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:

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

Důkaz. Důkaz věty o kompaktnosti se opírá o Hilbertovu větu o bázi, kterou lze zformulovat analogicky k našemu tvrzení tak, že každý systém polynomů obsahuje konečný s ním ekvivalentní. Abychom mohli tuto větu využít, musíme rovnice na slovech nějak převést na polynomy.

Nejprve dokážeme pomocné tvrzení:

Lemma. Monoid $\mathrm{SL}(\mathbb{N}_0)$ (monoid matic s jednotkovým determinantem a celými nezápornými koeficienty) je generován maticemi

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

a je volný.

Důkaz. 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

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

Ověřme, že platí jedna z následujících podmínek:

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

Platí, že 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 nyní $a \leq c$ a $b \geq d$, je $(a-c)d + (d-b)c \leq 0$. Pokud je tedy $a \leq c$, musí být $b < d$, a pokud je $b \geq d$ musí být $a > c$.
- Zbývá možnost $a > c$ a $b < d$. Pak $(a-c)(d-b) \geq 1$ a $(a-c)b + (d-b)c \geq 0$. Rovnost $(a-c)b + (d-b)c + (a-c)(d-b) = 1$ je tedy splněna pouze, pokud $b = c = 0$ a $a - c = b - d = 1$, tedy pokud $\mathbf{m}$ je jednotková.

Z toho plyne, že pokud $\mathbf{m}$ 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 $a + b + c + d$. □

Nechť $\Xi = \{x_1, x_2, \ldots, x_n\}$ je množina neznámých. Pro každé $x_j \in \Xi$ definujme matici

$$m_j = \begin{pmatrix} a^{(j)} & b^{(j)} \\ c^{(j)} & d^{(j)} \end{pmatrix},$$

kde $X = \{a^{(j)}, b^{(j)}, c^{(j)}, d^{(j)} \mid j = 1, \ldots, n\}$ je množina proměnných, chápaných jako nové neznámé. Označme M monoid (s běžným maticovým násobením) generovaný množinou $\{m_1, m_2, \ldots, m_n\}$, a nechť $\psi : \Xi^* \to M$ je homomorfismus monoidů definovaný pomocí $\psi : x_j \mapsto m_j$.

Uvažujme homomorfismus monoidů $\varphi : \Xi^* \to \{\mathbf{a}, \mathbf{b}\}^*$. Zobrazení φ definuje ohodnocení $\tilde{\varphi}$ neznámých z X předpisem

$$\varphi(x_j) = \begin{pmatrix} \tilde{\varphi}\left(a^{(j)}\right) & \tilde{\varphi}\left(b^{(j)}\right) \\ \tilde{\varphi}\left(c^{(j)}\right) & \tilde{\varphi}\left(d^{(j)}\right) \end{pmatrix}.$$

Toto ohodnocení rozšíříme na dosazovací homomorfismus $\tilde{\varphi} : \mathbb{Z}[X] \to \mathbb{Z}$ a pro

$$m = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in M$$

budeme zápisem $\tilde{\varphi}(m)$ rozumět

$$\tilde{\varphi}(m) := \begin{pmatrix} \tilde{\varphi}(p) & \tilde{\varphi}(q) \\ \tilde{\varphi}(r) & \tilde{\varphi}(s) \end{pmatrix} \in \mathbb{N}_{2\times 2}\,.$$

Z definic snadno ověříme, že následující diagram komutuje.

$$\begin{tikzcd} \Xi^* \arrow[rr, "\psi"] \arrow[dr, "\varphi"'] & & M \arrow[dl, "\tilde{\varphi}"] \\ & \mathrm{SL}(\mathbb{N}) & \end{tikzcd}$$

Uvažujme soustavu 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

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

Podle Hilbertovy věty o bázi má S' konečný ekvivalentní podsystém, můžeme uvažovat podsystém tvaru

$$T' = \left\{ \left(U_i^{(k)}, V_i^{(k)}\right) \;\middle|\; i \in J, k = 1, 2, 3, 4 \right\},$$

kde J je konečná množina indexů.

Je-li nyní φ řešení soustavy

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

je $\tilde{\varphi}$ řešení soustavy T' a tudíž i řešení soustavy S'. Proto je φ řešením S, a T je tedy ekvivalentní podsystém systému S. $\square$