Maticové numerační systémy

Tomáš Vávra

TIGR seminar

14. března 2022

Už na Diskrétní matematice jste se naučili zapisovat přirozená čísla v různých soustavách.

Např. při základu 5:

$$\begin{aligned} 57 &= 2 + 5 \cdot 11 \\ &= 2 + 5 \cdot (1 + 5 \cdot 2) \\ &= 2 \cdot 5^2 + 1 \cdot 5 + 2 \\ &= (212)_5. \end{aligned}$$

Co ale když chceme zapisovat necelá čísla?

(A navíc v soustavě s neceločíselným základem)

Jak najít rozvoj neceléhо čísla?

Nechť už známe rozvoj, např.

$$[0,1) \ni x_0 = 2 \cdot 5^{-1} + 1 \cdot 5^{-2} + 2 \cdot 5^{-3}$$

Cifry můžeme hledat iterativně

$$x_1 = 5x_0 - 2 = 1 \cdot 5^{-1} + 2 \cdot 5^{-2}$$

$$x_2 = 5x_1 - 1 = 2 \cdot 5^{-1}$$

$$x_3 = 5x_2 - 2 = 0$$

Obecně máme

$$
\begin{aligned}
x_1 = 5x_0 - d_1 &\implies x_0 = \frac{d_1}{5} + \frac{x_1}{5} \\
x_2 = 5x_1 - d_2 &\implies x_0 = \frac{d_1}{5} + \frac{d_2}{5^2} + \frac{x_2}{5^2} \\
x_3 = 5x_2 - d_3 &\implies x_0 = \frac{d_1}{5} + \frac{d_2}{5^2} + \frac{d_3}{5^3} + \frac{x_3}{5^3} \\
&\vdots
\end{aligned}
$$

Pokud nakonec $x_i = 0$, pak máme konečný rozvoj

Pokud udržíme x_i omezené, pak máme konvergenci

Pokud x_i z konečné množiny, pak periodický rozvoj

Zatím umíme rozvíjet malá čísla (např. z $[0, 1)$)

Pro čísla ≥ 1 prvně vydělíme mocninou základu

$$\frac{11.4}{5^2} = 0.456 \in [0, 1)$$

Potom rozvineme

$$5 \cdot 0.456 - 2 = 0.28$$

$$5 \cdot 0.28 - 1 = 0.4$$

$$5 \cdot 0.4 - 2 = 0$$

Čili

$$\frac{11.4}{5^2} = 2 \cdot 5^{-1} + 1 \cdot 5^{-2} + 2 \cdot 5^{-3}$$

$$11.4 = 2 \cdot 5^1 + 1 \cdot 5^0 + 2 \cdot 5^{-1} = (21.2)_5$$

Klasické nastavení je $\beta > 1$, cifry z $\mathcal{D} = \{0, 1, \ldots, \lfloor \beta \rfloor\}$

Méně klasické je $\beta < -1$, cifry z $\mathcal{D} = \{0, 1, \ldots, \lfloor |\beta| \rfloor\}$

