Nezávislé systémy rovnic

Nechť $S = \{(u_i, v_i) \mid i \in I_S\}$ a $T = \{(u_i, v_i) \mid i \in I_T\}$ jsou systémy rovnic. Řekneme, že S a T jsou *ekvivalentní*, pokud mají stejná řešení.

Systém S se nazývá *nezávislý* pokud není ekvivalentní žádné své vlastní podmnožině. Jak velké mohou být nezávislé systémy rovnic s daným počtem neznámých není známo. Je ale známo, že nemohou být nekonečné:

Věta (O kompaktnosti). Každý systém rovnic nad konečnou množinou neznámých obsahuje konečný ekvivalentní podsystém.

Důkaz věty o kompaktnosti se opírá o Hilbertovu větu o bázi, kterou lze zformulovat analogicky k našemu tvrzení tak, že každý systém polynomiálních rovnic s konečným počtem neznámých nad noetherovským okruhem (v našem případě to bude $\mathbb{Z}$) obsahuje konečný s ním ekvivalentní. Vztah k obvyklé formulací, že každý ideál nad noetherovským okruhem je konečně generovaný, je dán tím, že polynomiální rovnice $(P_i(X), Q_i(X)) \in \mathbb{Z}[X] \times \mathbb{Z}[X]$ převedeme na polynomy $P_i(X) - Q_i(X)$ a všimneme si, že pokud pro nějaké ohodnocení proměnných $\varphi : X \to \mathbb{Z}$ platí po dosazení $P(\varphi(X)) - Q(\varphi(X)) = 0$ pro bázové prvky ideálu generovaného polynomy $P_i(X) - Q_i(X)$, pak tato rovnost platí pro všechny polynomy v ideálu.

Abychom mohli Hilbertovu větu využít, musíme rovnice na slovech nějak převést na polynomy. Uděláme to pomocí matic dvakrát dva, které které budeme chápat jako monoid s běžným maticovým násobením.

Nejprve reprezentujeme monoid $\{a, b\}^*$.

Lemma. Monoid $\mathrm{SL}_2(\mathbb{N})$ matic s jednotkovým determinantem a přirozenými koeficienty je volně generován maticemi

$$\mathbf{a} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{b} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Důkaz. Chceme ukázat, že každý prvek $\mathrm{SL}_2(\mathbb{N})$ lze právě jedním způsobem vyjádřit jako součin matic $\mathbf{a}$ a $\mathbf{b}$ (přičemž prázdný součin je jednotková matice). Všimněme si, že

$$\mathbf{a}^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{b}^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}.$$

a uvažujme

$$\mathbf{m} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{N}).$$

Ukažme, že pokud $\mathbf{m}$ není jednotková, pak je jeden z řádků dominantní. Jinak řečeno, platí jedna z následujících podmínek:

(1) $\mathbf{m}$ je jednotková matice,
(2) $a \geq c$ a $b \geq d$,
(3) $a \leq c$ a $b \leq d$.

Ještě jinak lze tvrzení formulovat tak, že pokud je součin dominancí diagonály kladný, tedy $(a - c)(d - b) \geq 1$, pak je $\mathbf{m}$ jednotková matice. Rovnost $ad - bc = 1$ je ekvivalentní rovnostem

$$(a - c)b + (d - b)c + (a - c)(d - b) = (a - c)d + (d - b)c = 1.$$

Je-li tedy $(a - c)(d - b) \geq 1$, plyne z druhého vyjádření, že musejí být oba činitelé kladní. Z prvního vyjádření pak plyne, že $b = c = 0$ a $a - c = b - d = 1$, tedy $\mathbf{m}$ je jednotková.

Pokud tedy $\mathbf{m}$ není jednotková, leží právě jedna z matic

$$\mathbf{a}^{-1}\mathbf{m} = \begin{pmatrix} a-c & b-d \\ c & d \end{pmatrix}, \quad \mathbf{b}^{-1}\mathbf{m} = \begin{pmatrix} a & b \\ c-a & d-b \end{pmatrix}$$

v $\mathrm{SL}(\mathbb{N}_0)$. Důkaz lemmatu dokončíme indukcí podle $a+b+c+d$. □

Dále zakódujeme do matic 2×2 neznámé. Nechť $\Xi = \{x_i \mid i = 1, 2, \dots n\}$ a $\mathbf{X} = \{\mathbf{x}_i \mid i = 1, 2, \dots n\}$, kde

$$\mathbf{x}_j = \begin{pmatrix} a^{(j)} & b^{(j)} \\ c^{(j)} & d^{(j)} \end{pmatrix}$$

a $X = \{a^{(j)}, b^{(j)}, c^{(j)}, d^{(j)} \mid j = 1, \dots, n\}$ je abeceda proměnných.

Lemma. Homomorfismus monoidů $\alpha : \Xi^* \to \langle \mathbf{X} \rangle$ definovaný pomocí $\alpha : x_i \mapsto \mathbf{x}_i$ je izomorfismus.

