí o vhodnosti systému.

Nakonec studujeme paralelní algoritmy pro sčítání v pozičních numeračních systémech, ukážeme jejich rozdíl oproti klasickému algoritmu na sčítání a následně se podíváme na jejich zobecnění v množině komplexních čísel. V poslední řadě prozkoumáme již vytvořené paralelní algoritmy v maticových systémech.

Kapitola 1

Číselné numerační systémy

Hlavním pojmem této práce je poziční numerační systém, pod kterým rozumíme dvojici $(\beta, \mathcal{A})$, kde $\beta \in \mathbb{C}, |\beta| > 1$ a $\mathcal{A} \subset \mathbb{C}$ je konečná množina obsahující 0. Číslo β nazýváme bází a množinu cifer $\mathcal{A}$ označujeme jako abecedu.

Smyslem numeračního systému je reprezentace čísel.

Definice 1. *Mějme x komplexní číslo. Řekneme, že x má v $(\beta, \mathcal{A})$ reprezentaci, pokud x se dá zapsat jako $x = \sum_{-\infty}^{n} a_i \beta^i$, kde $a_n, a_{n-1}, \ldots \in \mathcal{A}$ a řetězec $a_n a_{n-1} \ldots$ nazýváme $(\beta, \mathcal{A})$-reprezentací čísla x. Pokud $n \geq 0$, zapisujeme $x = (a_n a_{n-1} \ldots a_0 \,.\, a_{-1} \ldots)_{(\beta,\mathcal{A})}$, v opačném případě $x = (0 \,.\, 0 \ldots 0\, a_n a_{n-1} \ldots)_{(\beta,\mathcal{A})}$.*

Jako první nenulová cifra se v řetězci vyskytuje ta s největší váhou (tj. u největší mocniny β). Na toto pořadí cifer jsme zvyklí z desítkové soustavy.

Dodejme, že podmínka $|\beta| > 1$ a konečnost abecedy zaručuje konvergenci sumy $\sum_{-\infty}^{n} a_i \beta^i$.

Z definice vidíme, že můžeme zkoumat numerační systémy, které reprezentují čísla z množiny komplexních čísel, ale numerační systém nemusí nutně reprezentovat celou tuto množinu. Z tohoto důvodu uvádíme následující definici.

Definice 2. *Nechť $(\beta, \mathcal{A})$ je poziční numerační systém. Množinu všech komplexních čísel s konečnou $(\beta, \mathcal{A})$-reprezentací značíme jako*

$$\mathrm{Fin}_{\mathcal{A}}(\beta) := \left\{ \sum_{j=-m}^{n} a_j \beta^j : m, n \in \mathbb{N}, a_j \in \mathcal{A} \right\}.$$

Definujme pro poziční numerační systémy celá čísla. Jsme zvyklí, že celá čísla mají reprezentaci „před tečkou“, proto uvažujeme nenulové cifry u nezáporných mocnin čísla β.

Definice 3. *Nechť $(\beta, \mathcal{A})$ je poziční numerační systém. Jako $(\beta, \mathcal{A})$-celá čísla označujeme množinu*

$$\mathbb{Z}_{\mathcal{A}}(\beta) := \left\{ \sum_{j=0}^{n} a_j \beta^j : n \in \mathbb{N}, a_j \in \mathcal{A} \right\}.$$

Pro paralelní sčítání budeme u systémů vyžadovat, aby byly redundantní.

Definice 4. *Numerační systém $(\beta, \mathcal{A})$ nazveme redundantní, pokud existuje číslo $x \in \mathrm{Fin}_{\mathcal{A}}(\beta)$, které má dvě různé konečné $(\beta, \mathcal{A})$-reprezentace.*

Zde je předpoklad konečné reprezentace důležitý. Například v dekadickém numeračním systému, který má bázi 10, abecedu $\{0,\dots,9\}$, a který není redundantní, můžeme najít u čísla 1 jednu konečnou reprezentaci a jednu nekonečnou reprezentaci: $1 = 1. = 0.\overline{9}$.

V následujících třech podkapitolách se budeme věnovat reprezentaci čísel z diskrétních množin. Po nich budou následovat dvě podkapitoly, kde studujeme rozvoje reálných i komplexních čísel.

1.1 Reprezentace celých čísel

Uvažujme zatím reprezentace čísel „před tečkou“, tedy reprezentace ve tvaru $\sum_{j=0}^{n} a_j \beta^j$, kde $n \in \mathbb{N}$ a $a_j \in \mathcal{A}$. Ukážeme na nich příklady numeračních systémů, které reprezentují množiny $\mathbb{N}$ a $\mathbb{Z}$. Pro tyto systémy je užitečné definovat relaci modulo β.

Definice 5. *Nechť $\beta \in \mathbb{Z}$. Řekneme, že čísla $a, b \in \mathbb{Z}$ jsou kongruentní modulo β, pokud existuje číslo $z \in \mathbb{Z}$ takové, že $a - b = z\beta$, a značíme $a \equiv_\beta b$.*

Tuto relaci využijeme k představení algoritmu pro hledání reprezentace v systému $(\beta, \mathcal{A})$.

První algoritmus v $\mathbb{N}$: Hledání reprezentace čísla v numeračním systému $(\beta, \mathcal{A})$, kde $\beta \in \mathbb{N}, \beta \geq 2$ a $\mathcal{A} = \{0, 1, \dots, \beta - 1\}$

---

vstup : číslo $x \in \mathbb{N}$, pro které hledáme reprezentaci v $(\beta, \mathcal{A})$
výstup: řetězec $a_n \dots a_0 \in \mathcal{A}^*$, který vyjadřuje reprezentaci x v $(\beta, \mathcal{A})$, tzn. $x = \sum_{i=0}^{n} a_i \beta^i$

```
1 i := 0
2 while x ≠ 0 do
3 |   najdi a_i ∈ A tak, aby a_i ≡_β x
4 |   x := β^{-1}(x − a_i)
5 |   i := i + 1
6 end
7 n := i − 1
8 a := a_n a_{n−1} ... a_0
9 return a
```

Příklad 6. *Systém, kde $\beta = 2, \mathcal{A} = \{0, 1\}$, nazýváme binární soustavou. Je zřejmé, že pro všechna $x \in \mathbb{N}$ lze najít reprezentaci pomocí prvního algoritmu. Použijme ho nyní pro nalezení reprezentace čísla 13.*

V prvním kroku zjevně $a_0 = 1$, protože $13 - 1 = 12 = 6 \cdot 2$. Nyní nové $x := 12/2 = 6$. Dále vidíme, že $a_1 = 0$, protože číslo 6 je dělitelné dvojkou, tedy $x := 6/2 = 3$. Analogicky dále postupujeme a nakonec dostaneme řetězec, který reprezentuje číslo 13, a to $(1101)_2$.

Příklad 7. *Nechť $\beta = 2$, $\mathcal{A} = \{-1, 0, 1\}$. Jedná o systém z předchozího příkladu rozšířený o jednu cifru v abecedě. V předchozím příkladě bylo možné reprezentovat množinu přirozených čísel, proto i tento systém reprezentuje všechna přirozená čísla. Navíc díky přidané cifře se tento systém stal redundantním, např. $(5)_{10} = (101)_{(\beta,\mathcal{A})} = (10\overline{1}\overline{1})_{(\beta,\mathcal{A})}$. Připomeňme, že píšeme mínus nad číslo.*

Ukážeme, že dokonce všechna celá čísla lze reprezentovat. Pokud má $z \in \mathbb{N}$ reprezentaci $a_n \dots a_0$, tak $-z$ má reprezentaci $\overline{a_n} \dots \overline{a_0}$. Díky faktu, že abeceda je symetrická, vidíme, že také záporná čísla jsou reprezentovatelná.

Později dokážeme věty 44 a 72, které pomůžou při zkoumání systémů v množině $\mathbb{Z}^d$. Nyní zmíníme závěry těchto vět pro případ, kdy $d = 1$, tedy pro $\mathbb{Z}$.

Příklad 8. *V případě $\beta = 3$ a $\mathcal{A} = \{-1, 0, 1\}$ platí, že množinu $\mathbb{Z}$ lze reprezentovat, protože systém splňuje předpoklady věty 72.*

Příklad 9. *Pro systém $\beta = 3$ a $\mathcal{A} = \{-1, 0, 2\}$ platí, že abeceda neobsahuje alespoň jeden prvek z každé třídy ekvivalence, proto s použitím věty 44 dostáváme, že množina $\mathbb{Z}$ není reprezentovaná.*

Příklad 10. *Zvolme systém jako $\beta = -2$, $\mathcal{A} = \{0, 1\}$. Také zde jsou splněny předpoklady věty 72, proto můžeme prozradit, že tento systém reprezentuje množinu $\mathbb{Z}$.*

Vidíme, že systémy, které mají nezápornou bázi či nezáporné cifry v abecedě, mohou být také vhodným systémem k reprezentaci množiny $\mathbb{Z}$.

1.2 Penneyho numerační systém

Dosud jsme měli příklady systémů, které měly jako bázi a cifry v abecedě čísla, která ležela na reálné ose. Nyní se zaměříme na systémy, které mají jako bázi čísla komplexní.

Definujme nejprve diskrétní podmnožinu komplexních čísel.

Definice 11. *Množinou Gaussových celých čísel rozumíme množinu $\mathbb{Z}[\mathrm{i}] = \{a + b\mathrm{i} : a, b \in \mathbb{Z}\}$.*

Připomeňme, že trojice $(\mathbb{Z}[\mathrm{i}], +, \cdot)$ tvoří okruh s operacemi sčítání a násobení komplexních čísel. To znamená, že pro všechna $x, y, z \in \mathbb{Z}[\mathrm{i}]$ platí:

1. $x + y \in \mathbb{Z}[\mathrm{i}]$, $x \cdot y \in \mathbb{Z}[\mathrm{i}]$, tj. množina $\mathbb{Z}[\mathrm{i}]$ je uzavřená na operace + a $\cdot$,
2. $(x + y) + z = x + (y + z)$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, tzn. operace + a $\cdot$ jsou asociativní,
3. $x + y = y + x$, což znamená, že operace + je komutativní,
4. $x \cdot (y + z) = (x \cdot y) + (x \cdot z), (y + z) \cdot x = (y \cdot x) + (z \cdot x)$, tedy, že platí distributivní zákony,
5. pro každé $x \in \mathbb{Z}[\mathrm{i}]$ existuje $a \in \mathbb{Z}[\mathrm{i}]$ takové, že $x + a = 0$, kde 0 je neutrální prvek vzhledem ke sčítání a a nazýváme opačný prvek k x.

Navíc okruh $(\mathbb{Z}[\mathrm{i}], +, \cdot)$ je zřejmě komutativní i vzhledem k násobení.

Walter F. Penney v roce 1965 zkoumal systémy, které reprezentují Gaussova celá čísla[9]. Zformuloval a dokázal tvrzení, že systém $\beta = \mathrm{i} - 1$ a $\mathcal{A} = \{0, 1\}$ reprezentuje všechna Gaussova celá čísla. Tento systém nazýváme Penneyho numeračním systémem. Důkaz následujícího tvrzení je převzat z knihy [8].

Věta 12. *Nechť $\beta = \mathrm{i} - 1$ a $\mathcal{A} = \{0, 1\}$. Pak všechna Gaussova celá čísla mají reprezentaci v $(\beta, \mathcal{A})$ ve tvaru $\sum_{i=0}^{n} a_i \beta^i$, kde $a_i \in \mathcal{A}$.*

Důkaz. Buď $z = x + \mathrm{i}y$ libovolné komplexní číslo, kde $x, y \in \mathbb{Z}$. Ukážeme, že toto číslo lze převést do tvaru $z = d_0 + d_1\beta + d_2\beta^2 + d_3\beta^3$, kde $d_0, d_1, d_2, d_3 \in \mathbb{N}$. Poté z tohoto tvaru najdeme reprezentaci čísla z.

Rozepišme z po složkách:

$$z = x + \mathrm{i}y = c + d\beta = c + \mathrm{i}d - d,$$

kde $d = y$ a $c = x + d = x + y$. Nyní platí, že $c, d \in \mathbb{Z}$. Převedeme koeficienty c, d do $\mathbb{N}$, k tomu poslouží identita

$$\beta^2 + 2\beta + 1 = -1, \tag{1.1}$$

která vznikne umocněním rovnice $\beta + 1 = i$. Pokud $c < 0$, rozepíšeme $c = -1 \cdot \bar{c}$, kde $\bar{c} \in \mathbb{N}$ a nyní použijeme identitu (1.1). Tímto dostáváme rovnost

$$z = c + d\beta = \bar{c} + 2\bar{c}\beta + \bar{c}\beta^2 + d\beta = \bar{c} + (2\bar{c} + d)\beta + \bar{c}\beta^2.$$

Analogicky můžeme provést postup pro d a dostaneme rozklad čísla $z = d_0 + d_1\beta + d_2\beta^2 + d_3\beta^3$, kde d_0, d_1, d_2, d_3 jsou již z množiny $\mathbb{N}$.

Nyní chceme převést cifry d_i z množiny přirozených čísel do množiny $\mathcal{A}$, a tím najít reprezentaci z v $(\beta, \mathcal{A})$.

Uvažujme obecnější případ, kdy $z = d_0 + d_1\beta + \cdots + d_k\beta^k, d_i \in \mathbb{N}, k \geq 3$ a označme $d = d_k \cdots d_0 \in \mathbb{N}^*$ a S funkci, která bude sčítat cifry:

$$\begin{aligned} S : \mathbb{C} \times \mathbb{N}^* &\to \mathbb{N} \\ (z, d) &\mapsto d_0 + \cdots + d_k. \end{aligned}$$

Ještě budeme využívat identitu ve tvaru

$$\beta^3 + \beta^2 = 2, \tag{1.2}$$

jejíž platnost lze snadno ověřit. Pokud budeme rovnici (1.2) vnímat jako reprezentaci čísla 2, vidíme, že obě reprezentace, tj. obě strany rovnice (1.2) mají stejný ciferný součet, a tedy i stejnou hodnotu funkce S. Nyní přejdeme k algoritmu pro nalezení $(\beta, \mathcal{A})$-reprezentace z.

Na cifru d_0 použijeme celočíselné dělení číslem 2 se zbytkem, tzn. najdeme r_0, q_0 takové, že $d_0 = r_0 + 2q_0, r_0 \in \{0, 1\}$. Rozepišme z pomocí čísel q_0, r_0 a použijeme identitu (1.2) na $2q_0$:

$$\begin{aligned} z &= d_0 + d_1\beta + d_2\beta^2 + d_3\beta^3 = r_0 + 2q_0 + d_1\beta + \cdots + d_k\beta^k = \\ &= r_0 + d_1\beta + (q_0 + d_2)\beta^2 + (q_0 + d_3)\beta^3 + \cdots + d_k\beta^k =: d_0^{(1)} + \cdots + d_k^{(1)}\beta^k. \end{aligned}$$

Díky tomu, že identita (1.2) a rovnice $d_0 = r_0 + 2q_0$ zachovávají ciferný součet, platí $S(z, d) = S(z, d^{(1)})$, kde $d^{(1)} = d_k^{(1)} \cdots d_0^{(1)}$. Nyní definujeme nové číslo

$$z_1 := (z - r_0)\beta^{-1} = (z - d_0^{(1)})\beta^{-1} = d_1^{(1)} + d_1^{(1)}\beta + \cdots + d_k^{(1)}\beta^{k-1}.$$

Z definice z_1 plyne, že pokud z_1 má reprezentaci $a_n \ldots a_1$, tak z má reprezentaci $a_n \ldots a_1 r_0$. Díky $d_0 \geq 0$ platí $S(z_1, d^{(1)}) \leq S(z, d^{(1)}) = S(z, d)$ a rovnost nastává právě tehdy, když $r_0 = d_0 = 0$. Opakováním tohoto procesu dostaneme posloupnost $(z_j)_{j=1}^{\infty}$:

$$\begin{aligned} z &= \beta z_1 + r_0 \\ z_1 &= \beta z_2 + r_1 \\ &\vdots \\ z_{j-1} &= \beta z_j + r_{j-1}, \end{aligned}$$

kde $r_i \in \mathcal{A}$ pro $i \in \{0, \ldots, j-1\}$ a zároveň $S(z, d) \geq S(z_1, d^{(1)}) \geq \cdots \geq S(z_{j-1}, d^{(j-1)})$. Máme tedy klesající posloupnost $(S(z_j, d^{(j)}))_{j=1}^{\infty}$ přirozených čísel, tudíž musí mít limitu. To již

implikuje existenci $n_0 \in \mathbb{N}$ splňujícího pro všechna $m \in \mathbb{N} : S(z_{n_0}, d^{(n_0)}) = S(z_{n_0+m}, d^{(n_0+m)})$. To znamená, že $r_n = 0$ pro všechna $n > n_0$ a tedy i $z_{n_0} = \beta^j z_{n_0+j}$ pro všechna $j \in \mathbb{N}$.

Z toho vyplývá, že $\lim_{n\to\infty} z_n = 0$, speciálně od jistého indexu n_1 počínaje, je $|z_n| < \frac{1}{2}$. Jediné $z_n \in \mathbb{Z}[\mathrm{i}]$, které je menší v absolutní hodnotě než $\frac{1}{2}$, je $z_n = 0$.

Takže tento algoritmus určitě skončí po konečném počtu iterací, protože $z_{n_1} = (0)_{(\beta,\mathcal{A})}$. Z definice posloupnosti $(z_j)_{j=1}^{\infty}$ plyne, že $z = (r_{n_1-1} \dots r_1 r_0)_{(\beta,\mathcal{A})}$ a našli jsme reprezentaci z v $(\beta, \mathcal{A})$. □

Z důkazu můžeme odvodit algoritmus, pro hledání reprezentace Gaussových celých čísel.

Algoritmus v Penneyho systému: Hledání reprezentace $x \in \mathbb{Z}[\mathrm{i}]$ v systému $(\beta, \mathcal{A})$, kde $\beta = \mathrm{i} - 1$ a $\mathcal{A} = \{0, 1\}$

---

vstup : číslo $x \in \mathbb{Z}[\mathrm{i}]$ pro které hledáme reprezentaci v $(\beta, \mathcal{A})$
výstup: řetězec $a_n \dots a_0 \in \mathcal{A}^*$, který vyjadřuje reprezentaci x v $(\beta, \mathcal{A})$, tzn. $x = \sum_{i=0}^{n} a_i \beta^i$

```
1  j := 0
2  while x ≠ 0 do
3  |  if Re(x) + Im(x) ∈ 2ℤ then a_j := 0;
4  |  else a_j := 1;
5  |  x := β^{-1}(x − a_j)
6  |  j := j + 1
7  end
8  n := j − 1
9  a := a_n a_{n−1} ... a_0
10 return a
```

Poznamenejme, že operace na třetím a čtvrtém řádku odpovídá hledání $a_j \in \mathcal{A}$ takového, že je kongruentní modulo β prvku x na množině $\mathbb{Z}[\mathrm{i}]$.

Pro ověření tohoto faktu se nejdříve zaměříme na dělení Gaussova čísla $x = a + b\mathrm{i}$, kde $a, b \in \mathbb{Z}$, číslem $\beta = \mathrm{i} - 1$:

$$\frac{x}{\beta} = \frac{a + b\mathrm{i}}{\mathrm{i} - 1} = \frac{a + b\mathrm{i}}{\mathrm{i} - 1} \cdot \frac{\mathrm{i} + 1}{\mathrm{i} + 1} = \frac{b - a}{2} - \mathrm{i}\frac{a + b}{2}. \tag{1.3}$$

Pokud se hledaná cifra a_j rovná nule, nastane rovnost $x = z\beta$ pro nějaké $z = c + \mathrm{i}d \in \mathbb{Z}[\mathrm{i}]$, kde $c, d \in \mathbb{Z}$. Po vydělení této rovnosti číslem β a s využitím vztahu (1.3) dostáváme

$$\frac{x}{\beta} = \frac{b - a}{2} - \mathrm{i}\frac{a + b}{2} = z = c + \mathrm{i}d.$$

Protože $c, d \in \mathbb{Z}$ platí, že $b - a \in 2\mathbb{Z}$ a $a + b \in 2\mathbb{Z}$. Obě podmínky jsou ekvivalentní a znamenají, že a, b jsou současně lichá, nebo současně sudá, tj. mají shodnou paritu. Tímto je jasné, že v algoritmu volíme a_j takové, že $a_j \equiv_M x$.

Analogicky můžeme provést tuto úvahu pro cifru 1 a zjistíme, že hledaná cifra je rovna 1 právě tehdy, když platí $a + b \in 2\mathbb{Z} + 1$, tedy že jedno z čísel a, b je liché a druhé sudé.

Ještě zmíníme souvislost mezi hledáním r_i v důkazu věty 12 a hledáním a_i v algoritmu. V důkazu po r_i požadujeme, aby splňovalo

$$x = r_i + d_{i+1}\beta^1 + \dots + d_n\beta^{n-i}. \tag{1.4}$$

Na druhou stranu v algoritmu hledáme a_i tak, aby $x - a_i = z\beta$ pro nějaké $z \in \mathbb{Z}[\mathrm{i}]$. Konkrétně ze vztahu (1.4) dostáváme $z = d_{i+1} + \cdots + d^n \beta^{n-i-1}$.

Z důkazu věty 12 také plyne, že tento algoritmus pro všechna $x \in \mathbb{Z}[\mathrm{i}]$ po konečně mnoha krocích skončí.

Příklad 13. *Pokusme se najít reprezentaci čísla* $3 - 2\mathrm{i}$ *v Penneyho systému.*

Zřejmě $a_0 = 1$. *V další iteraci máme* $x = -2$. *Vidíme, že nové* x *má obě složky sudé, proto* $a_1 = 0$. *Ve třetím kroku získáme* $x = 1 + i$ *a* $a_2 = 0$. *Analogicky postupujeme, než dojdeme k* $x = 0$. *Výsledná reprezentace čísla je* $3 - 2\mathrm{i} = (111001)_{(\mathrm{i}-1,\{0,1\})}$.

Uveďme ještě jeden systém zkoumaný Penneym.

Příklad 14. *Systém ve tvaru* $\beta = \mathrm{i} + 1$ *a* $\mathcal{A} = \{0, 1\}$ *nereprezentuje množinu* $\mathbb{Z}[\mathrm{i}]$, *protože například číslo* $z = \mathrm{i}$ *nemá* $(\beta, \mathcal{A})$*-reprezentaci. Důkaz lze najít v* [8].

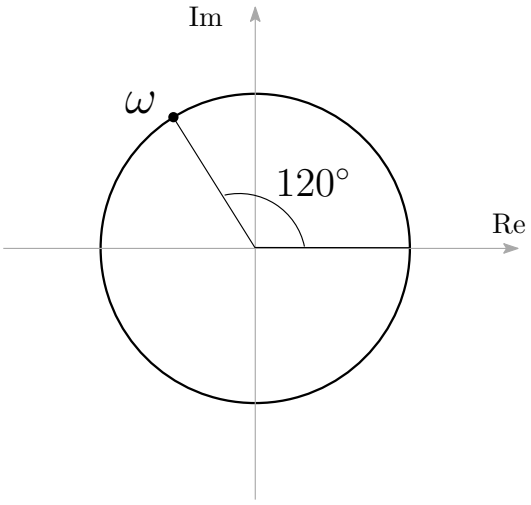
1.3 Eisensteinův numerační systém

V této části budeme zkoumat množinu, která je podobná Gaussovým celým číslům, ale s tím rozdílem, že je v jednom směru vychýlená o 30 stupňů. Toho docílíme tím, že místo komplexní jednotky v definici množiny použijeme jinou komplexní jednotku.

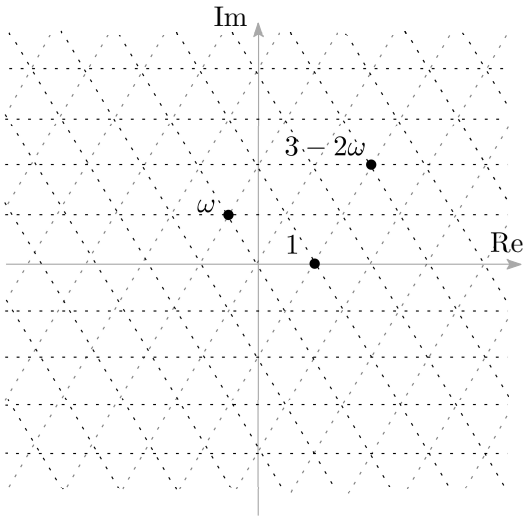
Definice 15. *Množinou Eisensteinových celých čísel rozumíme množinu* $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$, *kde* $w = e^{\mathrm{i}\frac{\pi}{3}} = -\frac{1}{2} + \mathrm{i}\frac{\sqrt{3}}{2}$.

Číslo w odpovídá třetí odmocnině z jedné, na rozdíl od komplexní jednotky, která je rovna čtvrté odmocnině z jedné.

Dále můžeme vidět, že množina Eisensteinových celých čísel tvoří trojúhelníkovou mřížku v komplexní rovině.



Číslo ω na jednotkové kružnici



Trojúhelníková mříž

Poznamenejme, že pro číslo ω platí:

$$\omega^3 = 1 \implies 0 = \omega^3 - 1 = (\omega - 1)(\omega^2 + \omega + 1) \implies \omega^2 = -\omega - 1.$$

Tento vztah budeme často využívat.

Nyní definujme operace + a · pro všechna $x, y \in \mathbb{Z}[\omega]$ podobně, jak jsou zavedeny v $\mathbb{C}$:

$$x + y = (a + b\omega) + (c + d\omega) := (a + c) + (b + d)\omega,$$
$$x \cdot y = (a + b\omega) \cdot (c + d\omega) := ac + (ad + bc)\omega + bd\omega^2 = ac - bd + (ad + bc - bd)\omega.$$

Je snadné ověřit, že množina $\mathbb{Z}[\omega]$ tvoří s těmito operacemi okruh.

Přesuňme se k systému, který reprezentuje Eisensteinova celá čísla. Podobně jako v předchozí kapitole volme bázi jako $\beta = \omega - 1$ a abecedu $\mathcal{A} = \{0, 1, 2\}$. Tento numerační systém se nazývá Eisensteinův.

Věta 16. *Nechť $\beta = \omega - 1$ a $\mathcal{A} = \{0, 1, 2\}$. Pak všechna Eisensteinova celá čísla mají reprezentaci v $(\beta, \mathcal{A})$ ve tvaru $\sum_{i=0}^{n} a_i \beta^i$, kde $a_i \in \mathcal{A}$.*

Důkaz této věty je analogický důkazu věty 12. Identita (1.1) se změní na rovnici

$$\beta^4 + 2\beta^3 + \beta^2 + 2 = -1$$

a identita (1.2) na

$$\beta^3 + 2\beta^2 = 3,$$

která zachovává ciferný součet. Navíc v důkazu používáme dělení číslem 3 se zbytkem. Pro úplnost ho uvedeme celý.

Důkaz. Buď $z = x + \omega y$ libovolné Eisensteinovo celé číslo, kde $x, y \in \mathbb{Z}$. Ukážeme, že toto číslo lze převést do tvaru $z = d_0 + d_1\beta + \cdots + d_5\beta^5$, kde $d_0, d_1, \ldots, d_5 \in \mathbb{N}$. Poté z tohoto tvaru najdeme reprezentaci čísla z.

Rozepišme si z po složkách:

$$z = x + \omega y = c + d\beta = c + \omega d - d,$$

kde $d = y$ a $c = x + d = x + y$. Nyní obecně platí, že $c, d \in \mathbb{Z}$. Převedeme koeficienty c, d do přirozených čísel, k tomu poslouží identita

$$\beta^4 + 2\beta^3 + \beta^2 + 2 = -1. \tag{1.5}$$

Pokud $c < 0$, rozepíšeme si $c = -1 \cdot \bar{c}$, kde $\bar{c} \in \mathbb{N}$ a nyní použijeme identitu (1.5) stejným způsobem jako ve větě 12. Analogicky můžeme provést postup pro d a dostaneme rozklad čísla $z = d_0 + d_1\beta + \cdots + d_5\beta^5$, kde $d_0, d_1, \ldots, d_5$ jsou již z množiny $\mathbb{N}$.

Nyní bychom chtěli převést cifry d_i z množiny přirozených čísel do množiny $\mathcal{A}$, a tím najít reprezentaci z v $(\beta, \mathcal{A})$.

Uvažujme obecnější případ, kdy $z = d_0 + d_1\beta + \cdots + d_k\beta^k, d_i \in \mathbb{N}, k \geq 5$ a označme $d = d_k \cdots d_0 \in \mathbb{N}^*$ a S funkci, která bude sčítat cifry:

$$S : \mathbb{C} \times \mathbb{N}^* \to \mathbb{N}$$
$$(z, d) \mapsto d_0 + \cdots + d_k.$$

Ještě budeme potřebovat identitu ve tvaru

$$\beta^3 + 2\beta^2 = 3, \tag{1.6}$$

u které lze snadno ověřit, že platí. Pokud budeme rovnici (1.6) vnímat jako reprezentaci čísla 3, vidíme, že obě reprezentace mají stejný ciferný součet, a tedy i stejnou hodnotu funkce S. Nyní přejdeme k algoritmu.

Na cifru d_0 použijeme celočíselné dělení číslem 3 se zbytkem, tzn. najdeme r_0, q_0 takové, že $d_0 = r_0 + 3q_0, r_0 \in \{0,1,2\}$. Rozepišme si z pomocí čísel q_0, r_0 a použijeme identitu (1.6) na $3q_0$:

$$\begin{aligned} z &= d_0 + d_1\beta + d_2\beta^2 + d_3\beta^3 = r_0 + 3q_0 + d_1\beta + \cdots + d_k\beta^k = \\ &= r_0 + d_1\beta + (2q_0 + d_2)\beta^2 + (q_0 + d_3)\beta^3 + \cdots + d_k\beta^k =: d_0^{(1)} + \cdots + d_k^{(1)}\beta^k. \end{aligned}$$

Díky tomu, že identita (1.6) a rovnice $d_0 = r_0 + 3q_0$ zachovávají ciferný součet, platí $S(z,d) = S(z,d^{(1)})$, kde $d^{(1)} = d_k^{(1)} \cdots d_0^{(1)}$. Nyní definujme nové číslo

$$z_1 := (z - r_0)\beta^{-1} = (z - d_0^{(1)})\beta^{-1} = d_1^{(1)} + d_1^{(1)}\beta + \cdots + d_k^{(1)}\beta^{k-1}.$$

Z definice z_1 plyne, že pokud z_1 má reprezentaci $a_n \dots a_1$, tak z má reprezentaci $a_n \dots a_1 r_0$. Díky $d_0 \geq 0$ platí $S(z_1, d^{(1)}) \leq S(z, d^{(1)}) = S(z,d)$ a rovnost nastává právě tehdy, když $r_0 = d_0 = 0$. Opakováním tohoto procesu dostaneme posloupnost $(z_j)_{j=1}^{\infty}$:

$$\begin{aligned} z &= \beta z_1 + r_0 \\ z_1 &= \beta z_2 + r_1 \\ &\vdots \\ z_{j-1} &= \beta z_j + r_{j-1}, \end{aligned}$$

kde $r_i \in \mathcal{A}$ pro $i \in \{0, \dots, j-1\}$ a zároveň $S(z,d) \geq S(z_1, d^{(1)}) \geq \cdots \geq S(z_{j-1}, d^{(j-1)})$. Máme tedy klesající posloupnost $(S(z_j, d^{(j)}))_{j=1}^{\infty}$ přirozených čísel, tudíž musí mít limitu. To již implikuje existenci $n_0 \in \mathbb{N}$ splňujícího pro všechna $m \in \mathbb{N} : S(z_{n_0}, d^{(n_0)}) = S(z_{n_0+m}, d^{(n_0+m)})$. To znamená, že $r_n = 0$ pro všechna $n > n_0$ a tedy i $z_{n_0} = \beta^j z_{n_0+j}$ pro všechna $j \in \mathbb{N}$.

