Azonosságok gyűrűkben

Vértesi Vera

Témavezető: Szabó Csaba

Országos Tudományos Diákköri Konferencia, 2005

A szóprobléma

- TERM-EQ($\mathbf{A}$)

  Adott: $\mathbf{A}$ véges algebra

  Bemenet: $t \stackrel{?}{\equiv} s$ azonoság, ahol t és s termek

  Kérdés: $t = s$ minden behelyettesítésre?

- Pl.: $x^p \stackrel{?}{\equiv} x$ $\mathbb{Z}_p$ 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

Előzmények – Csoportok

- Véges algebrákra eldönthető (behelyettesítéssel)

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

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

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

- Tétel: *Horváth G.*, *Szabó Cs.* (2003)
  G metaciklikus csoportra $\mathrm{TERM\text{-}EQ}(G)$ P-beli.

- többi?

Előzmények – Gyűrűk

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

Pl.: $\mathbb{Z}_2$
Boole-gyűrű: egységelemes, $x^2 = x$

Boole-algebra:

$$\begin{array}{rcl} x \wedge y & \leftrightarrow & x \cdot y \\ x \vee y & \leftrightarrow & x + y + xy \\ \bar{x} & \leftrightarrow & 1 + x \end{array}$$

3-SAT megfogalmazható:

$$(x_1 \vee x_2 \vee \bar{x_3}) \wedge \cdots \wedge (x_{n_1} \vee x_{n_2} \vee x_{n_3}) \rightsquigarrow$$

$$((x_1 + x_2 + x_1x_2) + (1 + x_3) + (1 + x_3)(x_1 + x_2 + x_1x_2)) \cdots$$

A szóprobléma értelmezései

TERM:

- bármilyen
  Pl.: $(x_1 + x_2 + \cdots + x_k)^n$

- TERM_Σ (monomok összege)
  Pl.: $x_1 x_2^3 x_3 + x_1 + x_2 x_1 x_3 + x_{19}$
  TERM_Σ-EQ$(\mathcal{R})$ probléma

- monomok
  TERM-EQ-probléma a multiplikatív félcsoportban

kevesebb megengedett szó $\Rightarrow$ könnyebb TERM-EQ

TERM_Σ-$\mathrm{EQ}(\mathcal{R})$ -probléma

- Tétel: *Lawrence J.*, *Willard R.* (1997)
  Ha $\mathcal{R} = M_n(\mathbb{F})$ véges egyszerű mátrixgyűrű, amelynek az invertálható elemei nemfeloldható csoportot alkotnak, akkor TERM_Σ-$\mathrm{EQ}(\mathcal{R})$ coNP-teljes

- Tétel: *Szabó*, *W* (2002)
  TERM_Σ-$\mathrm{EQ}(M_2(\mathbb{Z}_2))$ és TERM_Σ-$\mathrm{EQ}(M_2(\mathbb{Z}_3))$ is coNP-teljes.

- Köv.: Ha $\mathcal{R} = M_n(\mathbb{F})$ véges egyszerű mátrixgyűrű, akkor TERM_Σ-$\mathrm{EQ}(M_n(\mathbb{F}))$ P-beli, ha $\mathcal{R}$ kommutatív;
  és coNP-teljes egyébként.

Mátrixgyűrűk multiplikatív félcsoportja

Tétel: *Szabó*, *W* (2002-2003)
$\mathcal{R} = M_n(\mathbb{F})$ véges egyszerű mátrixgyűrű multiplikkatív félcsoportjára $\text{TERM-EQ}(M_n(\mathbb{F}))$ P-beli, ha $\mathcal{R}$ kommutatív; és coNP-teljes egyébként.

- Ha $M_n(\mathbb{F})$ multiplikatív félcsoportja kommutatív $\surd$

- Ha az invertálható elemek feloldható csoportot alkotnak:

  Tétel: *Szabó*, *W* (2002)
  $\text{TERM-EQ}(M_2(\mathbb{Z}_2))$ és $\text{TERM-EQ}(M_2(\mathbb{Z}_3))$ is coNP-teljes.

