A szóprobléma véges mátrixgyűrűk felett

Vértesi Vera
Témavezető: Szabó Csaba

2003. április 15.

A szóprobléma

$\mathcal{A}$ algebra

- TERM-EQ($\mathcal{A}$) : $t_1 \equiv t_2$

  (term: gyűrű felett egész együtthatós, többváltozós polinom)

  Pl. $\left(x_1^{-1}x_2^{-1}x_1x_2\right)^3 \overset{?}{\equiv} x_2^6$ S_3-ban

  $\|$ $\|$

  $[x_1, x_2]^3 \equiv id$ id

  $[x_1, x_2] \in S_3' = A_3$

  Pl. $x^p \overset{?}{\equiv} x$ $\mathbb{Z}_p$ felett — kis Fermat-tétel

Pl. $x_1x_2 - x_2x_1 \not\equiv 0$ $M_n(\mathbb{F})$ felett

Pl. $[(x_1x_2 - x_2x_1)^2, x_3] \equiv 0$ $M_2(\mathbb{F})$-ben

- POL-EQ($\mathcal{A}$) : $p_1 \equiv p_2$

  Pl. $M_2(\mathbb{F})$ felett

  $A \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) (BA-AB)^2 \stackrel{?}{\equiv} (BA-AB)^2 A \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$

  $(BA - AB)^2$ skalármátrix

  Pl. $x_1(1\ 2\ 3)x_2 \stackrel{?}{\equiv} x_2(1\ 2)$ S_3-ban

  $x_1 = id, x_2 = id$ esetén $\neq$

POL-EQ($\mathcal{A}$) könnyű $\Rightarrow$ TERM-EQ($\mathcal{A}$) könnyű

TERM-EQ($\mathcal{A}$) nehéz $\Rightarrow$ POL-EQ($\mathcal{A}$) nehéz

Előzmények – Csoportok

- Tétel: *Novikov*, *Boone* (1955)
  A szóprobléma végesen prezentált csoportokra eldönthetetlen.

- Véges csoportokra eldönthető (behelyettesítéssel)

? Bonyolultság ? — P, NP, coNP, NP-teljes, coNP-teljes

- Tétel: *Lawrence J.*, *Willard R.* (1993)
  G véges nemfeloldható csoportra $\text{TERM-EQ}(G)$ coNP-teljes.

- Tétel: *Goldmann M.*, *Russel A.* (2001)
  G nilpotens csoportra $\text{TERM-EQ}(G)$ P-beli

- többi ?

Előzmények – Véges gyűrűk

A szóprobléma kétféle értelmezése:
$\mathcal{R}$ gyűrű

- TERM-EQ($\mathcal{R}$)
- TERM-EQ$_\Sigma$($\mathcal{R}$) : monomok összege
  Pl. $x_1 x_2^3 + x_1 + x_2 x_1 x_3 + x_{19}$
  ~~$(x_1 + x_2)^n$~~
- POL-EQ($\mathcal{R}$)
- POL-EQ$_\Sigma$($\mathcal{R}$)

Előzmények – Véges gyűrűk

- Tétel: *Burris S.*, *Lawrence J.* (1993)
  TERM-EQ($\mathcal{R}$) P-beli, ha $\mathcal{R}$ nilpotens,
  TERM-EQ($\mathcal{R}$) coNP-teljes egyébként

- Tétel: *Lawrence J.*, *Willard R.* (1997)
  ha $\mathcal{R}$ véges gyűrű $\mathcal{J}$ Jacobson-radikállal, akkor
  1. ha $\mathcal{R}/\mathcal{J}$ kommutatív, akkor TERM-EQ$_\Sigma(\mathcal{R})$ P-beli
  2. ha $\mathcal{R}$ véges egyszerű mátrixgyűrű, amelynek az invertálható elemei nemfeloldható csoportot alkotnak, akkor TERM-EQ$_\Sigma(\mathcal{R})$ coNP-teljes

- Kérdés: $M_2(\mathbb{Z}_2), M_2(\mathbb{Z}_3)$

- Tétel: *Seif S.*, *Szabó Cs.* (1997)
  $\mathcal{R}$ véges, egyszerű mátrixgyűrűre $\mathrm{POL\text{-}EQ}_{\Sigma}(\mathcal{R})$ coNP-teljes

Előzmények – Félcsoportok

- Tétel: *Seif S.*, *Szabó Cs.* (1997)
  S 0-egyszerű félcsoportra

  1. $\text{POL-EQ}(S) \iff \text{CSP}$
     Spec. $\text{POL-EQ}(M_2(\mathbb{Z}_2))$ coNP-teljes
  2. $\text{TERM-EQ}(S)$ P-beli

- Tétel: *Volkov M.* (2002)
  $\approx 2^{1700}$ elemű S félcsoport, amelyre $\text{TERM-EQ}(S)$ coNP-teljes

- Tétel: *Kisielewicz A.* (2002)