Z toho vyplývá, že $\lim_{n\to\infty} z_n = 0$, speciálně od jistého indexu n_1 počínaje, je $|z_n| < \frac{1}{2}$. Jediné $z_n \in \mathbb{Z}[\omega]$, které je menší v absolutní hodnotě než $\frac{1}{2}$, je $z_n = 0$.

Takže tento algoritmus určitě skončí po konečném počtu iterací, protože $z_{n_1} = (0)_{(\beta,\mathcal{A})}$. Z definice posloupnosti $(z_j)_{j=1}^{\infty}$ plyne, že $z = (r_{n_1-1} \dots r_1 r_0)_{(\beta,\mathcal{A})}$ a našli jsme reprezentaci z v $(\beta, \mathcal{A})$. □

Podobně jako v předchozí podkapitole můžeme odvodit algoritmus pro hledání reprezentace.

Dokažme, že v algoritmu v Eistensteinově systému volíme cifry $a_j \in \mathcal{A}$ takové, že $a_j \equiv_\beta x$. Rozepišme dělení čísla $x = a + b\omega$, kde $a, b \in \mathbb{Z}$, číslem $\omega - 1$. S použitím faktu, že $\frac{1}{w-1} = -\frac{2}{3} - \frac{2\omega}{3}$ dostáváme

$$\frac{x}{\omega - 1} = \frac{a + b\omega}{\omega - 1} = -\frac{2a + b}{3} - \frac{a - b}{3}\omega. \tag{1.7}$$

Při použití stejné úvahy jako v předchozí podkapitole můžeme vidět, že $x \equiv_\beta 0$ platí právě tehdy, když $2a + b \in 3\mathbb{Z}$ a to je ekvivalentní s $a - b \in 3\mathbb{Z}$.

Pro případ, kdy hledaná cifra je rovna 1 platí, že $a + b\omega \equiv_\beta 1$. Tuto rovnici můžeme ekvivalentně přepsat jako $a - 1 + b\omega \equiv_\beta 0$ a po dosazení do vztahu (1.7) dostáváme, že $2a + b \in 3\mathbb{Z} + 2$. Zbytek ověření probíhá analogicky.

Algoritmus v Eistensteinově systému: Algoritmus pro hledání reprezentace $x \in \mathbb{Z}[\omega]$ v systému $(\beta, \mathcal{A})$, kde $\beta = \omega - 1$ a $\mathcal{A} = \{0, 1, 2\}$

vstup : číslo $x \in \mathbb{Z}[\omega]$ pro které hledáme reprezentaci v $(\beta, \mathcal{A})$
výstup: řetězec $a_n \dots a_0 \in \mathcal{A}^*$, který vyjadřuje reprezentaci x v $(\beta, \mathcal{A})$, tzn. $x = \sum_{i=0}^{n} a_i \beta^i$

```
j := 0
while x ≠ 0 do
    rozepišme x jako x = a + bω
    if 2a + b ∈ 3ℤ then a_j := 0;
    if 2a + b ∈ 3ℤ + 2 then a_j := 1;
    else a_j := 2;
    x := β^{-1}(x − a_j)
    j := j + 1
end
n := j − 1
a := a_n a_{n−1} ... a_0, kde a ∈ A*
return a
```

1.4 Nekonečné $(\beta, \mathcal{A})$-rozvoje

Často pracujeme s čísly, které nepatří do množiny $\mathbb{Z}_{\mathcal{A}}(\beta)$. Připomeňme, že $\mathbb{Z}_{\mathcal{A}}(\beta) = \{\sum_{j=0}^{n} a_j \beta^j : n \in \mathbb{N}, a_j \in \mathcal{A}\}$. Příkladem takových čísel mohou být prvky z množiny $\mathbb{R} \setminus \mathbb{Z}$. Zkoumejme otázku, jak najít jejich reprezentaci. Pro zjednodušení uvažujme systém $\beta = 3$ a $\mathcal{A} = \{0, 1, 2\}$.

Nejprve vezmeme v úvahu čísla, která mají reprezentaci „za tečkou“, tj. mají nenulové cifry u záporných mocnin báze. Nechť $x = \sum_{i=1}^{\infty} a_i \beta^{-i}$, kde $a_i \in \mathcal{A}$. Zvolme libovolné $a_1, a_2, a_3, \dots$ z abecedy $\mathcal{A}$, pak

$$0 \leq x = \sum_{i=1}^{\infty} a_i \beta^{-i} \leq \sum_{i=1}^{\infty} 2\beta^{-i} = 2 \sum_{i=1}^{\infty} \beta^{-i} = 2 \frac{\frac{1}{3}}{1 - \frac{1}{3}} = 1.$$

Vidíme, že můžeme takto reprezentovat nanejvýš čísla z intervalu $[0, 1]$. Levý kraj intervalu odpovídá případu, kdy číslo x bude mít v reprezentaci samé cifry 0, pravý kraj případu, kdy budou v reprezentaci samé cifry 2.

Zkusme odvodit, jak budeme hledat řetězec reprezentující x. Nechť $x \in [0, 1]$ a x má tvar

$$x = \sum_{i=1}^{\infty} a_i \beta^{-i}, \tag{1.8}$$

kde $a_i \in \mathcal{A}$. Po vynásobení rovnice (1.8) číslem β dostáváme

$$\beta x = \sum_{i=1}^{\infty} a_i \beta^{-i+1} = a_1 + \sum_{i=2}^{\infty} a_i \beta^{-i+1} = a_1 + \sum_{i=1}^{\infty} a_{i+1} \beta^{-i} \in a_1 + [0, 1] \implies \beta x - a_1 \in [0, 1].$$

Pokud bychom měli zaručenou existenci cifry a_1, takto bychom ji mohli najít, tedy jako cifru z abecedy $\mathcal{A}$ splňující $\beta x - a_1 \in [0, 1]$. Tento postup bychom poté mohli zopakovat pro číslo $\beta x - a_1 = \sum_{i=1}^{\infty} a_{i+1} \beta^{-i}$ a nalézt cifru a_2. Dalším opakováním bychom našli řetězec $a_1 a_2 \dots$ reprezentující číslo x.

Ověřme, že vždy najdeme cifru $a \in \mathcal{A}$ takovou, že pro libovolné $y \in [0,1]$ platí $\beta y - a \in [0,1]$.

$$y \in [0,1] \implies \beta y \in [0,3] \implies \exists a \in \{0,1,2\} : \beta y - a \in [0,1]\,.$$

Proveďme pozorování, které se bude hodit v nadcházející části. Interval $[0,1]$ splňuje vlastnost $\beta\,[0,1] = \mathcal{A} + [0,1]$. Skutečně

$$\beta\,[0,1] = 3\,[0,1] = [0,3] = [0,1] \cup (1 + [0,1]) \cup (2 + [0,1]) = \mathcal{A} + [0,1]\,, \tag{1.9}$$

kde v poslední rovnosti využíváme množinový součet, tedy že $\mathcal{A} + [0,1] = \{a + [0,1] : a \in \mathcal{A}\}$.

Rovnici (1.9) můžeme interpretovat tak, že interval $3\,[0,1]$ je pokryt sjednocením množin $a+[0,1]$, kde $a \in \mathcal{A}$. Tudíž i takto by se dala dokázat existence cifry $a \in \mathcal{A}$ takové, že $\beta y - a \in [0,1]$ pro $y \in [0,1]$.

Vraťme se k postupu hledání řetězce reprezentující číslo $x = \sum_{i=1}^{\infty} a_i \beta^{-i}$ a uveďme ho v algoritmu.

Druhý algoritmus: Algoritmus pro hledání reprezentace „za tečkou“ pro systém $(3, \{0,1,2\})$

---

vstup : číslo $x \in [0,1]$
výstup: řetězec $a = a_1 a_2 \ldots$, kde $a_1, a_2, \ldots \in \mathcal{A}$, který vyjadřuje reprezentaci x „za tečkou“ tzn. $x = \sum_{i=1}^{\infty} a_i \beta^{-i}$

```
1 i := 1
2 while x ≠ 0 do
3 |   najdi a_i ∈ {0,1,2} tak, aby 3x − a_i ∈ [0,1]
4 |   x := 3x − a_i
5 |   i := i + 1
6 end
7 a := a_1 a_2 a_3 ...
8 return a
```

Příklad 17. *Najdeme rozvoj čísla s dekadickým zápisem $x = 0.15$ v systému $\beta = 3$ a $\mathcal{A} = \{0,1,2\}$. V prvním kroku platí, že $3 \cdot 0.15 \in [0,1]$, takže hledaná cifra splňuje $a_1 = 0$. Pro nové x platí $x := 3 \cdot 0.15 = 0.45$. V druhém kroku je $a_2 = 1$, protože $3 \cdot 0.45 - 1 = 0.35 \in [0,1]$. Tudíž nové $x := 0.35$.*

Ve třetím kroku $a_3 = 1$ a $x := 3 \cdot 0.35 - 1 = 0.05$. Ve čtvrtém kroku dostáváme $a_4 = 0$ a $x := 0.15$ a jsme zase u původního čísla. Rozvoj tudíž bude periodický. Proto $0.15 = (0.01100110\ldots)_{(3,\{0,1,2\})} = (0.(0110)^{\omega})_{(3,\{0,1,2\})}$, kde $0.(v)^{\omega}$ značíme periodické číslo, tedy $0.(v)^{\omega} = 0.vvv\ldots$.

Prozkoumejme detailněji systém $\beta = 3$ a $\mathcal{A} = \{0,1,2\}$. Pomocí prvního algoritmu dokážeme najít pro všechna přirozená čísla reprezentaci, tzn. pro všechna $N \in \mathbb{N}$ najdeme $a_1 \ldots a_n \in \mathcal{A}^*$ takový, že $N = \sum_{i=0}^{n} a_i \beta^i$.

Rozepišme čísla z $\mathbb{R}$ takové, že $x > 0$, jako $x = \lfloor x \rfloor + \{x\}$, kde $\{x\} \in [\,0,1)$. Následně najdeme reprezentaci „za tečkou“ pro $\{x\}$ pomocí druhého algoritmu a získáme rovnost $\{x\} = \sum_{j=1}^{\infty} b_j \beta^{-j}$ pro $b_1, b_2, \ldots \in \mathcal{A}$.

Nakonec můžeme spojit tyto dvě reprezentace a dostaneme pro libovolné $x \in \mathbb{R}$ takové, že $x > 0$:

$$x = \lfloor x \rfloor + \{x\} = \sum_{i=0}^{n} a_i \beta^i + \sum_{j=1}^{\infty} b_j \beta^{-j} = \sum_{i=0}^{n} a_i \beta^i + \sum_{j=-\infty}^{-1} b_{-j} \beta^j = \sum_{i=-\infty}^{n} a_i \beta^i,$$

kde jsme pro $i < 0$ definovali $a_i := b_{-i}$. Tudíž jsme našli řetězec $a_n a_{n-1} \ldots$, který reprezentuje číslo x v $(\beta, \mathcal{A})$.

Tuto konstrukci lze provést také jiným způsobem. Mějme $x \in \mathbb{R}$, takové, že $x > 0$. Pokud $x \in [0, 1]$, použijeme rovnou druhý algoritmus pro nalezení reprezentace. Pokud $x > 1$, pak určitě existuje $k \in \mathbb{N}$ takové, že $\frac{x}{\beta^k} \in [0, 1]$. Nyní využijeme druhý algoritmus pro číslo $\frac{x}{\beta^k}$ a získáme čísla $b_1, b_2, \ldots \in \mathcal{A}$ taková, že $\frac{x}{\beta^k} = \sum_{j=1}^{\infty} b_j \beta^{-j}$. Po vynásobení této rovnice číslem β^k dostaneme

$$x = \sum_{j=1}^{\infty} b_j \beta^{-j+k} = \sum_{j=-\infty}^{-1} b_{-j} \beta^{+j-k} = \sum_{j=-\infty}^{-1-k} b_{-j-k} \beta^j.$$

Tudíž jsme našli reprezentaci čísla x v $(\beta, \mathcal{A})$, a to $b_{-k-1} b_{-k-2} \ldots$.

1.5 Zobecnění nekonečných $(\beta, \mathcal{A})$-rozvojů

V předchozí části jsme ukázali, že všechna čísla z množiny $V := [0, 1]$ měla v systému $\beta = 3$ a $\mathcal{A} = \{0, 1, 2\}$ reprezentaci „za tečkou“. Taktéž jsme dokázali, že pro tento systém platí rovnost

$$\beta V = \mathcal{A} + V. \tag{1.10}$$

V první větě této podkapitoly dokážeme, že pro poziční numerační systémy je podmínka (1.10) postačující k tomu, aby množina V měla reprezentaci „za tečkou“. V následující větě, kterou máme z [12], představíme dodatkový předpoklad, který zaručí reprezentaci celé množiny $\mathbb{R}$ či $\mathbb{C}$.

Věta 18. *Nechť $(\beta, \mathcal{A})$ je poziční numerační systém. Pokud existuje omezená množina $V \subset \mathbb{C}$ taková, že*

$$\beta V \subset \mathcal{A} + V, \tag{1.11}$$

pak každý prvek $x \in V$ lze zapsat ve tvaru $x = \sum_{i=1}^{\infty} a_i \beta^{-i}$, kde $a_i \in \mathcal{A}$ pro každé $i \in \mathbb{N}$.

Důkaz. Nechť $x \in V$ je libovolné číslo z množiny V. Označme $x_1 := x$ a po vynásobení číslem β získáme $\beta x_1 \in \beta V$. Předpokladu (1.11) zaručuje existenci $a_1 \in \mathcal{A}$ a $x_2 \in V$ takových, že $\beta x_1 = a_1 + x_2$. Po vydělení číslem β dostaneme

$$x_1 = a_1 \beta^{-1} + x_2 \beta^{-1}. \tag{1.12}$$

Stejný postup můžeme provést pro číslo $x_2 \in V$ a získáme $x_2 = a_2 \beta^{-1} + x_3 \beta^{-1}$. Po dosazení do vztahu (1.12) dostáváme $x_1 = a_1 \beta^{-1} + a_2 \beta^{-2} + x_3 \beta^{-2}$. A takto můžeme pokračovat až dojdeme k vyjádření $x_1 = x = \sum_{i=1}^{\infty} a_i \beta^{-i}$, kde $a_i \in \mathcal{A}$. □

Příklad 19. *Uvažujme již dříve zmiňovaný systém $\beta = -2$ a $\mathcal{A} = \{0, 1\}$. Pak lze snadno nahlédnout, že $V = \left[-\frac{2}{3}, \frac{1}{3}\right]$ splňuje předpoklad věty (18), tedy že $-2\left[-\frac{2}{3}, \frac{1}{3}\right] = \left[-\frac{2}{3}, \frac{4}{3}\right] \subset \left[-\frac{2}{3}, \frac{1}{3}\right] \cup (1 + \left[-\frac{2}{3}, \frac{1}{3}\right])$. Z již zmiňované věty plyne, že každé $x \in \left[-\frac{2}{3}, \frac{1}{3}\right]$ má $(\beta, \mathcal{A})$-reprezentaci.*

Uveďme nyní důsledek věty 18.

Důsledek 20. *Nechť $(\beta, \mathcal{A})$ je poziční numerační systém, kde $\beta \in \mathbb{R}$ a $\mathcal{A} \subset \mathbb{R}$ nebo $\beta \in \mathbb{C}$ a $\mathcal{A} \subset \mathbb{C}$. Pokud existuje omezená množina $V \subset \mathbb{R}$, respektive $V \subset \mathbb{C}$, splňující (1.11) a navíc platí*

$$0 \in V^\circ,$$

pak každé $x \in \mathbb{R}$, respektive každé $x \in \mathbb{C}$, má $(\beta, \mathcal{A})$-reprezentaci ve tvaru $x = \sum_{i=-\infty}^{n} a_i \beta^i$.

Důkaz. Nechť $x \in \mathbb{R}$, respektive $x \in \mathbb{C}$, je libovolné číslo. Pak z předpokladu $0 \in V^\circ$ plyne, že existuje $n \in \mathbb{N}$ takové, že $x\beta^{-n} \in V$. Při použití věty 18 dostáváme, že $x\beta^{-n}$ lze napsat ve tvaru $x\beta^{-n} = \sum_{i=1}^{\infty} a_i \beta^{-i}$. Po vynásobení číslem β^n získáme

$$x = \sum_{i=1}^{\infty} a_i \beta^{-i+n} = \sum_{i=1-n}^{\infty} a_{i+n} \beta^{-i} = \sum_{i=-\infty}^{n-1} a_{-i+n} \beta^i,$$

čímž je důkaz dokončen. □

Může se naskytnout otázka, jak takovou množinu V najít. Ověřme, že množina ve tvaru

$$V = \left\{ \sum_{i=1}^{\infty} a_i \beta^{-i} : a_i \in \mathcal{A} \right\}$$

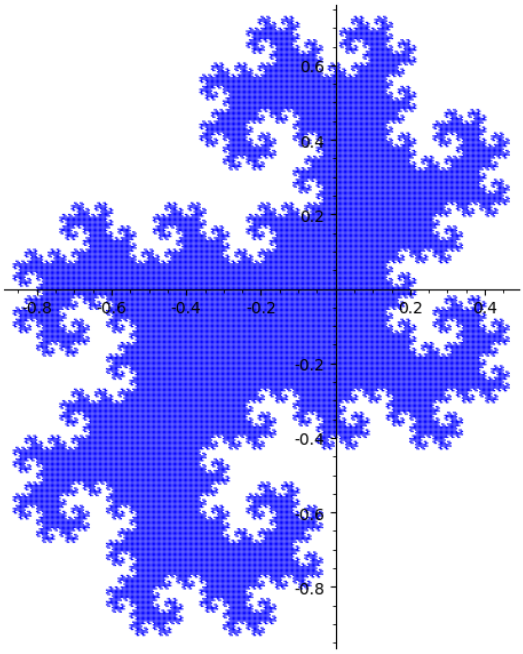
splňuje předpoklad (1.11). Zřejmě platí

$$\beta V = \left\{ a_1 + \sum_{i=1}^{\infty} a_{i+1} \beta^i : a_i \in \mathcal{A} \right\} = \mathcal{A} + V.$$

V případě, že $\beta \in \mathbb{C} \setminus \mathbb{R}$ a neredundantního systému, má takto definovaná množina V fraktální tvar. V následující části ukážeme vykreslené množiny $V = \left\{ \sum_{i=1}^{\infty} a_i \beta^{-i} : a_i \in \mathcal{A} \right\}$ pro různé numerační systémy.

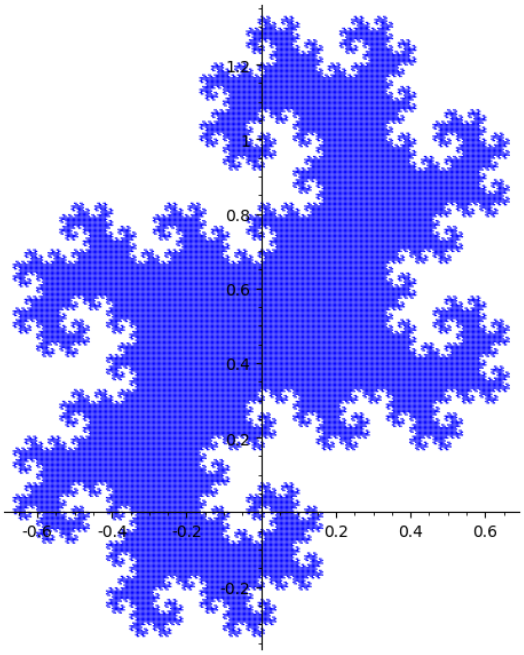
Obrázky byly vytvořeny v programovacím jazyku SageMath [11]. Zdrojový kód s pokyny na instalaci a spuštění lze nalézt v [4]. Dodejme, že pro vykreslení množiny byla použita funkce `show(points())`.

Na obrázku 1.1 vidíme množinu V pro Penneyho systém. Zřejmě platí, že $0 \in V^\circ$, tudíž bychom mohli odůvodnit větou 20, že se jedná o systém reprezentující $\mathbb{C}$. Poznamenejme, že na rozdíl od věty 12 uvažujeme reprezentace ve tvaru $\sum_{i=-\infty}^{n} a_i \beta^i$. Dále můžeme vidět, že posunuté množiny V, tedy množiny ve tvaru $V + z$, kde $z \in \mathbb{Z}[\mathrm{i}]$, do sebe zapadají při posunování ve směru reálné a imaginární osy o číslo z.



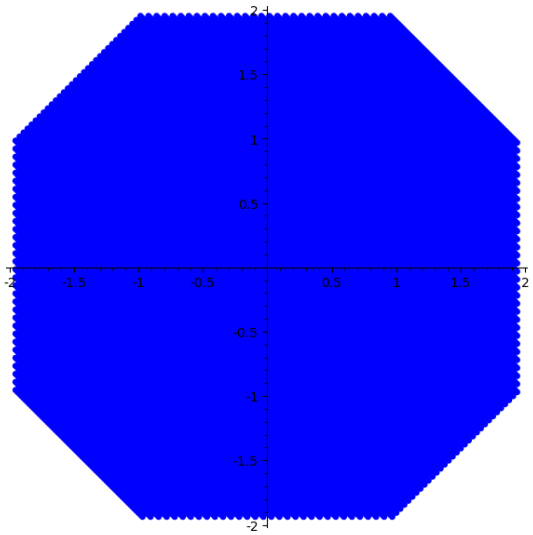
Obrázek 1.1: Množina V pro systém $\beta = \mathrm{i} - 1$ a $\mathcal{A} = \{0, 1\}$

Na obrázku 1.2 se nachází množina V pro systém $\beta = i + 1$ a $\mathcal{A} = \{0, 1\}$, o kterém jsme dříve zmiňovali, že nereprezentuje množinu $\mathbb{Z}[\mathrm{i}]$. Zde již neplatí, že $0 \in V^\circ$, proto nemůžeme použít větu 20. Vidíme, že se jedná o posunutou verzi množiny z obrázku 1.1, takže i zde platí, že do sebe posunuté množiny zapadají.



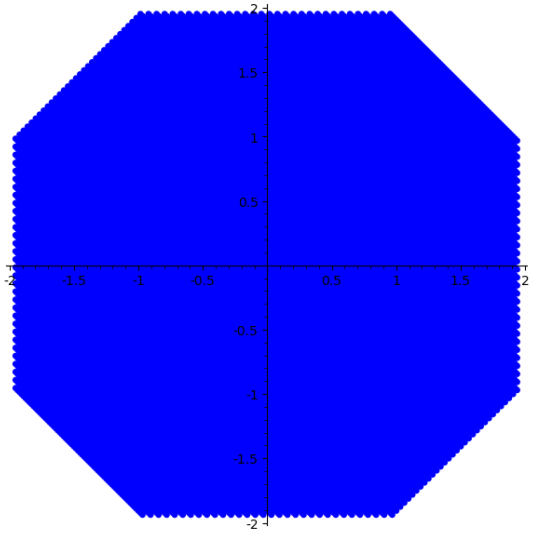
Obrázek 1.2: Množina V pro systém $\beta = \mathrm{i} + 1$ a $\mathcal{A} = \{0, 1\}$

Nyní ukážeme dlaždici V pro systém s Penneyho bází a redundantní abecedou ve tvaru $\mathcal{A} = \{0, 1, -1, \mathrm{i}, -\mathrm{i}\}$. Díky tomu, že uvažujeme redundantní abecedu, množina V nemá fraktální tvar. Dalším důsledkem redundantní abecedy je fakt, že posunuté množiny ve tvaru $V + z$, kde $z \in \mathbb{Z}[\mathrm{i}]$, se překrývají.



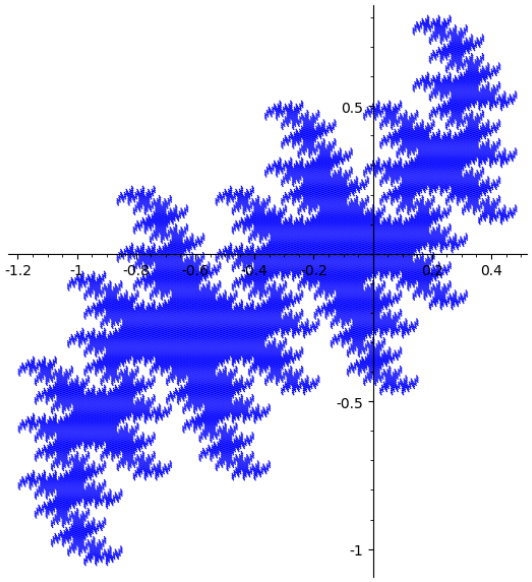
Obrázek 1.3: Množina V pro systém $\beta = \mathrm{i} - 1$ a $\mathcal{A} = \{0, 1, -1, \mathrm{i}, -\mathrm{i}\}$

Následuje dlaždice pro systém $\beta = \mathrm{i} + 1$ a $\mathcal{A} = \{0, 1, -1, \mathrm{i}, -\mathrm{i}\}$. Tento systém s abecedou $\mathcal{A} = \{0, 1\}$ nereprezentoval množinu $\mathbb{Z}[\mathrm{i}]$. Pokud ale uvažujeme abecedu $\mathcal{A} = \{0, 1, -1, \mathrm{i}, -\mathrm{i}\}$, můžeme s použitím věty 20 a faktu, že $0 \in V^\circ$, konstatovat, že se jedná o systém reprezentující $\mathbb{C}$. Znovu pozorujeme, že se množiny posunuté o vektor $z \in \mathbb{Z}[\mathrm{i}]$ překrývají. To je způsobeno redundantní abecedou.



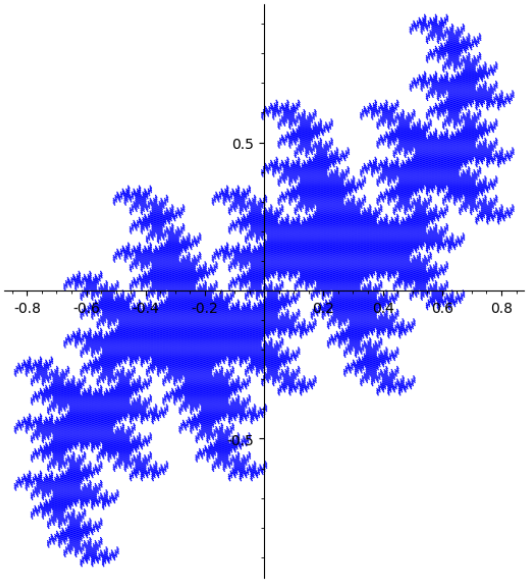
Obrázek 1.4: Množina V pro systém $\beta = \mathrm{i} + 1$ a $\mathcal{A} = \{0, 1, -1, \mathrm{i}, -\mathrm{i}\}$

Obrázek 1.5 patří Eisensteinově bázi s abecedou $\mathcal{A} = \{0, 1, 2\}$. Upozorněme, že se jedná o osy ve směru reálném a ve směru odpovídajícímu číslu ω. Vidíme, že $0 \in V^\circ$. Posunuté množiny $V + z$ pro $z \in \mathbb{Z}[\omega]$, stejně jako u Penneyho systému, do sebe zapadají.



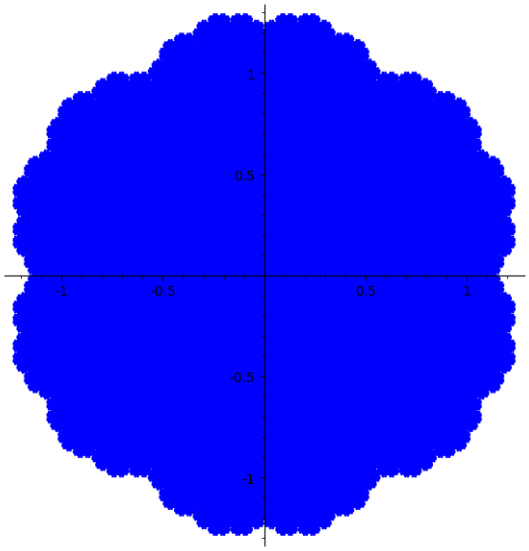
Obrázek 1.5: Množina V pro systém $\beta = \omega - 1$ a $\mathcal{A} = \{0, 1, 2\}$

Na obrázku 1.6 vidíme množinu V patřící systému s Eisensteinovou bází, ale s abecedou $\mathcal{A} = \{-1, 0, 1\}$. Neplatí již, že $0 \in V^\circ$. Z obrázku je zřejmé, že se jedná o posunutou verzi 1.5, proto i zde do sebe posunuté množiny zapadají.



Obrázek 1.6: Množina V pro systém $\beta = \omega - 1$ a $\mathcal{A} = \{-1, 0, 1\}$

Poslední obrázek, který zmíníme, je pro Eisensteinovu bázi a redundantní abecedu $\mathcal{A} = \{0\} \cup \{e^{\mathrm{i}\frac{2\pi}{3}k} : k \in \{0,1,2,3,4,5\}\} = \{0,1,-1,\omega,-\omega,\omega^2,-\omega^2\}$. Znovu můžeme pozorovat, jak posunuté kopie $V + z$ pro $z \in \mathbb{Z}[\omega]$ se překrývají. Zřejmě $0 \in V^\circ$.



Obrázek 1.7: Množina V pro systém $\beta = \omega - 1$ a $\mathcal{A} = \{0,1,-1,\omega,-\omega,\omega^2,-\omega^2\}$

Kapitola 2

Maticové numerační systémy

V této kapitole zavedeme numerační systémy reprezentující vektory s celočíselnými složkami. Obdobně jako v předchozí kapitole, budeme definovat pojmy jako maticový numerační systém a reprezentace. U pozičního numeračního systému jsme potřebovali předpoklad, že $|\beta| > 1$, tuto úlohu bude nyní zastávat vlastnost, že matice je expanzivní.

Definice 21. *Čtvercovou matici, která má všechna vlastní čísla v absolutní hodnotě ostře větší než 1, nazýváme expanzivní.*

Expanzivní matice je již nutně regulární, tudíž má i nenulový determinant.

Definice 22. *Buď $M \in \mathbb{Z}^{d,d}$ expanzivní a $d \in \mathbb{N}$. Nechť $\mathcal{A}$ je konečná množina vektorů z $\mathbb{Z}^d$ obsahující nulový vektor. Pak dvojici $(M, \mathcal{A})$ nazveme maticovým numeračním systémem, matici M jeho bází a množinu $\mathcal{A}$ abecedou.*

V této práci se omezíme pouze na reprezentace s nenulovými vektory u nezáporných mocnin báze, tzn. na reprezentaci „před tečkou“.