Důkaz. Chceme ukázat, že $\langle \mathbf{X} \rangle$ je volně generovaný množinou $\mathbf{X}$. Uvažme tedy nějaký součin $\mathbf{x} = \mathbf{x}_{k_1}\mathbf{x}_{k_2} \cdots \mathbf{x}_{k_n}$. Chceme ukázat, že indexy k_i jsou dány jednoznačně. Označíme-li

$$\mathbf{x}_{k_2} \cdots \mathbf{x}_{k_n} = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

pak

$$\mathbf{x} = \begin{pmatrix} a^{(k_1)}A + b^{(k_1)}C & a^{(k_1)}B + b^{(k_1)}D \\ c^{(k_1)}A + d^{(k_1)}C & c^{(k_1)}B + d^{(k_1)}D \end{pmatrix}.$$

Všimněme se, že $c^{(k_1)}B + d^{(k_1)}D$ obsahuje jako jeden z monomů $d^{(k_1)}d^{(k_2)} \cdots d^{(k_n)}$, z něhož je zřejmá množina indexů, ale nikoli jejich pořadí, protože okruh je komutativní. Podobně ale polynom D obsahuje monom $d^{(k_2)} \cdots d^{(k_n)}$, a proto $a^{(k_1)}B + b^{(k_1)}D$ obsahuje monom $b^{(k_1)}d^{(k_2)} \cdots d^{(k_n)}$, a to jako jediný monom s jedním b a jinak samými d. Z tohoto monomu tedy můžeme určit k_1, a důkaz dokončit indukcí. Můžeme si případně také všimnout, že monomy s jediným b v $a^{(k_1)}B + b^{(k_1)}D$ jsou tvaru

$$a^{(k_1)}a^{(k_2)} \cdots a^{(k_{j-1})} \cdot b^{(k_j)} \cdot d^{(k_{j+1})}a^{(k_{j+2})} \cdots a^{(k_n)},$$

ze kterých lze určit všechna k_j, kde j je dáno počtem a. □

Věta o kompaktnosti. Z charakteristiky $\mathrm{SL}_2(\mathbb{N})$ plyne, že Σ^* lze vnořit do $\mathrm{SL}_2(\mathbb{N})$ pro libovolnou nejvýše spočetnou abecedu $\Sigma = \{a_i \mid i \in I \subset \mathbb{N}\}$, a to předpisem $\iota : a_i \mapsto \mathbf{b}\mathbf{a}^i$. Zde využíváme fakt, že $\{ba^i \mid i \in \mathbb{N}\}$ je kód.

Spolu s izomorfismem $\alpha : \Xi^* \to M$ máme pro jakýkoli homomorfismus $\varphi : \Xi^* \to \Sigma^*$ komutující diagram

$$\begin{tikzcd} \Xi^* \arrow[r, "\varphi"] \arrow[d, "\alpha"'] & \Sigma^* \arrow[d, hook, "\iota"] \\ \langle \mathbf{X} \rangle \arrow[r, "\tilde{\varphi}"] & \mathrm{SL}_2(\mathbb{N}) \end{tikzcd},$$

kde $\tilde{\varphi} = \iota \circ \varphi \circ \alpha^{-1}$. Nechť je nyní

$$S = \{(u_i, v_i) \mid i \in I\}$$

systém rovnic v neznámých Ξ a

$$\tilde{S} = \{(\alpha(u_i), \alpha(v_i)) \mid i \in I\}$$

odpovídající systém rovnic v neznámých $\mathbf{X}$, což je vlastně systém polynomiálních rovnic

$$S' = \left\{ \left(U_i^{(k)}, V_i^{(k)}\right) \;\middle|\; i \in I, k = 1,2,3,4 \right\} ,$$

nad X, kde

$$\alpha(u_i) = \begin{pmatrix} U_i^{(1)} & U_i^{(2)} \\ U_i^{(3)} & U_i^{(4)} \end{pmatrix}, \quad \alpha(v_i) = \begin{pmatrix} V_i^{(1)} & V_i^{(2)} \\ V_i^{(3)} & V_i^{(4)} \end{pmatrix}.$$

Podle Hilbertovy věty o bázi má S' konečný ekvivalentní podsystém T', a tedy i $\tilde{S}$ má konečný ekvivalentní podsystém

$$\tilde{T} = \{(\alpha(u_i), \alpha(v_i)) \mid i \in J\},$$

kde J je množina indexů, které se vyskytují v T'.

Je snadno vidět, že

$$T = \{(u_i, v_i) \mid i \in J\}$$

je ekvivalentní podsystém S. Pro libovolný homomorfismus $\varphi : \Xi^* \to \Sigma^*$ a libovolnou rovnici (u_i, v_i) totiž platí, že $\varphi(u_i) = \varphi(v_i)$, právě když $\tilde{\varphi}(\alpha(u_i)) = \tilde{\varphi}(\alpha(v_i))$. $\square$

**

Věta o kompaktnosti platí i pro volné grupy (rozmyslete si, proč je tvrzení ve volných grupách silnější). Důkaz je stejný jako výše, pouze je třeba namísto matic **a** a **b** použít matice

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix},$$

které generují volnou grupu. Naproti tomu matice **a** a **b** splňují netriviální grupovou relaci

$$\mathbf{aba}^{-1} = \mathbf{ba}^{-1}\mathbf{b}^{-1} = \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix} .$$