Some new results on the equivalence problem

Gábor Horváth

University of Debrecen, Hungary

September 8, 2014

The equivalence (identity checking) problem

fixed finite algebra $\mathcal{A}$

Identity

two polynomials p_1, p_2 over $\mathcal{A}$

$$p_1 \approx p_2 \iff \begin{array}{l}\text{for every } a_1, \ldots, a_n \in \mathcal{A} \\ p_1(a_1, \ldots, a_n) = p_2(a_1, \ldots, a_n)\end{array}$$

Equivalence problem (identity checking problem)

Input: two polynomials p_1, p_2 over $\mathcal{A}$
Question: is $p_1 \approx p_2$ or not?

What is the complexity?
Always in coNP.

The equation solvability problem

fixed finite algebra $\mathcal{A}$

Equation solvability problem

Input: two polynomials p_1, p_2 over $\mathcal{A}$
Question: is $p_1 = p_2$ solvable or not?

Always decidable.
What is the complexity?
Always in NP.

Boolean algebra $\mathcal{B}$

Equation solvability

- NP-complete
- SAT, 3-SAT
- $(x_1 \vee x_2 \vee x_3) \wedge (x_4 \vee x_5 \vee \bar{x}_6) \wedge \cdots \stackrel{?}{=} 1$

Equivalence

- coNP-complete
- 'polynomial reduction' to 3-SAT
- $(x_1 \vee x_2 \vee x_3) \wedge (x_4 \vee x_5 \vee \bar{x}_6) \wedge \cdots \stackrel{?}{\approx} 0$

$\mathrm{Aut}(f) = \mathrm{Aut}\,\mathcal{B}$ or $\mathrm{Aut}(f) = \mathrm{Aut}\,\mathcal{M}$?

Theorem (Bodor, Kalina, Szabó (2014))

$\mathrm{Aut}(f) \in \{\mathrm{Aut}\,\mathcal{B}, \mathrm{Aut}\,\mathcal{M}\}$ *for nonlinear* f,
$\mathrm{Aut}(f) = \mathrm{Aut}\,\mathcal{B} \iff f(x_1, x_2, \ldots, x_n) \approx f(0, x_2 + x_1, \ldots, x_n + x_1)$

- Input: $f(x_1, x_2, \ldots, x_n)$
- Question: $\mathrm{Aut}(f) = \mathrm{Aut}\,\mathcal{B}$ or $\mathrm{Aut}(f) = \mathrm{Aut}\,\mathcal{M}$?

$\mathrm{Aut}(f) = \mathrm{Aut}\,\mathcal{B}$ or $\mathrm{Aut}(f) = \mathrm{Aut}\,\mathcal{M}$?

Theorem (Bodor, Kalina, Szabó (2014))

$\mathrm{Aut}(f) \in \{\mathrm{Aut}\,\mathcal{B}, \mathrm{Aut}\,\mathcal{M}\}$ *for nonlinear* f,
$\mathrm{Aut}(f) = \mathrm{Aut}\,\mathcal{B} \iff f(x_1, x_2, \ldots, x_n) \approx f(0, x_2 + x_1, \ldots, x_n + x_1)$

- Input: $f(x_1, x_2, \ldots, x_n)$
- Question: $f(x_1, x_2, \ldots, x_n) \approx f(0, x_2 + x_1, \ldots, x_n + x_1)$?

$\mathrm{Aut}(f) = \mathrm{Aut}\,\mathcal{B}$ or $\mathrm{Aut}(f) = \mathrm{Aut}\,\mathcal{M}$?

Theorem (Bodor, Kalina, Szabó (2014))

$\mathrm{Aut}(f) \in \{\mathrm{Aut}\,\mathcal{B}, \mathrm{Aut}\,\mathcal{M}\}$ *for nonlinear* f,
$\mathrm{Aut}(f) = \mathrm{Aut}\,\mathcal{B} \iff f(x_1, x_2, \ldots, x_n) \approx f(0, x_2 + x_1, \ldots, x_n + x_1)$

- Input: $f(x_1, x_2, \ldots, x_n)$
- Question: $f(x_1, x_2, \ldots, x_n) \approx f(0, x_2 + x_1, \ldots, x_n + x_1)$?
- $x_1 = 0 \Longrightarrow f(0, x_2, \ldots, x_n) \approx f(0, x_2 + 0, \ldots, x_n + 0)$

$\mathrm{Aut}(f) = \mathrm{Aut}\,\mathcal{B}$ or $\mathrm{Aut}(f) = \mathrm{Aut}\,\mathcal{M}$?