Definice 23. *Nechť $(M, \mathcal{A})$ je maticový numerační systém a $x \in \mathbb{Z}^d$. Řekneme, že x má $(M, \mathcal{A})$-reprezentaci, pokud $x = \sum_{i=0}^{n} M^i a_i$, kde $a_n, \ldots, a_0 \in \mathcal{A}$ a řetězec $a_n \ldots a_0$ vyjadřuje reprezentaci vektoru x v systému $(M, \mathcal{A})$.*

Definice 24. *Nechť $(M, \mathcal{A})$ je maticový numerační systém. Množinu všech vektorů s konečnou $(M, \mathcal{A})$-reprezentací značíme jako*

$$\mathrm{Fin}_{\mathcal{A}}(M) := \left\{ \sum_{j=0}^{n} M^j a_j : n \in \mathbb{N}, a_j \in \mathcal{A} \right\}.$$

Definice 25. *Maticový systém $(M, \mathcal{A})$ nazveme redundantní, pokud existuje vektor $x \in \mathrm{Fin}_{\mathcal{A}}(M)$ takový, že má dvě různé konečné $(M, \mathcal{A})$-reprezentace.*

V předchozí kapitole jsme pracovali s množinami $\mathbb{Z}, \mathbb{R}, \mathbb{C}, \mathbb{Z}[\mathrm{i}], \mathbb{Z}[\omega]$, které jsou s příslušnými operacemi okruhy. Nyní přecházíme do množiny $\mathbb{Z}^d$, která je slabší algebraickou strukturou. Množina $\mathbb{Z}^d$ s operací $+$ představuje tzv. $\mathbb{Z}$-modul.

Definice 26. *$\mathbb{Z}$-modul nad okruhem $\mathbb{Z}$ je tvořen abelovskou grupou $(G, +)$ a operací $\mathbb{Z} \times G \to G$(které říkáme skalární násobení), označovanou $(\alpha, x) \mapsto \alpha \cdot x$, splňující pro všechna $\alpha, \beta \in \mathbb{Z}$ a $x, y \in G$:*

1. $\alpha \cdot (x + y) = \alpha \cdot x + \alpha \cdot y$,
2. $(\alpha + \beta) \cdot x = \alpha \cdot x + \beta \cdot x$,
3. $(\alpha\beta) \cdot x = \alpha \cdot (\beta x)$,
4. $1 \cdot x = x$.

Můžeme vidět, že libovolný komutativní okruh $(R, +, \cdot)$, který je nadmnožinou $\mathbb{Z}$, je $\mathbb{Z}$-modulem. V prvních dvou bodech se jedná pouze o zúžení distributivních zákonů na $\mathbb{Z}$, ve třetím bodě o zúžení asociativity pro operaci $\cdot$ a ve čtvrtém o neutrální prvek 1 pro $\cdot$. Navíc musíme využít faktu, že okruh R tvoří s operací $+$ abelovskou grupu.

Tudíž platí, že množiny, s kterými jsme doposud pracovali, byly také $\mathbb{Z}$-moduly.

Definujme zobrazení, které popisuje podobnost dvou $\mathbb{Z}$-modulů.

Definice 27. *Nechť Z_1, Z_2 jsou $\mathbb{Z}$-moduly. Řekneme, že bijektivní zobrazení $\varphi : Z_1 \to Z_2$ je izomorfismem $\mathbb{Z}$-modulů Z_1 a Z_2, pokud pro všechna $x, y \in Z_1$ a $\alpha \in \mathbb{Z}$ platí:*

1. $\varphi(x + y) = \varphi(x) + \varphi(y)$,
2. $\varphi(\alpha \cdot x) = \alpha \cdot \varphi(x)$.

Poznamenejme, že používáme stejný symbol $+$ (resp. $\cdot$) pro operace v Z_1 i Z_2. Nedorozumění nehrozí.

V další části ukážeme vztah mezi maticovými reprezentacemi $\mathbb{Z}^2$ a číselnými reprezentacemi Gaussových celých čísel. Zbytek kapitoly pak bude věnován potřebným větám z teorie matic.

2.1 Souvislost maticových a číselných systémů

Díky tomu, že $\mathbb{Z}[\mathrm{i}]$ jako $\mathbb{Z}$-modul je izomorfní $\mathbb{Z}^2$, ukážeme souvislost mezi celočíselným numeračním systémem a maticovým numeračním systémem na $\mathbb{Z}^{2,2}$.

Příklad 28. *Mějme Penneyho poziční systém, tzn. $\beta = \mathrm{i} - 1, \mathcal{A} = \{0, 1\}$. Rozepišme působení báze β na Gaussovo celé číslo:*

$$(a + \mathrm{i}b)\beta = (a + \mathrm{i}b)(\mathrm{i} - 1) = (-a - b) + \mathrm{i}(a - b).$$

Napišme komplexní číslo $(-a - b) + \mathrm{i}(a - b)$ jako vektor o dvou složkách a hledejme matici $M \in \mathbb{Z}^{2,2}$, která splňuje

$$M \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} -a - b \\ a - b \end{pmatrix},$$

což zřejmě splňuje matice

$$M = \begin{pmatrix} -1 & -1 \\ 1 & -1 \end{pmatrix}. \tag{2.1}$$

Tento postup nyní formalizujeme.

Nechť φ je izomorfismus $\mathbb{Z}$-modulů $\mathbb{Z}[\mathrm{i}]$ a $\mathbb{Z}^2$ definovaný jako

$$\varphi(a + bi) = \begin{pmatrix} a \\ b \end{pmatrix} \tag{2.2}$$

pro každé $a + b\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$. Ověřme, že se skutečně jedná o izomorfismus. Nechť $x = a + b\mathrm{i}, y = c + d\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$ a $\alpha \in \mathbb{Z}$. Pak

$$\varphi((a + b\mathrm{i}) + (c + d\mathrm{i})) = \varphi((a + c) + (b + d)\mathrm{i}) = \begin{pmatrix} a + c \\ b + d \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} c \\ d \end{pmatrix} = \varphi(x) + \varphi(y),$$

$$\varphi(\alpha \cdot x) = \varphi(\alpha(a + b\mathrm{i})) = \varphi(\alpha a + \alpha b\mathrm{i}) = \begin{pmatrix} \alpha a \\ \alpha b \end{pmatrix} = \alpha \begin{pmatrix} a \\ b \end{pmatrix} = \alpha\varphi(x).$$

Uveďme některé vlastnosti izomorfismu φ.

Věta 29. *Nechť φ je izomorfismus $\mathbb{Z}$-modulů $\mathbb{Z}[\mathrm{i}]$ a $\mathbb{Z}^2$ definovaný vztahem (2.2) a nechť matice M má tvar*

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

Pak platí

1. $\varphi(1) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$,
2. $\varphi(z\beta) = M\varphi(z)$ *pro každé* $z \in \mathbb{Z}[\mathrm{i}]$,
3. $\varphi(\beta^n) = M^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ *pro každé* $n \in \mathbb{N}$.

Důkaz. 1. Plyne přímo z definice izomorfismu φ.

2. Nechť $z \in \mathbb{Z}[\mathrm{i}]$. Pak

$$\varphi(z\beta) = \varphi((a + b\mathrm{i})(\mathrm{i} - 1)) = \varphi((-a - b) + (a - b)\mathrm{i}) = \begin{pmatrix} -a - b \\ a - b \end{pmatrix} = M \begin{pmatrix} a \\ b \end{pmatrix} = M\varphi(z),$$

kde jsme v předposledním kroku využili tvaru matice M.

3. Důkaz provedeme matematickou indukcí. Pro $n = 1$ máme:

$$\varphi(\beta) = \varphi(\beta \cdot 1) = M\varphi(1) = M \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

kde jsme použili předchozí dva body tvrzení. Krok $n - 1 \to n$ odvodíme takto:

$$\varphi(\beta^n) = \varphi(\beta\beta^{n-1}) = M\varphi(\beta^{n-1}) = MM^{n-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = M^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

□

Využijeme znalosti o Penneyho systému a převedeme je do maticového systému s bází $M = \begin{pmatrix} -1 & -1 \\ 1 & -1 \end{pmatrix}$. Z věty 12 plyne, že pro všechna $z \in \mathbb{Z}[\mathrm{i}]$ existuje $a_n \dots a_0 \in \mathcal{A}^*$ takový, že

$$z = \sum_{i=0}^{n} a_i \beta^i. \tag{2.3}$$

Použijme na rovnici (2.3) izomorfismus φ:

$$\varphi(z) = \varphi\left(\sum_{i=0}^{n} a_i\beta^i\right) = \sum_{i=0}^{n} \varphi(a_i\beta^i) = \sum_{i=0}^{n} a_i \cdot \varphi(\beta^i) = \sum_{i=0}^{n} a_i \cdot M^i \begin{pmatrix}1\\0\end{pmatrix} = \sum_{i=0}^{n} M^i \begin{pmatrix}a_i\\0\end{pmatrix}, \quad (2.4)$$

kde ve třetím kroku využíváme faktu, že $a_i \in \{0,1\} \subset \mathbb{Z}$ a můžeme tudíž použít 2. vlastnost izomorfismu $\mathbb{Z}$-modulů. V poslední rovnosti se vyskytují vektory $\begin{pmatrix}a_i\\0\end{pmatrix}$, tedy $\begin{pmatrix}0\\0\end{pmatrix}$ a $\begin{pmatrix}1\\0\end{pmatrix}$.

Pokud rozepíšeme $z = a + b\mathrm{i}$ pro $a, b \in \mathbb{Z}$, dostáváme ze vztahu (2.4) pro libovolná $a, b \in \mathbb{Z}$:

$$\begin{pmatrix}a\\b\end{pmatrix} = \sum_{i=0}^{n} M^i \begin{pmatrix}a_i\\0\end{pmatrix}.$$

Dokážeme tedy pro všechny vektory ze $\mathbb{Z}^2$ najít maticovou reprezentaci v systému $M = \begin{pmatrix}-1 & -1\\1 & -1\end{pmatrix}, \widetilde{\mathcal{A}} = \left\{\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}\right\}$. Tento systém odpovídá maticové formě Penneyho systému.

Příklad 30. *Prozkoumejme Eisensteinův numerační systém. Mějme $\beta = \omega - 1$ a $\mathcal{A} = \{0,1,2\}$. Nechť ψ je zobrazení $\psi : \mathbb{Z}[\omega] \to \mathbb{Z}^2$ definované jako $z = a + b\omega \mapsto \begin{pmatrix}a\\b\end{pmatrix}$. Analogicky, jako u Penneyho systému, se dá ověřit, že je to izomorfismus.*

Hledejme matici N, která bude mít pro $z \in \mathbb{Z}[\omega]$ vlastnost: $\psi(z\beta) = N\psi(z)$:

$$\begin{aligned}\psi(z\beta) &= \psi((a+b\omega)(\omega-1)) = \psi(a\omega - a + b\omega^2 - b\omega) = \psi(-a-b+(a-2b)\omega) = \\ &= \begin{pmatrix}-a-b\\a-2b\end{pmatrix} \overset{!}{=} N\begin{pmatrix}a\\b\end{pmatrix} = N\psi(z) \implies N = \begin{pmatrix}-1 & -1\\1 & -2\end{pmatrix}.\end{aligned}$$

Lze dokázat, obdobně jako v důkazu 29, že izomorfismus ψ splňuje pro všechna $n \in \mathbb{N}$:

$$\psi(\beta^n) = N^n \begin{pmatrix}1\\0\end{pmatrix}.$$

S využitím věty 16 a podobných úprav jako ve vztahu (2.4) můžeme pro všechna $a, b \in \mathbb{Z}$ psát:

$$\psi(z) = \begin{pmatrix}a\\b\end{pmatrix} = \sum_{i=0}^{n} N^i \begin{pmatrix}a_i\\0\end{pmatrix},$$

kde na pravé straně se vyskytují vektory $\begin{pmatrix}a_i\\0\end{pmatrix}$, tedy $\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}2\\0\end{pmatrix}$. Našli jsme tud96 maticový systém $N = \begin{pmatrix}-1 & -1\\1 & -2\end{pmatrix}, \widehat{\mathcal{A}} = \left\{\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}2\\0\end{pmatrix}\right\}$, který reprezentuje všechny vektory ze $\mathbb{Z}^2$. Tento systém odpovídá maticové formě Eistensteinově systému.

2.2 Třídy ekvivalence v $\mathbb{Z}^d$

Stejně jako při reprezentování čísel v pozičních systémech, hraje i v maticových systémech důležitou roli kongruence.

Definice 31. *Nechť $M \in \mathbb{Z}^{d,d}$ a $x, y \in \mathbb{Z}^d$. Řekneme, že x je v relaci s y modulo M, pokud existuje $z \in \mathbb{Z}^d$ takový, že $x - y = Mz$ a značíme $x \equiv_M y$.*

Poznámka. *Tento vztah můžeme za předpokladu regularity matice M přepsat do tvaru:*

$$x \equiv_M y \Leftrightarrow \exists z \in \mathbb{Z}^d : x - y = Mz \Leftrightarrow \exists z \in \mathbb{Z}^d : M^{-1}(x - y) = z \Leftrightarrow M^{-1}(x - y) \in \mathbb{Z}^d$$

Snadno se ověří, že platí následující tvrzení:

Tvrzení 32. *Pro relaci modulo M platí:*

1. *relace modulo M je na $\mathbb{Z}^d$ ekvivalence,*
2. *pro všechny vektory $x_1, x_2, y_1, y_2 \in \mathbb{Z}^d$ platí*

$$x_1 \equiv_M y_1 \text{ a } x_2 \equiv_M y_2 \implies x_1 + x_2 \equiv_M y_1 + y_2,$$

3. *pro všechny vektory $x_1, y_1 \in \mathbb{Z}^d$ a pro všechna $k \in \mathbb{Z}$ platí*

$$x_1 \equiv_M y_1 \implies kx_1 \equiv_M ky_1.$$

Připomeňme, že k tomu, aby byla relace ekvivalencí, musí být reflexivní, symetrická a tranzitivní. Dále vlastnosti 2 a 3 zaručují, že relace modulo M je kongruence na $\mathbb{Z}$-modulu $\mathbb{Z}^d$. Z tohoto důvodu budeme tyto dva pojmy často zaměňovat.

Nyní může nastat otázka, na čem závisí počet tříd ekvivalence u dané matice. Odpověď na tuto otázku je uváděna u autorů, kteří se věnují maticovým numeračním systémům, vždy bez důkazu. Proto v této kapitole uvedeme i důkazy.

Věta 33. *Pokud $M \in \mathbb{Z}^{d,d}$ je singulární matice, pak počet tříd ekvivalence $\equiv_M$ je nekonečno.*

Důkaz. Cílem důkazu bude najít nekonečně mnoho vektorů, které nebudou navzájem ekvivalentní modulo M, a tudíž budou reprezentovat nekonečně mnoho tříd ekvivalence modulo M.

Nechť $M \in \mathbb{Z}^{d,d}$ je singulární matice, pak zřejmě je i M^T singulární matice. Z Frobeniovy věty plyne, že pro homogenní soustavu se singulární maticí existuje nenulové řešení, označme ho $u \in \mathbb{R}^d, u \neq 0$. Splňuje tedy $M^T u = 0$. Protože matice M^T je celočíselná, musí určitě existovat vektor u s racionálními složkami, který řeší homogenní soustavu s maticí M^T.

Bez újmy na obecnosti předpokládejme tedy $u \in \mathbb{Q}^d, u \neq 0$. Nyní hledejme vektor s celočíselnými složkami, který řeší rovnici $M^T x = 0$. Libovolný nenulový násobek řešení homogenní soustavy zřejmě také řeší danou soustavu, tudíž můžeme vzít libovolný násobek vektoru u. Definujme tedy nový vektor $w := g \cdot u$, kde $g \in \mathbb{Z}$ je společný jmenovatel všech složek vektoru u. Tudíž $w \in \mathbb{Z}^d \setminus \{0\}$ a $M^T w = 0$.

Nyní budeme zkoumat celočíselné násobky vektoru w. Tvrdíme, že vektory $k_1 \cdot w$ a $k_2 \cdot w$, kde $k_1, k_2 \in \mathbb{Z}$, jsou ekvivalentní modulo M právě tehdy, když $k_1 = k_2$. Z definice relace modulo M vyplývá, že

$$k_1 \cdot w \equiv_M k_2 \cdot w \Leftrightarrow \exists z \in \mathbb{Z}^d : (k_1 - k_2) \cdot w = Mz.$$

Po vynásobení poslední rovnosti zleva vektorem w^T a s využitím vlastnosti $M^T w = 0$, a tedy i $(M^T w)^T = w^T M = 0^T$, dostáváme

$$k_1 \cdot w \equiv_M k_2 \cdot w \Leftrightarrow \exists z \in \mathbb{Z}^d : (k_1 - k_2) \cdot w = Mz \implies \exists z \in \mathbb{Z}^d : (k_1 - k_2) w^T w = w^T M z = 0.$$

Protože w je nenulový vektor, musí být i $w^T w > 0$ a tedy platí, že pokud vektory $k_1 \cdot w$ a $k_2 \cdot w$ jsou ekvivalentní modulo M, pak nutně $k_1 = k_2$. Obměnou této implikace dostáváme

$$k_1 \neq k_2 \implies k_1 \cdot w \not\equiv_M k_2 \cdot w.$$

Našli jsme tedy nekonečně mnoho vektorů ve tvaru $k_j w$, kde $k_j \in \mathbb{Z}$, které nejsou navzájem kongruentní, tedy počet tříd ekvivalence modulo M je nekonečno.

□

Pro odvození počtu tříd ekvivalence u regulární matice M budeme využívat rovnoběžnostěny v $\mathbb{Z}^d$. Kopiemi rovnoběžnostěnu budeme pokrývat celou množinu $\mathbb{Z}^d$.

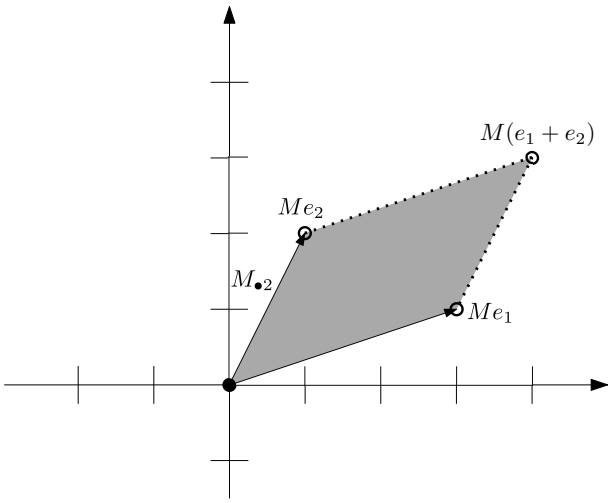
Definice 34. *Rovnoběžnostěnem matice M nazveme množinu*

$$R_M = \{M\alpha : \alpha \in \mathbb{R}^d, \alpha \in [0,1)^d\}. \tag{2.5}$$

Podmínka $\alpha \in [0,1)^d$ říká, že všechny složky vektoru $\alpha \in \mathbb{R}^d$ jsou z intervalu $[0,1)$.

Jedná se o rovnoběžnostěn generovaný vektory $M_{\bullet 1}, \ldots, M_{\bullet d}$, kde výrazem $M_{\bullet j}$ rozumíme j-tý sloupec matice M.

Poznamenejme, že uzávěr R_M má právě 2^d vrcholů. Tyto vrcholy získáme kombinováním a dosazováním vektorů e_j ze standardní báze do předpisu $M(e_{i_1} + \cdots + e_{i_k})$, kde $(i_1, \ldots, i_k)$ je k-tice vzájemně různých prvků z množiny $\{1, \ldots, d\}$.



Obrázek 2.1: R_M pro matici $M = \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix}$

Z obrázku 2.1 můžeme vidět, že z vrcholů uzávěru R_M do rovnoběžnostěnu patří pouze ten z počátku. Následně můžeme vidět souvislost mezi determinantem matice M a objemem rovnoběžnostěnu. Jak ukáže následující lemma, tato čísla se skutečně rovnají.

Lemma 35. *Objem rovnoběžnostěnu R_M matice $M \in \mathbb{Z}^{d,d}$ je roven $|\det M|$.*

Důkaz. Pro singulární matici je tvrzení zřejmé. Nechť M je regulární. Označme $\alpha = \begin{pmatrix}\alpha_1\\ \vdots \\ \alpha_d\end{pmatrix}$. Z definice objemu vyplývá

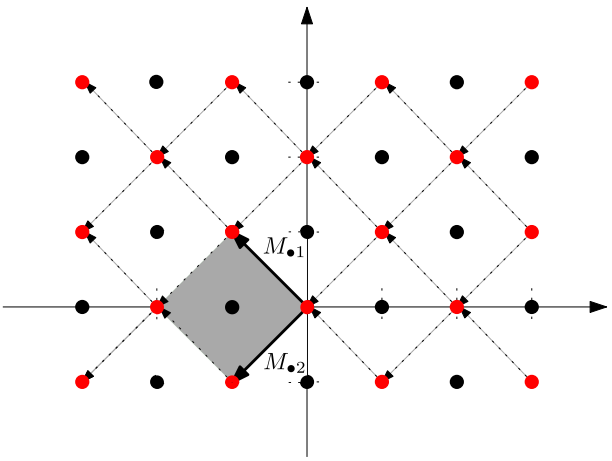
$$\mathrm{vol}(R_M) = \int_{R_M} 1\,\mathrm{d}x_1 \dots \mathrm{d}x_d = \left[\begin{pmatrix}x_1\\ \vdots \\ x_d\end{pmatrix} = M\begin{pmatrix}\alpha_1\\ \vdots \\ \alpha_d\end{pmatrix}\right] = \int_{\alpha\in[0,1)^d} 1\cdot|\det M|\,\mathrm{d}\alpha_1 \dots \mathrm{d}\alpha_d =$$
$$= |\det M| \int_{\alpha\in[0,1)^d} 1\,\mathrm{d}\alpha_1 \dots \mathrm{d}\alpha_d = |\det M|,$$

kde jsme v druhém kroku využili větu o substituci v integrálu s Jakobiánem $|\det M|$. □

Příklad 36. *Na Penneyho systému v maticové formě, tedy na systému s bází* $M = \begin{pmatrix}-1 & -1\\ 1 & -1\end{pmatrix}$ *a abecedou* $\mathcal{A} = \left\{\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}\right\}$, *ukážeme, kdy dva vektory* $x, y \in \mathbb{Z}^d$ *jsou kongruentní:*

$$x \equiv_M y \Leftrightarrow \exists z \in \mathbb{Z}^2 : x - y = Mz \Leftrightarrow \exists z_1, z_2 \in \mathbb{Z} : x - y = M\begin{pmatrix}z_1\\ z_2\end{pmatrix} = M_{\bullet 1}z_1 + M_{\bullet 2}z_2.$$

Tedy vektory jsou kongruentní modulo M právě tehdy, když se liší o celočíselnou kombinaci sloupců matice M.



Obrázek 2.2: Třídy ekvivalence pro matici $\begin{pmatrix}-1 & -1\\ 1 & -1\end{pmatrix}$. Jedna třída je vyznačená červenými puntíky a druhá černými

Na obrázku 2.2 je také vyznačen rovnoběžnostěn matice. Pokud vezmeme v úvahu, jaké vrcholy a hrany obsahuje rovnoběžnostěn(viz obrázek 2.1), můžeme vidět souvislost mezi počtem celočíselných vektorů, které leží rovnoběžnostěnu, a počtem tříd ekvivalence. Obě tato čísla jsou rovna dvěma.

Nyní dokážeme pozorování z komentáře pod obrázkem 2.2, tedy že počet tříd ekvivalence modulo M je roven počtu celočíselných vektorů ležící v R_M. K tomu budeme potřebovat tři pomocná tvrzení. První z nich známe z lineární algebry.

Tvrzení 37. *Nechť $\mathbb{R}^d$ je vektorový prostor s euklidovskou normou $||.||$, $n \in \mathbb{R}^d$ normálový vektor a $D > 0$. Pak existuje $c \in \mathbb{R}$ takové, že pro každé $h \in \mathbb{R}$ je vzdálenost nadrovin H_1 a H_2 s neparametrickými rovnicemi $n^T x = h$ a $n^T x = h + c$ alespoň D, tj. pro všechna $x_1, x_2 \in \mathbb{R}^d$ takové, že $n^T x_1 = h$ a $n^T x_2 = h + c$ platí $||x_2 - x_1|| > D$.*

Přejdeme k druhému pomocnému tvrzení.

Lemma 38. *Nechť $M \in \mathbb{Z}^{d,d}$ je regulární matice. Pak počet tříd ekvivalence $\equiv_M$ je roven počtu vektorů $x \in \mathbb{Z}^d$ takových, že $x \in R_M$, kde R_M je rovnoběžnostěn matice M, tj. počet tříd je roven $\#\mathbb{Z}^d \cap R_M$.*

Důkaz. V první části důkazu ukážeme, že množina $\mathbb{Z}^d \cap R_M$ obsahuje všechny třídy ekvivalence. Toho docílíme tím, že pro libovolný $y \in \mathbb{Z}^d$ najdeme prvek z $\mathbb{Z}^d \cap R_M$, který je s y kongruentní.

Nechť $y \in \mathbb{Z}^d$. Pak určitě soustava rovnic $y = M\gamma$ má řešení z $\mathbb{Z}^d$, protože matice M je regulární. Označme $\gamma = \left(\gamma_1, \ldots, \gamma_d\right)^T$ řešení soustavy $y = M\gamma$ a položme $z_i := \lfloor \gamma_i \rfloor$ a $\alpha_i := \gamma_i - z_i$. Pak určitě $\alpha_i \in [0, 1)$ a $\gamma_i = z_i + \alpha_i$. Označme z a α jako vektory z příslušných složek z_i, α_i. Dostáváme

$$y = M\gamma = M(z + \alpha) = Mz + M\alpha \implies y - M\alpha = Mz \implies y \equiv_M M\alpha.$$

Díky volbě $z \in \mathbb{Z}^d$ vyplývá, že vektor y je v relaci s $M\alpha$ modulo M. Protože $y \in \mathbb{Z}^d$ a $Mz \in \mathbb{Z}^d$, tak platí i $M\alpha \in \mathbb{Z}^d$. Navíc z konstrukce α vyplývá, že $\alpha \in [0, 1)^d$ a tedy $M\alpha \in R_M$. Našli jsme tedy vektor $M\alpha$ z množiny $\mathbb{Z}^d \cap R$, který je v relaci s y.

V druhé části důkazu ukážeme, že žádné dva různé prvky ze $\mathbb{Z}^d \cap R_M$ nejsou navzájem kongruentní. To ukážeme sporem. Mějme $y_1, y_2 \in \mathbb{Z}^d \cap R_M$ a $y_1 - y_2 = Mz$ pro nějaké $z \in \mathbb{Z}^d$. Protože $y_1, y_2 \in R_M$, tak mají tvar $y_1 = M\alpha_1, y_2 = M\alpha_2$ pro $\alpha_1, \alpha_2 \in [0, 1)^d$. Nyní dostáváme

$$M\alpha_1 - M\alpha_2 = Mz \implies z = \alpha_1 - \alpha_2 \in (-1, 1)^d,$$

kde jsme využili předpoklad, že matice M je regulární. Zároveň s faktem, že $z \in \mathbb{Z}^d$ dostáváme, že $z = 0$ a tedy $y_1 = y_2$.

Proto množina $\mathbb{Z}^d \cap R_M$ obsahuje od každé třídy ekvivalence právě jednoho reprezentanta, a tím je důkaz hotov. □

Lemma 39. *Nechť $M \in \mathbb{Z}^{d,d}$ je regulární matice. Pak $\#\mathbb{Z}^d \cap R_M = |\det M|$.*

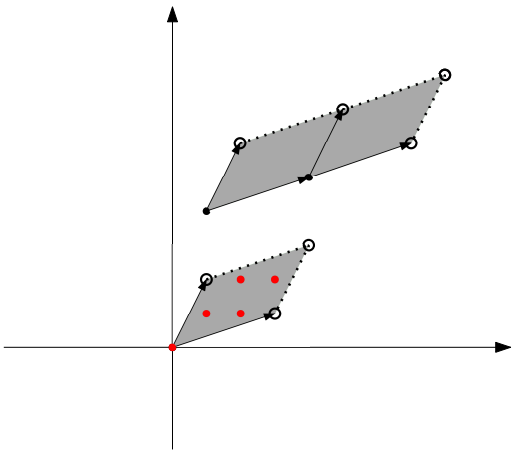
Důkaz. Mějme $N \in \mathbb{N}$, a uvažujme rovnoběžnostěn R_M vynásobený N. Pak dostáváme

$$N \cdot R_M = \{N \cdot M\alpha : \alpha \in [0, 1)^d\} = \{M\gamma : \gamma \in [0, N)^d\} \tag{2.6}$$

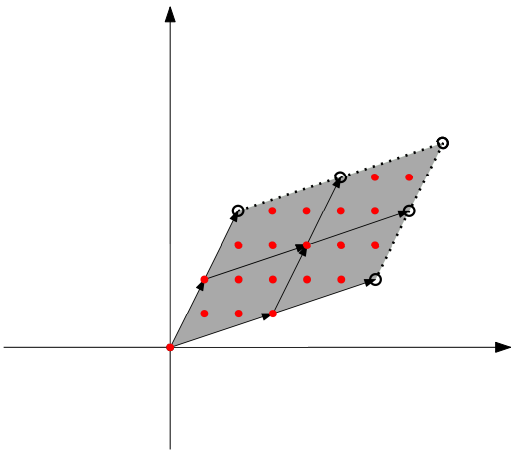
$$= \{M\alpha + Mz : \alpha \in [0, 1)^d, z \in \{0, \ldots, N-1\}^d\} = R_M \oplus \{Mz : z \in \{0, \ldots, N-1\}^d\}, \tag{2.7}$$

kde jsme v předposledním kroku využili jednoznačného rozkladu u složek vektoru β na celou a zlomkovou část. Ze vztahu (2.6) a (2.7) vidíme, že množina $N \cdot R_M$ je sjednocením posunutých kopií rovnoběžnostěnu R_M. Díku tomu, že $\#\{Mz : z \in \{0, \ldots, N-1\}^d\} = N^d$, je těchto posunutých kopií právě N^d. Označme $p := \#(R \cap \mathbb{Z}^d)$, pak díky disjunktnosti posunutých kopií platí $\#((NR_M) \cap \mathbb{Z}^d) = N^d p$.

Nyní disjunktně pokryjeme prostor krychličkami kolem každého celočíselného vektoru. Pro každý $z \in \mathbb{Z}^d$ je tato krychlička tvaru $z + \left[-\frac{1}{2}, \frac{1}{2}\right)^d$ a má objemem 1.



Rovnoběžníky, které pokryvají prostor, kde $p = 5$

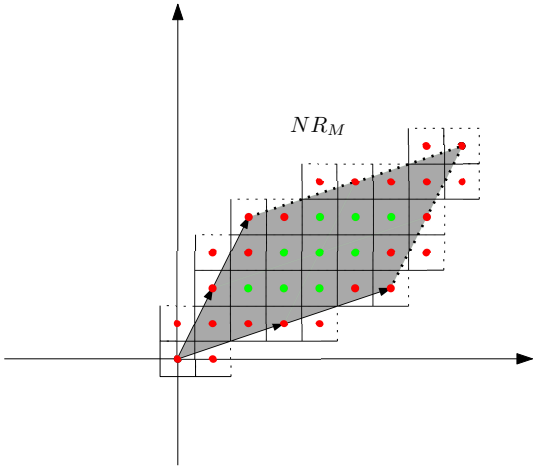


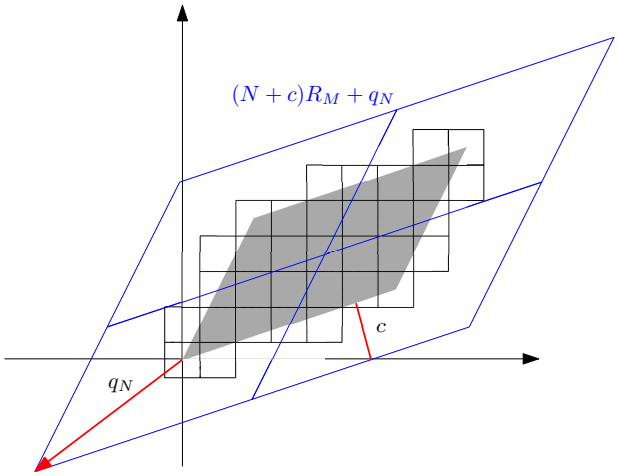
Rovnoběžník NR_M pro $N = 2$ a $N^d p = 20$

Označme číslem P_N počet krychliček, které mají s NR_M neprázdný průnik a Q_N počet krychliček, které mají s doplňkem NR prázdný průnik, tj. celé leží v NR_M. Pak zřejmě platí

$$Q_N \leq \text{vol}\,(NR_M) = N^d |\det M| \leq P_N \quad \text{a} \quad Q_N \leq N^d p \leq P_N.$$

Objem NR_M je $N^d|\det M|$, protože objem rovnoběžnostěnu R_M je $|\det M|$ a násobíme ho konstantou N v d dimenzích.