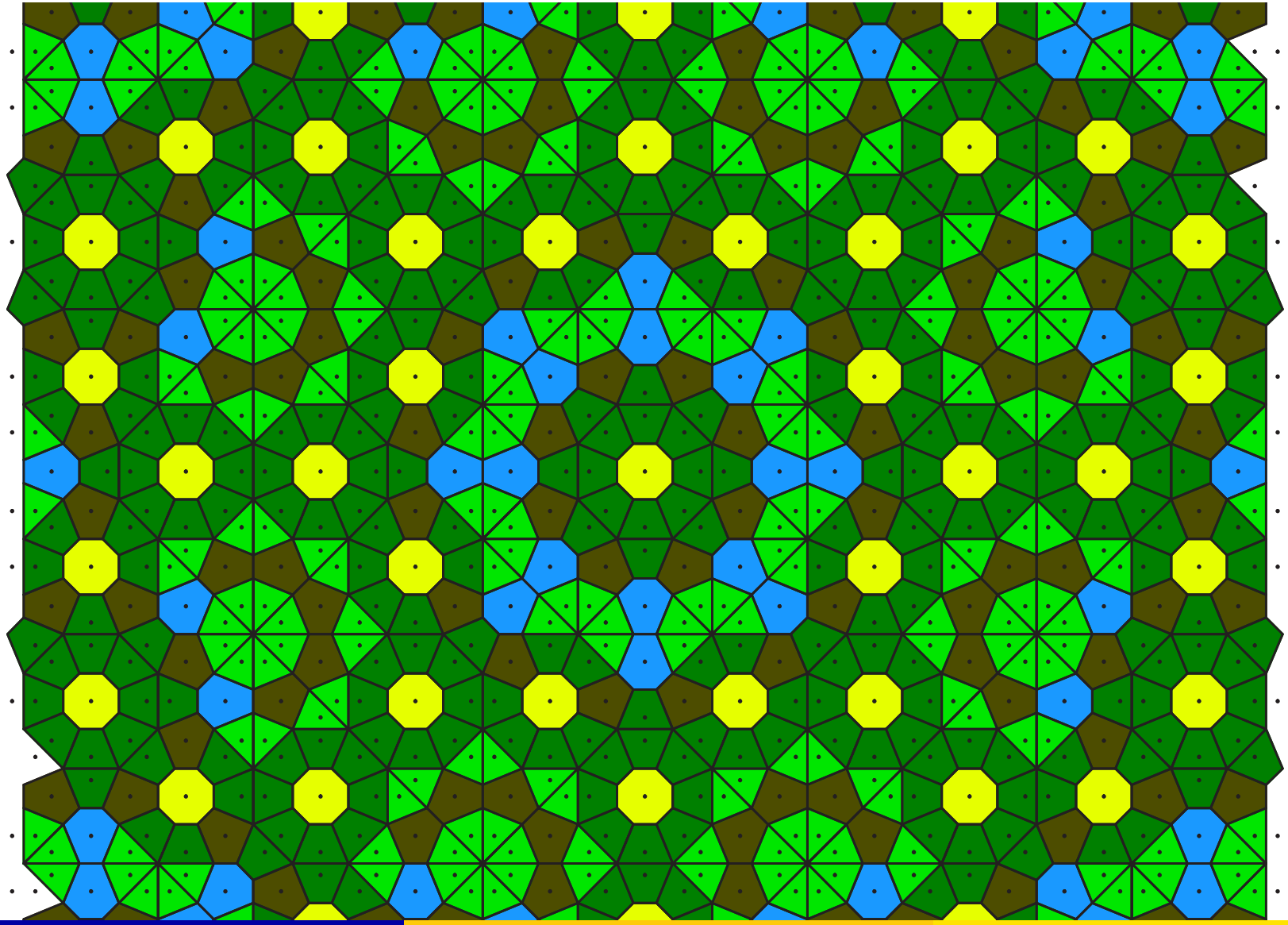
Lze také $\beta \in \mathbb{C}$, cifry z $\mathcal{D} =$???

Rozvoje pokaždé získáváme pomocí $T_\beta(x) = \beta x - d(x)$

Interesting questions

1. Given β and $d(x)$, what are (purely) periodic points?
2. What are the points that end in 0?
3. Invariant measure on $[0, 1]$, i.e. $\mu(T_\beta^{-1}(A)) = \mu(A)$ for all A measurable
4. Arithmetic operations on representations $(1. + 1. = (10.01)_\varphi)$
5. Fractals associated with representations
6. Properties of "integers"

Obrázek (celá čísla s komplexními ciframi)



To samé můžeme dělat s maticemi (základ) a vektory (cifry)

Pokud $M \in \mathbb{Z}^{m\times m}, d \in \mathbb{Z}^n$, pak $Mx - d$ generuje rozvoje vektorů

Theorem (Pelantová, Vávra, 2022)

Nechť $M \in \mathbb{Z}^{m\times m}$ je regulární matice. Potom existuje konečná množina $\mathcal{D} \subset \mathbb{Z}^m$ taková, že každý vektor $z \in \mathbb{Z}^m$ se dá vyjádřit jako

$$z = \sum_{k\in I} M^k d_k, \quad d_k \in \mathcal{D},\ I \subset \mathbb{Z} \text{ konečná}$$

Definujme $T_d(x) = Mx - d(x)$, $x_0 = x$, $x_k = T_d(x_{k-1})$, potom

$$x = M^{-1}d_1 + M^{-2}d_2 + \cdots + M^{-k}d_k + M^{-k}x_k.$$

Pokud x_k leží v konečné množině $\mathcal{F}$ nezávislé na x_0, pak přidáním všech $d_k + \mathcal{F}$ získáme konečný rozvoj.

