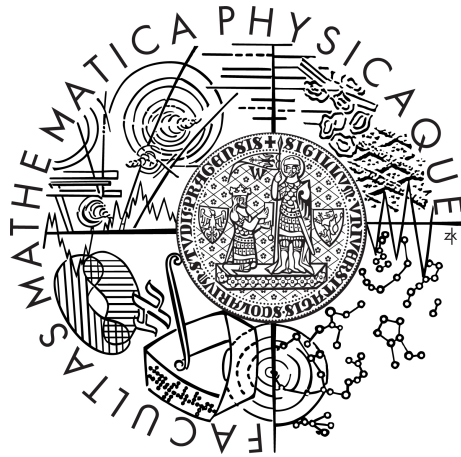


Univerzita Karlova v Praze  
Matematicko-fyzikální fakulta

## DIPLOMOVÁ PRÁCE



Gabriela Těthalová

## Kódování pozice na přímce a v rovině

Katedra algebry

Vedoucí diplomové práce: doc. RNDr. Jiří Tůma, DrSc.

Studijní program: Matematika

Studijní obor: Matematické metody informační bezpečnosti

Praha 2013

Chtěla bych poděkovat vedoucímu své diplomové práce, doc. RNDr. Jiřímu Tůmovi, DrSc., za pravidelné přínosné konzultace, cenné rady a připomínky a vstřícný přístup.

Prohlašuji, že jsem tuto diplomovou práci vypracovala samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V Praze dne 26.7.2013.

Gabriela Těthalová

Název práce: Kódování pozice na přímce a v rovině

Autor: Gabriela Těthalová

Katedra: Katedra algebry

Vedoucí diplomové práce: doc. RNDr. Jiří Tůma, DrSc., Katedra algebry

Abstrakt: Úvod do tématu kódování pozice tvoří dva příklady pozičních kódů na přímce, které využívají vyjadřování čísel v soustavě o základu 4 a De Bruijnovu posloupnost zkonstruovanou s využitím LFSR. Hlavní náplní této práce je popis dvou pozičních kódů v rovině na základě patentů společnosti Anoto. Tyto poziční kódy využívají vyjadřování čísel ve smíšené bázi a také speciální typ posloupností označovaných jako kvazi De Bruijnovy. Druhý z popisovaných pozičních kódů představuje aplikaci Čínské věty o zbytcích. Práce se věnuje konstrukci pozičních kódů, popisům dekódování a důkazům detekovatelnosti. V závěru je detailněji porovnáván princip kódování souřadnice  $y$  u obou kódů.

Klíčová slova: poziční kód, kvazi De Bruijnova posloupnost, smíšená báze, Anoto Pattern

Title: Position coding on line and plane

Author: Gabriela Těthalová

Department: Department of Algebra

Supervisor: doc. RNDr. Jiří Tůma, DrSc., Department of Algebra

Abstract: The introduction into the position coding consists of two examples of position codes on line which use the positional number system of base 4 and De Bruijn sequence constructed with the use of LFSR. The main aim of this thesis is the description of two positional codes on plane based on the patents of the Swedish company Anoto. These positional codes use mixed radix number representation and also a specific type of sequences called quasi De Bruijn sequences. The second of the described position codes represents an application of the Chinese Remainder Theorem. The thesis focuses on the position code construction, description of decoding, and the proofs of detectability. A detailed comparison of the principles of the coding of the coordinate  $y$  of both discussed codes is provided in the final part of the thesis.

Keywords: positional code, quasi De Bruijn sequence, mixed radix, Anoto Pattern

# Obsah

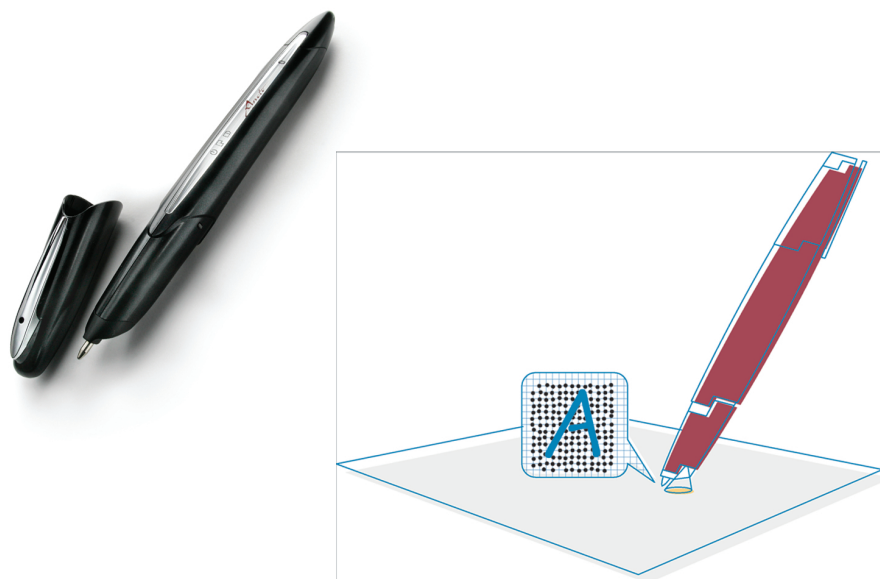
Úvod	1
<b>1 Kódování pozice na přímce</b>	<b>3</b>
1.1 Kódování pozice s využitím markerů	3
1.2 Kódování pozice s využitím De Bruijnovy posloupnosti	4
1.2.1 Konstrukce De Bruijnovy posloupnosti	5
1.2.2 Poziční kód na přímce	6
<b>2 Poziční kód na ploše</b>	<b>8</b>
2.1 Anoto Pattern: základní verze	8
2.2 Konstrukce pozičního kódu	9
2.3 Dekódování pozice	15
<b>3 Anoto Pattern: verze pro využití v praxi</b>	<b>23</b>
3.1 Kódování	23
3.2 Detekovatelnost	29
3.2.1 Konstrukce kvazi De Bruijnových posloupností	34
3.3 Poznámka o určení rotace povrchu	37
3.4 Rozšíření	38
<b>4 Srovnání se základní verzí</b>	<b>40</b>
4.1 Závěrečná diskuse	44
<b>Závěr</b>	<b>45</b>
<b>Seznam použité literatury</b>	<b>46</b>
<b>Seznam tabulek</b>	<b>47</b>

# Úvod

Nejvýznamnější motivací pro téma pozičního kódování je existující příklad využití této teorie v praxi. Švédská technologická firma Anoto vyvinula produkt nazývaný digitální pero (viz Obrázek 1), který slouží k digitalizaci ručně psaného textu. Koncept digitálního pera spočívá v kombinaci klasického pera a čtecího zařízení snímajícího část povrchu papíru, po kterém perem píšeme. Tento papír je potištěný drobnými tečkami, jejichž rozmístění je určeno matematickým předpisem, což je přesně ta komponenta vynálezu firmy Anoto, kterou se v této práci budeme zabývat.

Zatímco kódování pozice na přímce je v literatuře popisováno, např. v [5] a [2], ke kódování pozice v rovině je obtížné nalézt vhodné zdroje. Článek [1] tvoří přehled různých známých metod kódování pozice v rovině, avšak systému kódování používaného firmou Anoto se nevěnuje příliš do detailu. Informace o principu kódování byly tedy čerpány přímo z patentů této společnosti, konkrétně z [6] a [7], kde ovšem nenalezneme přesné matematické formulace, ale spíše neúplný slovní popis s příkladem dekódování. Přesně formulovat a podrobně vyložit poznatky získané z těchto patentů byl jeden z cílů této práce.

Práce je rozdělena na čtyři kapitoly. Úvod do tématu tvoří popis dvou způsobů kódování pozice na přímce. Ve druhé kapitole se začneme věnovat příkladu pozičního kódu v rovině patentovaného společností Anoto, který na případech souřadnic  $x$  a  $y$  ukazuje první dvě možné metody kódování, ale není vhodný pro praktické využití z důvodu malých rozměrů kódované plochy. Ve třetí kapitole je předvedena verze kódu Anoto, která je pro praxi vhodná a představuje zajímavou aplikaci Čínské věty o zbytcích. Metody kódování souřadnice  $y$  v případě obou těchto pozičních kódů v rovině jsou porovnány v závěru práce.



Obrázek 1: Elektronické pero a grafická podoba pozičního kódu Anoto na papíře, převzato z [8]

# 1. Kódování pozice na přímce

**Definice.** Zobrazení z množiny celočíselných bodů  $\theta : \{0, \dots, d\} \rightarrow \{0, \dots, n\}$ , kde  $d \geq n$  a  $d, n \in \mathbb{N}$ , budeme říkat *poziční kód na přímce*.

**Definice.** Řekneme, že poziční kód na přímce  $\theta$  je  $k$ -detekovatelný, jestliže pro každý celočíselný interval  $I = \{x, x+1, \dots, x+k-1\} \subseteq \{0, \dots, d\}$ , lze ze znalosti  $\theta \upharpoonright_I$  jednoznačně určit  $x$ .

Restriktci  $\theta$  na interval  $I$  z předchozí definice budeme v této kapitole říkat *okno*.

## 1.1 Kódování pozice s využitím markerů

Způsob kódování pozice na přímce s využitím markerů předvedeme na příkladu konstrukce 9-detekovatelného pozičního kódu. Nejprve uvedeme zřejmé lemma popisující zápis čísla v číselné soustavě o základu 4.

**Lemma 1.1.** Každý prvek  $d$  z množiny  $\{0, \dots, 4^8 - 1\}$  lze jednoznačně vyjádřit ve tvaru

$$d = a_0 + 4 \cdot a_1 + 4^2 \cdot a_2 + \dots + 4^7 \cdot a_7,$$

kde  $a_0, \dots, a_7 \in \{0, 1, 2, 3\}$ .

V případě potřeby, například při vyjadřování dvou po sobě jdoucích čísel ve čtyřkové soustavě, si ke koeficientům z Lemma 1.1 přidáme ještě index vyjadřovaného čísla, tzn. píšeme  $d = 4^7 a_{7,d} + \dots + 4 a_{1,d} + a_{0,d}$ .

Každé  $x \in \{0, \dots, 9 \cdot 4^8 - 1\}$  zapíšeme ve tvaru  $x = 9d + r$ , kde  $r \in \{0, \dots, 8\}$ . Zobrazení  $\theta : \{0, \dots, 9 \cdot 4^8 - 1\} \rightarrow \{0, 1, 2, 3\} \cup \{\bullet\}$  definujeme následujícím způsobem:

$$\theta(x) = \theta(9d + r) = \begin{cases} \bullet & \text{pokud } r = 0, \\ a_{8-r} & \text{jinak,} \end{cases}$$

přičemž  $a_7, \dots, a_0$  jsou koeficienty vyjádření čísla  $d$  dle Lemma 1.1, tzn.  $a_7 = a_{7,d} = \lfloor d/4^7 \rfloor$ ,  $a_6 = a_{6,d} = \lfloor (d - 4^7 \cdot a_7)/4^6 \rfloor$  atd.

Symbolu  $\bullet$  budeme říkat *marker*.

Představíme-li si osu  $x$  jako svislici, na níž nás zajímají pouze celočíselné body, přiřazuje poziční kód na přímce  $\theta$  násobkům čísla 9 marker a zbylým osmi souřadnicím pod tímto markerem přiřazuje osmici koeficientů, které jednoznačně určují jeho polohu.

**Pozorování 1.2.** Bud'  $d \in \{0, \dots, 4^8 - 2\}$  a  $i \in \{1, \dots, 7\}$ . Pro koeficienty z vyjádření čísel  $d$  a  $(d+1)$  dle Lemma 1.1 platí

$$a_{0,d+1} = a_{0,d} + 1 \pmod{4},$$
$$a_{i,d+1} = \begin{cases} a_{i,d} + 1 \pmod{4}, & \text{pokud } (d+1) = 0 \pmod{4^i}, \\ a_{i,d}, & \text{jinak.} \end{cases}$$

Na  $\theta$  můžeme pohlížet jako na 5-ární posloupnost  $\{\theta(x)\}_{x=0}^{(9 \cdot 4^8 - 1)}$ .

**Lemma 1.3.** *Ze znalosti libovolných devíti po sobě jdoucích členů posloupnosti  $\theta$ , které si označíme  $\xi_0, \dots, \xi_8$ , lze jednoznačně určit takové  $x \in \{0, \dots, 9 \cdot 4^8 - 1\}$ , že  $\xi_0 = \theta(x), \dots, \xi_8 = \theta(x + 8)$ .*

*Důkaz.* Předpokládejme, že máme k dispozici nějakou podposloupnost posloupnosti  $\theta$  délky 9, kterou jsme označili  $\xi_0, \dots, \xi_8$ . Z konstrukce  $\theta$  existuje právě jedno  $i \in \{0, \dots, 8\}$  takové, že  $\xi_i = \bullet$ , kde  $\bullet$  je marker. Pro  $i = 0$  je situace nejjednodušší, protože pak  $x = 9 \cdot (4^7 a_7 + \dots + 4a_1 + a_0)$ , kde  $a_7 = \xi_1, a_6 = \xi_2, \dots, a_0 = \xi_8$ .

Podívejme se na případ  $i > 0$ . Označme si písmenem  $d$  pořadové číslo markeru, je tedy  $d \in \{0, \dots, 4^8 - 1\}$ . Pořadové číslo markeru je hodnota, kterou při kódování vyjadřujeme ve čtyřkové soustavě. Souřadnici  $x$  tedy budeme hledat ve tvaru  $x = 9(d + 1) - i$ .

Situace vypadá tak, že členy  $\xi_0, \dots, \xi_{i-1}$  jsou rovny posledním (nejméně významným)  $i$  koeficientům z vyjádření čísla  $d$  dle Lemma 1.1, přičemž  $d$  je pozice předešlého markeru, čili  $\xi_0 = a_{i-1,d}, \dots, \xi_{i-1} = a_{0,d}$ . Na druhé straně členy  $\xi_{i+1}, \dots, \xi_8$  představují po řadě koeficienty  $a_{7,d+1}, \dots, a_{i,d+1}$ , kde  $(d + 1)$  je pozice aktuálního markeru. Ke spočítání  $(d + 1)$  stačí určit koeficienty  $a_{i-1,d}, \dots, a_{0,d}$  podle Pozorování 1.2. Z  $(d + 1)$  snadno dostaneme  $x = 9(d + 1) - i$ .  $\square$

V minulém důkazu jsme jednoznačně dekódovali souřadnici  $x$ . Označíme-li  $I = \{x, x + 1, \dots, x + 8\}$ , dostaneme z definice  $k$ -detekovatelnosti následující tvrzení, které již není třeba dokazovat.

**Tvrzení 1.4.** *Zobrazení  $\theta$  je 9-detekovatelný poziční kód na přímce.*

**Poznámka.** Analogicky k výše popsanému případu můžeme pro libovolné  $m > 1$  sestavit poziční kód na přímce využívající  $m + 1$  symbolů ( $m$  koeficientů a marker). Označme písmenem  $k$  velikost okna a předpokládejme, že v každém okně se vyskytne právě jeden marker. Aby bylo možné docílit  $k$ -detekovatelnosti, musí být proto splněna podmínka

$$(m + 1)^k \geq k \cdot m^{k-1},$$

Pro  $m = 4$  a  $k = 9$  platí

$$5^9 = 1953125 \geq 589824 = 9 \cdot 4^8,$$

**Poznámka.** Při vyjádření pozice markerů pomocí číselné soustavy o základu  $m$  lze sestavit poziční kód  $\theta : \{0, \dots, k \cdot m^{k-1} - 1\} \rightarrow \{0, \dots, m - 1\} \cup \{\bullet\}$ .

## 1.2 Kódování pozice s využitím De Bruijnovy posloupnosti

Využití De Bruijnovy posloupnosti je přímočaré řešení vedoucí ke konstrukci pozičního kódu na přímce s maximální možnou hodnotou  $d$ , která je ovšem vykoupena časově náročným dekódováním. V dalším budeme využívat následující definice:



**Definice.** Buď  $A$  abeceda,  $|A| = q, l = q^n$ . Potom  $q$ -ární posloupnost

$$a_0, a_1, \dots, a_{l-1}$$

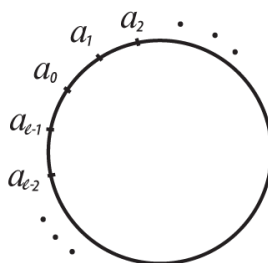
s vlastností, že se libovolná  $q$ -ární posloupnost délky  $n$  vyskytne právě jednou jako podposloupnost  $a_i, a_{i+1}, \dots, a_{i+l-1}$ , kde  $i \in \{0, \dots, l-1\}$  a v indexech sčítáme modulo  $l$ , nazveme *De Bruijnovou posloupností řádu  $n$* .

Dále budeme využívat posloupnost, jejíž název je převzatý z [1].

**Definice.** Buď  $A$  abeceda,  $|A| = q, n \leq l$ . Potom  $q$ -ární posloupnost

$$a_0, a_1, \dots, a_{l-1}$$

s vlastností, že se libovolná  $q$ -ární posloupnost délky  $n$  vyskytne nejvýše jednou jako podposloupnost  $a_i, a_{i+1}, \dots, a_{i+l-1}$ , kde  $i \in \{0, \dots, l-1\}$  a v indexech sčítáme modulo  $l$ , nazveme *kvazi De Bruijnovou posloupností řádu  $n$* .



Obrázek 1.1: Kvazi De Bruijnova posloupnost délky  $l$

**Pozorování 1.5.** Platí, že je-li  $P$  De Bruijnova posloupnost řádu  $n$ , pak je  $P$  také kvazi De Bruijnova posloupnost řádu  $n$ .

### 1.2.1 Konstrukce De Bruijnovy posloupnosti

Uvažujme, že  $q$  je prvočíslo a  $n \in \mathbb{N}$ . Konstrukci  $q$ -ární kvazi De Bruijnovy posloupnosti řádu  $n$  lze provést s využitím lineárního posuvného registru se zpětnou vazbou (LFSR).

Připomeňme některé poznatky z teorie konečných těles. Buď

$$f(x) = x^n + c_{n-1}x^{n-1} + \dots + c_1x + c_0,$$

kde  $c_0, \dots, c_{n-1} \in F_q$ , nějaký primitivní polynom nad  $F_q$ . Zvolme pevně prvních  $n$  členů  $(a_1, \dots, a_n)$  z  $F_q$ . Členy  $(a_1, \dots, a_n)$  a  $f(x)$  jednoznačně určují  $q$ -ární kvazi De Bruijnovu posloupnost řádu  $n$  a délky  $q^n - 1$ , kterou označíme  $a_1, \dots, a_{q^n-1}$ . Polynom  $f(x)$  vyjadřuje rekurzivní vztah pro členy této posloupnosti:

$$a_{n+j} = -c_{n-1}a_{n-1+j} - \dots - c_1a_{1+j} - c_0a_j \pmod{q},$$

kde  $j = 0, 1, 2, \dots$  a v indexech sčítáme modulo  $q^n - 1$ .

Polynomu  $f(x)$  se říká *charakteristický polynom* posloupnosti  $a_1, \dots, a_{q^n-1}$ . Zdůrazněme, že posloupnost  $a_1, \dots, a_{q^n-1}$  si představujeme jako cyklus, tzn. po prvku  $a_{q^n-1}$  následují prvky  $a_1, a_2, \dots$ .

**Definice.** Buď  $A = a_1, \dots, a_l$  kvazi De Bruijnova posloupnost řádu  $n$ . Každou  $n$ -tici po sobě jdoucích prvků  $A$  nazveme *stav* a označíme  $s_x = (a_x, \dots, a_{x+n-1})$ , kde  $x \in \{1, \dots, l\}$ .

Posloupnosti  $(a_1, \dots, a_n)$  z předchozí konstrukce budeme říkat počáteční stav.

**Lemma 1.6.** *Buď  $a_1, \dots, a_{q^n-1}$   $q$ -ární kvazi De Bruijnova posloupnost řádu  $n$  s počátečním stavem  $(a_1, \dots, a_n) = (0, \dots, 0, 1)$ , kterou jsme vygenerovali pomocí LFSR s využitím primitivního polynomu  $f(x)$  nad  $F_q$ . Položíme-li  $a_0 = 0$ , je posloupnost  $a_0, a_1, \dots, a_{q^n-1}$  De Bruijnova posloupnost řádu  $n$ .*

*Důkaz.* Dle definice De Bruijnovy posloupnosti je třeba dokázat, že se libovolná  $q$ -ární posloupnost délky  $n$  vyskytne právě jednou jako podposloupnost  $a_i, \dots, a_{i+q^n-1}$ , kde  $i \in \mathbb{N}_0$  a v indexech počítáme modulo  $q^n$ . S novým prvkem  $a_0 = 0$  přidáme do posloupnosti  $a_1, \dots, a_{q^n-1}$  také nové podposloupnosti  $a_{q^n-n+k}, \dots, a_{q^n-1+k}$ , kde  $k \in \{1, \dots, n\}$ . Naším úkolem bude ukázat, že se tyto nové podposloupnosti nikde v posloupnosti  $a_0, \dots, a_{q^n-1}$  neopakují. Připomeňme, že v indexech sčítáme modulo  $q^n$ .