Nalevo je rovnoběžnostěn NR_M s krychličkami, kde zeleně jsou označeny krychličky započítané do Q_N a P_N a červeně pouze do P_N. Napravo je rovnoběžnostěn $(N + c)R_M + q_N$. V obou případech $N = 2$.

Nyní chceme vytvořit větší rovnoběžnostěn takový, aby se do něj vešel rovnoběžnostěn NR_M i s přečnívajícími krychličkami. Navíc požadujeme, aby měl stejné centrum. Hledáme tedy $c > 0$ a $q_N \in \mathbb{R}^d$ takové, aby pro každý bod $x \notin (N + c)R_M + q_N$ a $y \in NR$ platilo $||y - x|| > \sqrt{d}$, kde $\sqrt{d}$ je diagonála jednotkové krychličky v dimenzi d. Tvrzení 37 zaručuje existenci takového c, které nezávisí na N, a snadno poté najdeme i q_N.

Zřejmě pak platí

$$P_N \leq \text{vol}\,((N + c)R + q_N) = (N + c)^d |\det M|,$$

kde využíváme znalosti, že se objem posunutím nemění. Analogicky pak najdeme i druhý odhad, kdy budeme zmenšovat rovnoběžnostěn NR, tedy

$$Q_N \geq \text{vol}\,((N-c)R_M + q_N) = (N-c)^d |\det M|.$$

Celkově získáváme

$$(N-c)^d|\det M| \leq N^d p \leq (N+c)^d|\det M| \implies \left(\frac{N-c}{N}\right)^d |\det M| \leq p \leq \left(\frac{N+c}{N}\right)^d |\det M|$$

pro všechna $N \in \mathbb{N}$. Limitním přechodem $N \to \infty$ dostáváme tvrzení věty. □

Nyní spojením lemmat 38 a 39 dostáváme následující důsledek.

Věta 40. *Nechť $M \in \mathbb{Z}^{d,d}$ je regulární matice. Pak počet tříd ekvivalence $\equiv_M$ je roven $|\det M|$.*

Příklad 41. *Prozkoumejme, kolik tříd ekvivalence má Penneyho a Eisensteinův systém v maticovém tvaru. První jmenovaný má dvě třídy ekvivalence, protože $\left|\det \begin{pmatrix} -1 & -1 \\ 1 & -1 \end{pmatrix}\right| = 2$, proto má v abecedě dva prvky, a to $\mathcal{A}_1 = \left\{\begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right\}$. Druhý jmenovaný má tři třídy ekvivalence, neboť $\left|\det \begin{pmatrix} -1 & -1 \\ 1 & -2 \end{pmatrix}\right| = 3$, a tudíž jsou v abecedě tři prvky: $\mathcal{A}_2 = \left\{\begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \end{pmatrix}\right\}$.*

2.3 Kompletní abeceda maticového systému

V této podkapitole zkoumáme vlastnosti abecedy $\mathcal{A}$, aby numerační systém $(M, \mathcal{A})$ mohl reprezentovat jednoznačně všechny vektory z množiny $\mathbb{Z}^d$.

Definice 42. *Nechť $(M, \mathcal{A})$ je maticový numerační systém. Nechť $\mathcal{A}$ splňuje:*

1. *pro všechny $x \in \mathbb{Z}^d$ existuje $a \in \mathcal{A}$ takový, že $x \equiv_M a$,*
2. *pro všechny $d, e \in \mathcal{A}$ takové, že $d \neq e$ platí $d \not\equiv_M e$.*

Pak řekneme, že $\mathcal{A}$ je kompletní abeceda maticového numeračního systému $(M, \mathcal{A})$.

Důsledek 43. *Mohutnost kompletní abecedy maticového systému s bází $M \in \mathbb{Z}^{d,d}$ se rovná $|\det M|$.*

Důkaz. Z prvního bodu definice kompletní abecedy plyne, že každá třída ekvivalence má v $\mathcal{A}$ alespoň jednoho reprezentanta. Druhý bod říká, že každá třída ekvivalence má nejvýše jednoho reprezentanta. To implikuje, že z každé třídy ekvivalence je v kompletní abecedě právě jeden reprezentant. Tedy mohutnost kompletní abecedy je počet tříd ekvivalence matice M, a ten je s využitím důsledku 40 roven $|\det M|$. □

Ukážeme, že první bod definice kompletní abecedy je nutnou podmínkou, aby abeceda reprezentovala všechny vektory ze $\mathbb{Z}^d$. Jinými slovy, pokud nějaká třída ekvivalence nemá reprezentanta v kompletní abecedě, už nelze reprezentovat všechny vektory ze $\mathbb{Z}^d$.

Věta 44. *Pokud numerační systém $(M, \mathcal{A})$ reprezentuje všechny vektory ze $\mathbb{Z}^d$, pak každá třída ekvivalence má alespoň jednoho reprezentanta v $\mathcal{A}$.*

Důkaz. Nechť $x \in \mathbb{Z}^d$. Podle předpokladu lze x napsat ve tvaru $x = \sum_{i=0}^{n} M^i a_i$, kde $a_i \in \mathcal{A}$. Pak určitě $x \equiv_M a_0$. Probráním všech $x \in \mathbb{Z}^d$ probereme všechny možné třídy ekvivalence modulo M, proto i $a_0 \in \mathcal{A}$ musí probíhat všechny třídy ekvivalence. Našli jsme tedy pro každou třídu ekvivalence modulo M reprezentanta v $\mathcal{A}$. □

U druhého bodu definice kompletní abecedy se jedná o nutnou podmínku neredundantnosti maticového systému. Jinými slovy, pokud máme systém s abecedou, která obsahuje z nějaké třídy ekvivalence více než jednoho reprezentanta, je nutně redundantní.

Věta 45. *Nechť numerační systém $(M, \mathcal{A})$ je neredundantní a reprezentuje všechny vektory ze $\mathbb{Z}^d$. Pak $\mathcal{A}$ obsahuje z každé třídy ekvivalence nejvýše jednoho reprezentanta.*

Důkaz. Důkaz provedeme sporem. Nechť $(M, \mathcal{A})$ je neredundantní a pro spor předpokládejme, že existuje třída ekvivalence, která má dva reprezentanty v $\mathcal{A}$, tedy, že existují $d, e \in \mathcal{A}$ takové, že $d \neq e$ a $d \equiv_M e$.

Dokážeme, že vektor d má dvě reprezentace. Z $d \equiv_M e$ plyne existence $z \in \mathbb{Z}^d$ takového, že $d = Mz + e$. Pro vektor z z předpokladu věty existuje řetězec $a_n \dots a_0 \in \mathcal{A}^*$, který reprezentuje z. Pak $a_n \dots a_0\, e$ reprezentuje vektor d.

Také řetězec $d \in \mathcal{A}^*$ je reprezentací vektoru d a určitě se tyto dva řetězce nerovnají, protože $d \neq e$. Došli jsme tedy ke sporu. □

Následující věta ukazuje, že systém obsahující kompletní abecedou je neredundantní.

Věta 46. *Nechť $(M, \mathcal{A})$ je maticový systém s kompletní abecedou. Pak každé $x \in \mathbb{Z}^d$ má nanejvýš jednu reprezentaci v $(M, \mathcal{A})$.*

Důkaz. Důkaz ukážeme sporem. Nechť $x \in \mathbb{Z}^d$ má dvě reprezentace, nechť tedy platí

$$x = \sum_{i=0}^{n} M^i a_i = \sum_{i=0}^{m} M^i b_i, \tag{2.8}$$

kde $m, n \in \mathbb{N}$ a $a_i, b_i \in \mathcal{A}$. Bez újmy na obecnosti mějme $n \geq m$. Dodefinujme $b_i = 0$ pro i splňující $n \geq i > m$. Protože tyto dvě reprezentace jsou různé, množina indexů $\{i \in \{0, \dots, n\} : a_i \neq b_i\}$ je neprázdná. Nechť $j := \min\{i \in \{0, \dots, n\} : a_i \neq b_i\}$. Pokud $j > 0$, odečteme od rovnice (2.8) číslo a_0 a vynásobme jí maticí M^{-1}, poté odečteme a_1 a vynásobíme M^{-1}. Takto pokračujeme až odečteme číslo a_{j-1} a vynásobíme M^{-1}. Dostáváme

$$\sum_{i=j}^{n} M^i a_i = \sum_{i=j}^{m} M^i b_i, \tag{2.9}$$

kde $a_j \neq b_j$. Pak z definice kompletní abecedy plyne, žě $a_j \not\equiv_M b_j$ a to spor s rovnicí (2.9). □

Spojením předchozích tří vět dostáváme důsledek.

Důsledek 47. *Nechť $(M, \mathcal{A})$ je maticový systém, který reprezentuje všechny vektory ze $\mathbb{Z}^d$. Pak je neredundantní právě tehdy, když $\mathcal{A}$ je kompletní abeceda.*

Důkaz. Implikace zprava doleva plyne z věty 46. Implikace zleva doprava plyne z vět 44 a 45. □

Vince v práci [13] dokázal následující silné tvrzení.

Věta 48. *Nechť $(M, \mathcal{A})$ je maticový systém, který je neredundantní. Pak každé vlastní číslo matice M je v absolutní hodnotě větší než 1, tj. matice M je expanzivní.*

V této práci zkoumáme maticové systémy, které mají kompletní abecedu, a tudíž podle věty 47 jsou neredundantní. Pak tvrzení věty 48 zdůvodňuje, proč uvažujeme pouze expanzivní matice.

Pokud bychom se neomezovali na systémy, které mají kompletní abecedu, vlastní čísla matice M by mohly být rovné i 1. To plyne z tvrzení 49, které ukázali Jankauskas a Thuswaldner v článku [6].

Věta 49. *Mějme $(M, \mathcal{A})$ maticový numerační systém reprezentující všechny vektory ze $\mathbb{Z}^d$. Pak pro každé vlastní číslo λ matice M platí, že $|\lambda| \geq 1$.*

Příklad 50. *Vraťme se k Penneyho a Eisensteinovu systému. Oba tyto systémy reprezentují množinu $\mathbb{Z}^d$, tudíž z věty 44 plyne, že každá třída ekvivalence má v abecedě alespoň jednoho reprezentanta. Se znalostí determinantu matice M a tedy i mohutnosti potenciální kompletní abecedy můžeme říct, že abeceda neobsahuje víc než jednoho reprezentanta z každé třídy. Tudíž oba tyto systémy disponují kompletní abecedou.*

2.4 Indukované maticové normy

V této části připomeneme vlastnosti normy vektorových prostorů. Tyto normy budeme hojně využívat ve třetí kapitole ke zkoumání maticových systémů. Nejdříve zavedeme skalární součin, tak jak se obvykle definuje v lineární algebře [2].

Definice 51. *Nechť V je vektorový prostor nad tělesem $T \subset \mathbb{C}$. Zobrazení $h : V \times V \to T$ nazveme skalárním součinem vektorového prostoru V, pokud pro všechny $x, y, z \in V, \alpha \in T$ platí:*

1. *pozitivní definitnost: $h(x, x) \geq 0$ a $h(x, x) = 0 \Leftrightarrow x = 0$,*
2. *hermitovskost: $h(x, y) = \overline{h(y, x)}$,*
3. *linearita v prvním argumentu: $h(\alpha x + y, z) = \alpha h(x, z) + h(y, z)$.*

Definice 52. *Nechť V je vektorový prostor nad tělesem $T \subset \mathbb{C}$, zobrazení $||.|| : V \to [0, \infty)$ nazveme normou na vektorovém prostoru V, pokud pro všechny $x, y \in V, \alpha \in T$ platí:*

1. *$||x|| = 0 \Leftrightarrow x = 0$,*
2. *$||\alpha x|| = |\alpha| \cdot ||x||$,*
3. *trojúhelníková nerovnost: $||x + y|| \leq ||x|| + ||y||$.*

Nyní uvedeme dva příklady norem.

Příklad 53. *Nechť h je skalární součin na V. Pak lze snadno ověřit, že zobrazení definované jako $x \mapsto \sqrt{h(x, x)}$ je norma na V. Tuto normu nazýváme normou indukovanou skalárním součinem h.*

Speciálně pro standardní skalární součin definovaný pro každé $x, y \in \mathbb{C}^d$ jako

$$h(x, y) = \sum_{i=1}^{n} x_i \overline{y_i} = y^* x$$

je indukovaná norma rovna

$$||x||_e = \sqrt{\sum_{i=1}^{n} |x_k|^2} = \sqrt{x^* x}.$$

Tuto normu nazýváme euklidovskou normou na $\mathbb{C}^d$ a značíme $||.||_e$.

Příklad 54. *Nechť $P \in \mathbb{C}^{d,d}$ je regulární matice. Ověříme, že zobrazení $\mathbb{C}^d \to [0, \infty)$ definované jako $x \mapsto ||Px||_e$ je normou na prostoru $\mathbb{C}^d$. Nechť $x, y \in \mathbb{C}^d$ a $\alpha \in T$:*

1. *$||Px||_e = 0 \Leftrightarrow x = 0$: S využitím Frobeniovy věty, která říká, že homogenní soustava s regulární maticí má pouze triviální řešení dostáváme:*

$$||Px||_e = 0 \Leftrightarrow Px = 0 \Leftrightarrow x = 0.$$

2. *Rovnost*

$$||P(\alpha x)||_e = ||\alpha(Px)||_e = |\alpha| \cdot ||Px||_e$$

a nerovnost

$$||P(x+y)||_e = ||Px + Py||_e \leq ||Px||_e + ||Py||_e$$

plyne z faktu, že euklidovská norma splňuje pozitivní homogenitu a trojúhelníkovou nerovnost.

Pro matice jako prvky vektorového prostoru $\mathbb{C}^{d,d}$ budeme využívat normy indukované normou v $\mathbb{C}^d$.

Definice 55. *Nechť $||.||$ je norma na vektorovém prostoru $\mathbb{C}^d$, a nechť $A \in \mathbb{C}^{d,d}$. Číslo $||A|| := \sup_{x \in \mathbb{C}^d, ||x||=1} ||Ax||$ nazveme indukovanou normou matice A příslušnou normě $||.||$.*

Věta 56. *Nechť $\mathbb{C}^d$ je vektorový prostor nad $\mathbb{C}$. Pak pro normu $||.||$ na prostoru $\mathbb{C}^d$ a její indukovanou normu matice $A \in \mathbb{C}^{d,d}$ platí:*

1. *indukovaná norma je normou na prostoru $\mathbb{C}^{d,d}$,*
2. *pro všechny $x \in \mathbb{C}^d$: $||Ax|| \leq ||A|| \cdot ||x||$,*
3. *$\varrho(A) \leq ||A||$.*

Důkaz. 1. Abychom ukázali, že se jedná o normu, musíme ověřit 3 body z definice normy. Nechť $A, B \in \mathbb{C}^{d,d}, \alpha \in T$:

(a) $||A|| = 0 \Leftrightarrow A = 0$: dokažme implikaci zleva doprava:

$$||A|| = \sup_{||x||=1} ||Ax|| = 0 \implies ||Ax|| = 0 \text{ pro každé } x \in \mathbb{C}^d \text{ takové, že } ||x|| = 1.$$

Odtud $Ax = 0$ pro každé $x \in \mathbb{C}^d$.

Opačná implikace je zřejmá.

(b) $||A + B|| \leq ||A|| + ||B||$: s využitím trojúhelníkové nerovnosti pro normu na $\mathbb{C}^d$ dostáváme:

$$||A+B|| = \sup_{||x||=1} ||(A+B)x|| \leq \sup_{||x||=1} (||Ax|| + ||Bx||) \leq$$
$$\leq \sup_{||x||=1} ||Ax|| + \sup_{||x||=1} ||Bx|| = ||A|| + ||B||.$$

(c) $||\alpha A|| = |\alpha| \cdot ||A||$:

$$||\alpha A|| = \sup_{||x||=1} ||(\alpha A)x|| = \sup_{||x||=1} |\alpha| \cdot ||Ax|| = |\alpha| \sup_{||x||=1} ||Ax|| = |\alpha| \cdot ||A||,$$

kde ve druhém kroku jsme využili vlastnosti normy na $\mathbb{C}^d$.

2. Pro všechny nenulové $x \in \mathbb{C}^d$ platí:

$$\frac{||Ax||}{||x||} \leq \sup_{x \neq 0} \frac{||Ax||}{||x||} = \sup_{x \neq 0} ||A\left(\frac{x}{||x||}\right)|| = \sup_{||y||=1} ||Ay|| = ||A||,$$

kde u druhého suprema využíváme faktu, že zkoumá jen množinu jednotkových vektorů. Nyní vynásobením $||x||$ získáváme $||Ax|| \leq ||A|| \cdot ||x||$ pro nenulové $x \in \mathbb{C}^d$. Navíc tato nerovnost platí i pro $x = 0$, získali jsme tedy platnost pro všechny $x \in \mathbb{C}^d$.

3. Nechť λ je vlastní číslo matice A a nechť u je vlastní vektor matice A příslušný vlastnímu číslu λ takový, že $||u|| = 1$. Pak platí:

$$||A|| = \sup_{||x||=1} ||Ax|| \geq ||Au|| = ||\lambda u|| = |\lambda| \cdot ||u|| = |\lambda|.$$

Tato nerovnost platí pro libovolné vlastní číslo matice A, platí tedy i pro maximum z vlastních čísel matice A. Dostáváme $||A|| \geq \max_{\lambda \in \sigma(A)} |\lambda| = \varrho(A)$.

□

Počítat indukovanou normu matice z definice vyžaduje prozkoumat nekonečnou množinu vektorů. Proto uvedeme speciální případ normy, u které bude počítání indukované normy z matice mnohem snazší.

Důkaz vět 57 a 60 je převzat z [5]. My je však rozepisujeme do detailů protože parametry, které se v konstrukci vyskytnou, potřebujeme znát v explicitním tvaru. V původním důkazu jsou uváděny pouze jako hodnoty pomocí Landauovy symboliky malé o.

Věta 57. *Nechť $A \in \mathbb{C}^{d,d}$ je diagonalizovatelná matice. Pak existuje norma na $\mathbb{C}^d$ taková, že pro její indukovanou normu matice A platí $||A|| = \varrho(A)$.*

Důkaz. Nechť A je diagonalizovatelná matice. Pak ji lze zapsat ve tvaru $A = P^{-1}DP$, kde P je regulární matice a D diagonální matice.

Nyní definujme normu $N : \mathbb{C}^d \to [0, \infty)$ pro každé $x \in \mathbb{C}^d$ jako $N(x) = ||Px||_e$. Z příkladu 54 plyne, že se opravdu jedná o normu, indukuje tedy maticovou normu pro A jako $||A|| = \sup_{||Px||_e=1} N(Ax)$. Rozepišme nyní výraz

$$\begin{aligned}(N(Ax))^2 = ||PAx||_e^2 = ||DPx||_e^2 = (DPx)^*(DPx) = (Px)^*D^*D(Px) = \\ = \sum_{i=1}^{d} \overline{(Px)_i}|\lambda_i|^2(Px)_i \leq (\varrho(A))^2(Px)^*(Px) = (\varrho(A))^2||Px||_e^2,\end{aligned}$$

kde jsme využili faktu, že matice D je diagonální a obsahuje vlastní čísla na diagonále. Nyní pro všechny vektory splňující $||Px||_e = 1$ platí $N(Ax) \leq \varrho(A)$, což implikuje:

$$||A|| = \sup_{||Px||_e=1} N(Ax) \leq \varrho(A).$$

Odhad z druhé strany $||A|| \geq \varrho(A)$ platí pro libovolnou indukovanou normu z věty 56. □

Přeformulujme tvrzení věty do tvaru, ve kterém vidíme jak se konstruuje daná indukovaná norma.

Důsledek 58. *Nechť $A \in \mathbb{C}^{d,d}$ je diagonalizovatelná matice a nechť P je regulární matice taková, že $A = P^{-1}DP$, kde D je diagonální matice. Pak zobrazení $x \mapsto ||Px||_e$ je norma na $\mathbb{C}^d$ a její indukovaná norma matice A splňuje $||A|| = \varrho(A)$.*

Předchozí věta platí pouze pro diagonalizovatelné matice, tudíž bychom chtěli zobecnit toto tvrzení i pro nediagonalizovatelné matice. K tomuto účelu nejprve dokážeme následující lemma.

Lemma 59. *Nechť všechny prvky matice $M \in \mathbb{C}^{d,d}$ jsou omezeny konstantou K, tj. pro všechna $i, j \in \{1, \dots, d\}$ platí $|M_{ij}| \leq K$. Pak pro každé $y \in \mathbb{C}^d$ platí $|y^*My| \leq dKy^*y$.*

Důkaz. Snadno si rozmyslíme, že pro libovolnou konvexní funkci $f : \mathbb{R} \to \mathbb{R}$ platí

$$f\left(\frac{1}{d}\sum_{i=1}^{d} a_i\right) \leq \frac{1}{d}\sum_{i=1}^{d} f(a_i),$$

což znamená, že funkční hodnota průměru je menší nebo rovna průměru funkčních hodnot. Speciálně pro funkci $f(x) = x^2$, která je zřejmě konvexní, platí

$$\left(\frac{1}{d}\sum_{i=1}^{d} a_i\right)^2 \leq \frac{1}{d}\sum_{i=1}^{d} a_i^2.$$

S využitím této nerovnosti můžeme upravit výraz

$$|y^*My| = \left|\sum_{i=1}^{d} \overline{y_i}(My)_i\right| = \left|\sum_{i=1}^{d} \overline{y_i}\sum_{j=1}^{d} M_{ij}y_j\right| \leq \sum_{i=1}^{d} |\overline{y_i}|\sum_{j=1}^{d} |M_{ij}||y_j| \leq K\sum_{i=1}^{d} |y_i|\sum_{j=1}^{d} |y_j| =$$
$$= K\left(\sum_{i=1}^{d} |y_i|\right)^2 \leq Kd\sum_{i=1}^{d} |y_i|^2 = Kdy^*y,$$

a tímto je důkaz hotov. □

Pro nediagonalizovatelné matice neplatí, že bychom byli schopni nalézt normu takovou, že její indukovaná norma přímo rovnala spektrálnímu poloměru. Ale zato dokážeme najít normu tak, aby její indukovaná norma byla spektrálnímu poloměru blízko.

Věta 60. *Nechť $A \in \mathbb{C}^{d,d}$ a nechť $P \in \mathbb{C}^{d,d}$ je regulární matice taková, že matice $P^{-1}AP$ má Jordanův tvar. Pak pro libovolné $\varepsilon > 0$ existuje norma $||.||_{P,\varepsilon}$ na $\mathbb{C}^d$ taková, že pro její indukovanou normu matice A platí $||A||_{P,\varepsilon} \leq \varrho(A) + \varepsilon$.*

Důkaz. Nechť $P^{-1}AP$ má Jordanův tvar. Pak lze psát$P^{-1}AP = J_{k_1}(\lambda_1) \oplus \ldots \oplus J_{k_s}(\lambda_s)$, kde $J_{k_i}(\lambda_i)$ jsou Jordanovy bloky řádu k_i příslušné vlastnímu číslu λ_i. Připomeňme, že Jordanův blok $J_m(\lambda)$ má tvar

$$J_m(\lambda_i) = \lambda I_m + \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \cdots & \cdots & \cdots & 0 \end{pmatrix} \in \mathbb{C}^{m,m}.$$

Zvolme $\delta > 0$ a definujme matici B_m řádu m jako

$$B_m := \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \delta & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \delta^{m-1} \end{pmatrix} \in \mathbb{R}^{m,m}. \tag{2.10}$$

Nyní pro blok $J_m(\lambda_i)$ provedeme úpravu s maticí B_m a dostaneme

$$B_m^{-1} J_m(\lambda_i) B_m = \lambda I_m + \delta \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \cdots & \cdots & \cdots & 0 \end{pmatrix}.$$

Zopakujme tento postup pro každý Jordanův blok matice $P^{-1}AP$. Definujme $B := B_{k_1} \oplus \ldots \oplus B_{k_s}$, kde k_i jsou řády příslušných Jordanových bloků. Pak získáme rovnost

$$B^{-1}P^{-1}APB = D + \delta E, \tag{2.11}$$

kde matice E je nulová až na prvky těsně nad diagonálou, kde se vyskytují jedničky a nuly.

Nyní přejdeme k definici normy, která závisí na ε a na matici P, která převádí matici A do Jordanového tvaru. Definujme normu pro všechny $x \in \mathbb{C}^d$ jako $||x||_{P,\varepsilon} := ||B^{-1}P^{-1}x||_e$. Skutečně se jedná o normu, protože matice B^{-1} je regulární, tedy i součin $B^{-1}P^{-1}$ je regulární. Zkoumejme nyní výraz $||A|| = \sup_{||x||_{P,\varepsilon}=1} ||Ax||_{P,\varepsilon}$. S využitím vztahu (2.11) a transformace $y = B^{-1}P^{-1}x$ dostáváme

$$\begin{aligned} &||Ax||_{P,\varepsilon}^2 = ||B^{-1}P^{-1}Ax||_e^2 = ||(D+\delta E)B^{-1}P^{-1}x||_e^2 = \\ &= ||(D+\delta E)y||_e^2 = y^*(D^*+\delta E^*)(D+\delta E)y = \\ &= y^*(D^*D + \delta D^*E + \delta E^*D + \delta^2 E^*E)y = y^*D^*Dy + \delta y^*(D^*E + E^*D + \delta E^*E)y. \end{aligned}$$

Pro vektory splňující $||x||_{P,\varepsilon} = ||B^{-1}P^{-1}x||_e = ||y||_e = 1$ a pro první část výrazu máme

$$y^*D^*Dy = \sum_{i=1}^{d} \overline{y_i}|\lambda_i|^2 y_i \leq \varrho(A)^2 y^*y = \varrho(A)^2 ||y||_e^2 = \varrho(A)^2.$$

Pro odhad druhé části výrazu můžeme vypozorovat, že matice $(D^*E + E^*D + \delta E^*E)$ má všechny prvky omezené konstantou $\varrho(A)+\delta$, tudíž lze použít lemma 59 a pro vektory $||y||_e = 1$ dostáváme

$$\delta y^*(D^*E + E^*D + \delta E^*E)y \leq \delta d(\varrho(A) + \delta)y^*y = \delta d(\varrho(A) + \delta).$$

Nyní můžeme oba odhady spojit a pro indukovanou normu matice A máme

$$||A||_{P,\varepsilon}^2 = \sup_{||x||_{P,\varepsilon}=1} ||Ax||_{P,\varepsilon}^2 \leq (\varrho(A))^2 + \delta d(\varrho(A) + \delta) \overset{!}{\leq} (\varrho(A) + \varepsilon)^2.$$

Pro pevné $\varepsilon > 0$ určitě můžeme najít $\delta > 0$ tak, aby platila nerovnost označena vykřičníkem, protože

$$\lim_{\delta \to 0^+} \delta d(\varrho(A) + \delta) = 0.$$

Našli jsme tedy normu $||.||_{P,\varepsilon}$ zkonstruovanou pomocí tohoto δ, pro jejíž indukovanou normu matice A platí

$$||A||_{P,\varepsilon} = \sup_{||x||_{P,\varepsilon}=1} ||Ax||_{P,\varepsilon} \leq \varrho(A) + \varepsilon.$$

□

Přeformulujme větu do tvrzení, které napoví, jak danou normu konstruovat.

Důsledek 61. *Nechť $A \in \mathbb{C}^{d,d}$ a nechť $P \in \mathbb{C}^{d,d}$ je regulární matice taková, že matice $P^{-1}AP$ má Jordanův tvar. Nechť $\delta > 0$ splňuje pro dané $\varepsilon > 0$ nerovnost $\varrho(A)^2 + \delta d(\varrho(A) + \delta) \leq (\varrho(A) + \varepsilon)^2$. Pak pro normu definovanou pro všechna $x \in \mathbb{C}^d$ jako $||x||_{P,\varepsilon} := ||B^{-1}P^{-1}x||_e$, kde vznik matice B s využitím čísla δ je popsán vtahem (2.10), platí, že její indukovaná norma splňuje nerovnost $||A||_{P,\varepsilon} \leq \varrho(A) + \varepsilon$.*

Kapitola 3

Reprezentace vektorů v maticovém systému

V této kapitole hledáme postačující a nutnou podmínku maticového systému, k tomu, aby reprezentoval celou množinu $\mathbb{Z}^d$. Nejdříve představíme obdobný algoritmus jako v pozičních numeračních systémech pro hledání reprezentace v maticovém numeračním systému.

Základní algoritmus pro maticové systémy: Hledání reprezentace pro $x \in \mathbb{Z}^d$ v maticovém systému $(M, \mathcal{A})$ s kompletní abecedou

vstup : vektor $x \in \mathbb{Z}^d$, pro který hledáme reprezentaci v $(M, \mathcal{A})$
výstup: řetězec $a \in \mathcal{A}^*$, který vyjadřuje reprezentaci x v $(M, \mathcal{A})$, tzn $x = \sum_{i=0}^{n} M^i a_i$

```
1 i := 0
2 while x ≠ 0 do
3 |   najdi a_i ∈ A tak, aby a_i ≡_M x
4 |   x := M^{-1}(x − a_i)
5 |   i := i + 1
6 end
7 n := i − 1
8 a := a_n a_{n−1} ... a_0
9 return a
```

Algoritmus má téměř stejný tvar jako první algoritmus pro hledání reprezentací u pozičních systémů, pouze jsme nahradili čísla vektory, bázi maticí, a kongruenci modulo β kongruencí modulo M.

Následující věta umožní zkoumat, kdy má vektor reprezentaci v $(M, \mathcal{A})$, pomocí základního algoritmu.

Věta 62. *Nechť $(M, \mathcal{A})$ je maticový numerační systém s kompletní abecedou. Pak základní algoritmus je pro dané $x \in \mathbb{Z}^d$ konečný právě tehdy, když x má v $(M, \mathcal{A})$ reprezentaci.*

Důkaz. Dokažme nejprve implikaci zleva doprava. Pokud základní algoritmus skončí po konečně mnoha krocích, dostaneme řetězec $a_n a_{n-1} \dots a_0$. Ověřme, že se jedná skutečně o $(M, \mathcal{A})$-reprezentaci vektoru x.

Označme $x^{(n)}$ vektor x v i-té iteraci. Zřejmě $x^{(0)} = x$. Pro a_0 platí, že existuje $z_0 \in \mathbb{Z}^d$ takový, že $x = x^{(0)} = Mz_0 + a_0$. Pro a_1 existuje z_1 takový, že $x^{(1)} = Mz_1 + a_1$, a navíc

$x^{(1)} = M^{-1}(x^{(0)} - a_0)$. Po spojení těchto dvou vztahů a vynásobení maticí M dostaneme $x = M^2 z_1 + M a_1 + a_0$. Takto pokračujeme až k indexu n, kde dostáváme existenci z_n takového, že $x = M^{n+1} z_n + \sum_{j=0}^{n} M^j a_j$ a z podmínky, že $x^{(i)} = 0$ a rovnosti $M z_n = x^{(n-1)} - a_n$ plyne, že $z_n = M^{-1}(x^{(n-1)} - a_n) = x^{(n)} = 0$ a tedy i $z_n = 0$. Dostali jsme rovnost $x = \sum_{j=0}^{n} M^j a_j$.

