The extended equivalence problem for finite groups

Gábor Horváth

Joint work with Csaba Szabó

16th July, 2007.

The Equivalence Problem

$\mathcal{A}$ finite algebra

- identity: two terms t_1, t_2 over $\mathcal{A}$.

  $t_1 \equiv t_2 \iff$ for every $a_1, \ldots, a_n \in \mathcal{A}$
  $t_1(a_1, \ldots, a_n) = t_2(a_1, \ldots, a_n)$

- equivalence problem: (identity checking problem)

  Input: two terms t_1, t_2 over $\mathcal{A}$
  Question: is $t_1 \equiv t_2$ or not?

- What is the complexity? (in the length of the terms)

Background, motivation

- See the talk of Vera Vértesi

Examples

- Ex. $x^p \equiv x$ over $\mathbb{Z}_p$ — Fermat's-theorem
- Ex. $x_1 x_2 - x_2 x_1 \not\equiv \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ over $M_n(\mathbb{F})$
- Ex. $[(x_1 x_2 - x_2 x_1)^2, x_3] \equiv \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ over $M_2(\mathbb{F})$

  since $(BA - AB)^2$ is always a scalar matrix

The first result

- Theorem: *Hunt, Stearns* (1990, *Journal of Symbolic computation)*

  $\mathcal{R}$ *is commutative, nilpotent* $\Longrightarrow$ *in P,*
  $\mathcal{R}$ *is commutative, not nilpotent* $\Longrightarrow$ *coNP-complete.*

Rings

- See the talk of Vera Vértesi

Semigroups

- See the talk of Vera Vértesi

Checking identities over Abelian groups

Given an Abelian group G

- $t(x_1, \ldots, x_n)$
  $t(x_1, \ldots, x_n) \equiv 1$ over G

Checking identities over Abelian groups

Given an Abelian group G

- $t(x_1, \ldots, x_n) = x_1^{k_1} \ldots x_n^{k_n}$
  $t(x_1, \ldots, x_n) \equiv 1$ over G

Checking identities over Abelian groups

Given an Abelian group G

- $t(x_1, \ldots, x_n) = x_1^{k_1} \ldots x_n^{k_n}$
  $t(x_1, \ldots, x_n) \equiv 1$ over G

- $x_1^{k_1} \ldots x_n^{k_n} \equiv 1$
  $x_i = 1, \forall i \neq m \implies x_m^{k_m} \equiv 1$

Checking identities over Abelian groups

Given an Abelian group G

- $t(x_1, \ldots, x_n) = x_1^{k_1} \ldots x_n^{k_n}$
  $t(x_1, \ldots, x_n) \equiv 1$ over G

- $x_1^{k_1} \ldots x_n^{k_n} \equiv 1$
  $x_i = 1, \forall i \neq m \Longrightarrow x_m^{k_m} \equiv 1$

- $\exp G \mid k_m$ for every m

Checking identities over Abelian groups

Given an Abelian group G

- $t(x_1, \ldots, x_n) = x_1^{k_1} \ldots x_n^{k_n}$
  $t(x_1, \ldots, x_n) \equiv 1$ over G

- $x_1^{k_1} \ldots x_n^{k_n} \equiv 1$
  $x_i = 1, \forall i \neq m \implies x_m^{k_m} \equiv 1$

- $\exp G \mid k_m$ for every m

- check those substitutions where only 1 variable is $\neq 1$

- $n \cdot |G|^1$ substitutions

Nilpotent groups

- Theorem: *S. Burris, J. Lawrence* (2004)
  nilpotent group (nilpotency class c) $\Longrightarrow$ in P.

- Idea of the proof:
  short normal form, long commutators are trivial

- check those substitutions where only c variable is $\neq 1$
  $\binom{n}{c} \cdot |G|^c \leq n^c \cdot |G|^c$ substitutions

Meta-cyclic groups

- Theorem: *G. Horváth, Cs. Szabó* (2005)
  meta-cyclic group, $\Longrightarrow$ in P.

- Idea of the proof:
  $G = A \rtimes B$, reduce to identity checking over $\mathbf{End}\ A$

- Works for other groups, too. Ex. A_4

Non-solvable groups

- Theorem: *J. Lawrence*
  finite simple non Abelian group $\Longrightarrow$ coNP-complete.