V případě  $k = n$  víme, že posloupnost  $a_0, \dots, a_{n-1} = 0, \dots, 0$ , a tedy z důvodu konstrukce pomocí LFSR se v původní posloupnosti  $a_1, \dots, a_{q^n-1}$  nevyskytne. Uvažujme  $k \in \{1, \dots, n-1\}$  a posloupnosti  $a_{q^n-n+k}, \dots, a_{q^n-1}$ . V původní posloupnosti po každé z těchto posloupností následuje posloupnost nul délky  $n-k$ . Původní posloupnost je kvazi De Bruijnova řádu  $n$  a délky  $q^n-1$ , jinými slovy posloupnosti délky  $n$  tvaru  $a_{q^n-n+k}, \dots, a_{q^n-1}, 0, \dots, 0$  se v ní vyskytnou právě jednou. Jelikož jsme přidali prvek  $a_0 = 0$ , platí opět, že po posloupnosti  $a_{q^n-n+k}, \dots, a_{q^n-1}$  následuje  $n-k$  nulových členů, tzn. výsledná posloupnost  $a_0, \dots, a_{q^n-1}$  je skutečně De Bruijnova řádu  $n$ .  $\square$

## 1.2.2 Poziční kód na přímce

Pro porovnání s předchozí sekcí o kódování pomocí markerů uvažujme, že máme k dispozici 5 symbolů, tzn.  $q = 5$ , a  $n = 9$ . Zvolme  $f(x) = x^9 + 2x^4 + 3$ . Dle [4] je  $f(x)$  primitivní polynom nad  $F_5$ . Zvolme dále počáteční stav  $(0, 0, 0, 0, 0, 0, 0, 0, 1)$  a pomocí vztahu  $a_{9+i} = 3a_{4+i} + 2a_i \pmod{5}$  vygenerujme kvazi De Bruijnovu posloupnost  $a_1, \dots, a_{5^9-1}$  řádu 9. Přidáním členu  $a_0 = 0$  před počáteční stav obdržíme dle Lemma 1.6 De Bruijnovu posloupnost řádu 9.

Uvažujme opět, že osa  $x$  je svislice a na jejích celočíselných bodech chceme definovat poziční kód. Na základě konstrukce z předchozího odstavce definujme zobrazení

$$\begin{aligned} \chi : \{0, \dots, 5^9 - 1\} &\rightarrow \{0, 1, 2, 3, 4\} \\ x &\mapsto a_x. \end{aligned}$$

Na zobrazení  $\chi$  lze zřejmě pohlížet jako na 5-ární De Bruijnovou posloupnost  $\{\chi(x)\}_{x=0}^{5^9-1}$  řádu 9.

**Lemma 1.7.** *Ze znalosti libovolných 9 po sobě jdoucích členů posloupnosti  $\chi$ , které si označíme  $\xi_0, \dots, \xi_8$ , lze jednoznačně určit takové  $x \in \{0, \dots, 9^5 - 1\}$ , že  $\xi_0 = \chi(x), \dots, \xi_8 = \chi(x+8)$ .*

*Důkaz.* Uvažujme libovolnou podposloupnost posloupnosti  $\chi$  délky 9 a označme její členy  $\xi_0, \dots, \xi_8$ . Poziční kód  $\chi$  byl definován tak, že pro  $\xi_0, \dots, \xi_8 = 0, 0, 0, 0, 0, 0, 0, 0, 0$  dostaneme okamžitě  $x = 0$  a pro  $\xi_0, \dots, \xi_8 = 0, 0, 0, 0, 0, 0, 0, 0, 1$  obdržíme  $x = 1$ .

V ostatních případech budeme postupovat následujícím způsobem. Na  $\xi_0, \dots, \xi_8$  se budeme dívat jako na stav LFSR určeného polynomem  $f(x) = x^9 + 2x^4 + 3$ . Označme si tento stav  $s_x$  a položme  $s_1 = (0, 0, 0, 0, 0, 0, 0, 0, 1)$ . Do LFSR nejprve vložíme stav  $s_1$  a následně budeme generovat následující stavy tak dlouho, dokud se nedostaneme do stavu  $s_x$ , což je vyjádřeno v Algoritmu 1. Tento algoritmus skončí po  $k$  cyklech, kde  $k \leq (5^9 - 10)$ , jelikož  $\chi$  je De Bruijnova posloupnost. Pro hledanou souřadnici zřejmě platí  $x = k + 1$ . □

Dekódování pozičního kódu  $\chi$  ilustrujeme pomocí algoritmu, který byl naznačen v důkazu předchozího lemmatu. Označením  $s_i[j], j \in \{1, \dots, 9\}$  rozumíme prvek na  $j$ -té pozici stavu  $s_i$ .

---

**Algoritmus 1** Dekódování pozičního kódu na přímce  $\chi$

---

**vstup:**  $s_1, s \in \{0, 1, 2, 3, 4\}^9$   
**výstup:**  $x \in \{0, \dots, 5^9 - 1\}$  takové, že  $s = s_x$

```

i := 1
si := (0, 0, 0, 0, 0, 0, 0, 0, 1)
if s = (0, 0, 0, 0, 0, 0, 0, 0, 0) then
    return 0
else
    while si ≠ s do
        novy := 2si[1] + 3si[5] (mod 5)
        pomocny := si
        i := i + 1
        for j = 1 → 8 do
            si[j] := pomocny[j + 1]
        end for
        si[9] := novy
    end while
    return i
end if

```

---

Díky předchozímu lemmatu můžeme již bez důkazu uvést následující tvrzení.

**Tvrzení 1.8.** *Zobrazení  $\chi$  je 9-detekovatelný poziční kód na přímce.*

**Poznámka.** Dle [3] trvá výpočet nového 16 bitového stavu binárního LFSR pomocí běžně dostupné čipové karty Mifare 9,44  $\mu s$ . Budeme-li předpokládat, že výpočet nového stavu v Algoritmu 1 trvá přibližně stejnou dobu, bude trvat dekodování pozice pozičního kódu na přímce  $\chi$  v nejhorším případě přibližně 18 s, tzn. v průměru zhruba 9 s, což je velmi dlouhá doba. Poziční kód  $\chi$  tedy není příliš vhodný pro praktické využití.

## 2. Poziční kód na ploše

Uvažujme soustavu souřadnic v rovině  $\mathbb{R}^2$  s počátkem v bodě  $(0, 0)$  a celočíselné body v obdélníku o vrcholech  $(0, 0)$ ,  $(d, 0)$ ,  $(d, s)$  a  $(0, s)$  pro nějaká předem daná přirozená čísla  $d$  a  $s$ .

**Definice.** Zobrazení z množiny celočíselných bodů  $\phi : \{0, \dots, d\} \times \{0, \dots, s\} \rightarrow \{0, 1\}^2$  se nazývá *poziční kód*.

**Definice.** Buď  $k > 0$ . Pro všechna  $(x, y) \in \{0, \dots, d - k + 1\} \times \{0, \dots, s - k + 1\}$  definujeme *k-okno* v bodě  $(x, y)$  jako množinu

$$D_{x,y}^{(k)} = \{(x + i, y + j) \in \mathbb{N}_0 \times \mathbb{N}_0 \mid 0 \leq i, j \leq k - 1\}.$$

Budeme pracovat s pozičními kódy, které umožňují jednoznačně určit souřadnice bodů v *k-okně* ze znalosti jeho obrazu. Tuto důležitou vlastnost popisuje následující definice.

**Definice.** Poziční kód  $\phi$  je *k-detekovatelný*, pokud pro všechna  $D_{x,y}^{(k)} \subseteq \{0, \dots, d\} \times \{0, \dots, s\}$  lze ze znalosti  $\phi \upharpoonright_{D_{x,y}^{(k)}}$  jednoznačně určit  $(x, y)$ .

Následující definice navazuje na definici kvazi De Bruijnovy posloupnosti z předchozí kapitoly. Kvazi De Bruijnovu posloupnost arity  $q$ , řádu  $n$  a délky  $l$  budeme značit  $Q(q, n, l)$ .

**Definice.** Uvažujme kvazi De Bruijnovu posloupnost  $a_0, \dots, a_{l-1}$ . Posloupnost  $a_i, a_{i+1}, \dots, a_{i+l-1}$ , kde sčítáme indexy modulo  $l$ , nazveme *i-tým posunutím* posloupnosti  $a_0, \dots, a_{l-1}$ . Indexu  $i$  budeme říkat *poziční číslo*.

Je zřejmé, že *i-té* posunutí kvazi De Bruijnovy posloupnosti  $Q(q, n, l)$  je opět kvazi De Bruijnova posloupnost. Poziční číslo pro nás bude důležité při kódování a dekódování.

**Pozorování 2.1.** Z definice kvazi De Bruijnovy posloupnosti je vidět, že poziční číslo  $i$  je jednoznačně určeno prvými  $n$  členy *i-tého* posunutí.

Výše uvedené definice nyní ilustrujeme na pozičním kódu patentovaném v [6]. Tento příklad slouží k popsání dvou způsobů kódování využitých pro kódování souřadnic  $x$  a  $y$ .

### 2.1 Anoto Pattern: základní verze

V této sekci popíšeme poziční kód, jehož vlastnosti a postup při dekódování jsou naznačeny v [6], patentu firmy Anoto. Konstrukce pozičního kódu je v tomto patentu založena na kvazi De Bruijnových posloupnostech, přičemž uvedený příklad využívá posloupnost  $Q(2, 4, 7)$ . Při volbě obvyklé (dle [6]) jednotkové vzdálenosti  $300\mu\text{m}$  bychom, jak později uvidíme, dokázali zakódovat plochu obdélníku o rozměrech  $28,8\text{mm} \times 299,7\text{mm}$ . Tento rozměr je pro praktické využití zjevně nevhodný.

Představme si nyní, že v soustavě souřadnic v rovině  $\mathbb{R}^2$  s počátkem v bodě  $(0, 0)$  je osa  $x$  orientována svisle s hodnotami narůstajícími směrem dolů, zatímco na k ní kolmé vodorovné ose  $y$  se hodnoty zvyšují ve směru zleva doprava.

Položme  $d = 999$ ,  $s = 96$  a  $k = 4$ . Pro přehlednost označme  $\mathbb{O} = \{0, \dots, 999\} \times \{0, \dots, 96\}$ . V následujících odstavcích se tudíž budeme věnovat konstrukci 4-detekovatelného pozičního kódu  $\phi : \mathbb{O} \rightarrow \{0, 1\}^2$ . Pro tento účel si zadefinujeme několik dalších objektů. Množinu  $D_{x,y}^{(4)}$  budeme v této kapitole značit  $D_{x,y}$  a nazývat *okno*.

**Definice.** Množinám

$$O_{m,n} = \{(4m + i, 3n + j) \mid (m, n) \in \{0, \dots, 249\} \times \{0, \dots, 31\}, 0 \leq i, j \leq 3\}$$

budeme říkat *speciální okna*.

Uvědomme si, že  $O_{m,n} = D_{4m,3n}$ . Z celočíselných bodů  $\mathbb{O}$  lze vytvořit  $1000 \cdot 96/12 = 8000$  různých speciálních oken, přičemž každá dvě sousední speciální okna  $O_{m,n}$  a  $O_{m,n+1}$  ve vodorovném směru  $y$  mají netriviální průnik, jímž je množina  $\{(4m + i, 3(n + 1)) \mid 0 \leq i \leq 3\}$ .

## 2.2 Konstrukce pozičního kódu

Posiční kód  $\phi$  je v patentu [6] konstruován pomocí následující binární kvazi De Bruijnovy posloupnosti  $Q(2, 4, 7)$ :

$$0, 0, 0, 1, 0, 1, 0.$$

Označme si ji písmenem  $P$  a její členy postupně jako  $a_0, \dots, a_6$ .

Uvažujme bod  $(x, y) \in \{0, \dots, 999\} \times \{0, \dots, 96\}$ . Jeho hodnotu  $\phi(x, y)$  budeme hledat ve tvaru

$$\phi(x, y) = (a_{\alpha(x)+y}, a_{\beta(y)+x}),$$

kde v indexech sčítáme modulo 7 a  $\beta$  a  $\alpha$  jsou vhodně zvolená zobrazení, která postupně souřadnicím  $x$  a  $y$  přiřazují poziční čísla:

$$\alpha : \{0, \dots, 999\} \rightarrow \{0, \dots, 6\},$$

$$\beta : \{0, \dots, 96\} \rightarrow \{0, \dots, 6\}.$$

**Definice.** Posloupnost pozičních čísel  $\{\alpha(x)\}_{x=0}^d$  nazveme *startovní posloupností ve směru  $x$*  a posloupnosti pozičních čísel  $\{\beta(y)\}_{y=0}^s$  budeme říkat *startovní posloupnost ve směru  $y$* .

Vyjádření, ve kterém hledáme hodnotu bodu  $(x, y)$  při zobrazení  $\phi$  poukazuje na podobu budovaného pozičního kódu. Kód  $\phi$  si můžeme představit jako postupné zapisování  $\beta(y)$ -tého posunutí posloupnosti  $P$  opakovaně za sebou do sloupců o délce  $s + 1 = 1000$  a podobně i  $\alpha(x)$ -tého posunutí posloupnosti  $P$  do řádků délky  $d + 1 = 97$ . Získáme tak matici  $M = (m_{xy})$  nad  $\mathbb{Z}_2^2$  o rozměrech  $1000 \times 97$ ,  $m_{xy} = \phi(x, y) = (a_{\alpha(x)+y}, a_{\beta(y)+x})$ , kde  $x$  a  $y$  počítáme od nuly. Vidíme, že pro nějaké pevné  $(x, y)$  není  $\phi \upharpoonright_{D_{x,y}}$  nic jiného než čtvercová podmatice matice  $M$

o rozměrech  $4 \times 4$ , tzn.  $\phi \upharpoonright_{D_{x,y}} = R = (r_{kl})$ ,  $r_{kl} = \phi(x+k, y+l)$ ,  $0 \leq k, l \leq 3$ .

Pro začátek poznamenejme, že budeme využívat vyjádření  $x = 4m + q$ ,  $q \in \{0, 1, 2, 3\}$ , které nám říká, že bod  $(x, y)$  leží v  $m$ -tém speciálním okně ve svislém směru  $x$ . Celkový počet speciálních oken ve směru  $x$  je  $1000/4 = 250$ . Obdobně vyjádření  $y = 3n + r$ ,  $r \in \{0, 1, 2\}$ , indikuje  $n$ -té speciální okno ve vodorovném směru  $y$ , jejichž celkový počet je  $(97 - 1)/3 = 32$ .

Věnujme se nyní konstrukci zobrazení  $\beta$ . Do startovní posloupnosti  $\beta$  chceme vložit informaci o souřadnici  $y$  bodu  $(x, y)$ . Konkrétně bude  $\beta$  vyjadřovat, v jakém speciálním okně  $O_{\bullet, n}$  bod  $(x, y)$  leží a na kterém místě (ze čtyř možných) se v rámci tohoto okna nachází ( $r$ ). K prvnímu využijeme následující zřejmé lemma.

**Lemma 2.2.** *Každý prvek  $n \in \{0, \dots, 31\}$  lze jednoznačně vyjádřit ve tvaru*

$$n = b_2 \cdot 8 + b_1 \cdot 2 + b_0 \cdot 1,$$

kde  $b_0 \in \{0, 1\}$  a  $b_1, b_2 \in \{0, 1, 2, 3\}$ .

**Poznámka.** Vyjádření z Lemmatu 2.2 se také nazývá zápisem ve smíšené bázi  $\{8, 2, 1\}$ .

Pro další použití si ke koeficientům z Lemmatu 2.2 přidáme ještě index označující vyjadřovaný prvek, čili pro  $n \in \{0, \dots, 31\}$  budeme psát  $n = 8b_{2,n} + 2b_{1,n} + b_{0,n}$ . Tento zápis je nezbytný pro vyjádření vztahů mezi koeficienty pro různá  $n$ .

**Lemma 2.3.** *Nechť  $n = 8b_{2,n} + 2b_{1,n} + b_{0,n}$ ,  $n \in \{0, \dots, 31\}$  je zápis ve smíšené bázi  $\{8, 2, 1\}$  dle Lemma 2.2. Potom platí*

$$\begin{aligned} b_{0,n+1} &= b_{0,n} + 1 && (\text{mod } 2), \\ b_{1,n+1} &= b_{0,n} + b_{1,n} && (\text{mod } 4). \end{aligned}$$

*Důkaz.* Koeficient  $b_{0,n}$  vyjadřuje, zda-li je  $n$  sudé nebo liché číslo. Pro  $n+1$  tedy dostaneme  $b_{0,n+1} = b_{0,n} + 1 \pmod{2}$ .

Pro  $n \in \{0, \dots, 30\}$  platí  $n+1 = 8b_{2,n} + 2b_{1,n} + b_{0,n} + 1 = 8b_{2,n+1} + 2b_{1,n+1} + b_{0,n+1}$ . Je-li  $b_{0,n} = 0$ , pak z prvního dokazovaného vztahu dostaneme  $b_{0,n+1} = 1$ , a tedy  $8b_{2,n} + 2b_{1,n} = 8b_{2,n+1} + 2b_{1,n+1}$ , tzn.  $b_{1,n} = b_{1,n} + b_{0,n} = b_{1,n+1} \pmod{4}$ .

Je-li  $b_{0,n} = 1$ , pak  $b_{0,n+1} = 0$  a  $8b_{2,n} + 2b_{1,n} + 2 = 8b_{2,n+1} + 2b_{1,n+1}$ , tzn.  $b_{1,n} + 1 = b_{1,n} + b_{0,n} = b_{1,n+1} \pmod{4}$ .  $\square$

Kódování pozice je ve vodorovném směru  $y$  realizováno pomocí rozdílů sousedních pozičních čísel tvořících startovní posloupnost  $\beta$ , kterou definujeme následovně.

Buď  $n \in \{0, \dots, 31\}$  a  $n = 8b_{2,n} + 2b_{1,n} + b_{0,n}$  vyjádření z Lemmatu 2.2. Zvolme  $\beta(0)$  libovolně z  $\{0, \dots, 6\}$ . Známe-li  $\beta(3n)$ , definujeme

$$\begin{aligned} \beta(3n+1) &= \beta(3n) + b_{2,n} + 3 && (\text{mod } 7), \\ \beta(3n+2) &= \beta(3n+1) + b_{1,n} + 3 && (\text{mod } 7), \\ \beta(3n+3) &= \beta(3n+2) + b_{0,n} + 1 && (\text{mod } 7). \end{aligned}$$

Označme si

$$\begin{aligned} \delta_{2,n} &= \beta(3n+1) - \beta(3n) = b_{2,n} + 3 && (\text{mod } 7), \\ \delta_{1,n} &= \beta(3n+2) - \beta(3n+1) = b_{1,n} + 3 && (\text{mod } 7), \\ \delta_{0,n} &= \beta(3n+3) - \beta(3n+2) = b_{0,n} + 1 && (\text{mod } 7). \end{aligned}$$

**Pozorování 2.4.** Pro všechna  $n \in \{0, \dots, 31\}$  platí

$$3 \leq \delta_{2,n} \leq 6,$$

$$3 \leq \delta_{1,n} \leq 6,$$

$$1 \leq \delta_{0,n} \leq 2.$$

Konstanty 3, 3, 1 si pro přehlednost pojmenujme po řadě  $\Delta_2, \Delta_1, \Delta_0$ .

**Pozorování 2.5.**  $\Delta_2 + \Delta_1 + \Delta_0 = 0 \pmod{7}$ .

Je dobré si v tuto chvíli uvědomit, že při dekódování budeme mít k dispozici čtvercovou matici  $R = \phi \upharpoonright_{D_{x,y}}$ . Položíme-li  $m = \lfloor x/4 \rfloor$  a  $n = \lfloor y/3 \rfloor$ , bude rovnost  $D_{x,y} = O_{4m,3n}$  platit pouze v 1/12 případech.

Omezíme-li se v této představě na souřadnici  $y$ , bude platit  $y = 3n$  jen pro 1/3 případů. Pro určení posunutí  $R$  vzhledem k  $\phi \upharpoonright_{O_{\bullet,n}}$  ve vodorovném směru  $y$  je tedy žádoucí odlišit jeden ze tří rozdílů pozičních čísel od ostatních. Z Pozorování 2.4 je vidět, že je tento požadavek splněn.