Pro opačnou implikaci z předpokladu plyne, že x má reprezentaci ve tvaru $x = \sum_{j=0}^{n} M^j e_j$, kde $e_j \in \mathcal{A}$. V prvním kroku hledáme $a_0 \in \mathcal{A}$ takový, že $a_0 \equiv_M x = \sum_{j=0}^{n} M^j a_j$. Protože $\mathcal{A}$ obsahuje z každé třídy právě jednoho reprezentanta plyne, že $a_0 = e_0$. Následně $x^{(1)} := \sum_{j=1}^{n} M^{j-1} e_j$, a stejným způsobem dostaneme zase rovnost $a_1 = e_1$.

Po $n+1$ krocích máme $x^{(n)} = \sum_{j=n}^{n} M^{j-n} e_j = e_n$. Nyní $a_n = e_n$ a

$x^{(n+1)} := M^{-1}(x^{(n)} - a_n) = M^{-1}(e_n - a_n) = 0$. Algoritmus tedy pro x, které má reprezentaci v $(M, \mathcal{A})$, v $n+1$-ím kroku skončil. □

Později budeme zkoumat jednotlivé iterace základního algoritmu, proto definujme funkci, která odpovídá operacím na řádku 3 a 4 v základním algoritmu.

Definice 63. *Nechť $(M, \mathcal{A})$ je maticový numerační systém s kompletní abecedou. Funkci $T : \mathbb{Z}^d \to \mathbb{Z}^d$ definovanou pro všechna $x \in \mathbb{Z}^d$ jako $T(x) := M^{-1}(x - a)$, kde $a \in \mathcal{A}$ splňuje $a \equiv_M x$, nazveme redukční funkcí základního algoritmu.*

Z faktu, že $\mathcal{A}$ je kompletní abeceda, plyne existence právě jednoho $a \in \mathcal{A}$ takového, že $a \equiv_M x$. Vektor x má tedy jednoznačně určený obraz a jedná se skutečně o funkci. Navíc z definice relace modulo M platí, že $M^{-1}(x - a) \in \mathbb{Z}^d$.

Poznámka 64. *Pokud má vektor $T(x)$ reprezentaci $e_m \dots e_0$ v $(M, \mathcal{A})$, pak vektor x má také v $(M, \mathcal{A})$ reprezentaci a je rovna $e_m \dots e_0\, a$, kde $a \in \mathcal{A}$ je vektor splňující $a \equiv_M x$.*

Ověřme nyní toto tvrzení. Podle předpokladů lze zapsat $T(x) = \sum_{i=0}^{m} M^i e_i$ a zároveň z definice plyne $T(x) = M^{-1}(x - a)$, kde $a \equiv_M x$. Po spojení těchto dvou rovností a vynásobením maticí M a přičtením vektoru a dostáváme

$$x = \sum_{i=0}^{m} M^{i+1} e_i + a,$$

a to znamená, že x má v $(M, \mathcal{A})$ reprezentaci $e_m \dots e_0\, a$.

Nyní představíme další algoritmus, který usnadní kontrolu konečnosti základního algoritmu.

Rozšířený algoritmus: Algoritmus pro kontrolu konečnosti základního algoritmu

vstup : vektor $x \in \mathbb{Z}^d$, pro který sledujeme, zda základní algoritmus skončí
výstup: odpověď, zda základní algoritmus po konečně krocích skončí

```
1 pole := prázdné pole vektorů ze Z^d
2 while x ≠ 0 do
3 |   if x je v poli then
4 |   |   return false
5 |   end
6 |   vlož x do pole
7 |   x := T(x)
8 end
9 return true
```

Krok na řádku 7, tedy kde volíme nové x jako $x := T(x)$, odpovídá dvěma krokům v základním algoritmu, a to hledání $a \in \mathcal{A}$ takového, že $a \equiv_M x$ a volbě $x := M^{-1}(x - a)$. Na rozdíl od základního algoritmu prvky z abecedy nezapisujeme do pole a nevracíme řetězec, který reprezentuje x.

Poznamenejme, že v tomto algoritmu vytváříme pole vektorů, kam zapisujeme, jakých hodnot vektor x v průběhu algoritmu nabýval. Pokud v některé z dalších iterací dostaneme vektor, kterého již vektor x nabýval, znamená to, že se rozšířený algoritmus zacyklil, a tedy, že základním algoritmus neskončí po konečně mnoha krocích.

Zřejmě platí, že rozšířený algoritmus skončí výstupem true, právě když skončí základní algoritmus. Můžeme tedy používat tento rozšířený algoritmus, díky větě 62. ke kontrole, zda vektor $x \in \mathbb{Z}^d$ má reprezentaci v $(M, \mathcal{A})$.

Testovat, zda maticový systém reprezentuje celou množinu $\mathbb{Z}^d$, tímto způsobem je nemožné, protože bychom museli otestovat nekonečně mnoho vektorů.

3.1 Koule v neeuklidovské metrice

Pro návrh konečné testovací množiny budeme využívat metriku, jejíž existenci zaručuje věta 60. Tuto větu budeme aplikovat na reálnou matici M^{-1}, kde M je báze numeračního systému. I když je matice M^{-1} reálná, matice P určující metriku může být komplexní. Tento hendikep nám pomůže odstranit tato podkapitola.

Tvrzení 65. *Nechť $R \in \mathbb{R}^{d,d}$ je regulární matice a $K \in \mathbb{R}, K > 0$. Pak množina $\{y \in \mathbb{R}^d : (Ry)^T Ry \leq K^2\}$ je omezená.*

Důkaz. Označme množinu $B := \{y \in \mathbb{R}^d : (Ry)^T Ry \leq K^2\}$. Najdeme omezenou množinu B' takovou, že $B \subset B'$, pak zřejmě množina B bude omezená. Pro vektory $y \in B$ platí

$$K^2 \geq (Ry)^T Ry = \sum_{i=1}^{d} (Ry)_i (Ry)_i = \sum_{i=1}^{d} (Ry)_i^2 \implies$$
$$\implies \forall i \in \{1, \ldots, d\} : (Ry)_i^2 \leq K^2 \Leftrightarrow \forall i \in \{1, \ldots, d\} : (Ry)_i \in [-K, K] .$$

Definujme množinu $B^{'}$ jako $B^{'} := \{y \in \mathbb{R}^d : (Ry)_i \ \in [-K, K], \forall i \in \{1, \ldots, d\}\}$. Pak jistě platí $B \subset B^{'}$. Nyní stačí ukázat, že $B^{'}$ je omezená. Pro vektory z množiny $B^{'}$ platí

$$y \in B^{'} \ \Leftrightarrow \ Ry \in [-K, K]^d \ \Leftrightarrow \ y \in R^{-1}\,[-K, K]^d\,.$$

Množina $[-K, K]^d$ je uzavřená a omezená množina ve vektorovém prostoru $\mathbb{R}^d$, je tedy i kompaktní. Násobení maticí R^{-1} je jistě spojité zobrazení, a to znamená, že zobrazuje kompaktní množiny na kompaktní množiny. To již implikuje, že množina $R^{-1}\,[-K, K]^d$ je kompaktní, tedy i omezená. □

Důsledek 66. *Nechť $R \in \mathbb{R}^{d,d}$ je regulární matice a $K \in \mathbb{R}, K > 0$. Pak množina $\{y \in \mathbb{Z}^d : (Ry)^T Ry \leq K^2\}$ je konečná.*

Důkaz. Průnik omezené množiny v $\mathbb{R}^d$ s mřížkou $\mathbb{Z}^d$ je konečná množina. □

Tvrzení 67. *Nechť $P \in \mathbb{C}^{d,d}$ regulární matice. Pak existuje regulární matice $R \in \mathbb{R}^{d,d}$ taková, že pro všechna $x \in \mathbb{R}^d$ platí $(Px)^* Px = (Rx)^T Rx$.*

Důkaz. Rozdělme si matici $P \in \mathbb{C}^{d,d}$ na reálnou a imaginární část $P = A + \mathrm{i}B$, kde $A, B \in \mathbb{R}^{d,d}$. S využitím definice euklidovské normy pro $x \in \mathbb{R}^d$ dostáváme

$$\begin{aligned}\mathbb{R} \ni ||Px||_e^2 = ||(A + \mathrm{i}B)x||_e^2 = ((A + \mathrm{i}B)x)^*(A + \mathrm{i}B)x = x^T(A - \mathrm{i}B)^T(A + \mathrm{i}B)x = \\ = x^T(A^TA + B^TB)x + \mathrm{i}x^T(A^TB - B^TA)x \implies ||Px||_e^2 = x^T(A^TA + B^TB)x.\end{aligned}$$

Označme matici $H := A^TA + B^TB$. Matice $H \in \mathbb{R}^{d,d}$ je zřejmě symetrická a navíc i pozitivně definitní, protože pro nenulové $x \in \mathbb{R}^d$ platí $x^*Hx = ||Px||_e^2 > 0$. Tudíž matici H můžeme rozložit podle Choleského rozkladu na $H = R^TR$, kde $R \in \mathbb{R}^{d,d}$. Dostali jsme tedy rovnost $||Px||_e^2 = (Px)^*Px = (Rx)^TRx$.

Zbývá dokázat, že R je regulární matice. Pokud by byla singulární, měla by netriviální jádro, to znamená, že by existoval nenulový $x \in \mathbb{R}^d$ takový, že $Rx = 0$ a to by byl spor s faktem, že $||Px||_e$ je norma. □

Nyní dokážeme důležité tvrzení, a to že množina $\{x \in \mathbb{Z}^d : ||x|| \leq K\}$, kterou můžeme interpretovat jako uzavřenou kouli v normě $||.||$, je konečná.

Věta 68. *Nechť $P \in \mathbb{C}^{d,d}$ je regulární matice, nechť $||.||$ je norma definovaná pro všechna $\mathbb{C}^d$ jako $||x|| = ||Px||_e$ a nechť $K \in \mathbb{R}$. Pak množina $B := \{x \in \mathbb{Z}^d : ||x|| \leq K\}$ je konečná.*

Důkaz. Pro $K \leq 0$ je množina zřejmě konečná. Uvažujme tedy případ $K > 0$. Pro regulární matici $P \in \mathbb{C}^{d,d}$ existuje z tvrzení 67 matice $R \in \mathbb{R}^{d,d}$ taková, že $(Rx)^TRx = (Px)^*Px = ||Px||_e^2$ pro všechna $x \in \mathbb{R}^d$. Podle důsledku 66 platí, že množina $\{x \in \mathbb{Z}^d : (Ry)^TRy < K^2\} = \{x \in \mathbb{Z}^d : ||Px||_e^2 \leq K^2\}$ je konečná. Díky podmínce $K > 0$ a kladnosti normy platí, že $x \in \mathbb{Z}^d$ splňuje $||Px||_e^2 \leq K^2$ právě tehdy, když $||Px||_e \leq K$. Tímto je důkaz hotov. □

Později se bude hodit odhad velikosti složek vektorů, které patří do množiny $\{x \in \mathbb{Z}^d : ||Px||_e \leq K\}$. K tomu poslouží následující poznámka.

Poznámka 69. *Nechť $\gamma > 0$ a $P \in \mathbb{C}^{d,d}$ je regulární matice. Hledejme číslo $\alpha \in \mathbb{R}$ takové, že pro všechna $y \in \{x \in \mathbb{Z}^d : ||Px||_e \leq \gamma\}$ platí $|y_i| \leq \alpha$ pro všechna $i \in \{1, \ldots, d\}$. Tedy že platí následující implikace*

$$y \in \{x \in \mathbb{Z}^d : ||Px||_e \leq \gamma\} \implies y \in [-\alpha, \alpha]^d\,. \tag{3.1}$$

Tvrzení věty 67 *říká, že platí rovnost* $\{x \in \mathbb{Z}^d : ||Px||_e \leq \gamma\} = \{x \in \mathbb{Z}^d : (Rx)^T(Rx) \leq \gamma^2\}$ *pro matici* $R \in \mathbb{R}^{d,d}$*, jejíž vznik je popsán v důkazu. Nejdříve jsme rozložili matici* $P \in \mathbb{C}^{d,d}$ *na reálnou a komplexní část, tedy* $P = A + \mathrm{i}B$*, kde* $A, B \in \mathbb{R}^{d,d}$*. Následně jsme dostali matici* $R \in \mathbb{R}^{d,d}$ *z Choleského rozkladu pro matici* $A^TA + B^TB$*, tedy* $A^TA + B^TB = R^TR$*.*

Nyní z důkazu věty 65 *můžeme vidět, že platí*

$$y \in \{x \in \mathbb{Z}^d : (Rx)^T(Rx) \leq \gamma^2\} \implies y \in R^{-1}\left[-\gamma, \gamma\right]^d = \gamma R^{-1}\left[-1, 1\right]^d.$$

Pokud se zaměříme pouze na jednu složku vektoru y*, můžeme z definice násobení matice a vektoru vyvodit, že* $y_i = \gamma \sum_{j=1}^{d} (R^{-1})_{ij} a_j$*, pro nějaké* $a_k \in [-1, 1]$*, kde* $k \in \{1, \ldots, d\}$*. Zkoumejme nyní číslo* y_i *v absolutní hodnotě a s využitím trojúhelníkové nerovnosti dostáváme*

$$|y_i| = \gamma \left| \sum_{j=1}^{d} (R^{-1})_{ij} a_j \right| \leq \gamma \sum_{j=1}^{d} |(R^{-1})_{ij}||a_j| \geq \gamma \sum_{j=1}^{d} |(R^{-1})_{ij}|.$$

Dostali jsme tedy odhad pro jednu složku vektoru y*. Nyní nalezneme odhad pro každou složku vektoru* y*, a vezmeme maximum z nich, abychom dostali univerzální konstantu pro všechny složky.*

Formálně dostáváme $\alpha := \gamma \max_{i \in \{1,\ldots,d\}} \sum_{j=1}^{d} |(R^{-1})_{ij}|$*. Číslo* $\sum_{j=1}^{d} |(R^{-1})_{ij}|$ *odpovídá součtu absolutních hodnot prvků* i*-tého řádku matice* R^{-1}*.*

3.2 Testovací množina pro maticové systémy

V této části se již dostáváme k postačující a nutné podmínce pro maticový systém, aby reprezentoval všechny vektory ze $\mathbb{Z}^d$. Nejprve vyslovíme dvě pomocné věty, které následně použijeme k důkazu výsledného tvrzení

První z těchto vět požaduje, aby pro vektory, které nejsou v množině $B := \{x \in \mathbb{Z}^d : ||x|| \leq c\}$ hodnota obecné funkce T v normě ostře klesala. Poté věta zaručí, že pro vektor, který není v množině B, se konečně mnoha iteracemi funkce T na tento vektor dostaneme do množiny B. Nestane se tedy, že by hodnota v normě klesala v doplňku množiny B do nekonečna.

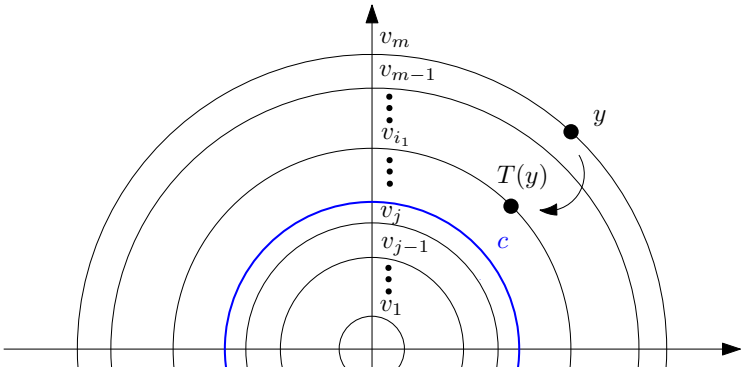
Věta 70. *Nechť* $||.||$ *je norma na* $\mathbb{C}^d$ *z věty* 68*,* T *je libovolná funkce* $\mathbb{Z}^d \to \mathbb{Z}^d$ *a* $c \in \mathbb{R}$ *je kladné číslo. Předpokládejme, že pro všechna* $y \in \mathbb{Z}^d$ *splňující* $||y|| > c$ *platí* $||T(y)|| < ||y||$*. Pak pro každé* $y \in \mathbb{Z}^d$ *existuje* $n \in \mathbb{N}$ *takové, že* $||T^n(y)|| \leq c$*.*

Důkaz. Nechť $y \in \mathbb{Z}^d$ je libovolný vektor. Pokud $||y|| \leq c$, pak můžeme za n zvolit nulu. Uvažujme tedy $||y|| > c$. Z věty 68 pro konstantu $K := ||y||$ plyne, že množina $C := \{x \in \mathbb{Z}^d : ||x|| \leq ||y||\}$ je konečná. Tudíž je konečná i množina $C' = \{||x|| \in \mathbb{Z}^d : x \in C\}$.

Označme $v_1, v_2, \ldots, v_m$ různé prvky množiny C', kde $m \in \mathbb{N}$ je počet prvků C', a požadujme navíc $v_1 < v_2 < \ldots < v_m$. Pak zřejmě $v_m = ||y|| > c$. Označme $j \in \{1, \ldots, m\}$ největší index takový, že $v_j \leq c$.

Po aplikaci funkce T na vektor y dostáváme $v_m = ||y|| > ||T(y)||$ a proto i vektor $T(y)$ patří do množiny C, musí tedy existovat index $i_1 \in \{1, \ldots, m\}$ takový, že $v_{i_1} = ||T(y)||$. Protože $v_m > ||T(y)|| = v_{i_1}$, musí navíc platit $i_1 < m$.

Tento postup můžeme zopakovat pro vektor $T(y)$ a dostaneme index i_2 takový, že $i_2 < i_1 < m$. Protože posloupnost indexů i_k je ostře klesající, musí existovat index $n \in \mathbb{N}$ takový, že $i_n \leq j$. Pak již nutně $||T^n(y)|| = v_{i_n} \leq v_j \leq c$. □



Obrázek 3.1: Znázornění čísel v_j a v_{i_1} na příkladu s euklidovskou normou, tedy pro volbu $P = I$

Následující věta zaručí, že redukční funkce T pro systém $(M, \mathcal{A})$ splňuje předpoklady předchozí věty, a to pro číslo $c = \max_{a\in\mathcal{A}} \frac{||M^{-1}||||a||}{1-||M^{-1}||}$. Připomeňme, že redukční funkce je definovaná pro $x \in \mathbb{Z}^d$ jako $T(x) = M^{-1}(x - a)$, kde $a \in \mathcal{A}$ splňuje $a \equiv_M x$.

Věta 71. *Nechť $(M, \mathcal{A})$ je maticový numerační systém s kompletní abecedou, nechť $||.||$ je norma na prostoru $\mathbb{R}^d$, jejíž indukovaná norma splňuje $||M^{-1}|| < 1$. Označme*

$$\gamma = \max_{a\in\mathcal{A}} \frac{||M^{-1}||||a||}{1 - ||M^{-1}||}.$$

Pak pro všechny $x \in \mathbb{Z}^d$ splňující $||x|| > \gamma$ platí, že $||T(x)|| < ||x||$, kde T je redukční funkcí základního algoritmu.

Důkaz. Nechť $x \in \mathbb{Z}^d$ je vektor splňující $||x|| > \gamma$ a $a \in \mathcal{A}$ takový, že $a \equiv_M x$. Pak s použitím trojúhelníkové nerovnosti a vlastnosti indukované normy dostáváme

$$||T(x)|| = ||M^{-1}(x - a)|| \leq ||M^{-1}||||x - a|| \leq ||M^{-1}||(||x|| + ||a||) \overset{?}{<} ||x||,$$

$$\frac{||M^{-1}||||a||}{1 - ||M^{-1}||} \overset{?}{<} ||x||.$$

Otazníkem jsme označili rovnici, jejíž vlastnost chceme ověřit. Díky tomu, že pro všechna $a \in \mathcal{A}$ platí

$$||x|| > \gamma = \max_{a\in\mathcal{A}} \frac{||M^{-1}||||a||}{1 - ||M^{-1}||} \geq \frac{||M^{-1}||||a||}{1 - ||M^{-1}||},$$

získáváme již platnost rovnice s otazníkem, tudíž i tvrzení věty pro všechna $x \in \mathbb{Z}^d$ splňující $||x|| > \gamma$. □

Dostáváme se nakonec k nejdůležitější větě této kapitole, a to k postačující a nutné podmínce pro to, aby maticový systém reprezentoval množinu $\mathbb{Z}^d$.

Věta 72. *Nechť $(M, \mathcal{A})$ je maticový numerační systém s kompletní abecedou, nechť $||.||$ je norma na prostoru $\mathbb{R}^d$, jejíž indukovaná norma splňuje $||M^{-1}|| < 1$, a buď*

$$\gamma = \max_{a\in\mathcal{A}} \frac{||M^{-1}||||a||}{1 - ||M^{-1}||}. \tag{3.2}$$

Označme

$$B := \{x \in \mathbb{Z}^d : ||x|| \leq \gamma\}. \tag{3.3}$$

Pak každé $x \in \mathbb{Z}^d$ má $(M, \mathcal{A})$-reprezentaci právě tehdy, když každé $x \in B$ má $(M, \mathcal{A})$-reprezentaci.

Důkaz. Implikace zleva doprava je zřejmá, dokazujme tedy opačný směr.

Nechť $x \in \mathbb{Z}^d$ je libovolný vektor a T je redukční funkce. Pokud $x \in B$, pak z předpokladu má reprezentaci, uvažujme tedy vektor $x \notin B$, tedy, že x splňuje $||x|| > \gamma$. Pak z věty 71 plyne, že redukční funkce T pro číslo γ splňuje předpoklady věty 70. Tato věta pak zaručuje existenci $n \in \mathbb{N}$ takového, že platí $T^n(x) \in B$. Tudíž vektor $T^n(x)$ má z předpokladu $(M, \mathcal{A})$-reprezentaci, označme ji $e_m \dots e_0$.

Označme postupně $a_1, \dots, a_n \in \mathcal{A}$ vektory splňující $a_i \equiv_M T^{i-1}(x)$ pro $i \in \{1, \dots, n\}$, jsou to vektory z postupných iterací redukční funkce pro vektor x. Z poznámky 64 plyne, že vektor $T^{n-1}(x)$ má podobnou reprezentaci jako $T^n(x)$, pouze s vektorem a_n přidaným na poslední pozici, tudíž reprezentace $T^{n-1}(x)$ je rovna $e_m \dots e_1 a_n$. Takto postupně můžeme pokračovat, až dostaneme $(M, \mathcal{A})$-reprezentaci vektoru x rovnu $e_m \dots e_1 a_1 \dots a_n$. □

Kapitola 4

Testování maticových systémů

Implementujeme program, který rozhodne pomocí věty 72, zda maticový systém reprezentuje celou množinu $\mathbb{Z}^d$. Pro účely této práce se omezíme pouze na diagonalizovatelné matice.

Program je vytvořen v programovacím jazyku SageMath [11], jeho zdrojový kód s pokyny na instalaci a spuštění lze nalézt v [4]. Poznamenejme, že pro nalezení spektra je použita funkce `M.eigenvalues()`, pro Jordanův rozklad funkce `M.jordan_form(transformation=True)` a pro Choleského rozklad funkce `M.cholesky()`. Ve všech případech `M` je matice s prvky z množiny `QQbar`, která představuje množinu všech algebraických čísel, respektive u Choleského rozkladu s prvky z množiny `RDF`, které představuje množinu reálných čísel.

Uveďme nejprve potřebnou teorii k implementaci algoritmu.

Uvažujme numerační systém $(M, \mathcal{A})$ s kompletní abecedou a diagonalizovatelnou bází. Při využití normy z tvrzení 58 pro matici M^{-1}, která splňuje $||M^{-1}|| = \varrho(M^{-1})$, má číslo γ z věty 72 tvar

$$\gamma = \max_{a \in \mathcal{A}} \frac{\varrho(M^{-1})||a||}{1 - \varrho(M^{-1})}.$$

Věta 72 následně tvrdí, že stačí zkontrolovat pouze reprezentaci vektorů z množiny $B := \{x \in \mathbb{Z}^d : ||Px||_e \leq \gamma\}$, aby systém $(M, \mathcal{A})$ s kompletní abecedou reprezentoval celou množinu $\mathbb{Z}^d$.

Procházení všech vektorů z množiny B ulehčí poznámka 69. Ta tvrdí, že existuje $\alpha \in \mathbb{R}$ takové, že $B \subset [-\alpha, \alpha]^d$. Budeme procházet všechny vektory z krychle $[-\alpha, \alpha]^d$ a o jednotlivých vektorech rozhodovat, zda patří či nepatří do množiny B. Při kladné odpovědi se pokusíme ověřit, zda má reprezentaci v $(M, \mathcal{A})$.

4.1 Kroky programu

Dostáváme se k implementaci programu. Vstupem je numerační systém $(M, \mathcal{A})$ s diagonalizovatelnou maticí M a výstupem je odpověď, zda $(M, \mathcal{A})$ reprezentuje celou množinu $\mathbb{Z}^d$.

Zde jsou kroky programu:

1. Zkontrolujeme, zda všechna vlastní čísla matice M jsou v absolutní hodnotě větší než 1.
2. Testujeme, zda abeceda $\mathcal{A}$ je kompletní abecedou, k tomu stačí následující dva body:
   - spočítáme, zda počet vektorů v abecedě $\mathcal{A}$ odpovídá číslu $|\det M|$,
   - pokud předchozí bod je splněn, zkontrolujeme, zda každá dvojice vektorů není v relaci modulo M.

3. Nalezneme matici P takovou, že platí rovnost $M^{-1} = P^{-1}DP$, kde D je diagonální matice
4. Definujeme funkci $N : \mathbb{Z}^d \to \mathbb{R}$, která odpovídá zobrazení $x \mapsto ||Px||_e$-
5. Vypočítáme číslo $\varrho(M^{-1})$, jedná se jednoduše o maximum z absolutních hodnot vlastních čísel matice M^{-1}.
6. Vypočítáme číslo $\gamma = \max_{a \in \mathcal{A}} \frac{\varrho(M^{-1})N(d)}{1-\varrho(M^{-1})}$.
7. Najdeme číslo α dle poznámky 69, tedy $\alpha := \gamma \max_{i \in \{1,\dots,d\}} \sum_{j=1}^{d} |(R^{-1})_{ij}|$, kde vznik matice R je popsán taktéž v poznámce 69.
8. Zkontrolujeme, zda všechny vektory z množiny $B := \{x : N(x) \leq \gamma\}$ mají reprezentaci, a to tak, že
   - procházíme všechny vektory z krychle $[-\alpha, \alpha]^d$,
   - pokud iterovaný vektor patří do množiny B, ověříme, jestli má reprezentaci.

Pokud na body 1., 2. a 8. dostaneme kladnou odpověď, jedná se o systém reprezentující celou množinu $\mathbb{Z}^d$.

Bod číslo 8 postupu programu shrneme v algoritmu. Ten používá pro kontrolu, zda má vektor reprezentaci upravený rozšířený algoritmus. Pro urychlení běhu programu jsme ještě navíc přidali pole, které obsahuje vektory, u kterých jsme již dříve zjistili, že mají reprezentaci. Do tohoto pole nahlížíme při dalších iteracích, abychom již reprezentované vektory nemuseli zpracovávat znovu.

Úplný algoritmus: Určení, zda množina B je reprezentovaná v $(M, \mathcal{A})$

vstup : $(M, \mathcal{A})$ s M expanzivní, diagonalizovatelnou, funkce $N(x) = ||Px||_e$, číslo γ, číslo α

výstup: Odpověď, zda množina B je reprezentovaná v $(M, \mathcal{A})$

```
1  reprezentovatelné_vektory := prázdné pole vektorů ze Z^d
2  navštívené_vektory:=prázdné pole vektorů ze Z^d
3  for x ∈ [−α, α]^d do
4      if N(x) ≤ γ then
5          while x ≠ 0 do
6              if x ∈ navštívené_vektory then
7                  return false
8              end
9              if x ∈ reprezentovatelné_vektory then
10                 pokračuj na řádek 15
11             end
12             vlož x do navštívené_vektory
13             x := T(x)
14         end
15         vlož vektory z pole navštívené_vektory do pole reprezentovatelné_vektory
16         vyprázdni pole navštívené_vektory
17     end
18 end
19 return true
```

4.2 Penneyho systém

V této části ukážeme běh programu na Penneyho systému v maticové formě. Mějme systém s maticí $M = \begin{pmatrix} -1 & -1 \\ 1 & -1 \end{pmatrix}$ a abecedou $\mathcal{A} = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}$ a rozhodneme, zda, tvoří systém reprezentující $\mathbb{Z}^2$.

1. Expanzivnost: $\sigma(M) = \{-1 - \mathrm{i}, -1 + \mathrm{i}\}$. Obě vlastní čísla jsou v absolutní hodnotě rovna $\sqrt{2}$.

2. Kompletní abeceda:

   - rovnost je splněna: $\#\mathcal{A} = 2 = |\det M|$,
   - $\begin{pmatrix} 0 \\ 0 \end{pmatrix} \not\equiv_M \begin{pmatrix} 1 \\ 0 \end{pmatrix} \Leftrightarrow M^{-1}\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 0 \end{pmatrix}\right) \notin \mathbb{Z}^2 \Leftrightarrow \frac{1}{2}\begin{pmatrix} -1 & -1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} -1 \\ 1 \end{pmatrix} \notin \mathbb{Z}^2$.

3. Matice Q, která obsahuje vlastní vektory příslušné všem vlastním číslům, splňuje $M^{-1} = QDQ^{-1}$, kde D je diagonální matice. Pro matici P platí, že $P = Q^{-1}$. První vlastní číslo matice M^{-1} je rovno $\frac{-1+\mathrm{i}}{2}$ a příslušný vlastní vektor je roven $\begin{pmatrix} 1 \\ -\mathrm{i} \end{pmatrix}$, druhé vlastní číslo a

vlastní vektor jsou rovny $\frac{-1-\mathrm{i}}{2}$ a $\begin{pmatrix}1\\ \mathrm{i}\end{pmatrix}$. Matice P je tedy rovna

$$P = \begin{pmatrix}1 & 1\\ \mathrm{i} & -\mathrm{i}\end{pmatrix}^{-1} = \frac{1}{2}\begin{pmatrix}1 & -\mathrm{i}\\ 1 & \mathrm{i}\end{pmatrix}.$$

4. Zobrazení $N(x) = ||Px||_e$ má tvar

$$N\left(\begin{pmatrix}x_1\\ x_2\end{pmatrix}\right) = \left|\left|P\begin{pmatrix}x_1\\ x_2\end{pmatrix}\right|\right|_e = \frac{1}{2}\left|\left|\begin{pmatrix}x_1 - \mathrm{i}x_2\\ x_1 + \mathrm{i}x_2\end{pmatrix}\right|\right|_e = \frac{1}{2}\sqrt{x_1^2 + x_2^2 + x_1^2 + x_2^2} =$$
$$= \frac{\sqrt{2}}{2}\sqrt{x_1^2 + x_2^2} = \frac{1}{\sqrt{2}}\left|\left|\begin{pmatrix}x_1\\ x_2\end{pmatrix}\right|\right|_e.$$

5. Pro číslo $\varrho(M^{-1})$ platí $\varrho(M^{-1}) = \max\{|\frac{-1+\mathrm{i}}{2}|, |\frac{-1-\mathrm{i}}{2}|\} = \frac{1}{\sqrt{2}}$.