Jak tedy ukázat, že $x_k \in \mathcal{F}$?

Převedením do Jordanova tvaru a použitím dalších triků se dá věta dokázat :-)

Theorem (J. Jankauskas, J. Thuswaldner, 2018)

Nechť $M \in \mathbb{Z}^{m\times m}$ je regulární matice, jejíž vlastní čísla splňují $|\lambda| \geq 1$. Potom existuje konečná množina $\mathcal{D} \subset \mathbb{Z}^m$ taková, že každý vektor $z \in \mathbb{Z}^m$ se dá vyjádřit jako

$$z = M^k d_k + M^{k-1} d_{k-1} + \cdots + M d_1 + d_0, \quad d_i \in \mathcal{D}.$$

Veliký problém je ale velikost minimální $\mathcal{D}$.

Především dělají problém vlastní čísla $|\lambda| = 1$

Co jsme udělali s Kevinem a Joshem

Nejjednodušší matice s vl. čísly $|\lambda| = 1$ je $M = (\pm 1)$

Druhá nejjednodušší je $\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$

Třetí je $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ a obecněji Jordanův blok $J_n(1)$

$$J_n(1) = \begin{pmatrix} 1 & 1 & 0 & \dots & \dots & 0 \\ 0 & 1 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & 1 & 0 \\ 0 & \dots & \dots & 0 & 1 & 1 \\ 0 & \dots & \dots & \dots & 0 & 1 \end{pmatrix}$$

Většinou se rozvoje typu $M^k d_k + \cdots + M d_1 + d_0$ dělají pomocí

$$x_{i+1} = M^{-1}(x_i - d_i)$$

My ale využili speciálního tvaru M:

$$z = (*, *, \ldots, *, z_k, 0, \ldots, 0)^T \quad \Longrightarrow \quad M^n z = (@, @, \ldots, @, z_k, 0, \ldots, 0)^T$$

Pokud umíme reprezentovat $(*, *, \ldots, *, \pm 1, 0, \ldots, 0)^T$ pro všechny pozice ± 1, pak umíme všechno:

1. Chceme reprezentovat $(z_1, z_2, \ldots, z_m)^T$ (BÚNO $z_m > 0$)
2. Nechť $(*, *, \ldots, *, 1)^T = M^k d_k + \cdots + d_0$, potom

$$(*, \ldots, r_{m-1}, z_m)^T = [(d_k \ldots d_0)^{z_m}]_M$$

3. Podobně vytvořit $(*, \ldots, z_{m-1} - r_{m-1}, 0)^T$ a nalepit před to, co už máme
4. atd.

Lemma

Nechť $M = J_n(1)$. Potom umím reprezentovat $\mathbb{Z}^n$, pokud umím reprezentovat $(*, \dots, *, \pm 1, 0, \dots, 0)^T$, kde ± 1 je na libovolné pozici.

Např. pokud $M = J_2(1)$, $d_1 = (0,1)^T$ a $d_2 = (0,-1)^T$, pak

$$[d_1] = (0,1)^T,$$

$$[d_2] = (0,-1)^T,$$

$$[d_1 d_2] = (1,0)^T,$$

$$[d_2 d_1] = (-1,0)^T.$$

Nechť $M = J_3$ a $d_1 = (0,0,1)^T, d_2 = (0,0,-1)^T$

Všimněte si, že $d_1, d_2 \equiv (0,0,1)^T \bmod 2$

R_i značí hodnoty rozvojů délky maximálně i

$$R_1 \equiv \{(0,0,1)^T\} \bmod 2,$$

$$R_2 \equiv \{(0,0,1)^T, (0,1,0)^T\} \bmod 2,$$

$$R_3 \equiv \{(0,0,1)^T, (0,1,0)^T, (1,1,1)^T\} \bmod 2,$$

$$R_4 \equiv \{(0,0,1)^T, (0,1,0)^T, (1,1,1)^T, (0,0,0)^T\} \bmod 2,$$

$$R_5 \equiv \{(0,0,1)^T, (0,1,0)^T, (1,1,1)^T, (0,0,0)^T\} \bmod 2.$$

Neumím reprezentovat $\mathbb{Z}^3$

Nechť $M = J_3$ a $d_1(0,0,1)^T, d_2 = (0,1,-2)^T$

$$
\begin{aligned}
[d_1] &= (0,0,1)^T, \\
[d_2] &= (0,1,-2)^T, \\
[d_1 d_2 d_1] &= (2,1,0)^T, \\
[d_2 d_1 d_1] &= (0,-2,0)^T, \\
[d_2 d_1 d_1 d_1 d_1 d_2 d_2 d_1 d_1] &= (1,0,0)^T, \\
[d_2 d_1 d_1 d_1 d_2 d_1 d_1 d_2 d_1] &= (-5,0,0)^T.
\end{aligned}
$$