**Lemma 2.6.** Pro všechna  $y \in \{0, \dots, 96\}$  platí

$$\beta(y) = \beta(3n + r) = \beta(3n) + \sum_{i=0}^{r-1} (b_{2-i,n} + \Delta_{2-i}) \pmod{7},$$

kde

$$\beta(3n) = \beta(0) + \sum_{j=0}^{n-1} (b_{0,j} + b_{1,j} + b_{2,j}) \pmod{7}.$$

*Důkaz.* Výpočty budeme provádět v  $\mathbb{Z}_7$  a budeme postupovat indukcí podle  $n$ . Z definice zobrazení  $\beta$  pro  $n = 0$  a  $n = 1$  plyne

$$\begin{aligned} \beta(1) &= \beta(0) + b_{2,0} + \Delta_2, \\ \beta(2) &= \beta(1) + b_{1,0} + \Delta_1 = \beta(0) + b_{2,0} + \Delta_2 + b_{1,0} + \Delta_1 \\ &= \beta(0) + \sum_{i=0}^1 (b_{2-i,0} + \Delta_{2-i}), \\ \beta(3) &= \beta(2) + b_{0,0} + \Delta_0 = \beta(0) + \sum_{i=0}^2 b_{2-i,0} + \sum_{i=0}^2 \Delta_{2-i} \\ &= \beta(0) + b_{0,0} + b_{1,0} + b_{2,0}. \end{aligned}$$

Zvolíme indukční předpoklad, že pro  $n \geq 0$  platí

$$\begin{aligned} \beta(3n) &= \beta(0) + \sum_{j=0}^{n-1} (b_{0,j} + b_{1,j} + b_{2,j}), \\ \beta(3n + 1) &= \beta(3n) + b_{2,n} + \Delta_2, \\ \beta(3n + 2) &= \beta(3n) + \sum_{i=0}^1 (b_{2-i,n} + \Delta_{2-i}). \end{aligned}$$

Ověřme nyní dokazované rovnosti pro  $n+1$ . S využitím definice  $\beta$  a indukčního předpokladu dostaneme

$$\begin{aligned}
\beta(3(n+1)) &= \beta(3n+2) + b_{0,n} + \Delta_0 = \beta(3n+1) + b_{1,n} + \Delta_1 + b_{0,n} + \Delta_0 \\
&= \beta(3n) + b_{2,n} + \Delta_2 + b_{1,n} + \Delta_1 + b_{0,n} + \Delta_0 \\
&= \beta(0) + \sum_{j=0}^{n-1} (b_{0,j} + b_{1,j} + b_{2,j}) + b_{0,n} + b_{1,n} + b_{2,n} \\
&= \beta(0) + \sum_{j=0}^n (b_{0,j} + b_{1,j} + b_{2,j}), \\
\beta(3(n+1)+1) &= \beta(3(n+1)) + b_{2,n+1} + \Delta_2, \\
\beta(3(n+1)+2) &= \beta(3(n+1)+1) + b_{1,n+1} + \Delta_1 \\
&= \beta(3(n+1)) + \sum_{i=0}^1 (b_{2-i,n+1} + \Delta_{2-i}).
\end{aligned}$$

□

Ke konstrukci pozičního kódu nám ještě zbývá definovat zobrazení  $\alpha$ . Výše bylo zmíněno, že ve svislém směru  $x$  disponujeme 250 speciálními okny. Zřejmě platí:

**Lemma 2.7.** *Každý prvek  $m \in \{0, \dots, 249\}$  lze jednoznačně vyjádřit ve tvaru*

$$m = c_3 \cdot 50 + c_2 \cdot 10 + c_1 \cdot 2 + c_0 \cdot 1,$$

kde  $c_0 \in \{0, 1\}$  a  $c_1, c_2, c_3 \in \{0, 1, 2, 3, 4\}$ .

Ke koeficientům si přidáme index vyjadřovaného čísla, který umožní popsat vztahy koeficientů pro různá  $m$ .

**Lemma 2.8.** *Nechť  $m = 50c_{3,m} + 10c_{2,m} + 2c_{1,m} + c_{0,m}$ ,  $m \in \{0, \dots, 249\}$  je zápis ve smíšené bázi  $\{50, 10, 2, 1\}$  dle Lemma 2.7. Potom platí*

$$\begin{aligned}
c_{0,m+1} &= c_{0,m} + 1 && \pmod{2}, \\
c_{1,m+1} &= c_{0,m} + c_{1,m} && \pmod{5}, \\
c_{2,m+1} &= \begin{cases} c_{2,m} + 1 \pmod{5} & \text{právě tehdy, když } c_{0,m} = 1 \text{ a } c_{1,m} = 4, \\ c_{2,m} & \text{jinak.} \end{cases}
\end{aligned}$$

*Důkaz.* První dva vztahy se dokáží podobně jako Lemma 2.3.

Poslední vztah je pozorování plynoucí z vlastností vyjádření dle Lemma 2.7.

□

Buď  $m \in \{0, \dots, 249\}$  a  $m = 50c_{3,m} + 10c_{2,m} + 2c_{1,m} + c_{0,m}$  vyjádření z Lemmatu 2.7. Potom definujeme

$$\begin{aligned}
\alpha(4m) &= c_{3,m} + 2, \\
\alpha(4m+1) &= c_{2,m} + 2, \\
\alpha(4m+2) &= c_{1,m} + 2, \\
\alpha(4m+3) &= c_{0,m}.
\end{aligned}$$



Ze stejného důvodu, jaký byl popsán v případě zobrazení  $\beta$ , je i jeden z každé čtveřice po sobě jdoucích členů startovní posloupnosti ve směru  $x$  odlišen od ostatních.

**Pozorování 2.9.** *Pro zobrazení  $\alpha$  platí*

$$\alpha(4n), \alpha(4n + 1), \alpha(4n + 2) \in \{2, \dots, 6\},$$

$$\alpha(4n + 3) \in \{0, 1\}.$$

Pro další použití si označíme  $\Theta_0 = 0$  a  $\Theta_1 = \Theta_2 = \Theta_3 = 2$ .

**Lemma 2.10.** *Pro všechna  $x \in \{0, \dots, 999\}$  platí*

$$\alpha(x) = \alpha(4m + q) = c_{3-q,m} + \Theta_{3-q}.$$

*Důkaz.* Plyne z definice  $\alpha$ . □

Posloupnosti  $\alpha$  a  $\beta$  určují posunutí posloupnosti  $P$  postupně na začátcích  $x$ -tého řádku a  $y$ -tého sloupce. Z toho  $\phi(0, 0) = (a_{\alpha(0)}, a_{\beta(0)})$ . Pro pevné  $x$  se kvůli kódování první souřadnice budeme muset posunout v opakování posloupnosti  $P$  vodorovně v  $x$ -tém řádku o  $y$ . Naopak zafixujeme-li hodnotu  $y$ , bude třeba se v případě druhé souřadnice posunout svisle v  $y$ -tém sloupci ještě o  $x$  na úroveň prvního znaku  $(\beta(y) + x)$ -tého posunutí posloupnosti  $P$ . Nakonec skutečně dostaneme

$$\phi(x, y) = (a_{\alpha(x)+y}, a_{\beta(y)+x}),$$

kde v indexech sčítáme modulo 7.

**Příklad 1.** Nyní si ukážeme konstrukci pozičního kódu  $\phi$  na ploše o velikosti 64 jednotkových vzdáleností. Uvažujme, že  $x, y \in \{0, \dots, 7\}$ . Zvolme  $\beta(0) = 0$  a připomeňme, že  $\delta_{i,n} = b_{i,n} + \Delta_i$ ,  $i \in \{0, 1, 2\}$ , kde  $\Delta_2 = \Delta_1 = 3$  a  $\Delta_0 = 1$ . Pro koeficienty z vyjádření  $n = 0$  platí  $b_{2,0} = 0, b_{1,0} = 0, b_{0,0} = 0$ , pro  $n = 1$  platí  $b_{2,1} = 0, b_{1,1} = 0, b_{0,1} = 1$  a pro  $n = 2$  je  $b_{2,2} = 0, b_{1,2} = 1, b_{0,2} = 0$ , což využijeme pro výpočet hodnot startovní posloupnosti  $\beta$  v Tabulce 2.1.

$y$	$n$	$\delta_{2,n}$	$\delta_{1,n}$	$\delta_{0,n}$	$\beta(y)$
0	0	3	—	—	0
1	0	—	3	—	3
2	0	—	—	1	6
3	1	3	—	—	0
4	1	—	3	—	3
5	1	—	—	2	6
6	2	3	—	—	1
7	2	—	4	—	4

Tabulka 2.1: Startovní posloupnost ve směru  $y$

Naším cílem je sestavit matici  $F = (f_{xy})$  takovou, aby  $f_{xy} = \phi(x, y)$ . Budeme-li zapisovat posloupnost  $P$ , do sloupečků s počátečním posunutím  $\beta(y)$ , dostaneme matici druhých souřadnic  $F$ , kterou označíme jako  $F^2$ :

$$F^2 = \begin{array}{|cccccccc|} \hline 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ \hline \end{array}$$

Matici prvních souřadnic  $F$  označíme jako  $F^1$ . Pro  $m = 0$  platí  $c_{3,0} = 0, c_{2,0} = 0, c_{1,0} = 0, c_{0,0} = 0$  a pro  $m = 1$  máme  $c_{3,1} = 0, c_{2,1} = 0, c_{1,1} = 0, c_{0,1} = 1$ . Můžeme tedy psát hodnoty  $\alpha(x)$  do Tabulky 2.2.

$x$	$m$	$\alpha(x)$
0	0	2
1	0	2
2	0	2
3	0	0
4	1	2
5	1	2
6	1	2
7	1	1

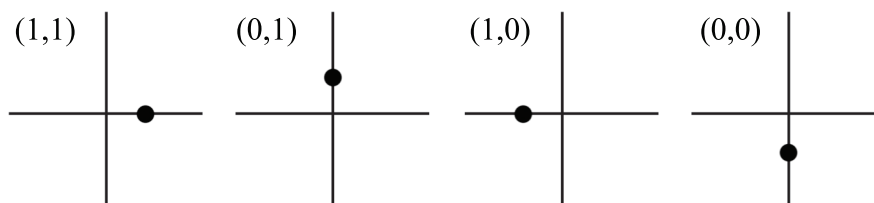
Tabulka 2.2: Startovní posloupnost ve směru  $x$

Budeme-li nyní zapisovat  $P$  do řádků s počátečním posunutím  $\alpha(x)$ , obdržíme matici  $F^1$  a následně i  $F$ :

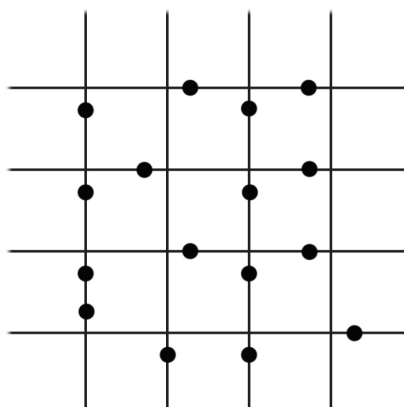
$$F^1 = \begin{array}{|cccccccc|} \hline 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ \hline \end{array}, \quad F = \begin{array}{|cccccc|} \hline (0, 0) & (1, 1) & (0, 0) & (1, 0) & (0, 1) & \dots \\ (0, 0) & (1, 0) & (0, 0) & (1, 0) & (0, 0) & \dots \\ (0, 0) & (1, 1) & (0, 0) & (1, 0) & (0, 1) & \dots \\ (0, 1) & (0, 0) & (0, 0) & (1, 1) & (0, 0) & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \\ \hline \end{array}$$

**Poznámka.** Grafická podoba pozičního kódu firmy Anoto má formu tištěných znaků – teček, které zaujmají vůči myšleným celočíselným bodům jednu ze čtyř poloh odpovídající čtyřem možným hodnotám. Z Obrázku 2.1 je patrné, že jeden znak je nositelem dvou bitů informace.

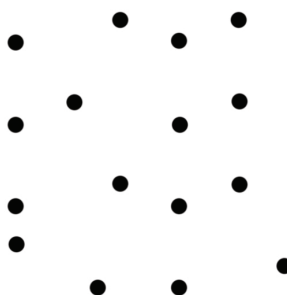
**Poznámka.** Uvažujme matici  $F = (f_{xy})$  z předchozího příkladu. Označme jako  $F'$  čtvercovou podmatici typu  $4 \times 4$  z jejího horního levého rohu. Grafická podoba matice  $F'$  je znázorněna na Obrázcích 2.2 a 2.3.



Obrázek 2.1: Grafická podoba pozičního kódu



Obrázek 2.2: Grafická podoba  $F'$  s pomocnou mřížkou



Obrázek 2.3: Grafická podoba  $F'$  bez pomocné mřížky

Na produktech firmy Anoto, což je například list papíru určený pro psaní elektronickým perem, se tiskne pouze poziční kód ve formě teček, tzn. bez mřížky jako na Obrázku 2.3. Obrázky jsou zvětšené, tzn. na reálném papíře je vzdálenost sousedních mřížkových bodů z Obrázku 2.2 pouhých  $300\mu m$ .

## 2.3 Dekódování pozice

Nyní vyložíme postup, jakým ze znalosti matice  $\phi \upharpoonright_{D_{x,y}}$  určíme  $(x,y)$ . Matici  $\phi \upharpoonright_{D_{x,y}}$ , kterou máme při dekódování k dispozici, jsme si již dříve označili  $R = (r_{kl}), r_{kl} \in \{0,1\}^2$ .

Prvky matice  $R$  jsou tedy dvojice čísel ze  $\mathbb{Z}_2$ . Pro potřeby dekodování z této matice odvodíme dvě pomocné matice  $R^1$  a  $R^2$  takovým způsobem, že matici  $R^1$  budou tvořit první souřadnice prvků  $R$  a podobně v případě matice  $R^2$  se omezíme na druhé souřadnice prvků  $R$ . Uvažujme projekce  $p_1$  a  $p_2$  z  $\{0, 1\}^2$  do  $\{0, 1\}$  takové, že  $p_1(u, v) = u$  a  $p_2(u, v) = v$ , a položme  $R^1 = (p_1(r_{kl}))$  a  $R^2 = (p_2(r_{kl}))$ . Vidíme, že matice  $R^1$  a  $R^2$  mají rovněž rozměry  $4 \times 4$ .

Při dekodování nalezneme jako první souřadnici  $y$ , a to ve známém tvaru  $y = 3n + r$ . Postup k jejímu nalezení vychází z vlastností posloupnosti  $\beta$ , respektive posloupnosti rozdílů jejich sousedních členů.

**Definice.** Posloupnosti  $\delta_{2,0}, \delta_{1,0}, \delta_{0,0}, \delta_{2,1}, \delta_{1,1}, \delta_{0,1}, \dots, \delta_{2,31}, \delta_{1,31}, \delta_{0,31}$  budeme říkat *posloupnost rozdílů* a budeme ji značit  $\mathbb{D}$ .

Také si na tomto místě připomeňme vlastnost zobrazení  $\beta$ , kterou budeme při dekodování rovněž používat.

**Pozorování 2.11.** Pro všechna  $n \in \{0, \dots, 32\}$ , kde  $n = 8b_{2,n} + 2b_{1,n} + b_{0,n}$  a  $i \in \{0, 1, 2\}$ , platí  $b_{i,n} = \delta_{i,n} - \Delta_i \pmod{7}$ .

Z Pozorování 2.4 je patrné, že jednotlivé členy posloupnosti rozdílů leží v jedné ze dvou různých množin:  $V = \{3, 4, 5, 6\}$  a  $M = \{1, 2\}$ . V posloupnosti  $\mathbb{D}$  dochází k pravidelnému střídání dvou prvků z množiny  $V$  a jednoho prvku z množiny  $M$ . Podívejme se pro ilustraci na začátek posloupnosti  $\mathbb{D}$ . Z Pozorování 2.4 dostáváme, že  $b_{2,0} \in V$ ,  $b_{1,0} \in V$  a  $b_{0,0} \in M$ , a tedy, nahradíme-li schematicky každý člen posloupnosti  $\mathbb{D}$  označením množiny, ve které se nachází, dostaneme opakování  $V, V, M, V, V, M, V, V, M, V, V, M, V, V, M, \dots$

Při zjišťování souřadnice  $y$  využijeme čtvercovou maticí  $R^2$ . Prvky  $R^2 = (r_{kl}^2)$  jsou čísla z  $\{0, 1\}$  a na její sloupce se můžeme dívat jako na posloupnosti z  $\{0, 1\}^4$ , jež si označíme následujícím způsobem:

$$r_0^2 = \begin{pmatrix} r_{00}^2 \\ r_{10}^2 \\ r_{20}^2 \\ r_{30}^2 \end{pmatrix}, \quad r_1^2 = \begin{pmatrix} r_{01}^2 \\ r_{11}^2 \\ r_{21}^2 \\ r_{31}^2 \end{pmatrix}, \quad r_2^2 = \begin{pmatrix} r_{02}^2 \\ r_{12}^2 \\ r_{22}^2 \\ r_{32}^2 \end{pmatrix}, \quad r_3^2 = \begin{pmatrix} r_{03}^2 \\ r_{13}^2 \\ r_{23}^2 \\ r_{33}^2 \end{pmatrix}$$

Jelikož  $n = 4$  (uvažujeme  $n$  z definice kvazi De Bruijnovy posloupnosti), tak díky způsobu, jakým jsme zkonstruovali poziční kód, a Pozorování 2.1, každá z těchto posloupností jednoznačně určuje nějaké poziční číslo. K jeho určení nám poslouží Tabulka 2.3, ve které jsme si očíslovali podposloupnosti délky čtyři tak, jak jdou za sebou v posloupnosti  $a_0, a_1, \dots, a_6, a_0, a_1, a_2$ , kde  $a_0, \dots, a_6 = P$ . Toto očíslování jsme vyjádřili bijekcí

$$\varphi : \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right\} \rightarrow \{0, \dots, 6\}.$$

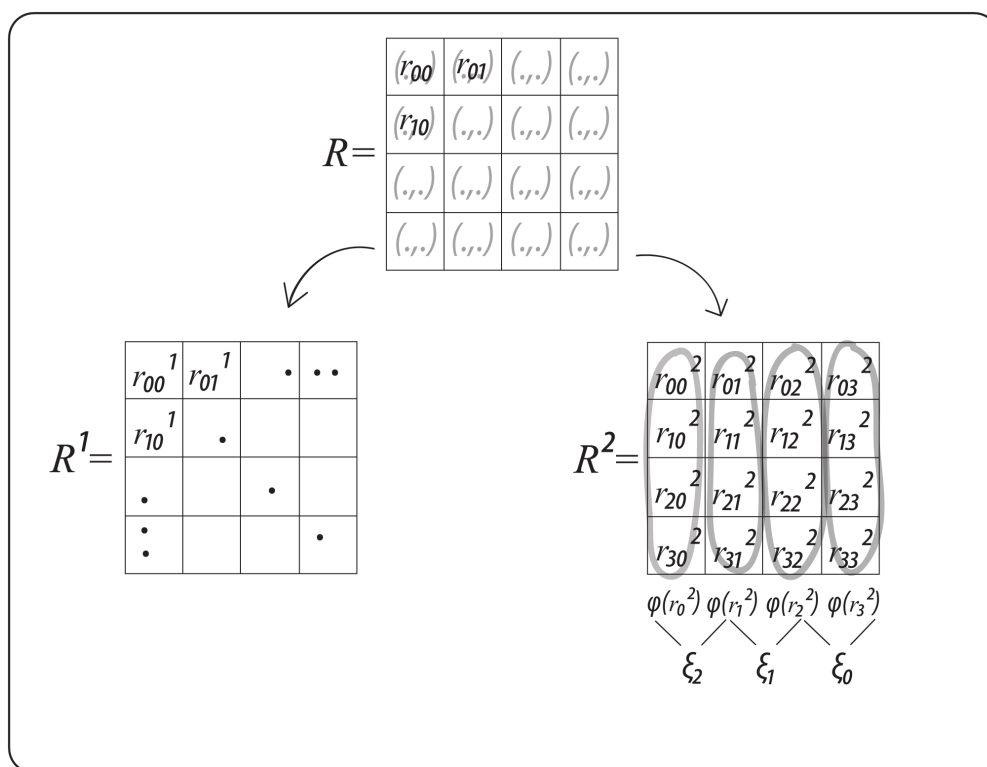
Označíme si nyní

$$\begin{aligned} \xi_2 &= \varphi(r_1^2) - \varphi(r_0^2) \pmod{7}, \\ \xi_1 &= \varphi(r_2^2) - \varphi(r_1^2) \pmod{7}, \\ \xi_0 &= \varphi(r_3^2) - \varphi(r_2^2) \pmod{7}. \end{aligned}$$

Posloupnost $r_i$	Poziční číslo $\varphi(r_i)$
0001	0
0010	1
0101	2
1010	3
0100	4
1000	5
0000	6

Tabulka 2.3: Hodnoty zobrazení  $\varphi$

Situace vypadá jako na Obrázku 2.4.



Obrázek 2.4: Schéma dekódování souřadnice  $y$

Získali jsme tři rozdíly pozičních čísel  $\xi_2, \xi_1, \xi_0$ . Z konstrukce zobrazení  $\beta$  plyne, že  $(\xi_2, \xi_1, \xi_0)$  je podposloupnost posloupnosti rozdílů  $\mathbb{D}$ . Otázkou je, jakým členům posloupnosti rozdílů se prvky této podposloupnosti rovnají. Výše jsme diskutovali o vlastnostech posloupnosti  $\mathbb{D}$ , a tedy víme, že každá trojice po sobě jdoucích členů  $\mathbb{D}$  se skládá z dvou prvků množiny  $V$  a jednoho prvku z množiny  $M$ , které jsou uspořádány v pořadí  $VVM$ ,  $VMV$  nebo  $MVV$ . O tom, který z uvedených třech případů nastane, zřejmě rozhoduje náležení jednoho z prvků trojice  $\xi_2, \xi_1, \xi_0$  do množiny  $M = \{1, 2\}$ .

Pokud  $\xi_0 \in M$ , nastává situace  $VVM$ . V tomto případě z úvah výše vyplývá existence čísla  $n \in \{0, \dots, 31\}$  takového, že  $\xi_0 = \delta_{0,n}$ ,  $\xi_1 = \delta_{1,n}$ ,  $\xi_2 = \delta_{2,n}$ . Jinými

slovy z důvodu nulového posunutí matice  $R$  ve vodorovném směru  $y$  vůči matici  $\phi \downarrow_{O_{\bullet,n}}$  je  $r = 0$ , a tedy  $y = 3n$ . S pomocí Pozorování 2.11 určíme koeficienty  $b_{i,n}$ ,  $i \in \{0, 1, 2\}$ , a  $n$  snadno dopočítáme z vyjádření  $n = 8b_{2,n} + 2b_{1,n} + b_0$ . Uvědomme si, že v dalších dvou případech zaznamenáme posunutí vůči této ideální situaci, čili  $r > 0$ , a koeficienty získané z rozdílů  $\xi_2, \xi_1, \xi_0$  budou částečně příslušet  $n$  a  $n + 1$ . Podívejme se na tyto zbývající možnosti podrobněji.