6. Pro číslo γ platí $\gamma = \max\{0, \frac{\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}}{1-\frac{1}{\sqrt{2}}}\} = \frac{1}{2-\sqrt{2}}$.

7. Nyní provedeme konstrukci čísla α. Nejprve najdeme matici A, B a poté provedeme Choleského rozklad pro matici $A^TA + B^TB$.

$$P = \begin{pmatrix}\frac{1}{2} & -\frac{1}{2}\mathrm{i}\\ \frac{1}{2} & \frac{1}{2}\mathrm{i}\end{pmatrix} = \begin{pmatrix}\frac{1}{2} & 0\\ \frac{1}{2} & 0\end{pmatrix} + \mathrm{i}\begin{pmatrix}0 & -\frac{1}{2}\\ 0 & \frac{1}{2}\end{pmatrix} = A + \mathrm{i}B$$

$$A^TA + B^TB = \begin{pmatrix}\frac{1}{2} & \frac{1}{2}\\ 0 & 0\end{pmatrix}\begin{pmatrix}\frac{1}{2} & 0\\ \frac{1}{2} & 0\end{pmatrix} + \begin{pmatrix}0 & 0\\ -\frac{1}{2} & \frac{1}{2}\end{pmatrix}\begin{pmatrix}0 & -\frac{1}{2}\\ 0 & \frac{1}{2}\end{pmatrix} = \begin{pmatrix}\frac{1}{2} & 0\\ 0 & \frac{1}{2}\end{pmatrix} =$$
$$= \begin{pmatrix}\frac{1}{\sqrt{2}} & 0\\ 0 & \frac{1}{\sqrt{2}}\end{pmatrix}^T\begin{pmatrix}\frac{1}{\sqrt{2}} & 0\\ 0 & \frac{1}{\sqrt{2}}\end{pmatrix} = R^TR \implies R^{-1} = \begin{pmatrix}\sqrt{2} & 0\\ 0 & \sqrt{2}\end{pmatrix}.$$

$\alpha = \gamma \max_{i\in\{1,\dots,d\}} \sum_{j=1}^{d} |(R^{-1})_{ij}| = \frac{1}{2-\sqrt{2}}\sqrt{2} = \frac{\sqrt{2}}{2-\sqrt{2}} = 1 + \sqrt{2} \approx 2.414$.

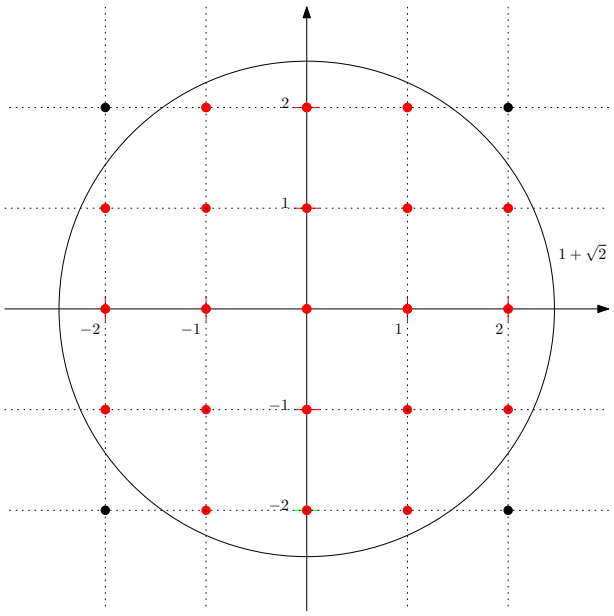
8. Celočíselné vektory patřící do množiny $[-\alpha, \alpha]^d$ jsou tyto:

$$\begin{pmatrix}-2\\ -2\end{pmatrix}, \begin{pmatrix}-2\\ -1\end{pmatrix}, \begin{pmatrix}-2\\ 0\end{pmatrix}, \begin{pmatrix}-2\\ 1\end{pmatrix}, \begin{pmatrix}-2\\ 2\end{pmatrix}, \begin{pmatrix}-1\\ -2\end{pmatrix}, \begin{pmatrix}-1\\ -1\end{pmatrix}, \begin{pmatrix}-1\\ 0\end{pmatrix}\begin{pmatrix}-1\\ 1\end{pmatrix}, \begin{pmatrix}-1\\ 2\end{pmatrix},$$
$$\begin{pmatrix}0\\ -2\end{pmatrix}, \begin{pmatrix}0\\ -1\end{pmatrix}, \begin{pmatrix}0\\ 0\end{pmatrix}, \begin{pmatrix}0\\ 1\end{pmatrix}, \begin{pmatrix}0\\ 2\end{pmatrix}, \begin{pmatrix}1\\ -2\end{pmatrix}, \begin{pmatrix}1\\ -1\end{pmatrix}, \begin{pmatrix}1\\ 0\end{pmatrix}, \begin{pmatrix}1\\ 1\end{pmatrix}, \begin{pmatrix}1\\ 2\end{pmatrix},$$
$$\begin{pmatrix}2\\ -2\end{pmatrix}, \begin{pmatrix}2\\ -1\end{pmatrix}, \begin{pmatrix}2\\ 0\end{pmatrix}, \begin{pmatrix}2\\ 1\end{pmatrix}, \begin{pmatrix}2\\ 2\end{pmatrix}.$$

Podmínku $N(x) \le \gamma$ můžeme přepsat do tvaru

$$N(x) = \frac{1}{\sqrt{2}}||x||_e \le \gamma = \frac{1}{2-\sqrt{2}},$$
$$||x||_e \le \frac{\sqrt{2}}{2-\sqrt{2}} = 1 + \sqrt{2},$$

tudíž vektory, aby patřily do množiny B, musí ležet v kružnici o poloměru $1 + \sqrt{2}$. Znázornění najdeme na obrázku 4.1. Zřejmě $\#B = 21$.



Obrázek 4.1: Červenou barvou jsou označeny vektory patřící do B

Po spuštění úplného algoritmu zjistíme, že v pořádku doběhl a tudíž všechny vektory z B mají reprezentaci. Pro ukázku uvedeme vektory, které program postupně zpracovává. Červeně jsou označeny vektory, u kterých jsme v jedné z předchozích iterací ověřili, že mají reprezentaci, tedy, že jsme je nalezli v poli reprezentovatelné_vektory.

- $\begin{pmatrix}-1\\-2\end{pmatrix} \to \begin{pmatrix}0\\2\end{pmatrix} \to \begin{pmatrix}1\\-1\end{pmatrix} \to \begin{pmatrix}-1\\0\end{pmatrix} \to \begin{pmatrix}1\\1\end{pmatrix} \to \begin{pmatrix}0\\-1\end{pmatrix} \to \begin{pmatrix}0\\1\end{pmatrix} \to \begin{pmatrix}1\\0\end{pmatrix} \to \begin{pmatrix}0\\0\end{pmatrix}$,
- $\begin{pmatrix}0\\-2\end{pmatrix} \to \begin{pmatrix}-1\\1\end{pmatrix} \to \begin{pmatrix}1\\0\end{pmatrix}$,
- $\begin{pmatrix}1\\-2\end{pmatrix} \to \begin{pmatrix}-1\\1\end{pmatrix}$,
- $\begin{pmatrix}-2\\-1\end{pmatrix} \to \begin{pmatrix}1\\2\end{pmatrix} \to \begin{pmatrix}1\\-1\end{pmatrix}$,
- $\begin{pmatrix}-1\\-1\end{pmatrix} \to \begin{pmatrix}0\\1\end{pmatrix}$,
- $\begin{pmatrix}0\\-1\end{pmatrix}$,
- $\begin{pmatrix}1\\-1\end{pmatrix}$,
- $\begin{pmatrix}2\\-1\end{pmatrix} \to \begin{pmatrix}-1\\0\end{pmatrix}$,

- $\begin{pmatrix}-2\\0\end{pmatrix} \to \begin{pmatrix}1\\1\end{pmatrix}$,
- $\begin{pmatrix}-1\\0\end{pmatrix}$,
- $\begin{pmatrix}0\\0\end{pmatrix}$,
- $\begin{pmatrix}1\\0\end{pmatrix}$,
- $\begin{pmatrix}2\\0\end{pmatrix} \to \begin{pmatrix}-1\\-1\end{pmatrix}$,
- $\begin{pmatrix}-2\\1\end{pmatrix} \to \begin{pmatrix}2\\1\end{pmatrix} \to \begin{pmatrix}0\\-1\end{pmatrix}$,
- $\begin{pmatrix}-1\\1\end{pmatrix}$,
- $\begin{pmatrix}0\\1\end{pmatrix}$,
- $\begin{pmatrix}1\\1\end{pmatrix}$,
- $\begin{pmatrix}2\\1\end{pmatrix}$,
- $\begin{pmatrix}-1\\2\end{pmatrix} \to \begin{pmatrix}2\\0\end{pmatrix}$,
- $\begin{pmatrix}0\\2\end{pmatrix}$,
- $\begin{pmatrix}1\\2\end{pmatrix}$.

4.3 Modifikace Penneyho systému

Nyní ukážeme běh programu na příkladu $M = \begin{pmatrix}1 & -1\\1 & 1\end{pmatrix}$ a abecedě $\mathcal{A} = \left\{\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}\right\}$, který získáme definováním izomorfismu mezi $\mathbb{Z}[\mathrm{i}]$ a $\mathbb{Z}^2$, a bude odpovídat systému $\beta = \mathrm{i}+1$ s abecedou $\mathcal{A} = \{0, 1\}$. O tomto pozičním systému jsme dříve zjistili, že nereprezentuje $\mathbb{Z}[\mathrm{i}]$.

1. Expanzivnost: $\sigma(M) = \{1-\mathrm{i}, 1+\mathrm{i}\}$. Obě vlastní čísla jsou znovu v absolutní hodnotě rovna $\sqrt{2}$.

2. Kompletní abeceda:

   - rovnost je splněna: $\#\mathcal{A} = 2 = |\det M|$,
   - $\begin{pmatrix}0\\0\end{pmatrix} \not\equiv_M \begin{pmatrix}1\\0\end{pmatrix} \Leftrightarrow M^{-1}\left(\begin{pmatrix}1\\0\end{pmatrix} - \begin{pmatrix}0\\0\end{pmatrix}\right) \notin \mathbb{Z}^2 \Leftrightarrow \frac{1}{2}\begin{pmatrix}1 & 1\\-1 & 1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1\\-1\end{pmatrix} \notin \mathbb{Z}^2$.

3. Stejně jako v předchozím případě určíme vlastní čísla a vlastní vektory matice M^{-1} a pak i matice Q a P. První vlastní číslo matice M^{-1} je rovno $\frac{1+\mathrm{i}}{2}$ a příslušný vlastní vektor je

roven $\begin{pmatrix}1\\ \mathrm{i}\end{pmatrix}$, druhé vlastní číslo a vlastní vektor jsou rovny $\frac{1-\mathrm{i}}{2}$ a $\begin{pmatrix}1\\ -\mathrm{i}\end{pmatrix}$. Matice P je tedy stejná jako v předchozím příkladě a je rovna $P = \begin{pmatrix}1 & 1\\ \mathrm{i} & -\mathrm{i}\end{pmatrix}^{-1} = \frac{1}{2}\begin{pmatrix}1 & -\mathrm{i}\\ 1 & \mathrm{i}\end{pmatrix}$.

4. Zobrazení $N(x) = ||Px||_e$ je, díky identické matici P, stejné jako v předchozím příkladě, tedy $N\left(\begin{pmatrix}x_1\\ x_2\end{pmatrix}\right) = \frac{1}{\sqrt{2}}\left|\left|\begin{pmatrix}x_1\\ x_2\end{pmatrix}\right|\right|_e$.

5. Číslo $\varrho(M^{-1})$ je rovno $\varrho(M^{-1}) = \max\{|\frac{1-\mathrm{i}}{2}|, |\frac{1+\mathrm{i}}{2}|\} = \frac{1}{\sqrt{2}}$.

6. Číslo γ je rovno $\gamma = \max_{a\in\mathcal{A}} \frac{\varrho(M^{-1})N(d)}{1-\varrho(M^{-1})} = \max\{0, \frac{\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}}{1-\frac{1}{\sqrt{2}}}\} = \frac{1}{2-\sqrt{2}}$.

7. Díky identické matici P vychází i číslo α stejně, tedy $\alpha = 1+\sqrt{2}$.

8. Vektory patřící do množiny $[-\alpha, \alpha]^d$ jsou stejné i množina B zůstala totožná, musíme tedy ověřit reprezentaci vektorů, které leží v kružnici o poloměru $1+\sqrt{2}$.

Po spuštění úplného algoritmu zjistíme, že odpověď je false. Po přezkoumání testovaných vektorů vidíme, že u pátého vektoru algoritmus najde testovaný vektor v poli navštívené_vektory, a tudíž se jedná o vektor, který nemá reprezentaci. Vypišme si chod algoritmu:

- $\begin{pmatrix}-1\\ -2\end{pmatrix} \to \begin{pmatrix}0\\ -2\end{pmatrix} \to \begin{pmatrix}1\\ -1\end{pmatrix} \to \begin{pmatrix}1\\ 0\end{pmatrix} \to \begin{pmatrix}0\\ 0\end{pmatrix}$,
- $\begin{pmatrix}0\\ -2\end{pmatrix}$,
- $\begin{pmatrix}1\\ -2\end{pmatrix} \to \begin{pmatrix}1\\ -1\end{pmatrix}$,
- $\begin{pmatrix}-2\\ -1\end{pmatrix} \to \begin{pmatrix}-1\\ -2\end{pmatrix}$,
- $\begin{pmatrix}-1\\ -1\end{pmatrix} \to \begin{pmatrix}0\\ -1\end{pmatrix} \to \begin{pmatrix}0\\ -1\end{pmatrix}$.

Vektor vyznačený červenou barvou patří do tzv. cyklu 1.řádu.

Definice 73. *Nechť $n \in \mathbb{N}\setminus\{0\}$. Podmnožinu $C \subset \mathbb{Z}^d$, $0 \notin C$ nazveme cyklem n-tého řádu maticového systému $(M, \mathcal{A})$, pokud $\#C = n$ a existuje $x \in C$ takové, že $T^n(x) = x$ a $C = \{x, T(x), \ldots, T^{n-1}(x)\}$.*

Neuvažujeme cyklus obsahující nulový vektor, protože tento cyklus by obsahoval pouze nulový vektor a byl by tedy nezajímavý.

Cyklus je vlastně množina vektorů, při kterých se algoritmus zacyklí, a tudíž podle věty 62 jsou to ty vektory, které nemají v $(M, \mathcal{A})$ reprezentaci.

Následující věta tvrdí, že neexistuje cyklus, který by měl neprázdný průnik s množinou B, tedy, že bude stačit prozkoumat vektory z množiny B k tomu, abychom našli všechny cykly.

Věta 74. *Nechť $(M, \mathcal{A})$ je maticový numerační systém s kompletní abecedou a označme B množinu (3.3). Pak neexistuje cyklus, který by splňoval $C \subset \mathbb{Z}^d \setminus B$, tzn. každý cyklus C obsahuje vektor $x \in C$ takový, že $x \in B$.*

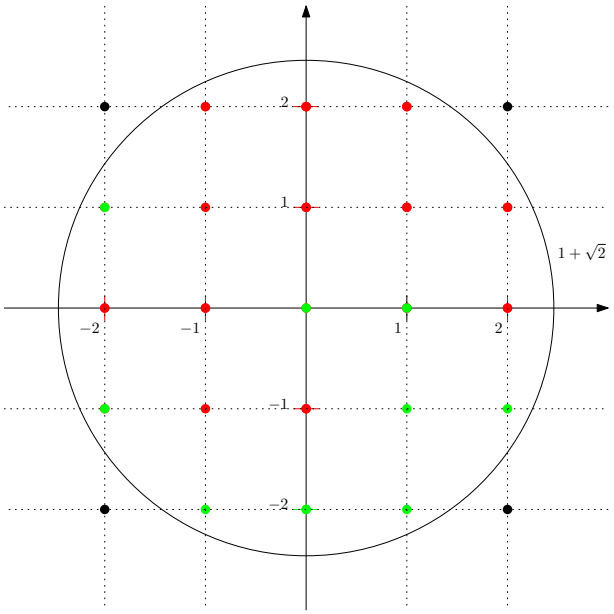
Důkaz. Důkaz provedeme sporem. Nechť existuje $n \in \mathbb{N}\setminus\{0\}$ takové, že $\#C = n$ a existuje $x \in C$ takový, že $T^n(x) = x$ a $C = \{x, T(x), \ldots, T^{n-1}(x)\}$, a současně pro všechna $y \in C$ platí $y \notin B$. Tudíž pro $m \in \{0, 1, \ldots, n-1\}$ platí $T^m(x) \notin B$.

Z věty 71 plyne, že pro vektory splňující $y \notin B$ platí $||T(y)|| < ||y||$. V našem případě pro vektory $x, T(x), \ldots, T^{n-1}(x)$, které neleží v množině B, máme $||x|| > ||T(x)|| > \ldots > ||T^{n-1}(x)|| > ||T^n(x)|| = ||x||$, což je spor. □

Pokud upravíme úplný algoritmus tak, aby neskončil u vektoru, který nemá reprezentaci, a prozkoumal všechny vektory z množiny B a přitom si zapisoval cykly, budeme schopni najít všechny cykly maticového systému.

Pokud tento upravený algoritmus použijeme na právě zkoumaný systém, zjistíme, že $C = \left\{\begin{pmatrix} 0 \\ -1 \end{pmatrix}\right\}$ je jediný cyklus.

Pro zajímavost ukážeme na obrázku vektory z množiny B, které nemají reprezentaci kvůli existujícímu cyklu.



Obrázek 4.2: Zeleně jsou označeny vektory, které mají $(M, \mathcal{A})$-reprezentaci, červeně ty, které reprezentaci nemají.

Představme kritérium, které rozhoduje o existenci cyklu řádu 1.

Věta 75. *Nechť $(M, \mathcal{A})$ je maticový numerační systém. Pokud $\det(I - M) = \pm 1$, pak tento maticový systém má cyklus řádu 1.*

Důkaz. Neuvažujeme systémy, které by měly v abecedě pouze nulový vektor, proto existuje $a \in \mathcal{A}$ takový, že $a \neq 0$. Dívejme se nyní na soustavu lineární rovnic $(I-M)x = a$. Z Cramerova pravidla pro řešení soustavy lineárních rovnic plyne, že

$$x_i = \frac{\det((I-M)^{(i)})}{\det(I-M)},$$

kde $(I-M)^{(i)}$ značí matici $I-M$, ve které je i-tý sloupec nahrazen vektorem a. Protože $\det(I-M) = \pm 1$, složky řešení jsou celočíselné. Z rovnice $(I-M)x = a$ také plyne, že $M^{-1}(x-a) = x$

a tedy $x \equiv_M a$. Pro redukční funkci pak platí $T(x) = M^{-1}(x-a) = x$ a tedy cyklus řádu jedna má tvar $C = \{x\}$. □

Příklad 76. *Větu* 75 *můžeme použít na systém* $M = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ *a* $\mathcal{A} = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}$. *Skutečně platí, že* $\det(I-M) = \det \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = 1$, *a tedy tento systém má cyklus* 1. *řádu, jak již jsme dříve zjistili.*

Na následujícím příkladě zjistíme, že podmínka $\det(I-M) = \pm 1$ není podmínkou postačující pro existenci cyklu řádu 1.

Příklad 77. *Pro maticový systém ve tvaru* $M = \begin{pmatrix} 0 & 0 & -2 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ *a abecedu* $\mathcal{A} = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \right\}$ *platí, že* $\det(I-M) = 2$. *Ale pro vektor* $y := \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix}$ *platí* $T(y) = y$ *a tudíž jsme našli cyklus* 1. *řádu přestože nejsou splněny předpoklady věty 75.*

Pokud bychom zkoumali řešení rovnice $(I-M)x = d$ *podle Cramerova pravidla, kde řešení má tvar* $x_i = \frac{\det((I-M)^{(i)})}{\det(I-M)}$, *dostáváme pro determinanty* $\det((I-M)^{(1)}) = -2, \det((I-M)^{(2)}) = 2$ *a* $\det((I-M)^{(3)}) = 2$. *Tudíž pro všechny indexy se dvojka ve jmenovateli zkrátila s cifrou v čitateli. Proto dostáváme celočíselné řešení této rovnice.*

4.4 Poziční systém jakožto maticový systém v $\mathbb{Z}^1$

Systém reprezentující podmnožiny $\mathbb{Z}$ s celočíselnou bází β a celočíselnými ciframi v abecedě $\mathcal{A} \subset \mathbb{Z}$ můžeme považovat za maticový systém reprezentující podmnožinu $\mathbb{Z}^d$ pro $d = 1$ a použít na něj příslušný aparát.

Uveďme tento postup pro poziční systém $\beta = -2$ a $\mathcal{A} = \{0, 1\}$. Mějme maticový systém ve tvaru $M = (-2)$ a $\mathcal{A} = \{0, 1\}$ a spusťme program.

1. Expanzivnost: $\sigma(M) = \{-2\}$.
2. Kompletní abeceda:
   - rovnost je splněna: $\#\mathcal{A} = 2 = |\det M|$,
   - $0 \not\equiv_M 1 \Leftrightarrow M^{-1}(1-0) \notin \mathbb{Z} \Leftrightarrow \frac{1}{-2} \notin \mathbb{Z}^2$.
3. Vlastní číslo matice M^{-1} je rovno $-\frac{1}{2}$ a vlastní vektor roven 1. Tudíž matice P má tvar $P = (1)$.
4. Pro zobrazení N platí $N(x) = x$.
5. Číslo $\varrho(M^{-1})$ je rovno $\varrho(M^{-1}) = \frac{1}{2}$.
6. Číslo γ je rovno $\gamma = \max_{a \in \mathcal{A}} \frac{\varrho(M^{-1})N(d)}{1-\varrho(M^{-1})} = \max\{0, \frac{\frac{1}{2} \cdot 1}{1-\frac{1}{2}}\} = 1$.
7. Číslo α je rovno $\alpha = 1$.

8. Čísla, u kterých musíme ověřit existenci reprezentace, patří do množiny $\{-1,0,1\}$. Pro číslo -1 platí $-1 = 1\cdot(-2)^1+1\cdot(-2)^0$. Tudíž zřejmě všechna čísla z $\{-1,0,1\}$ mají reprezentaci a se jedná tedy o systém reprezentující množinu $\mathbb{Z}$.

4.5 Další maticové systémy

Nyní otestujeme numerační systémy, které lze najít v [7]. Výsledky programu implementovaného v této práci se shodují s již publikovanými závěry v [7], v některých případech jsou výsledky této práce rozšířením původních, a to díky otestování různých abeced.

Pokud báze M je expanzivní, uvedeme také počet prvků množiny B a případný počet cyklů.

1. Eisensteinův systém v maticovém tvaru: $M = \begin{pmatrix} -1 & -1 \\ 1 & -2 \end{pmatrix}, \mathcal{A} = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \end{pmatrix} \right\}$, $\#B = 31$. Tento systém reprezentuje množinu $\mathbb{Z}^2$.

2. Eisensteinův systém se symetrickou abecedou: $M = \begin{pmatrix} -1 & -1 \\ 1 & -2 \end{pmatrix}$, $\mathcal{A} = \left\{ \begin{pmatrix} -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}, \#B = 7$. Tento systém nereprezentuje množinu $\mathbb{Z}^2$ a množina všech cyklů je rovna $C_1 = \left\{ \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ -1 \end{pmatrix} \right\} \right\}$.

3. Maticový systém s maticí $M = \begin{pmatrix} 0 & 0 & -2 \\ 1 & 0 & -a \\ 0 & 1 & 0 \end{pmatrix}$, kde $a \in \{-1,0,1\}$ a různé abecedy:

   (a) pro $a = 1$ není matice expanzivní,

   (b) pro $a = 0$:

      i. s abecedou $\mathcal{A} = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\}, \#B = 117$, tvoří systém reprezentující $\mathbb{Z}^3$,

      ii. s abecedou $\mathcal{A} = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \right\}, \#B = 491$, tvoří systém reprezentující $\mathbb{Z}^3$,

      iii. abeceda s nulovým vektorem a dalším vektorem z množiny $\left\{ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} \right\}$ není možná, protože by byly v relaci modulo M,

      iv. s abecedou $\mathcal{A} = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \right\}, \#B = 491$, nereprezentuje množinu $\mathbb{Z}^3$, celkem obsahuje 3 cykly,

      v. s abecedou $\mathcal{A} = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \right\}, \#B = 801$, nereprezentuje množinu $\mathbb{Z}^3$, celkem obsahuje 1 cyklus,

vi. s abecedou $\mathcal{A} = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \right\}$, $\#B = 801$, nereprezentuje množinu $\mathbb{Z}^3$, celkem obsahuje 3 cykly,

vii. s abecedou $\mathcal{A} = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix} \right\}$, $\#B = 1371$, nereprezentuje množinu $\mathbb{Z}^3$, celkem obsahuje 2 cykly,

viii. s abecedou $\mathcal{A} = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\}$, $\#B = 1371$, nereprezentuje množinu $\mathbb{Z}^3$, celkem obsahuje 5 cyklů.

(c) pro $a = 1$:

i. s abecedou $\mathcal{A} = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\}$, $\#B = 841$, tvoří systém reprezentující $\mathbb{Z}^3$,

ii. abeceda s nulovým vektorem a dalším vektorem z množiny $\left\{ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} \right\}$ není možná, protože by byly v relaci modulo M,

iii. s abecedou $\mathcal{A} = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \right\}$, $\#B = 5305$, nereprezentuje množinu $\mathbb{Z}^3$, celkem obsahuje 1 cyklus,

iv. s abecedou $\mathcal{A} = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\}$, $\#B = 14881$, nereprezentuje množinu $\mathbb{Z}^3$, celkem obsahuje 4 cykly,

v. s abecedou $\mathcal{A} = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \right\}$, $\#B = 5481$, nereprezentuje množinu $\mathbb{Z}^3$, celkem obsahuje 5 cyklů,

vi. s abecedou $\mathcal{A} = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \right\}$, $\#B = 4123$, nereprezentuje množinu $\mathbb{Z}^3$, celkem obsahuje 3 cykly,

vii. s abecedou $\mathcal{A} = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \right\}$, $\#B = 1525$, nereprezentuje množinu $\mathbb{Z}^3$, celkem obsahuje 1 cyklus,

viii. s abecedou $\mathcal{A} = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix} \right\}$, $\#B = 7799$, nereprezentuje množinu $\mathbb{Z}^3$, celkem obsahuje 1 cyklus.

(d) pro matici ve tvaru $\begin{pmatrix} 0 & 0 & 0 & -b \\ 1 & 0 & 0 & -a \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ a abecedu $\mathcal{A} = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} |b|-1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right\}$,
kde $a, b \in \mathbb{Z}$:

i. pro volbu $b = 2, a \in \{-100, \ldots, 100\} \setminus \{-1, 0, 1\}$ platí, že M není expanzivní,
ii. pro volbu $b = 2, a = 1$: $\#B = 93081$, platí, že nereprezentuje $\mathbb{Z}^4$ a má 1 cyklus,
iii. pro volbu $b = 2, a = 0$: $\#B = 1355$, platí, že reprezentuje $\mathbb{Z}^4$,
iv. pro volbu $b = 2, a = -1$: $\#B = 93081$, platí, že reprezentuje $\mathbb{Z}^4$,
v. pro volbu $b = -2, a \in \{-100, \ldots, 100\} \setminus \{0\}$ není matice M expanzivní,
vi. pro volbu $b = -2, a = 0$: $\#B = 1535$, platí, že nereprezentuje $\mathbb{Z}^4$ a má 5 cyklů,
vii. pro volbu $b = 3, a \in \{-100, \ldots, 100\} \setminus \{-3, \ldots, 3\}$ není matice M expanzivní,
viii. pro volbu $b = 3, a = 2$: $\#B = 111717$, platí, že nereprezentuje $\mathbb{Z}^4$ a má 1 cyklus,
ix. pro volbu $b = 3, a = 1$: $\#B = 8261$, platí, že reprezentuje $\mathbb{Z}^4$,
x. pro volbu $b = 3, a = 0$: $\#B = 1539$, platí, že reprezentuje $\mathbb{Z}^4$,
xi. pro volbu $b = 3, a = -1$: $\#B = 8261$, platí, že reprezentuje $\mathbb{Z}^4$,
xii. pro volbu $b = 3, a = -2$: $\#B = 111717$, platí, že nereprezentuje $\mathbb{Z}^4$ a má 1 cyklus,
xiii. pro volbu $b = -3, a \in \{-100, \ldots, 100\} \setminus \{-1, 0, 1\}$ není matice M expanzivní,
xiv. pro volbu $b = -3, a = 1$: $\#B = 26059$, platí, že nereprezentuje $\mathbb{Z}^4$ a má 2 cykly,
xv. pro volbu $b = -3, a = 0$: $\#B = 1539$, platí, že nereprezentuje $\mathbb{Z}^4$ a má 5 cyklů,
xvi. pro volbu $b = -3, a = -1$: $\#B = 26059$, platí, že nereprezentuje $\mathbb{Z}^4$ a má 2 cykly,
xviii. pro volbu $b = 4, a = 0$: $\#B = 1719$, platí, že reprezentuje $\mathbb{Z}^4$,
xix. pro volbu $b = 5, a = 0$: $\#B = 1885$, platí, že reprezentuje $\mathbb{Z}^4$,
xx. pro volbu $b = 6, a = 0$: $\#B = 2037$, platí, že reprezentuje $\mathbb{Z}^4$,
xxi. pro volbu $b = 7, a = 0$: $\#B = 2199$, platí, že reprezentuje $\mathbb{Z}^4$,
xxii. pro volbu $b = 8, a = 0$: $\#B = 2411$, platí, že reprezentuje $\mathbb{Z}^4$,
xxiii. pro volbu $b = 9, a = 0$: $\#B = 2511$, platí, že reprezentuje $\mathbb{Z}^4$,
xxiv. pro volbu $b = 10, a = 0$: $\#B = 2713$, platí, že reprezentuje $\mathbb{Z}^4$.

Kapitola 5

Paralelní sčítání

V této kapitole uvedeme poznatky o paralelním sčítání v pozičních a maticových numeračních systémech. V první části představíme algoritmy v pozičních systémech, a to klasický algoritmus na sčítání, paralelní algoritmus od Avizienise[1] a zobecněné paralelní algoritmy z práce [3]. V druhé části se budeme věnovat paralelním algoritmům v maticových systémech [10].

5.1 Sčítání v pozičním numeračním systému

Mějme poziční numerační systém $(\beta, \mathcal{A})$. Úlohou sčítání je pro čísla ve tvaru $x = \sum_{i=n}^{m} x_i\beta^i$ a $y = \sum_{i=n}^{m} y_i\beta^i$, kde $x_i, y_i \in \mathcal{A}$, najít číslo z, pro které bude platit $z = x + y = \sum_{i=p}^{q} z_i\beta^i$, kde rovněž $z_i \in \mathcal{A}$.

Uveďme na začátek klasický algoritmus pro sčítání.