Theorem (Bodor, Kalina, Szabó (2014))

$\mathrm{Aut}(f) \in \{\mathrm{Aut}\,\mathcal{B}, \mathrm{Aut}\,\mathcal{M}\}$ *for nonlinear* f,
$\mathrm{Aut}(f) = \mathrm{Aut}\,\mathcal{B} \iff f(x_1, x_2, \ldots, x_n) \approx f(0, x_2 + x_1, \ldots, x_n + x_1)$

- Input: $f(x_1, x_2, \ldots, x_n)$
- Question: $f(x_1, x_2, \ldots, x_n) \approx f(0, x_2 + x_1, \ldots, x_n + x_1)$?
- $x_1 = 0 \Longrightarrow f(0, x_2, \ldots, x_n) \approx f(0, x_2 + 0, \ldots, x_n + 0)$

Question is $x_1 = 1$:

$$f(1, x_2, \ldots, x_n) \approx f(0, x_2 + 1, \ldots, x_n + 1)?$$

$\mathrm{Aut}(f) = \mathrm{Aut}\,\mathcal{B}$ or $\mathrm{Aut}(f) = \mathrm{Aut}\,\mathcal{M}$?

Theorem (Bodor, Kalina, Szabó (2014))

$\mathrm{Aut}(f) \in \{\mathrm{Aut}\,\mathcal{B}, \mathrm{Aut}\,\mathcal{M}\}$ *for nonlinear* f,
$\mathrm{Aut}(f) = \mathrm{Aut}\,\mathcal{B} \iff f(x_1, x_2, \ldots, x_n) \approx f(0, x_2 + x_1, \ldots, x_n + x_1)$

- Input: $f(x_1, x_2, \ldots, x_n)$
- Question: $f(x_1, x_2, \ldots, x_n) \approx f(0, x_2 + x_1, \ldots, x_n + x_1)$?
- $x_1 = 0 \Longrightarrow f(0, x_2, \ldots, x_n) \approx f(0, x_2 + 0, \ldots, x_n + 0)$

Question is $x_1 = 1$:

$$f(1, x_2, \ldots, x_n) \approx f(0, x_2 + 1, \ldots, x_n + 1)?$$
$$f(1, x_2, \ldots, x_n) \approx f(0, \bar{x}_2, \ldots, \bar{x}_n)?$$

$f(1, x_2, \ldots, x_n) \approx f(0, \bar{x}_2, \ldots, \bar{x}_n)$?

reduce to $g(x_2, \ldots, x_n) \approx 0$

Let

$$f(x_1, x_2, \ldots, x_n) := \bar{x}_1 \wedge g(\bar{x}_2, \ldots, \bar{x}_n).$$

$$f(1, x_2, \ldots, x_n) \approx f(0, \bar{x}_2, \ldots, \bar{x}_n)$$

$f(1, x_2, \ldots, x_n) \approx f(0, \bar{x}_2, \ldots, \bar{x}_n)$?

reduce to $g(x_2, \ldots, x_n) \approx 0$

Let

$$f(x_1, x_2, \ldots, x_n) := \bar{x}_1 \wedge g(\bar{x}_2, \ldots, \bar{x}_n).$$

$$f(1, x_2, \ldots, x_n) \approx f(0, \bar{x}_2, \ldots, \bar{x}_n)$$

$$\Updownarrow$$

$$\bar{1} \wedge g(\bar{x}_2, \ldots, \bar{x}_n) \approx \bar{0} \wedge g(\bar{\bar{x}}_2, \ldots, \bar{\bar{x}}_n)$$

$f(1, x_2, \ldots, x_n) \approx f(0, \bar{x}_2, \ldots, \bar{x}_n)$?

reduce to $g(x_2, \ldots, x_n) \approx 0$

Let

$$f(x_1, x_2, \ldots, x_n) := \bar{x}_1 \wedge g(\bar{x}_2, \ldots, \bar{x}_n).$$

$$\begin{array}{c} f(1, x_2, \ldots, x_n) \approx f(0, \bar{x}_2, \ldots, \bar{x}_n) \\ \Updownarrow \\ \bar{1} \wedge g(\bar{x}_2, \ldots, \bar{x}_n) \approx \bar{0} \wedge g(\bar{\bar{x}}_2, \ldots, \bar{\bar{x}}_n) \\ \Updownarrow \\ 0 \approx g(x_2, \ldots, x_n) \end{array}$$

$f(1, x_2, \ldots, x_n) \approx f(0, \bar{x}_2, \ldots, \bar{x}_n)$?

reduce to $g(x_2, \ldots, x_n) \approx 0$

Let

$$f(x_1, x_2, \ldots, x_n) := \bar{x}_1 \wedge g(\bar{x}_2, \ldots, \bar{x}_n).$$

$$\begin{array}{c} f(1, x_2, \ldots, x_n) \approx f(0, \bar{x}_2, \ldots, \bar{x}_n) \\ \Updownarrow \\ \bar{1} \wedge g(\bar{x}_2, \ldots, \bar{x}_n) \approx \bar{0} \wedge g(\bar{\bar{x}}_2, \ldots, \bar{\bar{x}}_n) \\ \Updownarrow \\ 0 \approx g(x_2, \ldots, x_n) \end{array}$$

$\Longrightarrow \mathrm{Aut}(f) = \mathrm{Aut}\,\mathcal{B}$ is coNP-complete

Rings

Theorem (Hunt, Stearnes (1990), Burris, Lawrence (1993), Horváth (2010), Károlyi, Szabó (2010))

$\mathcal{R}$ is nilpotent $\Longrightarrow$ problems are in P,

$\mathcal{R}$ is not nilpotent $\Longrightarrow$ problems are (co)NP-complete.