V případě, že  $\xi_1 \in \{1, 2\}$ , nastává možnost  $VMV$  a existuje takové  $n$  z  $\{0, \dots, 31\}$ , že  $\xi_2 = \delta_{1,n}$ ,  $\xi_1 = \delta_{0,n}$  a  $\xi_0 = \delta_{2,n+1}$ . Pro posunutí platí  $r = 1$ . Díky Pozorování 2.11 získáme koeficienty  $b_{0,n}, b_{1,n}$  a  $b_{2,n+1}$  a z Lemma 2.3 určíme zbylé koeficienty  $b_{0,n+1}, b_{1,n+1}$  potřebné k výpočtu  $n + 1$ . Z této znalosti snadno spočteme také  $y = 3n + 1$ .

Nakonec je-li  $\xi_2 \in \{1, 2\}$ , a nastává tedy poslední varianta  $MVV$ , platí pro nějaké  $n$  z  $\{0, \dots, 31\}$   $\xi_2 = \delta_{0,n}$ ,  $\xi_1 = \delta_{2,n+1}$ ,  $\xi_0 = \delta_{1,n+1}$  a posunutí  $r = 2$ . Ze znalosti  $b_{0,n}$  spočteme  $b_{0,n+1}$  pomocí Lemma 2.3 a snadno určíme  $y = 3n + 2$ .

Při dekódování souřadnice  $x$  využijeme matici  $R^1 = (r_{kl}^1)$  a znalost souřadnice  $y$ . Souřadnici  $x$  budeme hledat ve tvaru  $x = 4m + q$ . Princip dekódování bude velmi podobný, ovšem nebudeme využívat rozdíly pozičních čísel, ale pouze poziční čísla samotná. Jako v případě posloupnosti rozdílů, i startovní posloupnost ve svislém směru  $x$  se vyznačuje střídáním množin, do kterých patří její členy, v pravidelném pořadí. Označíme-li množiny  $W = \{2, \dots, 6\}$  a  $Z = \{0, 1\}$  a zaměníme člen posloupnosti  $\alpha$  za název množiny, ve které leží, dostaneme posloupnost  $W, W, W, Z, W, W, W, Z, W, W, W, Z, \dots$ .

Označme si řádky matice  $R^1$  podobně jako sloupce  $R^2$  v případě  $y$ :

$$\begin{aligned} r_0^1 &= r_{00}^1, r_{01}^1, r_{02}^1, r_{03}^1, \\ r_1^1 &= r_{10}^1, r_{11}^1, r_{10}^1, r_{13}^1, \\ r_2^1 &= r_{20}^1, r_{21}^1, r_{22}^1, r_{23}^1, \\ r_3^1 &= r_{30}^1, r_{31}^1, r_{32}^1, r_{33}^1. \end{aligned}$$

Znalost  $y$  nám pomůže při určování příslušných členů startovní posloupnosti  $\alpha$ , představuje totiž posunutí posloupnosti  $P$  zapisované opakovaně do zkoumaného řádku. Aplikujme nyní bijekci  $\varphi$  na řádky matice  $R^1$  a odečteme příslušné posunutí  $y$ . Výsledek označme

$$\nu_{3-i} = \varphi(r_i^1) - y \pmod{7}, i \in \{0, 1, 2, 3\}.$$

Uvědomme si, že  $(\nu_3, \nu_2, \nu_1, \nu_0)$  je podposloupnost startovní posloupnosti  $\alpha$ . Díky rozměrům matice  $R^1$  budeme mít vždy k dispozici čtveřici pozičních čísel, která díky výše zmíněné vlastnosti startovní posloupnosti jednoznačně určí hodnotu  $q$ .

Podobně jako u dekódování souřadnice  $y$  odpovídá  $\nu_0 \in Z$  situaci  $WWWZ$  indikující  $q = 0$ . V takovém případě tedy lze říci, že existuje  $m \in \{0, \dots, 249\}$  takové, že  $\nu_3 = \alpha(4m)$ ,  $\nu_2 = \alpha(4m + 1)$ ,  $\nu_1 = \alpha(4m + 2)$ ,  $\nu_0 = \alpha(4m + 3)$  a  $x = 4m$ . K výpočtu  $m$  využijeme vyjádření  $m = 50c_{3,m} + 10c_{2,m} + 2c_{1,m} + c_{0,m}$  pomocí koeficientů, které snadno dopočítáme s využitím následujícího důsledku Lemmatu 2.10. Pro přehlednost značení v něm budeme uvažovat vyjádření  $x = 4m + p$ .

**Pozorování 2.12.** Pro všechna  $m \in \{0, \dots, 249\}$  a  $p \in \{0, 1, 2, 3\}$  platí

$$c_{3-p,m} = \alpha(4m + p) - \Theta_{3-p} \pmod{7}.$$

Pokud  $\nu_1 \in Z$ , nacházíme se v situaci  $WWZW$ , tzn.  $q = 1$ , a existuje  $m \in \{0, \dots, 249\}$  takové, že  $\nu_3 = \alpha(4m + 1), \nu_2 = \alpha(4m + 2), \nu_1 = \alpha(4m + 3), \nu_0 = \alpha(4(m + 1))$ . Vidíme, že s pomocí Pozorování 2.12 obdržíme koeficienty  $c_{2,m}, c_{1,m}, c_{0,m}$  a  $c_{3,m+1}$ . Budeme tedy vyjadřovat číslo  $m + 1$ , k jehož výpočtu nám dopomůže Lemma 2.8. Podobně tomu bude i v posledních dvou případech. Nakonec snadno určíme  $x = 4m + 1$ .

Případ  $\nu_2 \in Z$  označíme jako  $WZWW$ . Máme  $q = 2$  a existuje  $m \in \{0, \dots, 249\}$  takové, že  $\nu_3 = \alpha(4m + 2), \nu_2 = \alpha(4m + 3), \nu_1 = \alpha(4(m + 1)), \nu_0 = \alpha(4(m + 1) + 1)$ . Zbytek je analogický k předchozímu případu a můžeme spočítat  $x = 4m + 2$ .

Nakonec je-li  $\nu_3 \in Z$ , jsme v situaci  $ZWWW$ , tzn.  $q = 3$  a existuje  $m \in \{0, \dots, 249\}$  takové, že  $\nu_3 = \alpha(4m + 3), \nu_2 = \alpha(4(m + 1)), \nu_1 = \alpha(4(m + 1) + 1), \nu_0 = \alpha(4(m + 1) + 2)$  a  $x = 4m + 3$ .

**Příklad 2.** Nyní si předvedeme dekódování souřadnic  $x$  a  $y$  na příkladu. Předpokládejme, že máme k dispozici matici

$$R = \begin{pmatrix} (1, 0) & (0, 0) & (1, 0) & (0, 0) \\ (0, 0) & (0, 0) & (0, 0) & (0, 0) \\ (0, 0) & (0, 1) & (1, 0) & (0, 0) \\ (1, 0) & (0, 0) & (1, 1) & (0, 0) \end{pmatrix}.$$

Označme si

$$R^1 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}, \quad R^2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Nejprve využijeme  $R^2$  k určení souřadnice  $y$ . Označíme

$$\begin{aligned} \xi_2 &= \varphi \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} - \varphi \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \pmod{7} = 1 - 6 \pmod{7} = 2 \pmod{7}, \\ \xi_1 &= \varphi \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} - \varphi \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \pmod{7} = 0 - 1 \pmod{7} = 6 \pmod{7}, \\ \xi_0 &= \varphi \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} - \varphi \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \pmod{7} = 6 - 0 \pmod{7} = 6 \pmod{7}. \end{aligned}$$

Vidíme, že  $\xi_2 \in \{1, 2\} = M$  a  $\xi_1, \xi_0 \in \{3, 4, 5, 6\} = V$ , a tedy jsme v situaci  $MVV$ , kde bereme v úvahu posunutí  $r = 2$ . Z konstrukce  $\phi$  víme, že pro nějaké

$n \in \{0, \dots, 31\}$  platí  $\xi_2 = \delta_{0,n} = b_{0,n} + 1$ ,  $\xi_1 = \delta_{2,n+1} = b_{2,n+1} + 3$  a  $\xi_0 = \delta_{1,n+1} = b_{1,n+1} + 3$ . Z toho dostaneme  $b_{2,n+1} = 3$ ,  $b_{1,n+1} = 3$  a  $b_{0,n} = 1$ . Z  $b_{0,n} = 1$  dopočítáme dle Lemma 2.3  $b_{0,n+1} = 1 + 1 \pmod{2} = 0 \pmod{2}$ . Nakonec  $n+1 = 8 \cdot 3 + 2 \cdot 3 + 0 = 30$  a  $y = 3n + r = 3 \cdot 29 + 2 = 89$ .

Pro dekódování souřadnice  $x$  budeme potřebovat matici  $R^1$  a znalost  $y = 89$ . Zobrazení  $\varphi$  budeme aplikovat na řádky matice  $R^1$ . Označíme si

$$\begin{aligned}\nu_3 &= \varphi(1010) - y \pmod{7} = 3 - 89 \pmod{7} = 5 \pmod{7}, \\ \nu_2 &= \varphi(0000) - y \pmod{7} = 6 - 89 \pmod{7} = 1 \pmod{7}, \\ \nu_1 &= \varphi(0010) - y \pmod{7} = 1 - 89 \pmod{7} = 3 \pmod{7}, \\ \nu_0 &= \varphi(1010) - y \pmod{7} = 3 - 89 \pmod{7} = 5 \pmod{7}.\end{aligned}$$

Vzhledem k tomu, že  $\nu_2 \in \{0, 1\} = Z$ , jsme v situaci, kterou jsme si při popisu dekódování označili jako  $WZWW$ , tzn.  $q = 2$ . Díky Pozorování 2.12 a z konstrukce pozičního kódu  $\phi$  existuje  $m \in \{0, \dots, 249\}$  takové, že  $c_{1,m} = \nu_3 - 2 = 3$ ,  $c_{0,m} = \nu_2 = 1$ ,  $c_{3,m+1} = \nu_1 - 2 = 1$  a  $c_{2,m+1} = \nu_0 - 2 = 3$ . Dle Lemma 2.8 dopočítáme  $c_{1,m+1} = c_{0,m} + c_{1,m} \pmod{5} = 1 + 3 \pmod{5} = 4 \pmod{5}$  a  $c_{0,m+1} = c_{0,m} + 1 \pmod{2} = 0 \pmod{2}$  a z toho  $m+1 = 50 \cdot 1 + 10 \cdot 3 + 2 \cdot 4 + 0 = 88$ , tzn.  $x = 4m + q = 4 \cdot 87 + 2 = 350$ . Výsledné souřadnice jsou tedy  $(x, y) = (89, 350)$ .

**Důsledek 2.13.** Ze znalosti matice  $R$  lze jednoznačně určit dvojici čísel  $(x, y)$  takovou, že  $R = \phi \upharpoonright_{D_{x,y}} = (\phi(x+i, y+j))_{0 \leq i, j \leq 3}$ .

*Důkaz.* Jednoznačnost je vidět z popisu výše nebo z Algoritmu 2. □

Z uvedeného důsledku okamžitě plyne následující důsledek:

**Důsledek 2.14.** Výše zkonstruované zobrazení  $\phi$  je 4-detekovatelný poziční kód.

Výše popsaný dekódovací algoritmus nyní uvedeme ve formě pseudokódu. Matici  $R = (r_{kl})$  budeme reprezentovat jako pole o rozměrech  $4 \times 8$ . Tuto reprezentaci označíme jako  $R^* = (r_{k^*l^*}) = (R^*[k^*, l^*])$ . Všechny prvky  $R^*$  náležejí do  $\mathbb{Z}_2$  a platí  $r_{kl} = (r_{k^*l^*}, r_{k^*(l^*+1)})$  pro každé  $0 \leq k, l \leq 3$ .

Jsou-li  $a, b$  dva řetězce bitů, budeme zápisem  $a \parallel b$  označovat operaci napojení řetězce  $b$  na konec řetězce  $a$ , tzn.  $a \parallel b = ab$ .

---

### Algoritmus 2 Dekódování souřadnic $x$ a $y$

---

**vstup:** pole  $R^*$  o rozměrech  $[0, \dots, 3] \times [0, \dots, 7]$

**výstup:** dvojice souřadnic  $(x, y)$

**function** *coefB0*( $e$ )

*coefB0* =  $e + 1 \pmod{2}$

**end function**

**function** *coefB1*( $f, g$ )

*coefB1* =  $f + g \pmod{4}$

**end function**

---



---

```

function koeffC1(f, g)
    koeffC1 = f + g (mod 5)
end function
function koeffC2(f, g, h)
    if f = 1 & g = 4 then
        koeffC2 = h + 1 (mod 5)
    else
        koeffC2 = h
    end if
end function
function vypocetN(f, g, h)
    vypocetN = 8f + 2g + h
end function
function vypocetM(e, f, g, h)
    vypocetM = 50e + 10f + 2g + h
end function

for i = 0 → 3 do
    Definuj prázdný řetězec si
    for j = 0 → 3 do si := si || R* [j, 2i + 1]
    end for
end for
for t = 0 → 2 do ξi :=  $\varphi(s_{3-t}) - \varphi(s_{2-t})$  (mod 7)
end for
if 1 ≤ ξ0 ≤ 2 then
    b2 := ξ2 - 3
    b1 := ξ1 - 3
    b0 := ξ0 - 1
    r := 0
else
    if 1 ≤ ξ1 ≤ 2 then
        b2 := ξ0 - 3
        b1 := koeffB1(ξ1 - 1, ξ2 - 3)
        b0 := koeffB0(ξ1 - 1)
        r := 1
    else
        b2 := ξ1 - 3
        b1 := ξ0 - 3
        b0 := koeffB0(ξ2 - 1)
        r := 2
    end if
end if
end if

```

---

---

```

if  $r > 0$  then  $n := \text{vypocet}N(b_2, b_1, b_0) - 1$ 
else
   $n := \text{vypocet}N(b_2, b_1, b_0)$ 
end if
 $y := 3n + r$ 

for  $u = 0 \rightarrow 3$  do
  Definuj prázdný řetězec  $r_u$ 
  for  $v = 0 \rightarrow 3$  do  $r_u := r_u \parallel R^*[2u, v]$ 
  end for
end for
for  $w = 0 \rightarrow 3$  do  $\nu_{3-w} := \varphi(r_w) - y \pmod{7}$ 
end for
if  $0 \leq \nu_0 \leq 1$  then
   $c_3 := \nu_3 - 2$ 
   $c_2 := \nu_2 - 2$ 
   $c_1 := \nu_1 - 2$ 
   $c_0 := \nu_0$ 
   $q := 0$ 
else
  if  $0 \leq \nu_1 \leq 1$  then
     $c_3 := \nu_0 - 2$ 
     $c_2 := \text{koeff}C2(\nu_1, \nu_2 - 2, \nu_3 - 2)$ 
     $c_1 := \text{koeff}C1(\nu_1, \nu_2 - 2)$ 
     $c_0 := \text{koeff}B0(\nu_1)$ 
     $q := 1$ 
  else
    if  $0 \leq \nu_2 \leq 1$  then
       $c_3 := \nu_1 - 2$ 
       $c_2 := \nu_0 - 2$ 
       $c_1 := \text{koeff}C1(\nu_2, \nu_3 - 2)$ 
       $c_0 := \text{koeff}B0(\nu_2)$ 
       $q := 2$ 
    else
       $c_3 := \nu_2 - 2$ 
       $c_2 := \nu_1 - 2$ 
       $c_1 := \nu_0 - 2$ 
       $c_0 := \text{koeff}B0(\nu_3)$ 
       $q := 3$ 
    end if
  end if
end if
if  $q > 0$  then  $m := \text{vypocet}M(c_3, c_2, c_1, c_0) - 1$ 
else
   $m := \text{vypocet}M(c_3, c_2, c_1, c_0)$ 
end if
 $x := 4m + q$ 
return  $(x, y)$ 

```

---

### 3. Anoto Pattern: verze pro využití v praxi

Nyní popíšeme poziční kód patentovaný rovněž firmou Anoto, který lze díky jeho schopnosti kódovat velké plochy pohodlně využívat v praxi. Již v [6] bylo uvedeno, že se pro reálné využití volí velikost matice představující restrikcí kódu na okno  $6 \times 6$ . Při našem zavedeném značení tedy bude naším cílem zkonstruovat 6-detekovatelný poziční kód  $\psi : \{0, \dots, d\} \times \{0, \dots, s\} \rightarrow \{0, 1\}^2$ .

V porovnání s příkladem 4-detekovatelného pozičního kódu popsáno v [6] se tato verze může díky stejnému způsobu kódování souřadnic  $x$  a  $y$  zdát jednodušší, ovšem i zde je využíván princip zapisování nějaké binární kvazi De Bruijnovy posloupnosti řádu 6 opakovaně za sebou postupně v řádcích i sloupcích s využitím nějakých startovních posloupností udávajících počáteční posunutí. Hlavní myšlenka ovšem tkví ve využití Čínské věty o zbytcích způsobem, který je naznačen při popisu dekódování v [7]. Na základě tohoto patentu a některých poznatků z [6] nyní zkonstruujeme poziční kód  $\psi$ .

Kódování souřadnic  $x$  a  $y$  bude probíhat stejným způsobem, stačí nám tedy popsat pouze případ jedné z nich, například  $y$  ve vodorovném směru (označení os zachováme stejné jako v minulé sekci z důvodu snadnějšího popisu dekódování).

V dalším budeme využívat následující verzi Čínské věty o zbytcích:

**Věta 3.1** (Čínská věta o zbytcích). *Nechť  $l_1, \dots, l_m$  jsou po dvou nesoudělná přirozená čísla. Označme  $L = \prod_{i=1}^m l_i$ . Potom zobrazení*

$$\begin{aligned} \varepsilon : \mathbb{Z}_L &\rightarrow \mathbb{Z}_{l_1} \times \dots \times \mathbb{Z}_{l_m} \\ a &\mapsto (a \pmod{l_1}, \dots, a \pmod{l_m}) \end{aligned}$$

*je izomorfismus grup.*

#### 3.1 Kódování

Nyní zkonstruujeme poziční kód popsáný v [7], nazvěme ho  $\psi$ . Dle [7] jsou dány binární kvazi De Bruijnovu posloupnost  $Q(2, 6, 63)$ , jež si označíme písmenem  $H$ :

$$\begin{aligned} H = & 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, \\ & 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1 \end{aligned}$$

a čtyři kvazi De Bruijnovy posloupnosti řádu 5, které si označíme  $D^1, \dots, D^4$ :

$$\begin{aligned} D^1 = & 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 2, 0, 1, 0, 0, 1, 0, 1, 0, 0, 2, 0, 0, 0, 1, 1, 0, 0, 0, 1, 2, 0, 0, 1, \\ & 0, 2, 0, 0, 2, 0, 2, 0, 1, 1, 0, 1, 0, 1, 1, 0, 2, 0, 1, 2, 0, 1, 0, 1, 2, 0, 2, 1, 0, 0, 1, 1, 1, 0, \\ & 1, 1, 1, 1, 0, 2, 1, 0, 1, 0, 2, 1, 1, 0, 0, 1, 2, 1, 0, 1, 1, 2, 0, 0, 0, 2, 1, 0, 2, 0, 2, 1, 1, 1, \\ & 0, 0, 2, 1, 2, 0, 1, 1, 1, 2, 0, 2, 0, 0, 1, 1, 2, 1, 0, 0, 0, 2, 2, 0, 1, 0, 2, 2, 0, 0, 1, 2, 2, 0, \\ & 2, 0, 2, 2, 1, 0, 1, 2, 1, 2, 1, 0, 2, 1, 2, 1, 1, 0, 2, 2, 1, 2, 1, 2, 0, 2, 2, 0, 2, 2, 2, 0, 1, 1, \\ & 2, 2, 1, 1, 0, 1, 2, 2, 2, 2, 1, 2, 0, 0, 2, 2, 1, 1, 2, 1, 2, 2, 1, 0, 2, 2, 2, 2, 2, 0, 2, 1, 2, 2, \\ & 2, 1, 1, 1, 2, 1, 1, 2, 0, 1, 2, 2, 1, 2, 2, 0, 1, 2, 1, 1, 1, 1, 2, 2, 2, 0, 0, 2, 1, 1, 2, 2 \end{aligned}$$

$$D^2 = 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 2, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, \\ 0, 0, 2, 0, 0, 0, 1, 2, 0, 1, 0, 1, 2, 1, 0, 0, 0, 2, 1, 1, 1, 0, 1, 1, 1, 0, 2, 1, 0, 0, 1, 2, 1, 2, \\ 1, 0, 1, 0, 2, 0, 1, 1, 0, 2, 0, 0, 1, 0, 2, 1, 2, 0, 0, 0, 2, 2, 0, 0, 1, 1, 2, 0, 2, 0, 0, 2, 0, 2, \\ 0, 1, 2, 0, 0, 2, 2, 1, 1, 0, 0, 2, 1, 0, 1, 1, 2, 1, 0, 2, 0, 2, 2, 1, 0, 0, 2, 2, 2, 1, 0, 1, 2, 2, \\ 0, 0, 2, 1, 2, 2, 1, 1, 1, 1, 1, 2, 0, 0, 1, 2, 2, 1, 2, 0, 1, 1, 1, 2, 1, 1, 2, 0, 1, 2, 1, 1, 1, 2, \\ 2, 0, 2, 2, 0, 1, 1, 2, 2, 2, 2, 1, 2, 1, 2, 2, 0, 1, 2, 2, 2, 0, 2, 0, 2, 1, 1, 2, 2, 1, 0, 2, 2, 0, \\ 2, 1, 0, 2, 1, 1, 0, 2, 2, 2, 2, 0, 1, 0, 2, 2, 1, 2, 2, 2, 1, 1, 2, 1, 2, 0, 2, 2, 2$$

$$D^3 = 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1$$

$$D^{4*} = 0, 0, 0, 0, 0, 1, 0, 2, 0, 0, 0, 0, 2, 0, 0, 2, 0, 1, 0, 0, 0, 1, 1, 2, 0, 0, 0, 1, 2, 0, 0, 2, 1, 0, \\ 0, 0, 2, 1, 1, 2, 0, 1, 0, 1, 0, 0, 1, 2, 1, 0, 0, 1, 0, 0, 2, 2, 0, 0, 0, 2, 2, 1, 0, 2, 0, 1, 1, 0, \\ 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 2, 0, 1, 1, 1, 1, 0, 0, 2, 0, 2, 0, 1, 2, 0, 2, 2, 0, 1, 0, 2, 1, 0, \\ 1, 2, 1, 1, 0, 1, 1, 1, 2, 2, 0, 0, 1, 0, 1, 2, 2, 2, 0, 0, 2, 2, 2, 0, 1, 2, 1, 2, 0, 2, 0, 0, 1, 2, \\ 2, 0, 1, 1, 2, 1, 0, 2, 1, 1, 0, 2, 0, 2, 1, 2, 0, 0, 1, 1, 0, 2, 1, 2, 1, 0, 1, 0, 2, 2, 0, 2, 1, 0, \\ 2, 2, 1, 1, 1, 2, 0, 2, 1, 1, 1, 0, 2, 2, 2, 0, 2, 0, 2, 2, 1, 2, 1, 1, 1, 1, 2, 1, 2, 1, 2, 2, 2, \\ 1, 0, 0, 2, 1, 2, 2, 1, 0, 1, 1, 2, 2, 1, 1, 2, 1, 2, 2, 2, 2, 1, 2, 0, 1, 2, 2, 1, 2, 2, 0, 2, 2, 2, \\ 1, 1$$

Vidíme, že posloupnost  $D^3$  je binární a  $D^1, D^2, D^4$  jsou ternární. Jejich délky jsou po řadě  $l_1 = 236, l_2 = 233, l_3 = 31$  a  $l_{4*} = 240$ .