- $\leq$ néhány ezer elemszámú S félcsoport, amelyre TERM-EQ(S) coNP-teljes

$M_2(\mathbb{Z}_2)$ multiplikatív félcsoportja

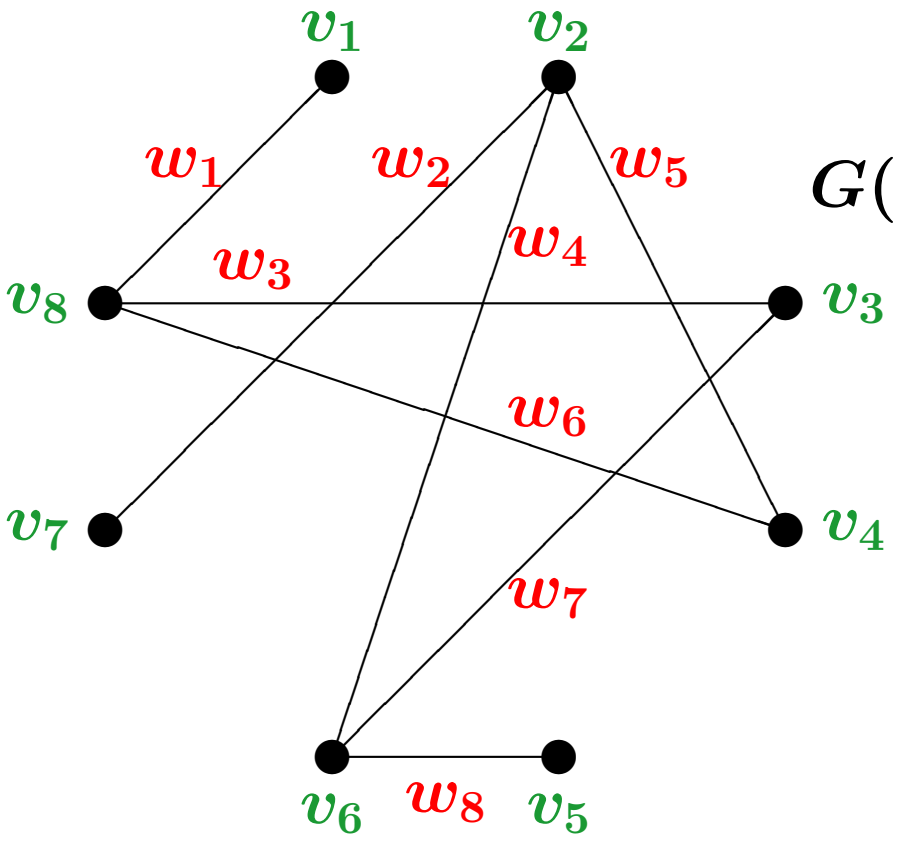
$M_2(\mathbb{Z}_2)$ ⟨ invertálható mátrixok $\simeq S_3$

szinguláris mátrixok $\simeq S$

- TERM-EQ(S_3) P-beli
- TERM-EQ(S) P-beli

DE

Tétel: $M_2(\mathbb{Z}_2)$ multiplikatív félcsoportjára TERM-EQ($M_2(\mathbb{Z}_2)$) coNP-teljes.



$G(V, E)$

$\Longleftrightarrow \quad p \equiv q$

nem 6-színezhető

$$k = (i, j) \in E\text{-re:} \quad w_k \neq 0 \iff v_i \neq v_j$$

Eredmények

- Tétel: $M_2(\mathbb{Z}_2)$ multiplikatív félcsoportjára TERM-EQ$(M_2(\mathbb{Z}_2))$ coNP-teljes.
- Köv.: TERM-EQ$_\Sigma(M_2(\mathbb{Z}_2))$ coNP-teljes.
- Köv.: $M_2(\mathbb{Z}_2)$ olyan 16 elemű félcsoport, amelyre TERM-EQ$(M_2(\mathbb{Z}_2))$ coNP-teljes.
- Köv.: $A_3 \cup S$ olyan 13 elemű félcsoport, amelyre TERM-EQ$(A_3 \cup S)$ coNP-teljes.

- Tétel: $M_2(\mathbb{Z}_3)$ multiplikatív félcsoportjára $\text{TERM-EQ}(M_2(\mathbb{Z}_3))$ coNP-teljes.

- Köv.: $\text{TERM-EQ}_\Sigma(M_2(\mathbb{Z}_3))$ coNP-teljes.

- Köv.: $n \geq 2$-re $\text{TERM-EQ}_\Sigma(M_n(T))$ coNP-teljes és $n = 1$-re P-beli.

Nyitott problémák

- Mi a bonyolultsága a szóproblémának:

  1. $M_n(T)$ multiplikatív félcsoportjában
  2. $S_1 = S \cup \{1\}$-ben

- Jellemezzük azokat az S félcsoportokat, amelyekre TERM-EQ(S) coNP-teljes. (Keressünk minél kisebbet!)