Klasický algoritmus pro sčítání: Mějme poziční systém $(\beta, \mathcal{A})$, kde $\beta \geq 2$, $\beta \in \mathbb{N}$ a $\mathcal{A} = \{0, \ldots, b-1\}$

---

vstup : dva řetězce $x_m \ldots x_n \in \mathcal{A}^*$ a $y_m \ldots y_n \in \mathcal{A}^*$ takové, že reprezentují čísla x a y, tzn. $x = \sum_{i=n}^{m} x_i\beta^i$ a $y = \sum_{i=n}^{m} y_i\beta^i$

výstup: řetězec $z_{m+1} \ldots z_n \in \mathcal{A}^*$ takový, že reprezentuje číslo $z = x + y$, tedy $z = x + y = \sum_{i=n}^{m+1} z_i\beta^i$

1 $q_{n-1} := 0$
2 **for** *i od n do m* **do**
3 $\quad w_i := x_i + y_i$
4 $\quad$ **if** $w_i + q_{i-1} \geq \beta$ **then** $q_i := 1$;
5 $\quad$ **else** $q_i := 0$;
6 $\quad z_i := w_i - q_i\beta$
7 **end**
8 **return** $q_m z_m \ldots z_n$

Jedná se o algoritmus, který běžně používáme, když sčítáme dvě čísla pod sebou.

Pokud platí, že pro nějaké i je součet $x_i + y_i + q_{i-1}$ větší nebo roven základu β, odečteme od tohoto součtu číslo β a přičteme jedničku ve vyšším řádu. To nezmění výslednou hodnotu, protože pro všechna $i \in \mathbb{N}$ platí

$$1 \cdot \beta^{i+1} - \beta \cdot \beta^i = 0. \tag{5.1}$$

Příklad 78. *Nechť $(\beta, \mathcal{A})$ je dekadický systém, a sečteme čísla $x = 956$ a $y = 747$.*

$x \mapsto$	9	5	6
$y \mapsto$	7	4	7
$w \mapsto$	16	9	13
$z \mapsto$	1	7	0	3

V našem příkladě identita (5.1) má tvar $1 \cdot 10 - 10 = 0$ pro $i = 0$, $1 \cdot 10^2 - 10 \cdot 10 = 0$ pro $i = 1$ a $1 \cdot 10^3 - 10 \cdot 10^2 = 0$ pro $i = 2$. Tyto identity můžeme považovat za reprezentaci čísla nula, přičíst je k číslu x a y a takto dostat cifry $13, 10$ a 17 zpátky do abecedy.

$x \mapsto$	9	5	6	
$y \mapsto$	7	4	7	
$w \mapsto$	16	9	13	
$0 \mapsto$		1	$\bar{1}0$	(*pro* $i = 0$)
$0 \mapsto$	1	$\bar{1}0$		(*pro* $i = 1$)
$0 \mapsto$	1	$\bar{1}0$		(*pro* $i = 2$)
$z \mapsto$	1	7	0	3

Z předpisu klasického algoritmu pro sčítání můžeme vyčíst, že identitu pro index i použijeme, pokud $q_i = 1$, v opačném případě, identitu nepoužíváme. Ale hodnota q_i závisí také na q_{i-1}, a ta taktéž závisí na hodnotě q_{i-2}. Tedy q_i závisí na všech předchozích hodnotách q_j pro $j < i$, neboli $q_i = q_i(q_{i-1}, q_{i-2}, \ldots)$.

Problém závislosti q_i na všech předchozích q_j pro $j < i$ se dá vyřešit tak, že přidáme do abecedy více cifer. Uveďme jako příklad paralelní algoritmus vytvořený Avizienisem [1].

Avizienisův algoritmus: Mějme poziční systém $(\beta, \mathcal{A})$, kde $\beta \in \mathbb{N}$, $\beta \geq 3$ a $\mathcal{A} = \{-a, \ldots, 0, \ldots a\}$, kde $\frac{\beta}{2} < a \leq \beta - 1$

vstup : dva řetězce $x_m \ldots x_n \in \mathcal{A}^*$ a $y_m \ldots y_n \in \mathcal{A}^*$ takové, že reprezentují čísla x a y, tzn. $x = \sum_{i=n}^{m} x_i \beta^i$ a $y = \sum_{i=n}^{m} y_i \beta^i$

výstup: řetězec $z_{m+1} \ldots z_n \in \mathcal{A}^*$ takový, že reprezentuje číslo $z = x + y$, tudíž $z = x + y = \sum_{i=n}^{m+1} z_i \beta^i$

```
1  q_{n-1} := 0
2  for i od n do m in parallel do
3  |  w_i := x_i + y_i
4  |  if w_i ≥ a then  q_i := 1 ;
5  |  if w_i ≤ −a then  q_i := −1 ;
6  |  else  q_i := 0 ;
7  end
8  for i od n do m in parallel do
9  |  z_i := w_i + q_{i−1} − q_i β
10 end
11 return q_m z_m ... z_n
```

Poznamenejme, že for cyklus v Avizienisově algoritmu je jiný než v klasickém algoritmu pro sčítání. Zde můžeme provádět výpočet zároveň pro každý index i.

Zkoumejme, na jakých číslech je z_i závislé. Číslo z_i získáváme z předpisu

$$z_i := w_i + q_{i-1} - q_i\beta,$$

a q_i závisí pouze na w_i. Takže ve výsledku dostáváme, že $z_i = z_i(w_i, w_{i-1})$.

Obdobně jako u klasického algoritmu můžeme z předpisu odvodit, že přičítáme identitu

$$1 \cdot \beta^{i+1} - \beta \cdot \beta^i = 0. \tag{5.2}$$

v i-tém řádu, pokud $q_i = 1$. Pro $q_i = -1$ má identita tvar

$$-1 \cdot \beta^{i+1} + \beta \cdot \beta^i = 0. \tag{5.3}$$

Pro $q_i = 0$ nepřičítáme nic.

Příklad 79. *Uvažujme Avizienisův algoritmus pro $\beta = 10$ a $a = 6$. Sčítejme čísla $(336)_{(\beta,\mathcal{A})}$ a $(236)_{(\beta,\mathcal{A})}$.*

$x \mapsto$	3	3	6
$y \mapsto$	2	3	6
$w \mapsto$	5	6	12
$z \mapsto$	6	$\bar{3}$	2

Platí $q_0 = 1, q_1 = 1, q_2 = 0$. Rozepišme použití identit (5.2) a (5.3):

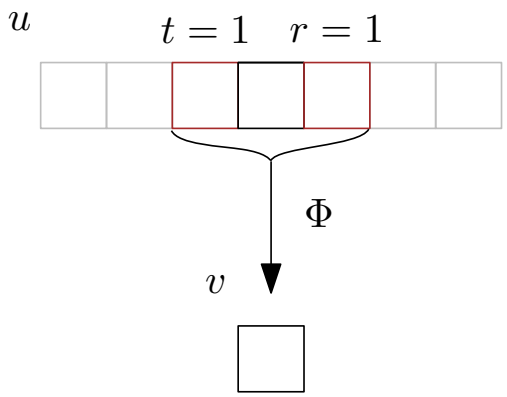
$x \mapsto$	3	3	6
$y \mapsto$	2	3	6
$w \mapsto$	5	6	12
$0 \mapsto$		1	$\bar{1}0$
$0 \mapsto$	1	$\bar{1}0$	
$z \mapsto$	6	$\bar{3}$	2

Zde platí, že rozhodnutí o použití identit v i-tém řádu, tedy hodnota q_i, závisí pouze na w_i, proto můžeme rozepsání identit udělat nezávisle na ostatních, na rozdíl od klasického algoritmu, kde hodnota q_i závisela na všech q_j pro $j < i$.

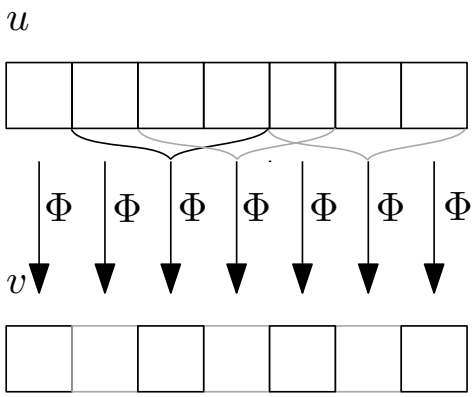
Tuto vlastnost algoritmu nyní definujeme formálně. Pro tyto účely nejprve přeformulujme úlohu sčítání. Mějme dva řetězce $x_m \dots x_n \in \mathcal{A}^*$ a $y_m \dots y_n \in \mathcal{A}^*$ reprezentující čísla x a y, a hledejme funkci $\varphi : (\mathcal{A} + \mathcal{A})^* \to \mathcal{A}^*$ takovou, aby pro všechny řetězce $w \in (\mathcal{A} + \mathcal{A})^*$ platilo $\sum_i w_i\beta^i = \sum_i \varphi(w)_i\beta^i$.

Tuto funkci využijeme tak, že definujeme řetězec $w := (x_m + y_m) \dots (x_n + y_n)$, a pro tento řetězec získáme nový řetězec $\varphi(w)$, který již má cifry z abecedy $\mathcal{A}$ a navíc hodnota čísla reprezentujícího řetězcem w se shoduje s číslem reprezentovaným řetězcem $\varphi(w)$.

Definice 80. *Nechť $\mathcal{A}, \mathcal{B}$ jsou konečné množiny obsahující 0. Řekneme, že funkce $\varphi : \mathcal{A}^* \to \mathcal{B}^*$ lze počítat paralelně, pokud existují čísla $r, t \in \mathbb{N}$ a funkce $\Phi : \mathcal{A}^p \to \mathcal{B}$, kde $p = r+t+1$ takové, že pro všechna $u = (u_i)_i \in \mathcal{A}^*$ a $v = (v_i)_i \in \mathcal{B}^*$ platí $\varphi(u) = v$ právě tehdy, když $\Phi(u_{i+t} \dots u_{i-r}) = v_i$ pro všechna i.*



3-lokální funkce



paralelní počítání pro funkci Φ

Jinými slovy, funkci φ můžeme počítat tak, že nad každou pozici vložíme jednu výkonnou jednotku, a všechny tyto jednotky spustíme zároveň. Z definice je zaručena nezávislost chodu jednotek, tedy že všechny můžou pracovat současně a nezávisle na sobě.

Parametr r nazýváme paměť, parametr t anticipace, a o funkci φ říkáme, že je p-lokální.

Avizienisův algoritmus je zřejmě 2-lokální s parametry $r = 1$ a $t = 0$.

5.2 Zobecněné poziční systémy

V této části předvedeme paralelní algoritmy na sčítání pro neceločíselné základy β. Jak uvidíme v následující větě, musíme uvažovat β algebraické číslo. Dále budeme požadovat, aby β splňovala tzv. silnou reprezentaci nuly(SRZ, od anglického strong representation of zero). Čerpáme z [3].

Definice 81. *Nechť $\beta \in \mathbb{C}$. Řekneme, že β je algebraické číslo, pokud existuje polynom s celočíselnými koeficienty, jehož je β kořenem.*

Věta 82. *Pokud existuje paralelní algoritmus pro sčítání na $(\beta, \mathcal{A})$, kde $\mathcal{A} \subset \mathbb{Z}$, pak β je algebraické číslo.*

Důkaz. Nechť $w \in (\mathcal{A} + \mathcal{A})^*$ je řetězec splňující $w_i = x_i + y_i$ pro všechna i. Fakt, že existuje paralelní algoritmus znamená, že jsme schopni najít řetězec $z \in \mathcal{A}^*$ reprezentující součet $x + y$ takový, že $\sum_i w_i \beta^i = \sum_i z_i \beta^i$. Jednoduchou úpravou dostáváme

$$\sum_i (z_i - w_i)\beta^i = 0.$$

Zřejmě dokážeme najít čísla x, y, aby existoval index i takový, aby $w_i \in (\mathcal{A} + \mathcal{A}) \setminus \mathcal{A}$ a tedy i $w_i \neq z_i$. Dostali jsme polynom s celočíselnými koeficienty, jehož je β kořenem. To již nutně znamená, že β je algebraické číslo. □

Předpoklad $\mathcal{A} \subset \mathbb{Z}$ lze nahradit předpokladem, aby $\mathcal{A}$ byla podmnožinou algebraických čísel.

Nyní definujeme druhou vlastnost, kterou budeme po čísle β požadovat.

Definice 83. *Nechť $\beta \in \mathbb{C}$ splňující $|\beta| > 1$. Řekneme, že β má vlastnost SRZ(strong representation of zero), pokud existují koeficienty $b_k, b_{k-1}, \ldots, b_1, b_0, b_{-1}, \ldots, b_{-h}$ pro indexy $k, h \in \mathbb{N}$ takové, že β je kořenem funkce ve tvaru*

$$S(x) = b_k x^k + \cdots + b_1 x + b_0 + b_{-1} x^{-1} + \cdots + b_{-h} x^{-h},$$

a koeficienty b_j *splňují*

$$b_0 > 2 \sum_{j\in\{-h,\dots,k\}\setminus\{0\}} |b_j|.$$

Z definice plyne, že řetězec $b_k \dots b_1 b_0 b_{-1} \dots b_{-h}$ v systému s bází β reprezentuje číslo 0.

Nyní přikročíme k představení paralelního algoritmu. Nechť $(\beta, \mathcal{A})$ je poziční numerační systém, β algebraické číslo takové, že splňuje SRZ.

Označme $B = b_0$, $M := \sum_{i\in\{-h,\dots,k\}\setminus\{0\}} |b_i|$, $a' := \lceil \frac{B-1}{2} \rceil$ a $c := \left\lceil \frac{B-1}{2(B-2M)} \right\rceil$. Zvolme symetrickou abecedu $\mathcal{A} := \{-a, \dots, 0, \dots, a\}$, kde $a = a' + cM$. Abecedu $\mathcal{A}' = \{-a', \dots, 0, \dots a'\} \subset \mathcal{A}$ budeme nazývat vnitřní abecedou.

Algoritmus pro paralelní sčítání metodou SRZ: Mějme poziční systém $(\beta, \mathcal{A})$, takový že β má vlastnost SRZ

vstup : dva řetězce $x_m \dots x_n \in \mathcal{A}^*$ a $y_m \dots y_n \in \mathcal{A}^*$ takové, že reprezentují čísla x a y, tzn. $x = \sum_{i=n}^{m} x_i \beta^i$ a $y = \sum_{i=n}^{m} y_i \beta^i$

výstup: řetězec $z_{m+k} \dots z_{n-h} \in \mathcal{A}^*$ takový, že reprezentuje číslo z splňující $z = x + y = \sum_{i=n-h}^{m+k} z_i \beta^i$

1 **for** i *od* n *do* m **in parallel do**
2 | $w_i := x_i + y_i$
3 | najdi $q_i \in \{-c, \dots, 0, \dots, c\}$ tak, aby $w_i - q_i B \in \mathcal{A}'$
4 **end**
5 **for** i *od* $n-h$ *do* $m+h$ **in parallel do**
6 | $z_i := w_i - \sum_{j=-h}^{k} q_{i-j} b_j$
7 **end**
8 **return** $z_{m+k} \dots z_{n-h}$

Abychom dokázali korektnost tohoto algoritmu, potřebujeme ověřit následující tři tvrzení:

1. vždy najdeme q_i s vlastností požadovanou na řádku 3,
2. hodnota součtu $x + y$ se nezmění,
3. výsledný řetězec z patří do množiny $\mathcal{A}^*$.

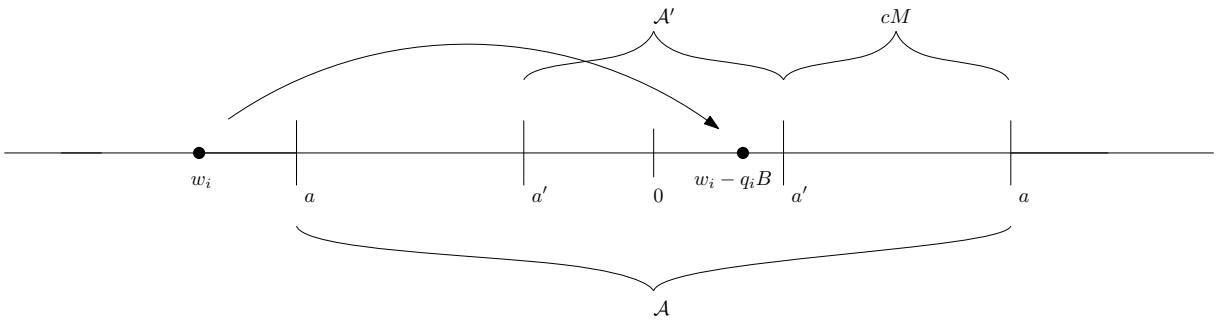
My se omezíme na naznačení důkazu posledních dvou tvrzení, úplný důkaz lze najít v [3]. Začněme důkazem, že cifra z_i bude vždy patřit do množiny $\mathcal{A}$. Zřejmě $w_i \in \mathcal{A} + \mathcal{A}$. Předpokládejme, že vždy najdeme $q_i \in \{-c, \dots, 0, \dots, c\}$ takové, že $w_i - q_i B \in \mathcal{A}'$. Poté můžeme cifru z_i rozepsat jako

$$z_i = w_i - \sum_{j=-h}^{k} q_{i-j} b_j = w_i - q_i b_0 - \sum_{\substack{j=-h \\ j\neq 0}}^{k} q_{i-j} b_j.$$

V absolutní hodnotě dostáváme

$$|z_i| = \left| w_i - q_i b_0 - \sum_{\substack{j=-h \\ j\neq 0}}^{k} q_{i-j} b_j \right| \leq |w_i - q_i b_0| + \left| \sum_{\substack{j=-h \\ j\neq 0}}^{k} q_{i-j} b_j \right| \leq a' + c \cdot \left| \sum_{\substack{j=-h \\ j\neq 0}}^{k} b_j \right| = a' + cM = a.$$

Znázorníme situaci na obrázku 5.1. Pro w_i najdeme cifru q_i takovou, že hodnota výrazu $(w_i - q_iB)$ se dostane do vnitřní abecedy $\mathcal{A}'$, tj. má velikost a'. Dále díky vlastnosti $B > 2M$ už víme, že koeficienty $|\sum_{\substack{j=-h \\ j\neq 0}}^{k} q_{i-j}b_j|$ nejsou v absolutní hodnotě větší než cM, takže celkový výsledný součet je omezen konstantou $a' + cM = a$, tj. nachází se uvnitř abecedy $\mathcal{A}$.



Obrázek 5.1

Nyní naznačíme důkaz tvrzení, že hodnota součtu $x + y$ se nezmění. Řetězec z dostaneme z řetězce w tak, že přičítáme řetězec $b_k \dots b_1 b_0 b_{-1} \dots b_{-h}$ vynásobený koeficientem q_i. Díky tomu, že řetězec $b_k \dots b_1 b_0 b_{-1} \dots b_{-h}$ reprezentuje nulu, hodnota součtu se nemění.

Algoritmus pro SRZ je $(h + k + 1)$-lokální funkce.

Nyní uvedeme příklady konkrétních voleb čísla β a příslušných funkcí.

Příklad 84. *Nechť $\beta = 10$ a uvažujme funkci $S(x) = -x + 10$. Vidíme, že β je SRZ, kde $B = 10$ a $M = 1$. Dále*

$$c = \left\lceil \frac{9}{16} \right\rceil = 1, a' = \left\lceil \frac{9}{2} \right\rceil = 5 \text{ a } a = a' + cM = 6.$$

Tento algoritmus v dekadickém systému se shoduje s algoritmem od Avizienise pro volbu $a = 6$.

Obecněji, pro přirozené číslo $b \geq 3$, bázi $\beta = b$ a polynom $-x + b = 0$ máme algoritmus pro paralelní sčítání v systému $(\beta, \{-a, \dots, 0, \dots, a\})$, kde $a = \lceil \frac{b+1}{2} \rceil$.

5.3 Maticové systémy

V předchozí části měly algoritmy následující tvar. Měli jsme funkci $S : \mathbb{C} \to \mathbb{C}$ takovou, že báze β byla jejím kořenem. Pro dvě čísla x, y s reprezentacemi $x_m \dots x_n$ a $y_m \dots y_n$ jsme vytvořili řetězec $w := (x_m + y_m) \dots (x_n + y_n)$, ke kterému jsme následně přičítali vhodné násobky řetězce reprezentujícího nulu, abychom čísla w_i dostali zpátky do množiny $\mathcal{A}$. Díky tomu, že jsme přičítali násobky nuly, výsledný součet $x + y$ nezměnil.

Nyní tento postup budeme aplikovat na maticové systémy.

Definice 85. *Nechť $(M, \mathcal{A})$ je maticový systém. Mějme čísla $h, k \in \mathbb{N}$ a maticovou funkci $P : (\mathbb{Z}^{d,d}) \to \mathbb{Z}^{d,d}$ ve tvaru*

$$P(X) = P_k X^k + \dots + P_1 X^1 + P_0 X^0 + \dots + P^{-h} X^{-h},$$

kde $P_k, \dots, P_{-h} \in \mathbb{Z}^{d,d}$ a $P(M) = 0$. Tuto funkci nazveme reprezentací nuly pro matici M.

Pracujme s maticovým systémem $(M, \mathcal{A})$. Mějme dva vektory x, y, které mají reprezentaci ve tvaru $x = \sum_{i\in\mathbb{Z}} M^i x_i$ a $y = \sum_{i\in\mathbb{Z}} M^i y_i$, kde $x_i, y_i \in \mathcal{A}$. Z definice maticových systémů

a reprezentací v nich plyne, že pouze konečně mnoho vektorů z abecedy je nenulových, proto bez újmy na obecnosti předpokládejme, že všechny ostatní vektory jsou rovny nule, díky tomu můžeme uvažovat sčítací index v množině celých čísel. Tento předpoklad ulehčí práci s indexy v následujícím výkladu.

Označme prozatímní součet $w = \sum_i M^i w_i$, kde $w_i = x_i + y_i \in (\mathcal{A} + \mathcal{A})$. Našim cílem bude najít vektory $z_i \in \mathcal{A}$, tak, aby $x + y = \sum_i M^i w_i = \sum_i M^i z_i$.

Tyto vektory z_i budeme hledat ve tvaru

$$z_i = w_i + \sum_{j=-h}^{k} P_j q_{i-j}, \tag{5.4}$$

kde P_j jsou koeficienty reprezentace nuly pro matici M a q_{i-j} jsou vhodné vektory. Označme množinu $\mathcal{Q} \subset \mathbb{Z}$ jako množinu všech možných vektorů q_i.

Přirozeně nastává otázka, jak volit reprezentaci nuly pro matici M. Obdobně jako v předchozí kapitole, máme na výběr více reprezentací. Pro každou matici M můžeme maticovou funkci například P zvolit jako $P(X) = -I \cdot X^1 + M \cdot X^0$.

Nyní provedeme konstrukci algoritmu pro paralelního sčítání na konkrétních příkladech.

Příklad 86. *[10] Mějme bázi ve tvaru* $M = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$ *a hledejme abecedu na které lze paralelně sčítat. Musíme najít vhodnou množinu* $\mathcal{Q}$*, předpis pro vektory* $q_i \in \mathcal{Q}$ *a reprezentaci nuly pro matici* M*.*

Uveďme dvě příklady reprezentací nul, které bychom mohli použít.

- $P_1(X) = \mathbf{I} \cdot X^1 - M \cdot X^0 = X - M = X - \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$,
- $P_2(X) = \mathbf{I} \cdot X^2 - M^2 \cdot X^0 = X^2 - M^2 = X^2 - \begin{pmatrix} 4 & 0 \\ 0 & 9 \end{pmatrix}$.

Zvolme reprezentaci nuly jako $P(X) = P_1(X) = X^1 - M$*. Pak předpis* (5.4) *pro* z_i *má tvar*

$$z_i = w_i + q_{i-1} - M q_i.$$

Zvolme abecedu jako

$$\mathcal{A} = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \,:\, a \in \{0,1,2\}, b \in \{0,1,2,3\} \right\} .$$

a $\mathcal{Q}$ *jako*

$$\mathcal{Q} = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \,:\, a, b \in \{0,1,2\} \right\} .$$

Ukažme nejprve, že výsledná hodnota $z = \sum_i M^i z_i$ *se rovná* $x + y$*. S využitím předpisu pro* z_i *dostáváme*

$$\begin{aligned} z = \sum_i M^i z_i = \sum_i M^i (w_i + q_{i-1} - M q_i) = \sum_i M^i w_i + \sum_i M^i q_{i-1} - \sum_i M^{j+1} q_i = \\ = \sum_i M^i (x_i + y_i) + \sum_l M^{l+1} q_l - \sum_i M^{i+1} q_i = \sum_i M^i x_i + \sum_i M^i y_i + 0 = x + y. \end{aligned}$$

Označne prozatimní součet $w = \sum_i M^i w_i$, *kde* $w_i = x_i + y_i \in (\mathcal{A} + \mathcal{A})$ *a* $\mathcal{W}$ *jako* $\mathcal{W} = (\mathcal{A} + \mathcal{A})$. *Množina* $\mathcal{W}$ *má tvar*

$$\mathcal{W} = \mathcal{A} + \mathcal{A} = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} : a \in \{0, \ldots, 4\}, b \in \{0, \ldots, 6\} \right\}.$$

Uvažujme vektory $w_i \in \mathcal{W}$ *a volme vektor* q_i *tak, aby vektor* $z_i = w_i + q_{i-1} - Mq_i$ *patřil do množiny* $\mathcal{A}$ *pro každý index* i. *Jak uvidíme později, volba vektoru* q_i *bude záviset nanejvýš na* w_{i-1}, *tedy* $q_i = q_i(w_i, w_{i-1})$.

V první řadě pokryjeme množinu $w_i + Q$ *posunutými kopiemi množiny* $\mathcal{A}$, *tedy množinami* $\mathcal{A} + Mq$ *pro různé vektory* $q \in Q$. *Označme množinu* $\mathcal{Q}_{w_i}$ *vektorů z* Q *splňující* $w_i + \mathcal{Q} \subset A + MQ_{w_i}$.

Pokud se podaří najít množiny $\mathcal{Q}_{w_i}$ *pro všechna* $w_i \in (\mathcal{A} + \mathcal{A})$, *pak již zřejmě bude platit, že pro všechna* $w_i \in (\mathcal{A} + \mathcal{A})$ *bude existovat* $q_i \in \mathcal{Q}_{w_i}$ *takový, že*

$$z_i = w_i + q_{i-1} - Mq_i \in \mathcal{A}.$$

Následuje výpis množin $\mathcal{Q}_{w_i}$ *pro vektory* w_i:

- *pro* $w_j \in \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$ *platí* $\mathcal{Q}_{w_i} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$,
- *pro* $w_j \in \left\{ \begin{pmatrix} 0 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 4 \end{pmatrix} \right\}$ *platí* $\mathcal{Q}_{w_i} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$,
- *pro* $w_j \in \left\{ \begin{pmatrix} 0 \\ 6 \end{pmatrix} \right\}$ *platí* $\mathcal{Q}_{w_i} = \begin{pmatrix} 0 \\ 2 \end{pmatrix}$,
- *pro* $w_j \in \left\{ \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix} \right\}$ *platí* $\mathcal{Q}_{w_i} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$,
- *pro* $w_j \in \left\{ \begin{pmatrix} 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ 4 \end{pmatrix} \right\}$ *platí* $\mathcal{Q}_{w_i} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$,
- *pro* $w_j \in \left\{ \begin{pmatrix} 2 \\ 6 \end{pmatrix} \right\}$ *platí* $\mathcal{Q}_{w_i} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$,
- *pro* $w_j \in \left\{ \begin{pmatrix} 4 \\ 0 \end{pmatrix}, \begin{pmatrix} 4 \\ 1 \end{pmatrix} \right\}$ *platí* $\mathcal{Q}_{w_i} = \begin{pmatrix} 2 \\ 0 \end{pmatrix}$,
- *pro* $w_j \in \left\{ \begin{pmatrix} 4 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 4 \end{pmatrix} \right\}$ *platí* $\mathcal{Q}_{w_i} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$,
- *pro* $w_j \in \left\{ \begin{pmatrix} 4 \\ 6 \end{pmatrix} \right\}$ *platí* $\mathcal{Q}_{w_i} = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$,
- *pro* $w_j \in \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$ *platí* $\mathcal{Q}_{w_i} = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}$,
- *pro* $w_i \in \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$ *platí* $\mathcal{Q}_{w_i} = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}$,

- *pro* $w_i \in \left\{\begin{pmatrix}1\\3\end{pmatrix}, \begin{pmatrix}1\\4\end{pmatrix}\right\}$ *platí* $\mathcal{Q}_{w_i} = \left\{\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}\right\}$,
- *pro* $w_i \in \left\{\begin{pmatrix}3\\0\end{pmatrix}, \begin{pmatrix}3\\1\end{pmatrix}\right\}$ *platí* $\mathcal{Q}_{w_i} = \left\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}2\\0\end{pmatrix}\right\}$,
- *pro* $w_i \in \left\{\begin{pmatrix}3\\3\end{pmatrix}, \begin{pmatrix}3\\4\end{pmatrix}\right\}$ *platí* $\mathcal{Q}_{w_i} = \left\{\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}2\\1\end{pmatrix}\right\}$,
- *pro* $w_i \in \left\{\begin{pmatrix}1\\6\end{pmatrix}\right\}$ *platí* $\mathcal{Q}_{w_i} = \left\{\begin{pmatrix}0\\2\end{pmatrix}, \begin{pmatrix}1\\2\end{pmatrix}\right\}$,
- *pro* $w_i \in \left\{\begin{pmatrix}3\\6\end{pmatrix}\right\}$ *platí* $\mathcal{Q}_{w_i} = \left\{\begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}2\\2\end{pmatrix}\right\}$,
- *pro* $w_i \in \left\{\begin{pmatrix}0\\2\end{pmatrix}\right\}$ *platí* $\mathcal{Q}_{w_i} = \left\{\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right\}$,
- *pro* $w_i \in \left\{\begin{pmatrix}2\\2\end{pmatrix}\right\}$ *platí* $\mathcal{Q}_{w_i} = \left\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}\right\}$,
- *pro* $w_i \in \left\{\begin{pmatrix}4\\2\end{pmatrix}\right\}$ *platí* $\mathcal{Q}_{w_i} = \left\{\begin{pmatrix}2\\0\end{pmatrix}, \begin{pmatrix}2\\1\end{pmatrix}\right\}$,
- *pro* $w_i \in \left\{\begin{pmatrix}0\\5\end{pmatrix}\right\}$ *platí* $\mathcal{Q}_{w_i} = \left\{\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}0\\2\end{pmatrix}\right\}$,
- *pro* $w_i \in \left\{\begin{pmatrix}2\\5\end{pmatrix}\right\}$ *platí* $\mathcal{Q}_{w_i} = \left\{\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1\\2\end{pmatrix}\right\}$,
- *pro* $w_i \in \left\{\begin{pmatrix}4\\5\end{pmatrix}\right\}$ *platí* $\mathcal{Q}_{w_i} = \left\{\begin{pmatrix}2\\1\end{pmatrix}, \begin{pmatrix}2\\2\end{pmatrix}\right\}$,
- *pro* $w_i \in \left\{\begin{pmatrix}1\\2\end{pmatrix}\right\}$ *platí* $\mathcal{Q}_{w_i} = \left\{\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}\right\}$,
- *pro* $w_i \in \left\{\begin{pmatrix}1\\5\end{pmatrix}\right\}$ *platí* $\mathcal{Q}_{w_i} = \left\{\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}0\\2\end{pmatrix}, \begin{pmatrix}1\\2\end{pmatrix}\right\}$,
- *pro* $w_i \in \left\{\begin{pmatrix}3\\2\end{pmatrix}\right\}$ *platí* $\mathcal{Q}_{w_i} = \left\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}2\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}2\\1\end{pmatrix}\right\}$,
- *pro* $w_i \in \left\{\begin{pmatrix}3\\5\end{pmatrix}\right\}$ *platí* $\mathcal{Q}_{w_i} = \left\{\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}2\\1\end{pmatrix}, \begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}2\\2\end{pmatrix}\right\}$.