**Poznámka.** Je snadné ověřit, že výše uvedené posloupnosti  $D^1, D^2, D^3$  převzaté z [7] skutečně mají deklarované vlastnosti, tzn. délky  $l_1 = 236, l_2 = 233, l_3 = 31$  a jsou kvazi De Bruijnovy řádu pět. Ve [7] se ovšem tvrdí, že délka posloupnosti  $D^{4*}$  je  $l_{4*} = 241$ , což zjevně není pravda. Pro naše potřeby do posloupnosti  $D^{4*}$  přidáme mezi pozice 80 a 81 právě jeden znak "1" a tím obdržíme posloupnost  $D^4$  s požadovanými vlastnostmi.

Vidíme, že posloupnost  $D^3$  je binární a  $D^1, D^2, D^3$  jsou ternární. Jejich délky jsou po řadě  $l_1 = 236, l_2 = 233, l_3 = 31$  a  $l_4 = 241$ . Všimněme si, že délky jsou po dvou nesoudělné.

Ke konstrukci pozičního kódu potřebujeme znát způsob, jakým budeme zapisovat posloupnost  $H$  opakovaně za sebou do sloupců. Opět tedy potřebujeme sestrojít posloupnost určující posunutí posloupnosti  $H$  na začátku každého sloupce. Označme si

$$\gamma : \{0, \dots, s\} \rightarrow \{0, \dots, 62\}.$$

**Definice.** Posloupnosti  $\{\gamma(y)\}_{y=0}^s$  budeme říkat *startovní posloupnost ve směru  $y$* .

Na začátku každého  $y$ -tého sloupce tedy budeme zapisovat  $\gamma(y)$ -té posunutí posloupnosti  $H$ .

Předpokládejme, že máme k dispozici nějakou další posloupnost  $\delta$ , kterou zapíšeme jako zobrazení

$$\delta : \{0, \dots, s-1\} \rightarrow M,$$

kde  $M = \{a, \dots, b\} \subseteq \{0, \dots, 62\}$ , pro které platí

$$\delta(y) = \gamma(y+1) - \gamma(y) \pmod{63}.$$

**Definice.** Posloupnost  $\{\delta(y)\}_{y=0}^{s-1}$  nazvěme *posloupnost rozdílů*.

Zkonstruujeme-li si v dalších odstavcích nějakou posloupnost rozdílů a zvolíme-li si hodnotu  $\gamma(0)$ , nic nám nebude bránit v sestrojení posloupnosti  $\gamma$  s využitím výše uvedeného vztahu a následně i celého pozičního kódu  $\psi$ . V tuto chvíli je podstatné, že nejprve budeme konstruovat posloupnost  $\delta$  a z ní následně odvodíme  $\gamma$ .

## Konstrukce posloupnosti rozdílů

Nejprve budeme směřovat k definici vyjádření ve smíšené bázi. První Lemma uvedeme bez důkazu, jelikož popisuje  $p$ -adický zápis čísel.

**Lemma 3.2.** Každý prvek  $\delta$  z  $\{0, \dots, p^k - 1\}$ , kde  $p \in \mathbb{P}$  a  $k \in \mathbb{N}$  lze jednoznačně vyjádřit ve tvaru

$$\delta = c_0 + p \cdot c_1 + p^2 \cdot c_2 + \dots + p^{k-1} \cdot c_{k-1},$$

kde  $c_0, \dots, c_{k-1} \in \{0, \dots, p-1\}$ .

**Lemma 3.3.** Každý prvek  $\delta$  z  $\{0, \dots, p_1^{k_1} p_2^{k_2} p_3^{k_3} - 1\}$ , kde  $p_1, p_2, p_3$  jsou (ne nutně různá) prvočísla a  $k_1, k_2, k_3 \in \mathbb{N}$ , lze jednoznačně vyjádřit ve tvaru

$$\begin{aligned} \delta = & c_0 + p_1 c_1 + \dots + p_1^{k_1-1} c_{k_1-1} + p_1^{k_1} \cdot (c_{k_1} + p_2 c_{k_1+1} + \dots + p_2^{k_2-1} c_{k_1+k_2-1}) + \\ & + p_1^{k_1} p_2^{k_2} \cdot (c_{k_1+k_2} + p_3 c_{k_1+k_2+1} + \dots + p_3^{k_3-1} c_{k_1+k_2+k_3-1}), \end{aligned}$$

kde

$$\begin{aligned} c_0, \dots, c_{k_1-1} & \in \{0, \dots, p_1 - 1\}, \\ c_{k_1}, \dots, c_{k_1+k_2-1} & \in \{0, \dots, p_2 - 1\}, \\ c_{k_1+k_2}, \dots, c_{k_1+k_2+k_3-1} & \in \{0, \dots, p_3 - 1\}. \end{aligned}$$

*Důkaz.* Označme si  $T = \{0, \dots, p_1^{k_1} - 1\}$ ,  $U = \{0, \dots, p_2^{k_2} - 1\}$  a  $V = \{0, \dots, p_3^{k_3} - 1\}$ . Dle Lemma 3.2 lze každý prvek  $t \in T$  jednoznačně vyjádřit ve tvaru

$$t = c_0 + p_1 c_1 + \dots + p_1^{k_1-1} c_{k_1-1},$$

každý prvek  $u \in U$  lze jednoznačně vyjádřit ve tvaru

$$u = c_{k_1} + p_2 c_{k_1+1} + \dots + p_2^{k_2-1} c_{k_1+k_2-1}$$

a každý prvek  $v \in V$  lze jednoznačně vyjádřit ve tvaru

$$v = c_{k_1+k_2} + p_3 c_{k_1+k_2+1} + \dots + p_3^{k_3-1} c_{k_1+k_2+k_3-1},$$

kde koeficienty  $c_i, 0 \leq i \leq k_1 + k_2 + k_3 - 1$  jsou jako ve znění dokazovaného Lemmatu.

Stačí nám tedy ukázat, že každý prvek  $\delta$  z  $\{0, \dots, p_1^{k_1} p_2^{k_2} p_3^{k_3} - 1\}$  lze jednoznačně vyjádřit ve tvaru  $\delta = t + p_1 k^1 u + p_1^{k_1} p_2^{k_2} v$ , kde  $t \in T, u \in U, v \in V$ .

Podívejme se nejprve na výraz  $t + p_1^{k_1} u$ . Tímto způsobem lze jednoznačně vyjádřit právě všechny prvky celočíselného intervalu, jehož největší prvek je roven  $p_1^{k_1} - 1 + p_1^{k_1} \cdot (p_2^{k_2} - 1) = p_1^{k_1} p_2^{k_2} - 1$ , čili  $\{0, \dots, p_1^{k_1-1}, p_1^{k_1}, \dots, p_1^{k_1} p_2^{k_2} - 1\}$ . Přidáme-li si do vyjádření prvků ještě sčítanec  $p_1^{k_1} p_2^{k_2} v$ , získáme právě všechny prvky množiny  $\{0, \dots, p_1^{k_1} p_2^{k_2} p_3^{k_3} - 1\}$ .  $\square$

**Definice.** Vyjádření čísel z  $\{0, \dots, p_1^{k_1} p_2^{k_2} p_3^{k_3} - 1\}$  dle Lemma 3.3 budeme nazývat *vyjádření ve smíšené bázi*

$$\{1, p_1, p_1^2, \dots, p_1^{k_1}, p_1^{k_1} p_2, \dots, p_1^{k_1} p_2^{k_2}, \dots, p_1^{k_1} p_2^{k_2} p_3^{k_3-1}\}.$$

Vraťme se nyní k posloupnostem  $D^1, \dots, D^4$ , které využijeme v naší konstrukci. Jak bylo zdůrazněno dříve, jejich arita je postupně 3, 3, 2, 3. Položíme-li  $p_1 = 3, p_2 = 2, p_3 = 3$  a  $k_1 = 2, k_2 = 1, k_3 = 1$ , dostaneme z Lemma 3.3, že každý prvek  $\{0, \dots, 53\}$  lze vyjádřit ve smíšené bázi  $\{1, 3, 9, 18\}$ .

Budeme chtít, aby arita posloupnosti  $\delta$  byla 54. Zkonstruujeme nyní posloupnost rozdílů  $\delta : \{0, \dots, s-1\} \rightarrow \{5 \dots, 58\}$ . Díky Lemma 3.3 platí:

**Lemma 3.4.** *Každý prvek  $\delta \in \{5, \dots, 58\}$  lze jednoznačně vyjádřit ve tvaru*

$$\delta = 5 + c_0 + c_1 \cdot 3 + c_2 \cdot 9 + c_3 \cdot 18,$$

kde  $c_2 \in \{0, 1\}$  a  $c_0, c_1, c_3 \in \{0, 1, 2\}$ .

Položme dále  $L = l_1 \cdot l_2 \cdot l_3 \cdot l_4$ , máme tedy  $L = 236 \cdot 233 \cdot 31 \cdot 241 = 410815348$ . Podle Čínské věty o zbytcích si sestrojme zobrazení  $\varepsilon$  následujícím způsobem

$$\begin{aligned} \varepsilon : \mathbb{Z}_L &\rightarrow \mathbb{Z}_{l_1} \times \mathbb{Z}_{l_2} \times \mathbb{Z}_{l_3} \times \mathbb{Z}_{l_4}, \\ a &\mapsto \begin{pmatrix} a \pmod{l_1} \\ a \pmod{l_2} \\ a \pmod{l_3} \\ a \pmod{l_4} \end{pmatrix}. \end{aligned}$$

V některých případech využijeme pro přehlednost prostorově úspornější značení  $\begin{pmatrix} a \pmod{l_1} \\ a \pmod{l_2} \\ a \pmod{l_3} \\ a \pmod{l_4} \end{pmatrix} = \begin{pmatrix} (a)_{l_1} \\ (a)_{l_2} \\ (a)_{l_3} \\ (a)_{l_4} \end{pmatrix}$ .

V případě posloupnosti  $D^1$  označme jako  $D^1[i]$  její  $i$ -tý prvek,  $i \in \{0, \dots, 235\}$ . Analogicky pro zbylé posloupnosti  $D^2, D^3, D^4$  a  $H$ .

Pro konstrukci posloupnosti rozdílů využijeme ještě další dvě zobrazení, jejichž označení a popis následuje.

Zobrazení

$$d = \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \end{pmatrix} : \mathbb{Z}_{l_1} \times \mathbb{Z}_{l_2} \times \mathbb{Z}_{l_3} \times \mathbb{Z}_{l_4} \rightarrow \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_3$$

přihadí každému prvku  $\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix}$ ,  $a_i \in \mathbb{Z}_{l_i}$ ,  $1 \leq i \leq 4$ , hodnotu  $\begin{pmatrix} D^1[a_1] \\ D^2[a_2] \\ D^3[a_3] \\ D^4[a_4] \end{pmatrix}$ , kde

$D^i[a_i]$  je  $a_i$ -tý prvek posloupnosti  $D^i$ .

Na základě Lemma 3.4 definujeme zobrazení

$$\tau : \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \rightarrow \{5, \dots, 58\},$$

$$\begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix} \mapsto 5 + b_1 + 3b_2 + 9b_3 + 18b_4.$$

Konečně pro všechna  $y \in \{0, \dots, L-1\}$  položme

$$\delta(y) = \tau(d(\varepsilon(y))), \quad (3.1)$$

čímž dostaneme posloupnost rozdílů  $\delta$ .

Ve chvíli, kdy již máme sestrojenou posloupnost rozdílů, můžeme získat také startovní posloupnost ve směru  $y$  způsobem, který jsme již dříve naznačili. Zvolme  $\gamma(0)$  libovolně z  $\{0, \dots, 62\}$ .

Pro všechna  $y \in \{0, \dots, L\}$  definujeme

$$\gamma(y) = \gamma(0) + \sum_{i=0}^{y-1} \delta(i) \pmod{63}.$$

Souřadnici  $x$  budeme kódovat naprosto stejným způsobem. Díky tomu platí rovnost  $d = s = L$  a můžeme konstrukci pozičního kódu dokončit.

**Definice.** Poziční kód  $\psi$  definujeme jako zobrazení

$$\psi : \{0, \dots, L\}^2 \rightarrow \{0, 1\}^2,$$

které každému bodu  $(x, y) \in \{0, \dots, L\}^2$  přiřadí hodnotu

$$\psi(x, y) = (H[\gamma(x) + y \pmod{63}], H[\gamma(y) + x \pmod{63}]).$$

**Příklad 3.** Nyní si předvedeme konstrukci pozičního kódu  $\psi$  pro  $x, y \in \{0, \dots, 9\}$ . Cílem tedy bude zakódovat plochu čtverce o velikosti  $10^2$  jednotkových vzdáleností. Jinými slovy, chceme sestrojiti matici  $M = (m_{xy})$  o rozměrech  $10 \times 10$  nad  $\mathbb{Z}_2^2$  tak, aby  $m_{xy} = \psi(x, y)$ . Matici prvních složek  $M$  označme  $M^1$  a matici druhých složek  $M^2$ .

Začněme se souřadnicí  $y$ . Zkonstruujeme prvních 9 členů posloupnosti  $\delta$  z vyjádření 3.1 a zvolíme  $\gamma(0) = 0$ . Následně dopočítáme  $\gamma(1), \dots, \gamma(9)$  ze vztahu  $\gamma(i+1) = \delta(i) + \gamma(i) \pmod{63}$ ,  $0 \leq i \leq 8$ . Vše zaneseme do Tabulky 3.1.

Posloupnost  $\gamma$  představuje počáteční posunutí posloupnosti  $H$  na začátku jednotlivých sloupců. Druhé složky pozičního kódu na čtverci o hraně 10 tedy tvoří

$y$	$\varepsilon(y)$	$d(\varepsilon(y))$	$\delta(y)$	$\gamma(y)$
0	(0, 0, 0, 0)	(0, 0, 0, 0)	5	0
1	(1, 1, 1, 1)	(0, 0, 0, 0)	5	5
2	(2, 2, 2, 2)	(0, 0, 0, 0)	5	10
3	(3, 3, 3, 3)	(0, 0, 0, 0)	5	15
4	(4, 4, 4, 4)	(0, 0, 0, 0)	5	20
5	(5, 5, 5, 5)	(1, 1, 1, 1)	36	25
6	(6, 6, 6, 6)	(0, 0, 0, 0)	5	61
7	(7, 7, 7, 7)	(0, 0, 0, 2)	41	3
8	(8, 8, 8, 8)	(0, 0, 1, 0)	14	44
9	-	-	-	58

Tabulka 3.1: Posloupnost rozdílů a startovní posloupnost ve směru  $y$

matici  $M^2$ , která vypadá následovně:

$$M^2 = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Souřadnici  $x$  budeme kódovat s využitím stejné posloupnosti rozdílů

$$\delta = 5, 5, 5, 5, 5, 36, 5, 41, 14,$$

ovšem nemusíme se při odvozování posloupnosti  $\gamma$  držet stejné volby  $\gamma(0)$  jako u  $y$ . Přidejme si k posloupnosti  $\gamma$  vážící se k souřadnici  $x$  pro přehlednost index 1 a zvolme  $\gamma^1(0) = 3$ . Následně obdržíme startovní posloupnost

$$\gamma^1 = 3, 8, 13, 18, 23, 28, 1, 6, 47, 61$$

a matici  $M^1$ . Kombinací prvků obou matic dostaneme na závěr výslednou matici  $M$ .

$$M^1 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \quad M = \begin{pmatrix} (0,0) & (0,0) & (0,1) \dots \\ (0,0) & (1,1) & (1,1) \dots \\ (1,0) & (0,0) & (1,1) \dots \\ \vdots & \vdots & \vdots \ddots \\ \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots \end{pmatrix}$$



**Poznámka.** Při volbě různých hodnot  $\gamma(0)$  z  $\{0, \dots, 62\}$  lze s využitím posloupnosti rozdílů  $\delta$  sestavit různé verze posloupnosti  $\gamma$ , díky které obdržíme varianty pozičního kódu  $\psi$ . Vzhledem k tomu, že souřadnici  $x$  kódujeme stejným způsobem s využitím stejné posloupnosti rozdílů  $\delta$ , můžeme získat  $63^2$  různých variant pozičního kódu  $\psi$ . Jsme tedy celkově schopni zakódovat plochu  $63^2$  čtverců o velikosti  $410815348^2$  jednotkových vzdáleností.

## 3.2 Detekovatelnost

Zobrazení  $\delta$  je definováno jako složení tří pomocných zobrazení. Shrňme si nyní jejich vlastnosti.

**Lemma 3.5.** *Zobrazení  $\tau : \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \rightarrow \{5, \dots, 58\}$  je bijekce, přičemž inverzní zobrazení  $\tau^{-1}$  přiřadí každému prvku  $u$  z množiny  $\{5, \dots, 58\}$  čtveřici*

$$\begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{pmatrix}, \text{ kde}$$

$$\begin{aligned} u_4 &= \lfloor (u - 5)/18 \rfloor \\ u_3 &= \lfloor (u - 5 - 18u_4)/9 \rfloor \\ u_2 &= \lfloor (u - 5 - 18u_4 - 9u_3)/3 \rfloor \\ u_1 &= u - 5 - 18u_4 - 9u_3 - 3u_2. \end{aligned}$$

*Důkaz.* Z Lemma 3.4 je zřejmé, že  $\tau$  je bijekce. Prvky  $u_1, \dots, u_4$  jsou určeny jednoznačně a platí  $u_4 \in \{0, 1, 2\}$ ,  $u_3 \in \{0, 1\}$ ,  $u_2 \in \{0, 1, 2\}$  a  $u_1 \in \{0, 1, 2\}$ . Tedy  $\tau^{-1}$  zobrazí  $\{5, \dots, 58\}$  na  $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ .  $\square$

**Lemma 3.6.** *Zobrazení  $d = \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \end{pmatrix} : \mathbb{Z}_{l_1} \times \mathbb{Z}_{l_2} \times \mathbb{Z}_{l_3} \times \mathbb{Z}_{l_4} \rightarrow \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_3$*

*je na, ale není prosté.*

*Důkaz.* Vzhledem k tomu, že  $l_1 = 236, l_2 = 233, l_3 = 31$  a  $l_4 = 241$ , nemůže být  $d$  prosté. Každý prvek  $\mathbb{Z}_3$  se vyskytuje v posloupnosti  $D^1$  na nějaké pozici z  $\{0, \dots, l_1 - 1\}$ , podobně pro  $D^2$  a  $D^4$ . Každý prvek  $\mathbb{Z}_2$  se nachází v posloupnosti  $D^3$  na nějaké pozici z  $\{0, \dots, l_3 - 1\}$ . Vidíme, že pro každou čtveřici prvků z  $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_3$  lze nalézt vzor, a  $d$  je tedy na.  $\square$

Důkaz následujícího lemmatu vychází z vlastností zobrazení  $\varepsilon$  a  $d$ , které slouží ke konstrukci posloupnosti  $\delta$ , již jsme vyjádřili zápisem 3.1.