- Idea of the proof: *L. Mérai, Cs. Szabó* (2005)
  Polynomial reduction to $|G|$-coloring of a graph $\mathbf{\Gamma}$

- Theorem: *G. Horváth, J. Lawrence, L. Mérai, Cs. Szabó* (2006)
  Non-solvable finite group $\Longrightarrow$ coNP-complete.

Simple groups

$$G = \{1\} \cup \{g \mid g \neq 1\}$$

$$[G, 1] = 1, \; [G, g] = G$$

Simple groups

$$G = \{1\} \cup \{g \mid g \neq 1\}$$

$$[G, 1] = 1, \ [G, g] = G$$

$$[[[\ldots[G, \bullet], \bullet]\ldots], \bullet]\ldots] = 1$$

Simple groups

$$G = \{1\} \cup \{g \mid g \neq 1\}$$

$$[G, 1] = 1, \;\; [G, g] = G$$

$$[[[\ldots[G, \bullet], \bullet]\ldots], \bullet]\ldots] = 1$$

$$[[[\ldots[G, \bullet], \bullet]\ldots], \bullet], \bullet], \bullet] = G$$

Simple groups

$$G = \{1\} \cup \{g \mid g \neq 1\}$$

$$[G, 1] = 1, \ [G, g] = G$$

$$[[[\ldots[G, \bullet], \bullet]\ldots], \bullet]\ldots] = 1$$

$$[[[\ldots[G, \bullet], \bullet]\ldots], \bullet], \bullet], \bullet] = G$$

graph $\mathbf{\Gamma}$

Simple groups

$G = \{1\} \cup \{g \mid g \neq 1\}$

$[G, 1] = 1,\ [G, g] = G$

$[[[\dots[G, \bullet], \bullet]\dots], \bullet]\dots] = 1$

$[[[\dots[G, \bullet], \bullet]\dots], \bullet], \bullet], \bullet] = G$

graph Γ

$[[[\dots\ [[y, e_1], e_2]\dots], e_k]], \dots], e_m] = w$

Simple groups

$$G = \{1\} \cup \{g \mid g \neq 1\}$$

$$[G, 1] = 1, \ \ [G, g] = G$$

$$[[[\ldots [G, \bullet], \bullet] \ldots], \bullet] \ldots] = 1$$

$$[[[\ldots [G, \bullet], \bullet] \ldots], \bullet], \bullet], \bullet] = G$$

graph Γ

$$[[[\ldots \ [[y, e_1], e_2] \ldots], e_k]], \ldots], e_m] = w$$

$$e \rightsquigarrow x_i x_j^{-1}$$

Simple groups

$$[[[\dots[G, \bullet], \bullet]\dots], \bullet]\dots] = 1$$

$$[[[\dots[G, \bullet], \bullet]\dots], \bullet], \bullet], \bullet] = G$$

$$[[[\dots\ [[y, e_1], e_2]\dots], e_k]], \dots], e_m] = w,$$

$$e \rightsquigarrow x_i x_j^{-1}$$

Simple groups

$$[[[\ldots[G,\bullet],\bullet]\ldots],\bullet]\ldots] = 1$$

$$[[[\ldots[G,\bullet],\bullet]\ldots],\bullet],\bullet],\bullet] = G$$

$$[[[\ldots\ [[y,e_1],e_2]\ldots],e_k]],\ldots],e_m] = w,$$

$$e \rightsquigarrow x_i x_j^{-1}$$

$$w \neq 1$$

Simple groups

$$[[[\ldots[G, \bullet], \bullet]\ldots], \bullet]\ldots] = 1$$

$$[[[\ldots[G, \bullet], \bullet]\ldots], \bullet], \bullet], \bullet] = G$$

$$[[[\ldots\ [[y, e_1], e_2]\ldots], e_k]], \ldots], e_m] = w,$$

$$e \rightsquigarrow x_i x_j^{-1}$$

$$w \not\equiv 1 \iff \text{all } e \neq 1$$

Simple groups

$$[[[\ldots[G,\bullet],\bullet]\ldots],\bullet]\ldots] = 1$$

$$[[[\ldots[G,\bullet],\bullet]\ldots],\bullet],\bullet],\bullet] = G$$

$$[[[\ldots\ [[y,e_1],e_2]\ldots],e_k]],\ldots],e_m] = w,$$

$$e \rightsquigarrow x_i x_j^{-1}$$