Pro vektory w_i*, kde* $\#\mathcal{Q}_{w_i} = 1$*, tedy případy, kdy stačí pouze jeden vektor z množiny* $\mathcal{Q}$ *na pokrytí* $w_i + Q$*, můžeme rovnou tento vektor zvolit jako* q_i*.*

- *Pro* $w_j \in \left\{\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right\} \Rightarrow q_i := \begin{pmatrix}0\\0\end{pmatrix}$,
- *pro* $w_j \in \left\{\begin{pmatrix}0\\3\end{pmatrix}, \begin{pmatrix}0\\4\end{pmatrix}\right\} \Rightarrow q_i := \begin{pmatrix}0\\1\end{pmatrix}$,

- *pro* $w_j \in \left\{\begin{pmatrix}0\\6\end{pmatrix}\right\} \Rightarrow q_i := \begin{pmatrix}0\\2\end{pmatrix}$,
- *pro* $w_j \in \left\{\begin{pmatrix}2\\0\end{pmatrix}, \begin{pmatrix}2\\1\end{pmatrix}\right\} \Rightarrow q_i := \begin{pmatrix}1\\0\end{pmatrix}$,
- *pro* $w_j \in \left\{\begin{pmatrix}2\\3\end{pmatrix}, \begin{pmatrix}2\\4\end{pmatrix}\right\} \Rightarrow q_i := \begin{pmatrix}1\\1\end{pmatrix}$,
- *pro* $w_j \in \left\{\begin{pmatrix}2\\6\end{pmatrix}\right\} \Rightarrow q_i := \begin{pmatrix}1\\2\end{pmatrix}$,
- *pro* $w_j \in \left\{\begin{pmatrix}4\\0\end{pmatrix}, \begin{pmatrix}4\\1\end{pmatrix}\right\} \Rightarrow q_i := \begin{pmatrix}2\\0\end{pmatrix}$,
- *pro* $w_j \in \left\{\begin{pmatrix}4\\3\end{pmatrix}, \begin{pmatrix}4\\4\end{pmatrix}\right\} \Rightarrow q_i := \begin{pmatrix}2\\1\end{pmatrix}$,
- *pro* $w_j \in \left\{\begin{pmatrix}4\\6\end{pmatrix}\right\} \Rightarrow q_i := \begin{pmatrix}2\\2\end{pmatrix}$.

Pro vektory w_i*, kde* $\#\mathcal{Q}_{w_i} > 1$*, budeme muset rozhodnout na základě* w_{i-1} *jaký vektor za* q_i *zvolíme. Nejprve pracujme s vektory* w_i*, pro které platí* $\#\mathcal{Q}_{w_i} = 2$*. Pro snazší zápis, definujme množiny* $\mathcal{W}_k \subset \mathcal{W}$ *a* $\mathcal{Q}_k \subset \mathcal{Q}$ *jako*

- $\mathcal{W} \supset \mathcal{W}_1 := \left\{\begin{pmatrix}a\\b\end{pmatrix} : a \in \{0,1,2\}, b \in \{0,1,2,3,4\}\right\}$,
- $\mathcal{Q} \supset \mathcal{Q}_1 := \left\{\begin{pmatrix}c\\d\end{pmatrix} : c \in \{0,1\}, d \in \{0,1,2\}\right\}$,
- $\mathcal{W} \supset \mathcal{W}_2 := \mathcal{W} \setminus \mathcal{W}_1 = \left\{\begin{pmatrix}a\\b\end{pmatrix} : a \in \{0,1,2\}, b \in \{5,6\}\right\} \bigcup$
  $\bigcup \left\{\begin{pmatrix}a\\b\end{pmatrix} : a \in \{3,4\}, b \in \{0,1,2,3,4,5,6\}\right\}$,
- $\mathcal{Q} \supset \mathcal{Q}_2 := \left\{\begin{pmatrix}c\\d\end{pmatrix} : c \in \{1,2\}, d \in \{0,1,2\}\right\}$,
- $\mathcal{W} \supset \mathcal{W}_3 := \left\{\begin{pmatrix}a\\b\end{pmatrix} : a \in \{0,1,2,3,4\}, b \in \{0,1,2,3,4\}\right\}$,
- $\mathcal{Q} \supset \mathcal{Q}_3 := \left\{\begin{pmatrix}c\\d\end{pmatrix} : c \in \{0,1,2\}, d \in \{0,1\}\right\}$,
- $\mathcal{W} \supset \mathcal{W}_4 := \mathcal{W} \setminus \mathcal{W}_3 = \left\{\begin{pmatrix}a\\b\end{pmatrix} : a \in \{0,1,2,3,4\}, b \in \{5,6\}\right\}$,
- $\mathcal{Q} \supset \mathcal{Q}_4 := \left\{\begin{pmatrix}c\\d\end{pmatrix} : c \in \{0,1,2\}, d \in \{1,2\}\right\}$.

A nyní předpisy pro q_i *na základě* w_{i-1}*:*

- *pro* $w_i \in \left\{ \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix} \right\}$*: pokud* $w_{i-1} \in \mathcal{W}_1$*, pak* $q_i := \begin{pmatrix}0\\0\end{pmatrix}$*, v opačném případě* $q_i := \begin{pmatrix}1\\0\end{pmatrix}$,
- *pro* $w_i \in \left\{ \begin{pmatrix}1\\3\end{pmatrix}, \begin{pmatrix}1\\4\end{pmatrix} \right\}$*: pokud* $w_{i-1} \in \mathcal{W}_1$*, pak* $q_i := \begin{pmatrix}0\\1\end{pmatrix}$*, v opačném případě* $q_i := \begin{pmatrix}1\\1\end{pmatrix}$,
- *pro* $w_i \in \left\{ \begin{pmatrix}3\\0\end{pmatrix}, \begin{pmatrix}3\\1\end{pmatrix} \right\}$*: pokud* $w_{i-1} \in \mathcal{W}_1$*, pak* $q_i := \begin{pmatrix}1\\0\end{pmatrix}$*, v opačném případě* $q_i := \begin{pmatrix}2\\0\end{pmatrix}$,
- *pro* $w_i \in \left\{ \begin{pmatrix}3\\3\end{pmatrix}, \begin{pmatrix}3\\4\end{pmatrix} \right\}$*: pokud* $w_{i-1} \in \mathcal{W}_1$*, pak* $q_i := \begin{pmatrix}1\\1\end{pmatrix}$*, v opačném případě* $q_i := \begin{pmatrix}2\\1\end{pmatrix}$,
- *pro* $w_i \in \left\{ \begin{pmatrix}1\\6\end{pmatrix} \right\}$*: pokud* $w_{i-1} \in \mathcal{W}_1$*, pak* $q_i := \begin{pmatrix}0\\2\end{pmatrix}$*, v opačném případě* $q_i := \begin{pmatrix}1\\2\end{pmatrix}$,
- *pro* $w_i \in \left\{ \begin{pmatrix}3\\6\end{pmatrix} \right\}$*: pokud* $w_{i-1} \in \mathcal{W}_1$*, pak* $q_i := \begin{pmatrix}1\\2\end{pmatrix}$*, v opačném případě* $q_i := \begin{pmatrix}2\\2\end{pmatrix}$,
- *pro* $w_i \in \left\{ \begin{pmatrix}0\\2\end{pmatrix} \right\}$*: pokud* $w_{i-1} \in \mathcal{W}_3$*, pak* $q_i := \begin{pmatrix}0\\0\end{pmatrix}$*, v opačném případě* $q_i := \begin{pmatrix}0\\1\end{pmatrix}$,
- *pro* $w_i \in \left\{ \begin{pmatrix}2\\2\end{pmatrix} \right\}$*: pokud* $w_{i-1} \in \mathcal{W}_3$*, pak* $q_i := \begin{pmatrix}1\\0\end{pmatrix}$*, v opačném případě* $q_i := \begin{pmatrix}1\\1\end{pmatrix}$,
- *pro* $w_i \in \left\{ \begin{pmatrix}4\\2\end{pmatrix} \right\}$*: pokud* $w_{i-1} \in \mathcal{W}_3$*, pak* $q_i := \begin{pmatrix}2\\0\end{pmatrix}$*, v opačném případě* $q_i := \begin{pmatrix}2\\1\end{pmatrix}$,
- *pro* $w_i \in \left\{ \begin{pmatrix}0\\5\end{pmatrix} \right\}$*: pokud* $w_{i-1} \in \mathcal{W}_3$*, pak* $q_i := \begin{pmatrix}0\\1\end{pmatrix}$*, v opačném případě* $q_i := \begin{pmatrix}0\\2\end{pmatrix}$,
- *pro* $w_i \in \left\{ \begin{pmatrix}2\\5\end{pmatrix} \right\}$*: pokud* $w_{i-1} \in \mathcal{W}_3$*, pak* $q_i := \begin{pmatrix}1\\1\end{pmatrix}$*, v opačném případě* $q_i := \begin{pmatrix}1\\2\end{pmatrix}$,
- *pro* $w_i \in \left\{ \begin{pmatrix}4\\5\end{pmatrix} \right\}$*: pokud* $w_{i-1} \in \mathcal{W}_3$*, pak* $q_i := \begin{pmatrix}2\\1\end{pmatrix}$*, v opačném případě* $q_i := \begin{pmatrix}2\\2\end{pmatrix}$.

Pro vektory w_i*, kde* $\#\mathcal{Q}_{w_i} = 4$*, definujme množiny* $\mathcal{W}_k \subset \mathcal{W}$ *a* $\mathcal{Q}_k \subset \mathcal{Q}$ *jako*

- $\mathcal{W} \supset \mathcal{W}_5 := \left\{ \begin{pmatrix}a\\b\end{pmatrix} : a \in \{0,1,2\}, b \in \{0,1,2,3,4\} \right\}$,
- $\mathcal{Q} \supset \mathcal{Q}_5 := \left\{ \begin{pmatrix}c\\d\end{pmatrix} : c \in \{0,1\}, d \in \{0,1\} \right\}$,
- $\mathcal{W} \supset \mathcal{W}_6 := \left\{ \begin{pmatrix}a\\b\end{pmatrix} : a \in \{3,4\}, b \in \{0,1,2,3,4\} \right\}$,
- $\mathcal{Q} \supset \mathcal{Q}_6 := \left\{ \begin{pmatrix}c\\d\end{pmatrix} : c \in \{1,2\}, d \in \{0,1\} \right\}$,
- $\mathcal{W} \supset \mathcal{W}_7 := \left\{ \begin{pmatrix}a\\b\end{pmatrix} : a \in \{0,1,2\}, b \in \{5,6\} \right\}$,

- $\mathcal{Q} \supset \mathcal{Q}_7 := \left\{ \begin{pmatrix} c \\ d \end{pmatrix} : c \in \{0,1\}, d \in \{1,2\} \right\}$,
- $\mathcal{W} \supset \mathcal{W}_8 := \left\{ \begin{pmatrix} a \\ b \end{pmatrix} : a \in \{3,4\}, b \in \{5,6\} \right\}$,
- $\mathcal{Q} \supset \mathcal{Q}_8 := \left\{ \begin{pmatrix} c \\ d \end{pmatrix} : c \in \{1,2\}, d \in \{1,2\} \right\}$.

Předpis pro vektory q_i vypadá následovně

- *pro* $w_i \in \left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right\}$
  - *pokud* $w_{i-1} \in \mathcal{W}_5$, *pak* $q_i := \begin{pmatrix} 0 \\ 0 \end{pmatrix}$,
  - *pokud* $w_{i-1} \in \mathcal{W}_6$, *pak* $q_i := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$,
  - *pokud* $w_{i-1} \in \mathcal{W}_7$, *pak* $q_i := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$,
  - *pokud* $w_{i-1} \in \mathcal{W}_8$, *pak* $q_i := \begin{pmatrix} 1 \\ 1 \end{pmatrix}$.
- *pro* $w_i \in \left\{ \begin{pmatrix} 1 \\ 5 \end{pmatrix} \right\}$
  - *pokud* $w_{i-1} \in \mathcal{W}_5$, *pak* $q_i := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$,
  - *pokud* $w_{i-1} \in \mathcal{W}_6$, *pak* $q_i := \begin{pmatrix} 1 \\ 1 \end{pmatrix}$,
  - *pokud* $w_{i-1} \in \mathcal{W}_7$, *pak* $q_i := \begin{pmatrix} 0 \\ 2 \end{pmatrix}$,
  - *pokud* $w_{i-1} \in \mathcal{W}_8$, *pak* $q_i := \begin{pmatrix} 1 \\ 2 \end{pmatrix}$.
- *pro* $w_i \in \left\{ \begin{pmatrix} 3 \\ 2 \end{pmatrix} \right\}$
  - *pokud* $w_{i-1} \in \mathcal{W}_5$, *pak* $q_i := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$,
  - *pokud* $w_{i-1} \in \mathcal{W}_6$, *pak* $q_i := \begin{pmatrix} 2 \\ 0 \end{pmatrix}$,
  - *pokud* $w_{i-1} \in \mathcal{W}_7$, *pak* $q_i := \begin{pmatrix} 1 \\ 1 \end{pmatrix}$,
  - *pokud* $w_{i-1} \in \mathcal{W}_8$, *pak* $q_i := \begin{pmatrix} 2 \\ 1 \end{pmatrix}$.

- *pro* $w_i \in \left\{ \begin{pmatrix} 3 \\ 5 \end{pmatrix} \right\}$
  - *pokud* $w_{i-1} \in \mathcal{W}_5$, *pak* $q_i := \begin{pmatrix} 1 \\ 1 \end{pmatrix}$,
  - *pokud* $w_{i-1} \in \mathcal{W}_6$, *pak* $q_i := \begin{pmatrix} 2 \\ 1 \end{pmatrix}$,
  - *pokud* $w_{i-1} \in \mathcal{W}_7$, *pak* $q_i := \begin{pmatrix} 1 \\ 2 \end{pmatrix}$,
  - *pokud* $w_{i-1} \in \mathcal{W}_8$, *pak* $q_i := \begin{pmatrix} 2 \\ 2 \end{pmatrix}$.

Při ověřování korektnosti algoritmu můžeme využít vlastnosti, že pro $k \in \{1, \ldots, 8\}$ platí

$$w_i \in \mathcal{W}_k \implies q_i \in \mathcal{Q}_k.$$

Z předpisu $z_i = w_i + q_{i-1} - Mq_i$ a faktu, že $q_i = q_i(w_{i-1}, w_i)$, získáváme $z_i = z_i(w_{i-2}, w_{i-1}, w_i)$. Jedná se tedy o 3-lokální funkci, kde $t = 2$ a $r = 0$.

Příklad 87. *[10] Mějme stejnou bázi jako v Penneyho systému, tedy* $M = \begin{pmatrix} -1 & -1 \\ 1 & -1 \end{pmatrix}$ *a hledejme abecedu na které lze paralelně sčítat. Musíme najít vhodnou množinu* $\mathcal{Q}$*, předpis pro vektory* $q_i \in \mathcal{Q}$ *a reprezentaci nuly pro matici* M*.*

Uveďme tři příklady reprezentací nul, které bychom mohli použít.

- $P_1(X) = I \cdot X^1 - M \cdot X^0 = X - M = X - \begin{pmatrix} \bar{1} & \bar{1} \\ 1 & \bar{1} \end{pmatrix}$,
- $P_2(X) = I \cdot X^2 - M^2 \cdot X^0 = X^2 - M^2 = X^2 - \begin{pmatrix} 0 & 2 \\ \bar{2} & 0 \end{pmatrix}$,
- $P_4(X) = I \cdot X^4 - M^4 \cdot X^0 = X^4 - M^4 = X^4 - \begin{pmatrix} \bar{4} & 0 \\ 0 & \bar{4} \end{pmatrix}$.

Zvolme reprezentaci nuly jako $P(X) = P_2(X) = X^2 - M^2$*. Pak předpis* (5.4) *pro* z_i *má tvar*

$$z_i = w_i + q_{i-2} - M^2 q_i.$$

Zvolme abecedu jako

$$\mathcal{A} = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \pm \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \pm \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \pm \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \pm \begin{pmatrix} 1 \\ \bar{1} \end{pmatrix} \right\} = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} : a, b \in \{\bar{1}, 0, 1\} \right\}$$

a $\mathcal{Q}$ *jako*

$$\mathcal{Q} = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} : a, b \in \{\bar{1}, 0, 1\} \right\},$$

která se shodou náhod rovná abecedě $\mathcal{A}$*.*

Ukažme nejprve, že výsledná hodnota $z = \sum_i M^i z_i$ *se rovná opravdu* $x+y$. *S využitím předpisu pro* z_i *dostáváme*

$$z = \sum_i M^i z_i = \sum_i M^i(w_i + q_{i-2} - M^2 q_i) = \sum_i M^i w_i + \sum_i M^i q_{i-2} - \sum_i M^{i+2} q_i =$$
$$= \sum_i M^i(x_i + y_i) + \sum_l M^{l+2} q_l - \sum_i M^{i+2} q_i = \sum_i M^i x_i + \sum_i M^i y_i + 0 = x + y.$$

Označme prozatimní součet $w = \sum_i M^i w_i$, *kde* $w_i = x_i + y_i \in (\mathcal{A} + \mathcal{A})$. *Uvažujme nejprve pouze vektory* w_i *z prvního kvadrantu, tedy*

$$w_i \in \left\{ \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}2\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}2\\1\end{pmatrix}, \begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}2\\2\end{pmatrix} \right\}.$$

Postup pro vektory w_i *z ostatních kvadrantů dostaneme jednoduše vynásobením vektorů maticí rotace* $R_{\frac{\pi}{2}} = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$.

Našim úkolem je zvolit vektor q_i *tak, aby vektor* $z_i = w_i + q_{i-2} - M^2 q_i$ *patřil do množiny* $\mathcal{A}$ *pro každý index* i. *Jak uvidíme později, volba vektoru* q_i *bude záviset nanejvýš na* w_{i-2}, *tedy* $q_i = q_i(w_i, w_{i-2})$.

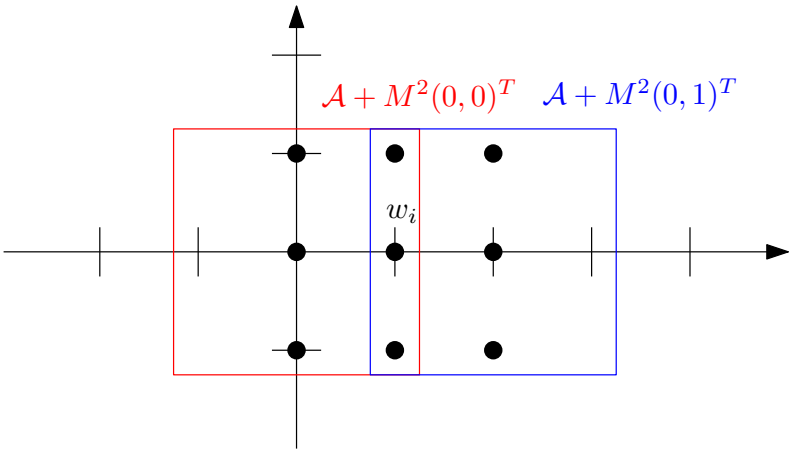
Nyní přejdeme k postupu. Pokryjme množinu $w_i + Q$ *posunutými kopiemi množiny* $\mathcal{A}$, *tedy množinami* $\mathcal{A} + M^2 q$ *pro různé vektory* $q \in Q$. *Označme množinu* $\mathcal{Q}_{w_i}$ *vektorů z* Q *splňující* $w_i + \mathcal{Q} \subset A + M^2 Q_{w_i}$.

Pokud se podaří najít množiny $\mathcal{Q}_{w_i}$ *pro všechna* $w_i \in (\mathcal{A} + \mathcal{A})$, *pak zřejmě bude platit, že pro všechna* $w_i \in (\mathcal{A} + \mathcal{A})$ *bude existovat* $q_i \in \mathcal{Q}_{w_i}$ *takový, že*

$$z_i = w_i + q_{i-2} - M^2 q_i \in \mathcal{A}.$$

Následuje výpis množin $\mathcal{Q}_{w_i}$ *pro vektory* w_i:

- *pro* $w_i = \begin{pmatrix}1\\0\end{pmatrix}$ *platí* $\mathcal{Q}_{w_i} = \left\{ \begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix} \right\}$, *znázornění můžeme vidět na obrázku 5.2,*



Obrázek 5.2: Černými body je vyznačena množina $w_i + Q$

- *pro* $w_i = \begin{pmatrix}2\\0\end{pmatrix}$ *platí* $\mathcal{Q}_{w_i} = \left\{\begin{pmatrix}0\\1\end{pmatrix}\right\}$,
- *pro* $w_i = \begin{pmatrix}1\\1\end{pmatrix}$ *platí* $\mathcal{Q}_{w_i} = \left\{\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}\bar{1}\\0\end{pmatrix}, \begin{pmatrix}\bar{1}\\1\end{pmatrix}\right\}$,
- *pro* $w_i = \begin{pmatrix}2\\1\end{pmatrix}$ *platí* $\mathcal{Q}_{w_i} = \left\{\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}\bar{1}\\1\end{pmatrix}\right\}$,
- *pro* $w_i = \begin{pmatrix}1\\2\end{pmatrix}$ *platí* $\mathcal{Q}_{w_i} = \left\{\begin{pmatrix}\bar{1}\\0\end{pmatrix}, \begin{pmatrix}\bar{1}\\1\end{pmatrix}\right\}$,
- *pro* $w_i = \begin{pmatrix}2\\2\end{pmatrix}$ *platí* $\mathcal{Q}_{w_i} = \left\{\begin{pmatrix}\bar{1}\\1\end{pmatrix}\right\}$.

Pro vektory w_i*, kde* $\#\mathcal{Q}_{w_i} = 1$*, tedy případy, kdy stačí pouze jeden vektor z množiny* $\mathcal{Q}$ *na pokrytí* $w_i + Q$*, můžeme rovnou tento vektor zvolit jako* q_i*.*

- $w_i = \begin{pmatrix}2\\0\end{pmatrix} \Rightarrow q_i := \begin{pmatrix}0\\1\end{pmatrix}$,
- $w_i = \begin{pmatrix}2\\2\end{pmatrix} \Rightarrow q_i := \begin{pmatrix}\bar{1}\\1\end{pmatrix}$,
- $w_i = \begin{pmatrix}0\\0\end{pmatrix} \Rightarrow q_i := \begin{pmatrix}0\\0\end{pmatrix}$.

Pro vektory w_i*, kde* $\#\mathcal{Q}_{w_i} > 1$ *budeme muset rozhodnout na základě* w_{i-2} *jaký vektor* q_i *zvolíme. Lze ověřit, že naše volba* q_i *splňuje následující tvrzení.*

Pro w_{i-2} *ve tvaru* $w_{i-2} = \begin{pmatrix}a\\b\end{pmatrix}$ *a pro všechny* $q_{i-2} \in \mathcal{Q}_{w_{i-2}}$ *takové, že* $q_{i-2} = \begin{pmatrix}c\\d\end{pmatrix}$*, platí*

- *pokud* $b \geq 0$*, pak* $c \leq 0$*,*
- *pokud* $a \geq 0$*, pak* $d \geq 0$*.*

To umožní volit pro víceprvkové množiny $\mathcal{Q}_{w_i}$ *vektory* q_i *jako:*

- *Pro* $w_i = \begin{pmatrix}1\\0\end{pmatrix}$*:*
  - *pokud* $w_{i-2} = \begin{pmatrix}a\\b\end{pmatrix}$*, kde* $b \in \{0, 1, 2\}$*, pak* $q_i := \begin{pmatrix}0\\0\end{pmatrix}$,
  - *pokud* $w_{i-2} = \begin{pmatrix}a\\b\end{pmatrix}$*, kde* $b \in \{\bar{1}, \bar{2}\}$*, pak* $q_i := \begin{pmatrix}0\\1\end{pmatrix}$.
- *Pro* $w_i = \begin{pmatrix}2\\1\end{pmatrix}$*:*
  - *pokud* $w_{i-2} = \begin{pmatrix}a\\b\end{pmatrix}$*, kde* $a \in \{0, \bar{1}, \bar{2}\}$*, pak* $q_i := \begin{pmatrix}0\\1\end{pmatrix}$,

  - *pokud* $w_{i-2} = \begin{pmatrix} a \\ b \end{pmatrix}$, *kde* $a \in \{1, 2\}$, *pak* $q_i := \begin{pmatrix} \bar{1} \\ 1 \end{pmatrix}$.

- *Pro* $w_i = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$:
  - *Pokud* $w_{i-2} = \begin{pmatrix} a \\ b \end{pmatrix}$, *kde* $b \in \{0, 1, 2\}$, *pak* $q_i := \begin{pmatrix} \bar{1} \\ 0 \end{pmatrix}$,
  - *Pokud* $w_{i-2} = \begin{pmatrix} a \\ b \end{pmatrix}$, *kde* $b \in \{\bar{1}, \bar{2}\}$, *pak* $q_i := \begin{pmatrix} \bar{1} \\ 1 \end{pmatrix}$.

- *Pro* $w_i = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$:
  - *pokud* $w_{i-2} = \begin{pmatrix} a \\ b \end{pmatrix}$, *kde* $a \in \{0, \bar{1}, \bar{2}\}$ *a* $b \in \{0, 1, 2\}$, *pak* $q_i := \begin{pmatrix} 0 \\ 0 \end{pmatrix}$,
  - *pokud* $w_{i-2} = \begin{pmatrix} a \\ b \end{pmatrix}$, *kde* $a \in \{0, 1, 2\}$ *a* $b \in \{0, \bar{1}, \bar{2}\}$, *kromě případu, kdy* $a = b = 0$, *pak* $q_i := \begin{pmatrix} \bar{1} \\ 1 \end{pmatrix}$,
  - *pokud* $w_{i-2} = \begin{pmatrix} a \\ b \end{pmatrix}$, *kde* $a \in \{1, 2\}$ *a* $b \in \{1, 2\}$, *pak* $q_i := \begin{pmatrix} \bar{1} \\ 0 \end{pmatrix}$,
  - *pokud* $w_{i-2} = \begin{pmatrix} a \\ b \end{pmatrix}$, *kde* $a \in \{\bar{1}, \bar{2}\}$ *a* $b \in \{\bar{1}, \bar{2}\}$, *pak* $q_i := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Z předpisu $z_i = w_i + q_{i-2} - M^2 q_i$ *a faktu, že* $q_i = q_i(w_{i-2}, w_i)$, *získáváme* $z_i = z_i(w_{i-4}, w_{i-2}, w_i)$. *Jedná se tedy o* 5*-lokální funkci, kde* $t = 4$ *a* $r = 0$.

Závěr

V první kapitole jsme ukázali, že Penneyho systém reprezentuje množinu $\mathbb{Z}[\mathrm{i}]$ a Eisensteinův systém reprezentuje $\mathbb{Z}[\omega]$ a následně jsme vytvořili vylepšené algoritmy pro hledání reprezentace v těchto systémech. Dále jsme pro Penneyho a Eisensteinovu bázi a jejich různé abecedy vykreslili obrázky množin $V = \left\{\sum_{i=1}^{\infty} a_i \beta^{-i} : a_i \in \mathcal{A}\right\}$, které na základě splnění vlastnosti $0 \in V^{\circ}$, dokázaly rozhodnout o tom, zda poziční numerační systém reprezentuje celou množinu $\mathbb{C}$.

V druhé kapitole jsme definovali maticové numerační systémy a ukázali, že Penneyho systém má svůj protějšek jakožto maticový numerační systém. Toho jsme docílili vytvořením izomorfismu mezi $\mathbb{Z}^2$ a Gaussovými celými čísly. Obdobnou vlastnost jsme ukázali pro Eisensteinův systém.

Dále jsme se zabývali otázkou, kolik je tříd ekvivalence kongruence modulo M, a byli jsme schopni dokázat, že je to právě absolutní hodnota z matice M. Pro tento důkaz jsme pokrývali prostor rovnoběžnostěny o obsahu $|\det M|$ a každý celočíselný vektor, který patřil do rovnoběžnostěnu, byl reprezentantem jedné třídy ekvivalence. Dále jsme definovali tzv. kompletní abecedu a ukázali jsme, že systém, který reprezentuje celou množinu $\mathbb{Z}^d$, má kompletní abecedu právě tehdy když jednoznačně reprezentuje vektory ze $\mathbb{Z}^d$.

V další části práce jsme sestrojili speciální normu na množině $\mathbb{Z}^d$, která umožnila vytvořit postačující podmínku maticového systému, aby reprezentoval celou množinu $\mathbb{Z}^d$. Ta pracuje s konečnou testovací množinou ve tvaru

$$\left\{x \in \mathbb{Z}^d : ||x|| \leq \max_{a \in \mathcal{A}} \frac{||M^{-1}||||a||}{1 - ||M^{-1}||}\right\},$$

a tvrdí, že pokud jsou všechny vektory z této množiny reprezentovány, pak systém již reprezentuje celý prostor.

S použitím této postačující podmínky jsme implementovali program, který rozhoduje o tom, zda maticový systém je vhodný k reprezentaci $\mathbb{Z}^d$. Tento program kontroloval mimo jiné i fakt, zda systém obsahuje kompletní abecedu. Následně jsme program využili k ověření výsledků z [7], a některé jsme byli schopni i rozšířit.

Tento program byl implementován pouze pro diagonalizovatelné báze, proto je možnost ho rozšířit i pro nediagonalizovatelné v dalším pokračování práce.

Na závěr práce se věnujeme paralelním algoritmům pro sčítání. Nejprve jsme porovnali klasický algoritmus pro sčítání s paralelním algoritmem od Avizienisiho, a následně jsme uvedli jeho zobecnění z práce [3]. Na konci práce je uveden paralelní algoritmus pro sčítání v Penneyho systému a v systému s maticí $\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$. Zde je taktéž možnost pokračování práce, a to ve vytvoření obecného paralelního algoritmu pro sčítání pro maticové numerační systémy.

Literatura

[1] A. Avizienis. Signed-digit numbe representations for fast parallel arithmetic. *IRE Transactions on Electronic Computers*, EC-10(3):389–400, 1961.

[2] L. Dvořáková. *Lineární algebra 2.* ČVUT Praha, 2015.

[3] C. Frougny, E. Pelantova, and M. Svobodová. Parallel addition in non-standard numeration systems. *Theoretical Computer Science - TCS*, 412, 02 2011.

[4] S. Hajduk. GitHub repository. `https://github.com/StefanHajduk/BachelorThesis`, 2020.

[5] E. Isaacson and H. Keller. *Analysis of Numerical Methods.* Dover Books on Mathematics. Dover Publications, 1994.

[6] J. Jankauskas and J. Thuswaldner. Characterization of rational matrices that admit finite digit representations. *Linear Algebra and its Applications*, 557:350 – 358, 2018.

[7] A. Kovács. *Radix expansion in lattices.* PhD thesis, Eötvös Loránd University, 2001.

[8] M. Lothaire. *Algebraic Combinatorics on Words.* Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2002.

[9] W. Penney. A "binary" system for complex numbers. *J. ACM*, 12(2):247–248, 1965.

[10] M. Svobodová. *konzultace*, 2020.

[11] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.0)*, 2020. `https://www.sagemath.org`.

[12] W. P. Thurston. *Groups, Tilings and Finite State Automata: Summer 1989 AMS Colloquium Lectures.* Geometry Computing Group, 1989.

[13] A. Vince. Replicating tessellations. *SIAM J. Discrete Math.*, page 6(3):501–521, 1993.