**Lemma 3.7.** *Pro všechna  $y, z \in \{0, \dots, L - 1\}$  platí*

$$\begin{aligned} (y \neq z) &\Rightarrow [(d(\varepsilon(y)), d(\varepsilon(y + 1)), \dots, d(\varepsilon(y + 4))) \\ &\neq (d(\varepsilon(z)), d(\varepsilon(z + 1)), \dots, d(\varepsilon(z + 4)))]. \end{aligned}$$

*Důkaz.* Předpokládejme, že máme nějaké pevné  $y$  a  $z$  z  $\{0, \dots, L-1\}$  takové, že  $y \neq z$ . Projdeme si první dva kroky konstrukce  $\delta$ .

Platí

$$\varepsilon(y) = \begin{pmatrix} (y)_{l_1} \\ (y)_{l_2} \\ (y)_{l_3} \\ (y)_{l_4} \end{pmatrix}, \quad \varepsilon(z) = \begin{pmatrix} (z)_{l_1} \\ (z)_{l_2} \\ (z)_{l_3} \\ (z)_{l_4} \end{pmatrix}.$$

Protože  $y \neq z$ , existuje index  $i \in \{1, 2, 3, 4\}$  takový, že  $(y)_{l_i} \neq (z)_{l_i}$ . Pokračujme dále se zobrazením  $d$ , které čtveřicím prvků přiřazuje pozice v posloupnostech  $D^1, \dots, D^4$ . Označme

$$\begin{aligned} A &= (d(\varepsilon(y)), d(\varepsilon(y+1)), \dots, d(\varepsilon(y+4))) \\ &= \begin{pmatrix} D^1[(y)_{l_1}] & D^1[(y+1)_{l_1}] & \dots & D^1[(y+4)_{l_1}] \\ D^2[(y)_{l_2}] & D^2[(y+1)_{l_2}] & \dots & D^2[(y+4)_{l_2}] \\ D^3[(y)_{l_3}] & D^3[(y+1)_{l_3}] & \dots & D^3[(y+4)_{l_3}] \\ D^4[(y)_{l_4}] & D^4[(y+1)_{l_4}] & \dots & D^4[(y+4)_{l_4}] \end{pmatrix}, \end{aligned}$$

$$\begin{aligned} B &= (d(\varepsilon(z)), d(\varepsilon(z+1)), \dots, d(\varepsilon(z+4))) \\ &= \begin{pmatrix} D^1[(z)_{l_1}] & D^1[(z+1)_{l_1}] & \dots & D^1[(z+4)_{l_1}] \\ D^2[(z)_{l_2}] & D^2[(z+1)_{l_2}] & \dots & D^2[(z+4)_{l_2}] \\ D^3[(z)_{l_3}] & D^3[(z+1)_{l_3}] & \dots & D^3[(z+4)_{l_3}] \\ D^4[(z)_{l_4}] & D^4[(z+1)_{l_4}] & \dots & D^4[(z+4)_{l_4}] \end{pmatrix}. \end{aligned}$$

Každá pětice čísel představující řádek matice  $A$  tvoří podposloupnost některé z posloupností  $D^1, \dots, D^4$ , jelikož  $(y, y+1, \dots, y+4)$  jsou po sobě jdoucí čísla. Analogicky pro matici  $B$ . Posloupnosti  $D^1, \dots, D^4$  jsou kvazi De Bruijnovy řádu pět. Platí-li tedy, že  $(y)_{l_i} \neq (z)_{l_i}$ , existuje index  $j \in \{0, \dots, 4\}$  takový, že  $D^i[(y)_{l_i} + j] \neq D^i[(z)_{l_i} + j]$ .  $\square$

**Lemma 3.8.** *Zobrazení  $\varepsilon : \mathbb{Z}_L \rightarrow \mathbb{Z}_{l_1} \times \mathbb{Z}_{l_2} \times \mathbb{Z}_{l_3} \times \mathbb{Z}_{l_4}$  je izomorfismus grup. Inverzní izomorfismus  $\varepsilon^{-1} : \mathbb{Z}_{l_1} \times \mathbb{Z}_{l_2} \times \mathbb{Z}_{l_3} \times \mathbb{Z}_{l_4} \rightarrow \mathbb{Z}_L$  přiřadí každé čtveřici prvků  $(v_1, \dots, v_4)$ ,  $v_i \in \mathbb{Z}_{l_i}$ ,  $1 \leq i \leq 4$ , jednoznačně určený prvek  $p$  ze  $\mathbb{Z}_L$ , který je řešením soustavy kongruencí*

$$\begin{aligned} p &= v_1 \pmod{l_1}, \\ p &= v_2 \pmod{l_2}, \\ p &= v_3 \pmod{l_3}, \\ p &= v_4 \pmod{l_4}. \end{aligned}$$

*Důkaz.* Čísla  $l_1, \dots, l_4$  byla zvolena tak, že  $l_1 = 236, l_2 = 233, l_3 = 31$  a  $l_4 = 241$ , tzn. jsou po dvou nesoudělná. Již dříve jsme položili  $L = l_1 \cdot l_2 \cdot l_3 \cdot l_4$ . Platí tedy předpoklady Čínské věty o zbytcích 3.1.  $\square$

**Tvrzení 3.9.** *Posloupnost rozdílů  $\delta$  je 54-ární kvazi De Bruijnova posloupnost řádu pět a délky  $L$ .*

*Důkaz.* Jelikož  $\delta = \tau(d(\varepsilon))$ , je abeceda  $\delta$  rovna oboru hodnot  $\tau$ , což je množina  $\{5, \dots, 58\}$ .

Zobrazení  $\tau$  je bijekce. S využitím tohoto faktu a Lemma 3.7 dostaneme, že pro všechna  $y, z \in \{0, \dots, L-1\}$  platí: jsou-li  $(\delta(y), \dots, \delta(y+4))$  a  $(\delta(z), \dots, \delta(z+1))$  dvě podposloupnosti posloupnosti  $\delta$ , pro které je splněno  $(\delta(y), \dots, \delta(y+4)) = (\delta(z), \dots, \delta(z+1))$ , potom  $y = z$ . To znamená, že každé podposloupnosti  $\delta$  délky pět je možné přiřadit jednoznačně určené poziční číslo  $z \in \{0, \dots, L-1\}$ . Jinými slovy, každá posloupnost délky pět z abecedy  $\{5, \dots, 58\}$  se vyskytne nejvýše jednou jako podposloupnost  $\delta$ , a tedy je  $\delta$  kvazi De Bruijnova řádu pět.  $\square$

## Dekódování

Podobně jako v minulé sekci si označíme písmenem  $R$  matici, jež máme při dekódování k dispozici. Je to matice typu  $6 \times 6$ , jejíž prvky náležejí  $\mathbb{Z}_2^2$ . Budeme hledat takovou dvojici  $(x, y)$ , aby platilo, že  $R = \psi \upharpoonright_{D_{x,y}^{(6)}}$ , kde  $D_{x,y}^{(6)}$  je 6-okno v bodě  $(x, y)$ . Jinými slovy, hledané  $(x, y)$  jsou souřadnice prvku v levém horním rohu matice  $R$ .

Omezme se nyní na souřadnici  $y$ , jelikož na souřadnici  $x$  je možné aplikovat stejný postup. Budeme tudíž pracovat s maticí  $R^2 = (r_{kl}^2)$  tvořenou druhými souřadnicemi prvků  $R$ .

Označme si sloupce matice  $R^2$  následujícím způsobem:

$$r_0^2 = \begin{pmatrix} r_{00}^2 \\ r_{10}^2 \\ r_{20}^2 \\ r_{30}^2 \\ r_{40}^2 \\ r_{50}^2 \end{pmatrix}, \quad r_1^2 = \begin{pmatrix} r_{01}^2 \\ r_{11}^2 \\ r_{21}^2 \\ r_{31}^2 \\ r_{41}^2 \\ r_{51}^2 \end{pmatrix}, \quad \dots, \quad r_5^2 = \begin{pmatrix} r_{05}^2 \\ r_{15}^2 \\ r_{25}^2 \\ r_{35}^2 \\ r_{45}^2 \\ r_{55}^2 \end{pmatrix}.$$

Na podposloupnostech posloupnosti  $H$  délky 6 definujeme zobrazení

$$\omega : \left\{ \left( \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \dots, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \right) \right\} \rightarrow \{0, \dots, 62\},$$

které každé podposloupnosti délky 6 přiřadí jednoznačně určené poziční číslo.

Zobrazení  $\omega$  je zřejmě bijekce. Z konstrukce  $\psi$  víme, že sloupce  $R^2$  jsou tvořeny podposloupnostmi  $H$  délky 6, a tedy na ně lze aplikovat  $\omega$ . Označme si

$$\begin{aligned} \xi_0 &= \omega(r_1^2) - \omega(r_0^2) \pmod{63}, \\ \xi_1 &= \omega(r_2^2) - \omega(r_1^2) \pmod{63}, \\ \xi_2 &= \omega(r_3^2) - \omega(r_2^2) \pmod{63}, \\ \xi_3 &= \omega(r_4^2) - \omega(r_3^2) \pmod{63}, \\ \xi_4 &= \omega(r_5^2) - \omega(r_4^2) \pmod{63}. \end{aligned}$$

**Lemma 3.10.** *Posloupnost  $\xi_0, \dots, \xi_4$  je podposloupnost posloupnosti rozdílů  $\delta$  délky pět.*

*Důkaz.* Z konstrukce  $\psi$  plyne existence takového bodu  $(x, y)$ , že

$$\xi_i = \omega(r_{i+1}^2) - \omega(r_i^2) \pmod{63} = (\omega(r_{i+1}^2) - x) - (\omega(r_i^2) - x) \pmod{63}, \quad 0 \leq i \leq 4$$

$$\text{a } (\omega(r_0^2) - x \pmod{63}, \dots, \omega(r_5^2) - x \pmod{63}) = (\gamma(y), \gamma(y+1), \dots, \gamma(y+5)),$$

což je vyjádřením faktu, že druhá složka zobrazení  $\psi$  je tvořena zapisováním posloupnosti  $H$  do sloupců s počátečním posunutím určeným posloupností  $\gamma$ . Z toho dostaneme  $\xi_i = \gamma(y+i+1) - \gamma(y+i) = \delta(y+i)$ .  $\square$

**Lemma 3.11.** *Ze znalosti matice  $R^2$  je možné jednoznačně dekodovat souřadnici  $y$ .*

*Důkaz.* Budeme pracovat s posloupností  $\xi_0, \dots, \xi_4$ , o které z Lemma 3.10 víme, že je podposloupnost posloupnosti  $\delta$ . Aplikujme na prvky  $\xi_0, \dots, \xi_4$  zobrazení  $\tau^{-1}$  a označme si

$$C = \left( \tau^{-1}(\xi_0), \dots, \tau^{-1}(\xi_4) \right).$$

$C$  je matice typu  $4 \times 5$ . Z konstrukce kódu  $\psi$  plyne, že řádky  $C$  tvoří podposloupnosti posloupností  $D^1, \dots, D^4$  délky pět. Jelikož tyto posloupnosti jsou kvazi De Bruijnovy řádu pět, můžeme řádkům  $C$  přiřadit jednoznačně určená poziční čísla  $\nu_1, \dots, \nu_4$ . Souřadnici  $y$  poté nalezneme jako řešení soustavy

$$\begin{aligned} y &= \nu_1 \pmod{l_1}, \\ y &= \nu_2 \pmod{l_2}, \\ y &= \nu_3 \pmod{l_3}, \\ y &= \nu_4 \pmod{l_4}. \end{aligned}$$

$\square$

**Tvrzení 3.12.** *Zobrazení  $\psi$  je 6-detekovatelný poziční kód.*

*Důkaz.* Předpokládejme, že máme k dispozici libovolnou čtvercovou matici  $R$  o rozměrech  $6 \times 6$ , která je podmaticí matice  $M = (m_{rs})$  o rozměrech  $(L+1) \times (L+1)$ , jež představuje poziční kód  $\psi$ , čili

$$m_{rs} = \psi(r, s) = (H[\gamma(r) + s \pmod{63}], H[\gamma(s) + r \pmod{63}]).$$

Matici prvních souřadnic  $R$  označíme  $R^1$  a matici jejích druhých souřadnic  $R^2$ .

Z matice  $R^2$  díky Lemma 3.11 jednoznačně určíme souřadnici  $y$ . Jak bylo popsáno výše, souřadnice  $x$  byla zakódována naprosto stejným způsobem jako  $y$ . Aplikujeme-li tedy zobrazení  $\omega$  na řádky matice  $R^1$  a nadále postupujeme analogicky s případem  $R^2$ , obdržíme jednoznačně určenou hodnotu  $x$ . Nakonec tedy určíme takový bod  $(x, y)$ , že  $R = \psi \upharpoonright_{D_{xy}^{(6)}}$ .  $\square$

**Příklad 4.** Nyní ukážeme, jak ze znalosti matice  $R$  typu  $6 \times 6$  dekodujeme souřadnice  $y$  a  $x$ . Předpokládejme, že máme k dispozici matici  $R$ , ze které jsme získali matici jejích prvních souřadnic  $R^1$  a matici druhých souřadnic  $R^2$ :

$$R^1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}, \quad R^2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

Podívejme se nejprve na matici  $R^2$ . Aplikujme na její sloupce zobrazení  $\omega$  a označme:

$$\xi_0^2 = \omega \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} - \omega \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \pmod{63} = 51 - 1 \pmod{63} = 50 \pmod{63},$$

$$\xi_1^2 = \omega \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} - \omega \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} \pmod{63} = 1 - 51 \pmod{63} = 13 \pmod{63},$$

$$\xi_2^2 = \omega \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} - \omega \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \pmod{63} = 33 - 1 \pmod{63} = 32 \pmod{63},$$

$$\xi_3^2 = \omega \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} - \omega \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \pmod{63} = 28 - 33 \pmod{63} = 58 \pmod{63},$$

$$\xi_4^2 = \omega \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} - \omega \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \pmod{63} = 34 - 28 \pmod{63} = 6 \pmod{63}.$$

Dle Lemma 3.10 je posloupnost  $(50, 13, 32, 58, 6)$  podposloupnost  $\delta$ . Její délka je 5, a tedy lze jednoznačně určit její poziční číslo v posloupnosti  $\delta$ , které je rovno souřadnici  $y$ . Pro každý prvek  $\xi_i^2$ ,  $0 \leq i \leq 4$ , nyní nalezneme hodnotu při zobrazení  $\tau^{-1}$ . Výsledek zapíšeme do matice

$$(\tau^{-1}(50), \tau^{-1}(13), \tau^{-1}(32), \tau^{-1}(58), \tau^{-1}(6)) = \begin{pmatrix} 0 & 2 & 0 & 2 & 1 \\ 0 & 2 & 0 & 2 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 2 & 0 & 1 & 2 & 0 \end{pmatrix}.$$

Na řádky této matice se budeme dívat jako na posloupnosti  $(0, 2, 0, 2, 1)$ ,  $(0, 2, 0, 2, 0)$ ,  $(1, 0, 1, 1, 0)$ ,  $(2, 0, 1, 2, 0)$ , ke kterým existují jednoznačně určená poziční čísla v posloupnostech  $D^1, \dots, D^4$ . Tato poziční čísla jsou  $(95, 98, 21, 90)$ .

Pro získání souřadnice  $y$  nyní již stačí vyřešit soustavu

$$\begin{aligned} y &= 95 \pmod{236}, \\ y &= 98 \pmod{233}, \\ y &= 21 \pmod{31}, \\ y &= 90 \pmod{241}. \end{aligned}$$

Výsledek je  $y = 331$ .

Postup pro dekodování souřadnice  $x$  je podobný. Nejprve aplikujeme zobrazení  $\omega$  na řádky matice  $R^2$  a po odečtení výsledných hodnot získáme  $\xi_0^1, \xi_1^1, \xi_2^1, \xi_3^1, \xi_4^1$ , což je podposloupnost  $\delta$ . Následně postupujeme zcela analogicky a dojdeme k výsledku  $x = 37$ .

### 3.2.1 Konstrukce kvazi De Bruijnových posloupností

Vidíme, že pro konstrukci pozičního kódu  $\psi$  a k dekodování jsme z vlastností posloupností  $D^1, \dots, D^4$  využili jejich aritu, nesoudělnost délek a fakt, že jsou kvazi De Bruijnovy řádu pět. Jinými slovy, pokud bychom měli k dispozici nějakou jinou čtveřici kvazi De Bruijnových posloupností řádu pět  $E^1, \dots, E^4$  s délkami  $l_1 = 236, l_2 = 233, l_3 = 31, l_4 = 241$ , přičemž  $E^1, E^2, E^4$  by byly ternární a  $E^3$  binární, výše popsaná konstrukce a dekodování pozičního kódu  $\psi$  by zůstala nezměněná. Podívejme se, jak bychom takové ternární posloupnosti mohli sestavit zkrácením vhodné De Bruijnovy posloupnosti. Binární kvazi De Bruijnovu posloupnosti řádu pět a délky 31 lze snadno zkonstruovat s využitím LFSR způsobem popsaným v první kapitole, a tedy se její konstrukci již věnovat nebudeme.

Uvažujme polynom  $f(x) = x^5 + 2x + 1$ . Dle [4] je  $f(x)$  primitivní polynom nad  $F_3$ . Zvolme počáteční stav  $(0, 0, 0, 0, 1)$ . V první kapitole jsme popsali postup, jak můžeme pomocí LFSR vygenerovat kvazi De Bruijnovu posloupnost  $a_1, \dots, a_{242}$  řádu 5 a délky  $3^5 - 1 = 242$ . Přidáním členu  $a_0 = 0$  před počáteční stav obdržíme dle Lemma 1.6 De Bruijnovu posloupnost řádu 5, označme si ji  $B = a_0, \dots, a_{242}$ .

$$\begin{aligned} B = & 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 2, 0, 0, 1, 1, 1, 0, 1, 0, 0, 2, 1, 2, 0, 2, 2, 1, 1, 2, 0, 2, 0, 1, 1, \\ & 2, 1, 1, 0, 1, 2, 0, 2, 1, 1, 1, 2, 2, 0, 0, 1, 0, 1, 0, 1, 2, 1, 2, 1, 1, 2, 1, 2, 0, 1, 2, 1, 1, 1, \\ & 1, 2, 0, 0, 0, 1, 1, 0, 0, 1, 0, 2, 0, 1, 2, 2, 1, 1, 1, 0, 2, 0, 0, 2, 2, 1, 0, 2, 0, 2, 2, 2, 1, 2, \\ & 0, 0, 2, 1, 1, 0, 2, 2, 0, 2, 2, 0, 1, 2, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 2, 0, 0, 0, 2, 1, 0, 0, 2, 2, \\ & 2, 0, 2, 0, 0, 1, 2, 1, 0, 1, 1, 2, 2, 1, 0, 1, 0, 2, 2, 1, 2, 2, 0, 2, 1, 0, 1, 2, 2, 2, 1, 1, 0, 0, \\ & 2, 0, 2, 0, 2, 1, 2, 1, 2, 2, 1, 2, 1, 0, 2, 1, 2, 2, 2, 2, 1, 0, 0, 0, 2, 2, 0, 0, 2, 0, 1, 0, 2, 1, \\ & 1, 2, 2, 2, 0, 1, 0, 0, 1, 1, 2, 0, 1, 0, 1, 1, 1, 2, 1, 0, 0, 1, 2, 2, 0, 1, 1, 0, 1, 1, 0, 2, 1, 0, \\ & 2, 2, 2, 2, 2 \end{aligned}$$

Připomeňme, že si kvazi De Bruijnovy posloupnosti představujeme jako cyklické, tzn. jako kdyby jejich začátky a konce byly spojeny k sobě.

**Lemma 3.13.** *Bud'  $P = a_0, \dots, a_{l-1}$   $q$ -ární kvazi De Bruijnova posloupnost řádu  $n$ . Jsou-li  $a_i, a_{i+1}, \dots, a_{i+n}$  a  $a_j, a_{j+1}, \dots, a_{j+n}$ , kde  $i \neq j$ ,  $0 \leq i, j \leq l-1$ , její podposloupnosti takové, že  $a_{i+1} = a_{j+1}, a_{i+2} = a_{j+2}, \dots, a_{i+n-1} = a_{j+n-1}$ , lze posloupnost  $P$  rozdělit na dvě posloupnosti*

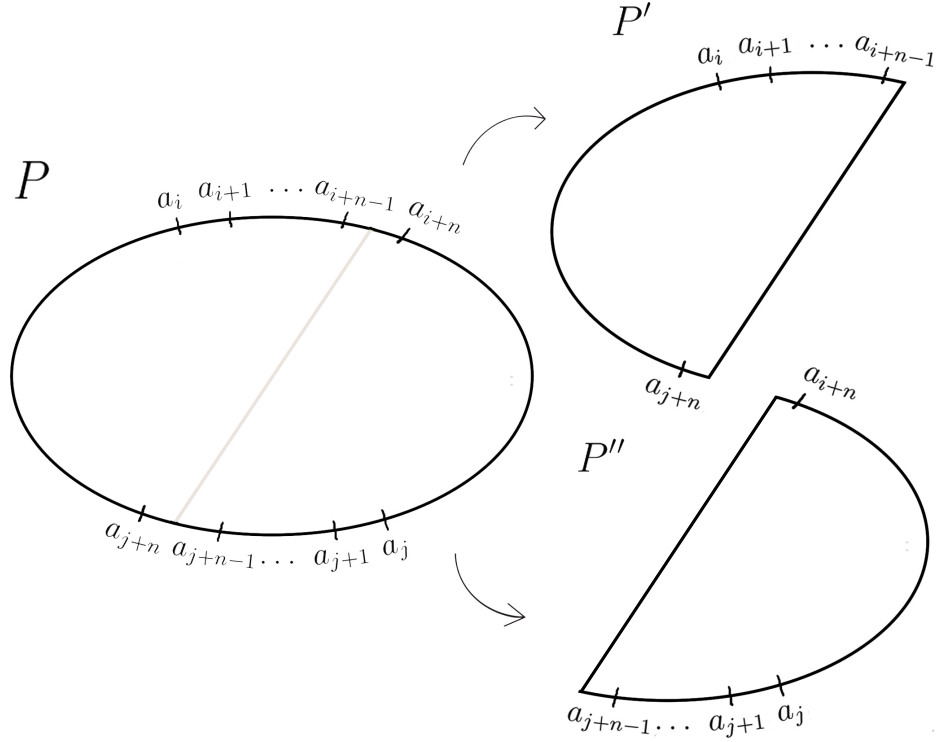
$$P' = a_i, a_{i+1}, \dots, a_{i+n-1}, a_{j+n}, a_{j+n+1}, \dots, a_{i-1}$$

a

$$P'' = a_j, a_{j+1}, \dots, a_{j+n-1}, a_{i+n}, a_{i+n+1}, \dots, a_{j-1},$$

které jsou opět kvazi De Bruijnovy řádu  $n$ .