$w \not\equiv 1 \iff$ all $e \neq 1 \iff$ all $x_i \neq x_j$

Simple groups

$$[[[\ldots[G,\bullet],\bullet]\ldots],\bullet]\ldots] = 1$$

$$[[[\ldots[G,\bullet],\bullet]\ldots],\bullet],\bullet],\bullet] = G$$

$$[[[\ldots\ [[y,e_1],e_2]\ldots],e_k]],\ldots],e_m] = w,$$

$$e \rightsquigarrow x_i x_j^{-1}$$

$w \not\equiv 1 \iff$ all $e \neq 1 \iff$ all $x_i \neq x_j \iff \Gamma$ is $|G|$-colorable

Correction...

Major problem:

- $w = [[[\ldots\ [[y, e_1], e_2]\ldots], e_k]], \ldots], e_m]$ has length $\approx 2^m$
- use $\left[\left[\,[y_1, e_1]\,, [y_2, e_2]\,\right], \left[\,[y_3, e_3]\,, [y_4, e_4]\,\right]\right]\ldots$
- Length is $O\left(4^{\log_2 m}\right) = O(m^2)$

Universal word (structure is the same)

Save the proof!

- Does not work over $\boldsymbol{G} = \left(\boldsymbol{G}, \mathbf{1}, ^{-1}, \cdot\right)$
- Works over $(\boldsymbol{G}, [,]) = \left(\boldsymbol{G}, \mathbf{1}, ^{-1}, \cdot, [,]\right)$
- $(\boldsymbol{G}, \boldsymbol{f}_1, \ldots, \boldsymbol{f}_n)$, where $\boldsymbol{f}_i$ is a group term

- The expressions shorten! $\Longrightarrow$ The complexity might change!

The extended equivalence problem

$(G, f_1, \ldots, f_n)$, where f_i is a group term

The extended equivalence is

- in P: *every* $f_1, \ldots f_n$ the equivalence problem for $(G, f_1, \ldots, f_n)$ is in P
- coNP-complete: *exist* $f_1, \ldots f_n$ that the equivalence problem for $(G, f_1, \ldots, f_n)$ is coNP-complete

Nilpotent groups

- Theorem:
  nilpotent group (nilpotency class c) $\Longrightarrow$ extended equivalence is in P.

- Idea of the proof:
  same as for the equivalence problem

- check those substitutions where only c variable is $\neq 1$
  $\binom{n}{c} \cdot |G|^c \leq n^c \cdot |G|^c$ substitutions

Non-nilpotent groups

non-solvable $\Longrightarrow$ extended equivalence is coNP-complete

non-nilpotent, solvable:

- $[[[\ldots\ [[y, e_1], e_2] \ldots], e_k]], \ldots], e_m] = w$
- $[[[\ldots\ [[G, G], G] \ldots], G]], \ldots], G] = N$
- $[N, C_G(N)] = 1$
- The wrong proof works with $|G/C_G(N)|$-coloring $\Longrightarrow$ coNP-complete for $(G, [,])$

Non-nilpotent groups

- $|G : C_G(N)| = 2$ we do not know the complexity for $(G, [,])$
- special case: N is Abelian
- investigation of $\mathbf{End}\, N$ (talk of Vera Vértesi)
  $\Longrightarrow$ group term f, such that (G, f) is coNP-complete
- induction on $|G|$
- Theorem: *G. Horváth*, *Cs. Szabó* (2007)
  non-nilpotent, solvable group $\Longrightarrow$ extended equivalence is coNP-complete

Summary

	equiv.	ext. equiv.
nilpotent	P	P
solvable	? P ?	coNP-complete, f
non-solvable	coNP-complete	coNP-complete
S_3	P	coNP-complete, [,] ?
A_4	P	coNP-complete, [,]
S_4	?	coNP-complete, [,]