Umím reprezentovat $\mathbb{Z}^3$

Theorem (Caldwell, Hare, Vávra, 2022?)

Nechť $M = J_2(1)$ *a* $\mathcal{D} = \{(a,b)^T, (c,d)^T\}$. *Potom umíme reprezentovat* $\mathbb{Z}^2$ *právě tehdy když* d_1, d_2 *nesplňují nějaké podmínky.*

Obdobný výsledek není známý ani pro základ 3 a cifry $-p, 0, q$

Příklady podmínek:

1. $bd > 0$
2. $\gcd(b,d) \neq 1$
3. $b \equiv d \bmod 4$ a $a \equiv c \bmod 2$
4. $\gcd(ad - bc, |b| + |d|) \geq 3$

Větší bloky

Theorem (Caldwell, Hare, Vávra, 2022?)

Nechť $M = J_n(1)$ *pro libovolné* $n \in \mathbb{N}$, *potom* 3 *cifry* $(0\ldots,0)^T$, $(0,\ldots,0,\pm 1)^T$ *stačí na reprezentování* $\mathbb{Z}^n$.

Pro $n = 4$ funguje $(0,0,0,1)^T, (0,0,1,-2)^T$, ale pro $n \geq 5$ nemáme 2-prvkovou množinu cifer.

Umíme reprezentovat $(*, \ldots, *, A, 0, \ldots, 0)^T$, kde můžeme volit

$$A = \pm 2^k \text{ nebo } A = \pm \prod_k (2^k - 1),$$

což jsou nesoudělná čísla...

Pro $A = 2^k$ volíme reprezentaci

$$[pmmp\ mppm\ mppm\ pmmp \ldots]_M, \quad \text{(Thue-Morse slovo)}$$

kde $p = (0, \ldots, 0, 1)^T$, $m = (0, \ldots, 0, -1)^T$

Matice podobné $J_n(1)$

Co když $M = P^{-1}J_n(1)P \in \mathbb{Z}^{n\times n}$ pro P regulární?

(podobnostní transformace)

$$z = \sum M^k d_k \quad \Longleftrightarrow \quad Pz = \sum (J_n(1))^k (Pd_k)$$

Zkoumáme pak systém se základem $J_n(1)$, ale pro vektory z $P\mathbb{Z}^n$ s ciframi z $P\mathbb{Z}^n$ (lattice numeration systems)

Theorem (C,H,V)

Nechť M je podobná $J_n(1)$. Potom stačí n cifer k reprezentování $\mathbb{Z}^n$.

Tato mez je ostrá, tj. existuje matice řádu n, která potřebuje právě n cifer.

Důkaz první části je relativně technický

Využívá faktu, že $P\mathbb{Z}^n = B\mathbb{Z}^n$, kde $B \in \mathbb{Z}^{n\times n}$ má speciální tvar

Uvažujme $\mathcal{D} = \{d^{(1)}, \dots, d^{(k)}\}$,

$$M = \begin{pmatrix} 1 & 2 & 0 & \dots & \dots & 0 \\ 0 & 1 & 2 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & 2 & 0 \\ 0 & \dots & \dots & 0 & 1 & 2 \\ 0 & \dots & \dots & \dots & 0 & 1 \end{pmatrix} \in \mathbb{Z}^{n \times n}$$

Všimněte si, že $M^k \equiv \mathrm{Id} \bmod 2$

Potom

$$\begin{aligned} M^m d_m + \cdots + M d_1 + d_0 &\equiv d_m + \cdots + d_1 + d_0 \bmod 2 \\ &\equiv a_0 d^{(1)} + \cdots + a_k d^{(k)} \bmod 2 \end{aligned}$$

To je maximálně 2^k vektorů a my potřebujeme $2^n \implies k \geq n$