- Ha az invertálható elemek nemfeloldható csoportot alkotnak:

  Tétel: *Lawrence*, *Willard* (1993)
  Véges nemfeloldható csoportokra TERM-EQ coNP-teljes.

Visszavezetés a multiplikatív csoportra

Tétel: Minden $M_n(\mathbb{F})$ ($|\mathbb{F}| = q$) nemkommutatív mátrixgyűrűre van T, melyre:

- Ha A szinguláris, akkor A^T projekció, azaz $(A^T)^2 = A^T$;
- Van $A \in GL_n(q) \setminus SL_n(q)$, melyre $A^T \neq 1$.

Tény: Minden S véges félcsoportban van olyan s, hogy A^s projekció minden $A \in S$-re.

$S = M_n(\mathbb{F}) \setminus GL_n(q)$-re: $\quad s = \operatorname*{lkkt}_{m<n}(\exp GL_m(q))$

Keresünk T-t:

1. $\operatorname*{lkkt}_{m<n}(\exp(GL_m(q))) \mid T$;
2. de $\exp(GL_n(q)) \nmid T$.

Zsigmondy-tétel

$$|GL_m(q)| = q^{\frac{m(m-1)}{2}}(q^m - 1)\cdots(q-1)$$

Tétel: *Zsigmondy*

Legyen $1 < a, n \in \mathbb{Z}$, ekkor az $n = 2, a = 2^\alpha - 1$ és $n = 6, a = 2$ esetek kivételével létezik olyan p prím, amelyre:

1. $p \mid a^n - 1$
2. $p \nmid a^i - 1, \qquad 0 < i < n$
3. $p \nmid n$

Kivétel:

- $(2^\alpha - 1)^2 - 1 = 2^\alpha((2^\alpha - 1) - 1)$ így
  $p \mid (2^\alpha - 1)^2 - 1 \;\Rightarrow\; p \mid (2^\alpha - 1) - 1$
- $2^6 - 1 = 63 = 9 \cdot 7$ és $7 \mid 2^3 - 1, 3 \mid 2^2 - 1$

Visszavezetés a multiplikatív csoportra

Kijött: $a = q$-ra tehát van p, hogy
$(p, \underset{m<n}{\text{lkkt}}(\exp(GL_m(q)))) = 1$, így

$$\begin{aligned} T &\equiv 0 \mod \underset{m<n}{\text{lkkt}}(\exp(GL_m(q))) \\ T &\not\equiv 0 \mod p \end{aligned}$$

szimultán kongruenciarendszernek van megoldása.
Kivétel: $\ldots$

Áll: $w \overset{?}{\equiv} 1$ $GL_n(q)$-ban $\iff$ $(w^T)^2 \overset{?}{\equiv} w^T$ $M_n(\mathbb{F})$ felett

$\boxed{\Rightarrow}$ $\surd$

$\boxed{\Leftarrow}$ Ha $w \not\equiv 1$ $GL_n(q)$ felett, akkor van olyan behelyettesítés is, hogy $w^T \neq 1$ (!) így $(w^T)^2 \not\equiv w^T$ $M_n(\mathbb{F})$-ben sem. $\surd$

TERM_Σ-EQ-Probléma Gyűrűkre

- Tétel: Ha $\mathcal{R} = M_{n_1}(\mathbb{F}_1) \oplus \cdots \oplus M_{n_k}(\mathbb{F}_k)$ mátrixgyűrűk direkt összege nem kommutatív (azaz $\exists n_i \geq 1$) akkor TERM_Σ-EQ coNP-teljes.

Ha $\mathcal{R}$ véges gyűrű,
$\mathcal{J}(\mathcal{R})$ a Jacobson-radikálja
Ekkor $\mathcal{R}/\mathcal{J}(\mathcal{R}) = M_{n_1}(\mathbb{F}_1) \oplus \cdots \oplus M_{n_k}(\mathbb{F}_k)$

- Tétel: $\mathcal{R}$ véges gyűrűre $\mathrm{TERM}_\Sigma\text{-EQ}(\mathcal{R})$ P-beli, ha $\mathcal{R}/\mathcal{J}(\mathcal{R})$ kommutatív; és coNP-teljes egyébként.