**Poznámka.** Rozdělení kvazi De Bruijnovy posloupnosti popsané v Lemmatu 3.13 je znázorněno na Obrázku 3.1.



Obrázek 3.1: Rozdělení posloupnosti  $P$  na  $P'$  a  $P''$

*Důkaz.* Je-li  $i \neq j$ , potom  $a_i \neq a_j$  a  $a_{i+n} \neq a_{j+n}$ , jelikož  $P$  je kvazi De Bruijnova řádu  $n$ . Tedy  $P' \neq P''$ .

Uvažujme posloupnost  $P'$ . Chceme dokázat, že pro všechna  $r, s \in \{j+n, j+n+1, \dots, i-1, i, i+1, \dots, i+n-1\}$  platí

$$(s \neq r) \Rightarrow (a_s, a_{s+1}, \dots, a_{s+n-1}) \neq (a_r, a_{r+1}, \dots, a_{r+n-1}). \quad (3.2)$$

Pokud by  $P'$  měla tuto vlastnost, vyskytovala by se v ní každá  $q$ -ární podposloupnost délky  $n$  nejvýše jednou, a tedy by byla kvazi De Bruijnova řádu  $n$ .

Pro  $r, s \in \{j + n, \dots, i\}$  vztah 3.2 zřejmě platí, neboť v takovém případě jsou  $a_r, \dots, a_{r+n-1}$  a  $a_s, \dots, a_{s+n-1}$  podposloupnosti  $P$ , která je kvazi De Bruijnova řádu  $n$ .

V případě, že  $r$  nebo  $s$  je prvkem  $\{i+1, \dots, i+n-1\}$ , budeme brát v úvahu také nově vzniklé podposloupnosti délky  $n$   $a_{i+1+k}, \dots, a_{j+n+k}$ , kde  $k \in \{0, \dots, n-2\}$ . Díky předpokladu  $a_{i+1} = a_{j+1}, \dots, a_{i+n-1} = a_{j+n-1}$  lze tyto nově vzniklé podposloupnosti přeznačit následujícím způsobem:

$$\begin{aligned} a_{i+1}, \dots, a_{i+n-1}, a_{j+n} &= a_{j+1}, \dots, a_{j+n-1}, a_{j+n} \\ a_{i+2}, \dots, a_{j+n}, a_{j+n+1} &= a_{j+2}, \dots, a_{j+n}, a_{j+n+1} \\ &\vdots \\ a_{i+n-1}, a_{j+n}, \dots, a_{j+2n-2} &= a_{j+n-1}, a_{j+n}, \dots, a_{j+2n-2}, \end{aligned}$$

z čehož je vidět, že jde zároveň o podposloupnosti  $P'$  i  $P$ , a tedy vlastnost 3.2 bude splněna. V případě posloupnosti  $P''$  budeme postupovat analogicky.  $\square$

Vraťme se nyní k posloupnosti  $B = a_0, \dots, a_{242}$ , kterou chceme pomocí Lemma 3.13 zkracovat na námi požadované délky. Přidržíme-li se značení z tohoto lemmatu, je  $l = 243, n = 5$  a  $q = 3$ . Tabulka 3.2 ukazuje konkrétní úseky v posloupnosti  $B$ , které splňují předpoklady Lemma 3.13. Indexy  $i$  a  $j$  mají stejný význam jako ve znění tohoto lemmatu. Výsledné dvě posloupnosti označíme  $B'$  a  $B''$ . Pro konstrukci pozičního kódu nás bude zajímat vždy ta delší, což bude při našem značení  $B'$ . Poznamenejme také, že rozdíl délek  $B$  a  $B'$  v posledním sloupci tabulky je roven délce  $B''$ .

$(i + 1, j + 1)$	podposloupnost $a_{i+1}, \dots, a_{j+4}$ v $B$	délka $B'$	rozdíl délek $B$ a $B'$
(0, 1)	0, 0, 0, 0, 0	242	1
(117, 118)	1, 1, 1, 1, 1	242	1
(238, 239)	2, 2, 2, 2, 2	242	1
(48, 50)	0, 1, 0, 1, 0, 1	241	2
(119, 121)	0, 2, 0, 2, 0, 2	241	2
(228, 231)	0, 1, 1, 0, 1, 1, 0	240	3
(107, 110)	0, 2, 2, 0, 2, 2, 0	240	3
(2, 6)	0, 0, 0, 1, 0, 0, 0, 1	239	4
(123, 127)	0, 0, 0, 2, 0, 0, 0, 2	239	4

Tabulka 3.2: Konstrukce posloupnosti  $B'$

**Důsledek 3.14.** *Na základě posloupnosti  $B$  a předchozí Tabulky 3.2 lze konstruovat kvazi De Bruijnovu posloupnost řádu 5 délky  $243 - i$ , kde  $i \in \{1, \dots, 21\}$ .*

*Důkaz.* Sečteme-li rozdíly délek v posledním sloupci tabulky dostaneme  $3 \cdot 1 + 2 \cdot 2 + 2 \cdot 3 + 2 \cdot 4 = 21$ .  $\square$



### 3.3 Poznámka o určení rotace povrchu

V předchozí části této kapitoly jsme viděli, že k dekodování souřadnic pozičního kódu  $\psi$  využíváme matici typu  $6 \times 6$  nad  $\mathbb{Z}_2^2$ , která představuje  $\psi \upharpoonright_{D_{xy}^{(6)}}$  pro nějakou dvojici  $(x, y)$ . V [7] se pro popis dekodování v praxi předpokládá práce s maticemi o rozměrech  $8 \times 8$ , potažmo s podposloupnostmi  $H$  délky 8. Je to z důvodu možnosti detekce rotace povrchu.

**Definice.** Binární posloupnosti  $a_0, \dots, a_l$  a  $a_l, a_{l-1}, \dots, a_0$  nazveme *převrácené*, binární posloupnosti  $a_0, \dots, a_l$  a  $(a_0 + 1) \bmod 2, \dots, (a_l + 1) \bmod 2$  nazveme *opačné*.

Posloupnost  $H$  je kvazi De Bruijnova řádu 6, a tím pádem je též kvazi De Bruijnova řádu 8. Byla zvolena tak, aby splňovala následující podmínky.

**Pozorování 3.15.** *Nechť  $P, Q, R$  jsou binární posloupnosti délky 8, přičemž  $P$  a  $Q$  jsou převrácené a  $P$  a  $R$  jsou opačné. Pak platí, že, je-li  $P$  podposloupnost  $H$ , nevyskytne se v posloupnosti  $H$  posloupnost  $Q$  ani posloupnost  $R$  jako podposloupnost.*

Uvažujme, že máme k dispozici matici typu  $8 \times 8$ , označme ji  $O$ , pro kterou existuje  $(x, y)$  takové, že  $O = \psi \upharpoonright_{D_{xy}^{(8)}}$ . Stejně jako při dekodování si oddělíme první a druhé složky prvků matice  $O$  a označíme postupně  $O^1$  matici prvních souřadnic a  $O^2$  matici druhých souřadnic prvků  $O$ . Z konstrukce pozičního kódu  $\psi$  plyne, že při nulové rotaci jsou řádky matice  $O^1$  a sloupce  $O^2$  podposloupnostmi  $H$  délky osm. Následující Tabulka 3.3 znázorňuje, co se děje při rotaci (ve směru hodinových ručiček) s „původními“ řádky a sloupci matice  $O$  (tím jsou myšleny řádky a sloupce  $O$  při nulové rotaci):

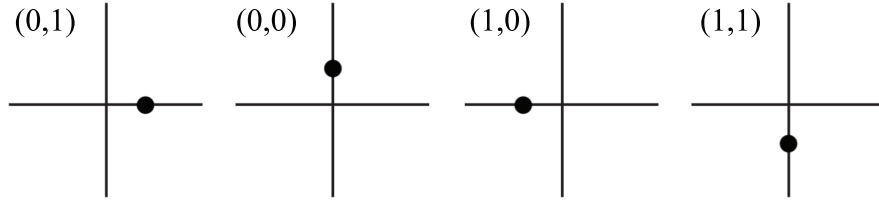
Ovšem podobně jako v případě pozičního kódu  $\phi$  z druhé kapitoly snímá čtecí

rotace	řádky $O^1$	sloupce $O^2$
90°	sloupce	převrácené řádky
180°	převrácené řádky	převrácené sloupce
270°	převrácené sloupce	řádky

Tabulka 3.3: Rotace matic  $O^1$  a  $O^2$

zařízení při dekodování v praxi matici  $O$  v její grafické podobě, kde její prvky odpovídají tečkám v jedné ze čtyř možných poloh. Existuje více vhodných způsobů, jak prvkům z  $\mathbb{Z}_2^2$  lze přiřadit tyto čtyři polohy. Podívejme se, jak bude situace vypadat v případě, že byly prvky  $O$  graficky zakódovány dle [7], což ilustruje Obrázek 3.2.

Tabulka 3.4 znázorňuje, jakým způsobem budou jednotlivé tečky interpretovány při rotaci povrchu o 90, 180 a 270 stupňů. Vidíme, že při rotaci o 180° se obě souřadnice změni na opačné. Při rotaci o 90° se na místě druhé souřadnice objeví opačná hodnota původní první souřadnice a naopak při rotaci o 270° se na místě první souřadnice objeví opačná hodnota původní druhé souřadnice. Shrňme nyní výše uvedené poznatky:



Obrázek 3.2: Grafické kódování prvků  $\mathbb{Z}_2^2$

poloha tečky	$90^\circ$	$180^\circ$	$270^\circ$
(1, 1)	(1, 0)	(0, 0)	(0, 1)
(0, 1)	(1, 1)	(1, 0)	(0, 0)
(1, 0)	(0, 0)	(0, 1)	(1, 1)
(0, 0)	(0, 1)	(1, 1)	(1, 0)

Tabulka 3.4: Vliv rotace povrchu na dekódování teček

- Při rotaci o  $180^\circ$  budou původní řádky  $O^1$  i původní sloupce  $O^2$  přečteny jako převrácené a opačné.
- Při rotaci o  $90^\circ$  budou původní řádky  $O^1$  přečteny jako opačné, přičemž budou tvořit sloupce matice  $O^{2*}$ , kde jsme symbolem  $O^*$  označili matici  $O$  otočenou o  $90^\circ$  ve směru hodinových ručiček.
- Při rotaci o  $270^\circ$  budou původní sloupce  $O^2$  přečteny jako opačné, přičemž budou tvořit řádky matice  $O^{1**}$ , kde  $O^{**}$  je označení pro matici  $O$  otočenou o  $270^\circ$  ve směru hodinových ručiček.

### 3.4 Rozšíření

Výše popsaný princip kódování pozice s využitím Čínské věty o zbytcích lze zformulovat obecněji. Navažme nyní na Lemma 3.3 a podívejme se na možnost zápisu prvku z celočíselného intervalu ve smíšené bázi. Důkaz následujícího lemmatu by byl podobný důkazu Lemma 3.3 avšak s mnohem větším množstvím nepříjemných indexů, a proto ho nebudeme uvádět.

**Lemma 3.16.** *Bud'  $M = \{0, \dots, p_1^{k_1} \cdots p_m^{k_m} - 1\}$ , kde  $p_1, \dots, p_m$  jsou (ne nutně po dvou různá) prvočísla a  $k_1, \dots, k_m \in \mathbb{N}$ . Potom každý prvek  $\delta$  z množiny  $M$  lze jednoznačně vyjádřit ve tvaru*

$$\delta = c_0 + p_1 c_1 + \cdots + p_1^{k_1-1} c_{k_1-1} + p_1^{k_1} \cdot (c_{k_1} + p_2 c_{k_1+1} + \cdots + p_2^{k_2-1} c_{k_1+k_2-1}) + \cdots + p_1^{k_1} \cdots p_{m-1}^{k_{m-1}} \cdot (c_{\sum_{i=1}^{m-1} k_i} + p_m c_{\sum_{i=1}^{m-1} k_i+1} + \cdots + p_m^{k_m-1} c_{\sum_{i=1}^m k_i-1}),$$

kde

$$\begin{aligned} c_0, \dots, c_{k_1-1} &\in \{0, \dots, p_1 - 1\}, \\ &\vdots \\ c_{\sum_{i=1}^{m-1} k_i}, \dots, c_{\sum_{i=1}^m k_i-1} &\in \{0, \dots, p_m - 1\}. \end{aligned}$$

**Definice.** Vyjádření čísel z  $\{0, \dots, p_1^{k_1} \cdots p_m^{k_m} - 1\}$  dle Lemma 3.16 budeme nazývat *vyjádření ve smíšené bázi*

$$\{1, p_1, p_1^2, \dots, p_1^{k_1}, p_1^{k_1} p_2, \dots, p_1^{k_1} \cdots p_m^{k_m-1}\}.$$

Vidíme, že smíšená báze může mít libovolnou velikost. Máme-li k dispozici kvazi De Bruijnovy posloupnosti určitého typu, můžeme si zkonstruovat poziční kódy použitelné na libovolně velké plochy. Postup by byl zcela analogický ke konstrukci pozičního kódu  $\psi$ , a proto následující tvrzení, které popisuje tuto skutečnost, uvádíme bez důkazu. Stačí připomenout, že hlavní myšlenka konstrukce  $n$ -detekovatelného pozičního kódu tkví v sestrojení nějaké posloupnosti rozdílů s dostatečně velkou aritou, která je kvazi De Bruijnova řádu  $(n-1)$ , a že k tomuto využíváme vhodné pomocné kvazi De Bruijnovy posloupnosti řádů  $(n-1)$  s prvočíselnou aritou.

**Tvrzení 3.17.** *Budte  $m, n, l, k_1, \dots, k_m \in \mathbb{N}$ . Předpokládejme, že máme danou nějakou binární kvazi De Bruijnovu posloupnost řádu  $n$  a délky  $l$  spolu s kvazi De Bruijnovými posloupnostmi řádu  $n-1$ , jež si označíme a očíslovíme jako  $D_1^1, \dots, D_1^{k_1}, \dots, D_m^1, \dots, D_m^{k_m}$ , které splňují následující podmínky:*

1. *jejich délky  $l_i^j, 1 \leq i \leq m, 1 \leq j \leq k_i$ , jsou po dvou nesoudělné,*
2. *arita posloupností  $D_i^1, \dots, D_i^{k_i}, 1 \leq i \leq m$ , je rovna  $p_i \in \mathbb{P}$ , přičemž*

$$p_1^{k_1} \cdots p_m^{k_m} \leq l.$$

*Potom lze k těmto posloupnostem sestrojít  $n$ -detekovatelný poziční kód*

$$\psi : \{0, \dots, L\}^2 \rightarrow \{0, 1\}^2, \quad \text{kde} \quad L = \prod_{i=1}^m (l_i^1 \cdots l_i^{k_i}).$$

**Poznámka.** Budeme-li se držet značení z minulého tvrzení, platí  $l_i^j \leq p_i^{n-1}$ , jelikož  $D_i^j$  jsou kvazi De Bruijnovy posloupnosti řádu  $n-1$ . Horní mez pro rozměr plochy, kterou bychom se mohli snažit tímto způsobem zakódovat, je tedy

$$L \leq \left( \prod_{i=1}^m p_i^{k_i} \right)^{n-1}.$$

## 4. Srovnání se základní verzí

Vzpomeňme si nyní na počáteční případ 4-detekovatelného pozičního kódu  $\phi$  z druhé kapitoly. Souřadnice  $y$  byla zakódována na základě podobného principu jako obě souřadnice v případě 6-detekovatelného pozičního kódu  $\psi$ , tzn. s využitím rozdílů členů nějaké startovní posloupnosti. Tuto startovní posloupnosti pozičních čísel jsme v případě konstrukce  $\phi$  označovali jako  $\beta$ . Posloupnost  $\beta$  hraje stejnou roli jako startovní posloupnost  $\gamma$  z třetí kapitoly. Nyní ukážeme, že ji lze vyjádřit ve tvaru

$$\beta(y) = \beta(0) + \sum_{i=0}^{y-1} \delta'(i) \pmod{7},$$

kde  $y \in \{0, \dots, 96\}$ ,  $\beta(0)$  je zvoleno libovolně z  $\{0, \dots, 6\}$  a  $\delta'$  je vhodně sestavená posloupnost rozdílů.

V této kapitole nás tedy bude zajímat, jestli kódování souřadnice  $y$  v případě pozičních kódů  $\phi$  a  $\psi$  popsaných na základě [6] a [7] představuje skutečně dvě různé metody nebo zda jde o jinak formulovaný totožný princip. Pro potřeby porovnávání  $\beta$  a  $\gamma$  poslouží definovat si  $\delta'$  jako složení tří vhodně zvolených pomocných zobrazení.

Pro všechna  $y$  budeme používat vyjádření  $y = 3n + r$ ,  $r \in \{0, 1, 2\}$ , na základě kterého definujeme zobrazení

$$\varepsilon' : \{0, \dots, 95\} \rightarrow \mathbb{Z}_3 \times \{0, \dots, 31\},$$

které přiřadí každému  $y = 3n + r$  dvojici  $(r, n)$ .

Dále zvolme posloupnosti

$$\begin{aligned} D^{1'} &= 2, 2, 0 \\ D^{2'} &= 0, 1, 2, 3 \end{aligned}$$

Zobrazení

$$d' : \mathbb{Z}_3 \times \{0, \dots, 31\} \rightarrow \{(0, 0), (0, 1), (2, 0), (2, 1), (2, 2), (2, 3)\}$$

přiřadí každé dvojici  $(r, n)$  z  $\mathbb{Z}_3 \times \{0, \dots, 31\}$  dvojici  $(D^{1'}[r], D^{2'}[b_{2-r,n}])$ , kde  $b_{2-r,n}$  je koeficient z vyjádření  $n = 8b_{2,n} + 2b_{1,n} + b_{0,n}$  ve smíšené bázi dle Lemma 2.2.

Pro každou dvojici  $(r, n)$  zřejmě platí  $D^{2'}[b_{2-r,n}] = b_{2-r,n}$ .

Usilujeme o alternativní vyjádření  $\beta$ , tím pádem chceme, aby abeceda posloupnosti rozdílů  $\delta'$  byla  $\{1, \dots, 6\}$ . Na základě tohoto požadavku definujeme zobrazení  $\tau'$ :

$$\begin{aligned} \tau' : \{(0, 0), (0, 1), (2, 0), (2, 1), (2, 2), (2, 3)\} &\rightarrow \{1, \dots, 6\}, \\ (D^{1'}, D^{2'}) &\mapsto 1 + D^{1'} + D^{2'}. \end{aligned}$$

Nakonec pro všechna  $y \in \{0, \dots, 95\}$  definujeme

$$\delta'(y) = \tau'(d'(\varepsilon'(y))). \tag{4.1}$$

**Lemma 4.1.** *Bud'  $n \in \{0, \dots, 31\}$  a  $n = 8b_{2,n} + 2b_{1,n} + b_{0,n}$ , kde  $b_{0,n} \in \{0, 1\}$  a  $b_{1,n}, b_{2,n} \in \{0, 1, 2, 3\}$ , vyjádření ve smíšené bázi  $\{8, 2, 1\}$ . Předpokládejme, že jsme zvolili nějaké  $\beta(0) \in \{1, \dots, 6\}$ . Připomeňme, že, známe-li  $\beta(3n)$ , je*

$$\beta(3n + 1) = \beta(3n) + b_{2,n} + 3 \pmod{7},$$

$$\beta(3n + 2) = \beta(3n + 1) + b_{1,n} + 3 \pmod{7},$$

$$\beta(3n + 3) = \beta(3n + 2) + b_{0,n} + 1 \pmod{7}.$$

Potom pro všechna  $y \in \{0, \dots, 96\}$  platí:

$$\beta(y) = \beta(0) + \sum_{i=0}^{y-1} \delta'(i) \pmod{7},$$

kde  $\delta'(i) = \tau'(d'(\varepsilon'(i)))$  a  $y \in \{0, \dots, 96\}$ .

*Důkaz.* Připomeňme, že předpokládáme pevně zvolené  $\beta(0)$  z  $\{1, \dots, 6\}$ . Budeme postupovat indukcí podle  $y$ . Pro  $y = 1$  platí  $\beta(1) = \beta(0) + b_{2,0} + 3 \pmod{7}$ . Jelikož platí rovnost

$$1 + 2 + b_{2,0} = \tau'(2, b_{2,0}) = \tau'(d'(0, 0)) = \tau'(d'(\varepsilon'(0))) = \delta'(0),$$

dostáváme  $\beta(1) = \beta(0) + \delta'(0) \pmod{7}$ .

Formulujme nyní indukční předpoklad, že pro nějaké  $y \geq 1$  platí  $\beta(y) = \beta(0) + \sum_{i=0}^{y-1} \delta'(i) \pmod{7}$ . Ověřme tento vztah pro  $y + 1$ . Rozlišíme tři případy:

1. Je-li  $y = 3n + 1$ , platí dle indukčního předpokladu  $\beta(3n + 1) = \beta(0) + \sum_{i=0}^{3n} \delta'(i) \pmod{7}$ . Dále  $\beta(y + 1) = \beta(3n + 2) = \beta(3n + 1) + b_{1,n} + 3 \pmod{7} = \beta(0) + \sum_{i=0}^{3n} \delta'(i) + b_{1,n} + 3 \pmod{7}$ . Dosadíme-li

$$\begin{aligned} b_{1,n} + 3 &= 1 + 2 + b_{1,n} = \tau'(2, b_{1,n}) = \tau'(d'(1, n)) = \tau'(d'(\varepsilon'(3n + 1))) \\ &= \delta'(3n + 1), \end{aligned}$$

dostaneme

$$\beta(y + 1) = \beta(3n + 2) = \beta(0) + \sum_{i=0}^{3n+1} \delta'(i) \pmod{7}.$$

2. Je-li  $y = 3n + 2$ , platí dle indukčního předpokladu  $\beta(3n + 2) = \beta(0) + \sum_{i=0}^{3n+1} \delta'(i) \pmod{7}$ , a tedy  $\beta(y + 1) = \beta(3n + 3) = \beta(3n + 2) + b_{0,n} + 1 \pmod{7} = \beta(0) + \sum_{i=0}^{3n+1} \delta'(i) + b_{0,n} + 1 \pmod{7}$ . Vyjádříme-li si

$$\begin{aligned} b_{0,n} + 1 &= 1 + 0 + b_{0,n} = \tau'(0, b_{0,n}) = \tau'(d'(2, n)) = \tau'(d'(\varepsilon'(3n + 2))) \\ &= \delta'(3n + 2), \end{aligned}$$

dostaneme

$$\beta(y + 1) = \beta(3n + 3) = \beta(0) + \sum_{i=0}^{3n+2} \delta'(i) \pmod{7}.$$

3. Nakonec je-li  $y = 3n + 3$ , platí dle indukčního předpokladu  $\beta(3n + 3) = \beta(0) + \sum_{i=0}^{3n+2} \delta'(i) \pmod{7}$ . Pro  $y + 1 = 3n + 4 = 3(n + 1) + 1$  z  $\{0, \dots, 96\}$  platí dle Lemma 2.6 rovnost

$$\beta(y + 1) = \beta(3(n + 1) + 1) = \beta(3(n + 1)) + b_{2,n+1} + 3 \pmod{7}.$$

Z toho  $\beta(y + 1) = \beta(0) + \sum_{i=0}^{3n+2} \delta'(i) + b_{2,n+1} + 3 \pmod{7}$ . Opět si vyjádříme

$$\begin{aligned} b_{2,n+1} + 3 &= 1 + 2 + b_{2,n+1} = \tau'(2, b_{2,n+1}) = \tau'(d'(0, n + 1)) \\ &= \tau'(d'(\varepsilon'(3n + 3))) = \delta'(3n + 3) \end{aligned}$$

a po dosazení obdržíme

$$\beta(y + 1) = \beta(3(n + 1) + 1) = \beta(0) + \sum_{i=0}^{3n+3} \delta'(i) \pmod{7}.$$

□

Nyní se podívejme podrobněji na vlastnosti zobrazení  $\tau'$ ,  $d'$  a  $\varepsilon'$ .

**Lemma 4.2.** *Zobrazení*

$$\tau' : \{(0, 0), (0, 1), (2, 0), (2, 1), (2, 2), (2, 3)\} \rightarrow \{1, \dots, 6\}$$

je bijekce. Inverzní zobrazení  $\tau'^{-1}$  přiřadí každému  $a \in \{1, \dots, 6\}$  dvojici  $(0, a - 1)$ , pokud  $a \in \{1, 2\} = M$ , nebo dvojici  $(2, a - 3)$ , pokud  $a \in \{3, 4, 5, 6\} = V$ .

*Důkaz.* Že jde o bijekci, je vidět ze zápisu  $\tau'$ . Pokud  $a \in M$ , potom mu zobrazení  $\tau'^{-1}$  přiřadí jeden z prvků  $\{(0, 0), (0, 1)\}$ . Pokud  $a \in V$ , bude jeho hodnota při  $\tau'^{-1}$  z  $\{(2, 0), (2, 1), (2, 2), (2, 3)\}$ . Přesná podoba  $\tau'^{-1}$  lze snadno odvodit opět z definice  $\tau'$ . □

**Lemma 4.3.** *Zobrazení*

$$d' : \mathbb{Z}_3 \times \{0, \dots, 31\} \rightarrow \{(0, 0), (0, 1), (2, 0), (2, 1), (2, 2), (2, 3)\}$$

není definováno po složkách, není prosté, ale je na.

*Důkaz.* Že  $d'$  není definováno po složkách je vidět z jeho zápisu. Platí  $|\mathbb{Z}_3 \times \{0, \dots, 31\}| = 96 > 6$ , tedy  $d'$  není prosté. Každý z prvků  $\{0, 2\}$ , které tvoří první složky prvků z  $\{(0, 0), (0, 1), (2, 0), (2, 1), (2, 2), (2, 3)\}$  nalezneme v posloupnosti  $D^1$  na nějaké pozici, která je prvkem  $\mathbb{Z}_3$ . Dále pro každý prvek  $a \in \{0, 1, 2, 3\}$  odpovídající druhé souřadnici nalezneme nějaké  $r \in \mathbb{Z}_3$  a  $n \in \{0, \dots, 31\}$  tak, že platí  $a = b_{2-r,n}$ , což je nějaké poziční číslo v posloupnosti  $D^2$ . Tedy  $d'$  je na. □

**Lemma 4.4.** *Pro všechna  $y, z \in \{0, \dots, 95\}$  platí*

$$\begin{aligned} (y \neq z) &\Rightarrow [(d'(\varepsilon'(y)), d'(\varepsilon'(y + 1)), d'(\varepsilon'(y + 2))) \\ &\neq (d'(\varepsilon'(z)), d'(\varepsilon'(z + 1)), d'(\varepsilon'(z + 2)))] \end{aligned}$$

*Důkaz.* Pro dva různé prvky  $y$  a  $z$  z  $\{0, \dots, 95\}$  označíme

$$\varepsilon'(y) = \begin{pmatrix} r_1^y \\ n_1^y \end{pmatrix}, \quad \varepsilon'(z) = \begin{pmatrix} r_1^z \\ n_1^z \end{pmatrix}$$

a

$$\varepsilon'(y+1) = \begin{pmatrix} r_2^y \\ n_2^y \end{pmatrix}, \quad \varepsilon'(y+2) = \begin{pmatrix} r_3^y \\ n_3^y \end{pmatrix}, \quad \varepsilon'(z+1) = \begin{pmatrix} r_2^z \\ n_2^z \end{pmatrix}, \quad \varepsilon'(z+2) = \begin{pmatrix} r_3^z \\ n_3^z \end{pmatrix}.$$

Protože  $y \neq z$ , je nutně  $r_1^y \neq r_1^z$  nebo  $n_1^y \neq n_1^z$ . Aplikujme nyní zobrazení  $d'$  na  $(\varepsilon'(y), \varepsilon'(y+1), \varepsilon'(y+2))$  a  $(\varepsilon'(z), \varepsilon'(z+1), \varepsilon'(z+2))$ . Označme

$$\begin{aligned} A' &= (d'(\varepsilon'(y)), d'(\varepsilon'(y+1)), d'(\varepsilon'(y+2))) \\ &= \begin{pmatrix} D^{1'}[r_1^y] & D^{1'}[r_2^y] & D^{1'}[r_3^y] \\ D^{2'}[b_{2-r_1^y, n_1^y}] & D^{2'}[b_{2-r_2^y, n_2^y}] & D^{2'}[b_{2-r_3^y, n_3^y}] \end{pmatrix}, \\ B' &= (d'(\varepsilon'(z)), d'(\varepsilon'(z+1)), d'(\varepsilon'(z+2))) \\ &= \begin{pmatrix} D^{1'}[r_1^z] & D^{1'}[r_2^z] & D^{1'}[r_3^z] \\ D^{2'}[b_{2-r_1^z, n_1^z}] & D^{2'}[b_{2-r_2^z, n_2^z}] & D^{2'}[b_{2-r_3^z, n_3^z}] \end{pmatrix}. \end{aligned}$$

Platí  $r_2^y = r_1^y + 1 \pmod{3}$ ,  $r_3^y = r_2^y + 1 \pmod{3}$  a podobně pro  $r_1^z, r_2^z, r_3^z$ , tzn. tyto indexy jsou po sobě jdoucí čísla. Zároveň si uvědomme, že posloupnost  $D^{1'}$  je kvazi De Bruijnova řádu tři a první řádky matic  $A'$  a  $B'$  tvoří její podposloupnosti délky tři. Nastává-li tedy případ  $r_1^y \neq r_1^z$ , nutně existuje  $i \in \{1, 2, 3\}$  takové, že  $D^{1'}[r_i^y] \neq D^{1'}[r_i^z]$ .

V případě, že  $n_1^y \neq n_1^z$ , nám stačí diskutovat situaci  $(n_1^y \neq n_1^z) \wedge (r_1^y = r_1^z)$ . Připomeňme vyjádření  $n_1^y = 8b_{2, n_1^y} + 2b_{1, n_1^y} + b_{0, n_1^y}$  a  $n_1^z = 8b_{2, n_1^z} + 2b_{1, n_1^z} + b_{0, n_1^z}$ . Z  $n_1^y \neq n_1^z$  existuje  $j \in \{0, 1, 2\}$  takové, že  $b_{j, n_1^y} \neq b_{j, n_1^z}$ .

Pokud  $r_1^y = r_1^z = 0$ , je  $n_1^y = n_2^y = n_3^y$  (analogicky pro  $z$ ), a tedy zřejmě  $b_{j, n_1^y} = D^{2'}[b_{j, n_1^y}] \neq D^{2'}[b_{j, n_1^z}] = b_{j, n_1^z}$ .

Pokud  $r_1^y = r_1^z = 1$ , nastává situace  $n_2^y = n_1^y, n_3^y = n_1^y + 1$  (analogicky pro  $z$ ):

$$A' = \begin{pmatrix} 2 & 0 & 2 \\ b_{1, n_1^y} & b_{0, n_1^y} & b_{2, n_1^y+1} \end{pmatrix}, \quad B' = \begin{pmatrix} 2 & 0 & 2 \\ b_{1, n_1^z} & b_{0, n_1^z} & b_{2, n_1^z+1} \end{pmatrix}.$$

Zaměříme-li se na druhé řádky těchto matic, rozlišíme dvě varianty:

1. buď existuje  $v \in \{0, 1\}$  takové, že  $b_{v, n_1^y} \neq b_{v, n_1^z}$ , pak  $b_{v, n_1^y} = D^{2'}[b_{v, n_1^y}] \neq D^{2'}[b_{v, n_1^z}] = b_{v, n_1^z}$ ,
2. anebo uvažujeme  $b_{1, n_1^y} = b_{1, n_1^z}$  a  $b_{0, n_1^y} = b_{0, n_1^z}$ . V takovém případě platí, že pokud  $b_{2, n_1^y+1} = b_{2, n_1^z+1}$ , tak lze s využitím Lemma 2.3 snadno spočítat  $n_1^y + 1$  a  $n_1^z + 1$ , přičemž vyjde  $n_1^y + 1 = n_1^z + 1$ , což je spor. Je tedy  $b_{2, n_1^y+1} = D^{2'}[b_{2, n_1^y+1}] \neq D^{2'}[b_{2, n_1^z+1}] = b_{2, n_1^z+1}$ .

Variantu  $r_1^y = r_1^z = 2$  lze vyšetřit podobnými úvahami jako v předchozím případě.  $\square$

**Lemma 4.5.** Zobrazení  $\varepsilon' : \{0, \dots, 95\} \rightarrow \mathbb{Z}_3 \times \{0, \dots, 31\}$  je bijekce.

*Důkaz.* Vyjádření  $y = 3n + r$  je zřejmě jednoznačné, proto je  $\varepsilon'$  prosté. Naopak ke každé dvojici  $(n, r)$  z  $\mathbb{Z}_3 \times \{0, \dots, 31\}$  existuje jednoznačně určené  $y = 3n + r$ , čili  $\varepsilon'$  je na.  $\square$

**Poznámka.** Vraťme se k zobrazení  $\varepsilon$  sestrojené dle Čínské věty o zbytcích, které je izomorfismem grup. Operace sčítání po složkách je na množině  $\mathbb{Z}_{l_1} \times \mathbb{Z}_{l_2} \times \mathbb{Z}_{l_3} \times \mathbb{Z}_{l_4}$  přirozeně definovaná.

Jestliže na  $\mathbb{Z}_3 \times \{0, \dots, 31\}$  dodefinujeme operaci sčítání  $\oplus$  způsobem, že

$$(r_1, n_1) \oplus (r_2, n_2) = (r_1 + r_2 \pmod{3}, n_1 + n_2 + \lfloor (r_1 + r_2)/3 \rfloor \pmod{32}),$$

lze snadno ukázat, že potom je  $\varepsilon'$  homomorfismus grup, a tedy také izomorfismus grup díky Lemmatu 4.5.

**Tvrzení 4.6.** *Posloupnost rozdílů  $\delta'$  je 6-ární kvazi De Bruijnova posloupnost řádu tři.*

*Důkaz.* Abeceda  $\delta'$  je z konstrukce  $\delta'$  rovna oboru hodnot  $\tau'$ , což je  $\{1, \dots, 6\}$ . Zobrazení  $\tau'$  je bijekce, můžeme tedy s využitím Lemma 4.4 vyslovit tvrzení, že pro všechna  $y, z \in \{0, \dots, 95\}$ ,  $y \neq z$  platí  $(\delta'(y), \delta'(y+1), \delta'(y+2)) \neq (\delta'(z), \delta'(z+1), \delta'(z+2))$ . To znamená, že každé podposloupnosti  $\delta'$  délky tři lze přiřadit jednoznačně určené poziční číslo  $z \in \{0, \dots, 95\}$ , jinými slovy,  $d'$  je kvazi De Bruijnova řádu tři.  $\square$

## 4.1 Závěrečná diskuse

Na tomto místě můžeme konstatovat, že, ačkoliv jsme docílili formálně stejných vyjádření zobrazení  $\delta'$  a  $\delta$ , která využíváme po řadě v konstrukcích startovních posloupností  $\beta$  a  $\gamma$ , našli jsme při podrobnějším zkoumání zásadní rozdíly.

Diskutujeme postupně jednotlivá pomocná zobrazení. Zobrazení  $\varepsilon$  i  $\varepsilon'$  jsou izomorfismy, avšak zatímco  $\varepsilon$  pochází z Čínské věty o zbytcích,  $\varepsilon'$  vyjadřuje dělení třemi se zbytkem.

Zobrazení  $d$  a  $d'$  jsme definovali tak, že jsou obě na, ale nikoliv prostá. Zobrazení  $d'$  není na rozdíl od  $d$  definováno po složkách. Další rozdíl zaměříme v důkazech příbuzných Lemmat 3.7 a 4.4. Zatímco v důkazu prvního jmenovaného lemmatu využíváme, fakt, že všechny posloupnosti  $D^1, D^2, D^3, D^4$  jsou kvazi De Bruijnovy řádu pět a řádky matic  $A$  a  $B$  tvoří jejich podposloupnosti, v důkazu Lemmatu 4.4 řešícího podobnou vlastnost v případě  $\delta'$  tomu tak není. Je sice pravda, že  $D^1$  i  $D^2$  jsou kvazi De Bruijnovy řádu tři, ale tuto vlastnost v případě  $D^2$  vůbec nevyužijeme, jelikož druhé řádky matic  $A'$  a  $B'$  její podposloupnosti tvořit nemusí. Naopak využijeme fakt, že konstrukce  $\delta'$  vychází z vyjádření  $n = 8b_{2,n} + 2b_{1,n} + b_{0,n}$  dle Lemma 2.2.

Zobrazení  $\tau'$  i  $\tau$  byly zkonstruovány jako bijekce. Díky tomu je lze jednoznačně invertovat.

Značné odlišnosti nalezneme také při dekódování, v případě  $\delta$  například neexistuje žádný ekvivalent Lemma 2.4, které umožňuje dekódování  $\phi$ .

Díky diskuzi, kterou jsme právě provedli, vidíme zásadní rozdíly v konstrukci posloupností  $\delta$  a  $\delta'$  a potažmo i kódování souřadnice  $y$  v případech pozičních kódů  $\phi$  a  $\psi$ .



# Závěr

Shrňme nyní poznatky z předešlých kapitol. Kódování pozice na přímce vždy spočívá v konstrukci nějaké De Bruijnovy nebo kvazi De Bruijnovy posloupnosti. Například pro kódování s využitím markerů jsme zkonstruovali kód  $\theta$ , na který lze nahlížet jako na kvazi De Bruijnovu posloupnost řádu 9 o délce  $9 \cdot 4^8$ , jejíž abeceda je  $\{0, 1, 2, 3\} \cup \{\bullet\}$  (to plyne z Lemma 1.3). Viděli jsme, že pro sestavení kvazi De Bruijnovy posloupnosti může sloužit vyjadřování pozice markeru v nějaké číselné soustavě nebo LFSR.

Při sestavování pozičních kódů v rovině jsme opět vycházeli z kvazi De Bruijnových posloupností, kterým jsme říkali startovní posloupnosti ve směru  $x$  nebo  $y$ . Zřejmě by na ně šlo nahlížet jako na poziční kódy na přímce. Při konstrukci startovních posloupností jsme použili další principy: vyjadřování pozice ve smíšené bázi, odlišení oken nebo využití pomocné posloupnosti rozdílů. Tyto posloupnosti rozdílů přitom byly samy také kvazi De Bruijnovými posloupnostmi, k jejich vytvoření jsme využili např. Čínskou větu o zbytcích.

Kódování pozice na přímce a v rovině tudíž spojuje stejný koncept, ovšem v případě pozičních kódů v rovině je dále rozvinut. V [1] je popisován Resnikův poziční kód využívaný v CERNu, na který můžeme pohlížet jako na metodu kódování pozice v rovině s využitím markerů. Společnost Anoto řeší otázku rozšíření pozičního kódu na přímce do roviny pomocí binárních kvazi De Bruijnových posloupností, které zapisuje opakovaně do řádků nebo sloupců a jejichž počáteční posunutí je určeno startovními posloupnostmi.

Kombinace různých metod konstrukce startovních posloupností s opakováním binárních kvazi De Bruijnových posloupností je způsob, kterým by bylo možné téma pozičního kódování dále rozvíjet. Zdaleka ne všechny nové varianty by byly optimální a vhodné pro praktické využití. Například využijeme-li ke kódování jedné souřadnice princip podobný kódování souřadnice  $x$  u pozičního kódu  $\phi$  v druhé kapitole, musíme druhou souřadnici zakódovat např. s využitím posloupnosti rozdílů, tedy tak, aby bylo její dekodování nezávislé na znalosti té první. Také by bylo možné se zaměřit na počet prvků přečtené matice (restrikce kódu na okno) potřebných k dekodování pozice. Kódy  $\phi$  a  $\psi$  jsou z tohoto pohledu optimální, jelikož rozměr čtvercové matice odpovídá řádu opakovaně zapisované kvazi De Bruijnovy posloupnosti.

Možných směrů k dalším úvahám je vícero, jako motivace může sloužit hledání dalších aplikací pozičního kódování v praxi.

# Seznam použité literatury

- [1] E. Aboufadel, L. Smietana, T. Armstrong: *Position Coding*, draft, June 1, 2007
- [2] B. Arazi: *Position recovery using binary sequences*, Electronic Letters, vol. 20, str. 61 – 62, 1984
- [3] F. D. Garcia, P. van Rossum, R. Verdult, R. W. Schreur: *Wirelessly Pickpocketing a Mifare Classic Card*, Radboud University Nijmegen, 2009
- [4] T. Hansen, G. L. Mullen: *Primitive polynomials over finite fields*, Mathematics of computation, vol. 59, str. 639 – 643, 1992
- [5] E. M. Petriu: *Absolute Position Measurement using Pseudo-Random Binary Encoding*, IEEE Instrumentation & Measurement Magazine, Sep. 1998
- [6] M. P. Pettersson, Tomas Edso: *Product provided with a coding pattern and apparatus and method for reading the pattern*, United States Patent, Patent No.: US 7,588,191 B2, Sep. 15, 2009
- [7] M. P. Pettersson: *Method and device for decoding a position-coding pattern*, World Intellectual Property Organisation, International Publication No.: WO 03/038741 A1, May 8, 2003
- [8] <http://www.flickr.com/photos/anotogroup>, přístup 19.7.2013

# Seznam tabulek

2.1	Startovní posloupnost ve směru $y$ . . . . .	13
2.2	Startovní posloupnost ve směru $x$ . . . . .	14
2.3	Hodnoty zobrazení $\varphi$ . . . . .	17
3.1	Posloupnost rozdílů a startovní posloupnost ve směru $y$ . . . . .	28
3.2	Konstrukce posloupnosti $B'$ . . . . .	36
3.3	Rotace matic $O^1$ a $O^2$ . . . . .	37
3.4	Vliv rotace povrchu na dekódování teček . . . . .	38