Rings

Theorem (Hunt, Stearnes (1990), Burris, Lawrence (1993), Horváth (2010), Károlyi, Szabó (2010))

$\mathcal{R}$ is nilpotent $\Longrightarrow$ problems are in P,
$\mathcal{R}$ is not nilpotent $\Longrightarrow$ problems are (co)NP-complete.

Sigma problems

- input polynomial is sum of monomials
- E.g. $x_1 x_2^3 + x_1 + x_2 x_1 x_3 + x_{19}$
- $(x_1 + x_2)^n$ is not allowed

Rings

Theorem (Hunt, Stearnes (1990), Burris, Lawrence (1993), Horváth (2010), Károlyi, Szabó (2010))

$\mathcal{R}$ is nilpotent $\Longrightarrow$ problems are in P,
$\mathcal{R}$ is not nilpotent $\Longrightarrow$ problems are (co)NP-complete.

Sigma problems

- input polynomial is sum of monomials
- E.g. $x_1x_2^3 + x_1 + x_2x_1x_3 + x_{19}$
- $(x_1 + x_2)^n$ is not allowed

Theorem (Szabó, Vértesi (2009), Horváth, Lawrence, Willard (2012))

$\mathcal{R}/\mathcal{J}$ is comm. $\Longrightarrow$ sigma problems are in P,
$\mathcal{R}/\mathcal{J}$ is not comm. $\Longrightarrow$ sigma problems are (co)NP-complete.

Groups

Theorem (Goldmann, Russell (1999), Horváth, Lawrence, Mérai, Szabó (2007))

G is not solvable $\Longrightarrow$ problems are (co)NP-complete.

Theorem (Goldmann, Russell (1999), Burris, Lawrence (2004), Horváth (2010))

G is nilpotent $\Longrightarrow$ problems are in P.

Meta-Abelian groups

Theorem (Horváth, Szabó (2006, 2010), Horváth (2014))

$G = A \rtimes B$, A, B are Abelian $\Longrightarrow$ equivalence is in P.
similar theorem for equation solvability, more technical

Example

S_3, A_4

$G = A \rtimes B$

Meta-Abelian groups

Theorem (Horváth, Szabó (2006, 2010), Horváth (2014))

$G = A \rtimes B$, A, B are Abelian $\Longrightarrow$ equivalence is in P.
similar theorem for equation solvability, more technical

Example

S_3, A_4

$G = A \rtimes B$

- $\varphi\colon B \to \operatorname{Aut} A$

Meta-Abelian groups

Theorem (Horváth, Szabó (2006, 2010), Horváth (2014))

$G = A \rtimes B$, A, B are Abelian $\Longrightarrow$ equivalence is in P.
similar theorem for equation solvability, more technical

Example

S_3, A_4

$G = A \rtimes B$

- $\varphi\colon B \to \operatorname{Aut} A$
- $\mathcal{S} := \varphi(B)$

Meta-Abelian groups

Theorem (Horváth, Szabó (2006, 2010), Horváth (2014))

$G = A \rtimes B$, A, B are Abelian $\Longrightarrow$ equivalence is in P.
similar theorem for equation solvability, more technical

Example

S_3, A_4

$G = A \rtimes B$

- $\varphi\colon B \to \operatorname{Aut} A$
- $\mathcal{S} := \varphi(B)$
- $\mathcal{R} = \langle \mathcal{S} \rangle \leq \operatorname{End} A$, commutative if B is commutative

Meta-Abelian groups

Theorem (Horváth, Szabó (2006, 2010), Horváth (2014))

$G = A \rtimes B$, A, B are Abelian $\Longrightarrow$ equivalence is in P.
similar theorem for equation solvability, more technical

Example

S_3, A_4

$G = A \rtimes B$

- $\varphi\colon B \to \operatorname{Aut} A$
- $\mathcal{S} := \varphi(B)$
- $\mathcal{R} = \langle \mathcal{S} \rangle \leq \operatorname{End} A$, commutative if B is commutative
- reduces to sigma problems over $\mathcal{R}$, BUT

Meta-Abelian groups

Theorem (Horváth, Szabó (2006, 2010), Horváth (2014))

$G = A \rtimes B$, A, B are Abelian $\Longrightarrow$ equivalence is in P.
similar theorem for equation solvability, more technical

Example

S_3, A_4

$G = A \rtimes B$

- $\varphi\colon B \to \operatorname{Aut} A$
- $\mathcal{S} := \varphi(B)$
- $\mathcal{R} = \langle \mathcal{S} \rangle \leq \operatorname{End} A$, commutative if B is commutative
- reduces to sigma problems over $\mathcal{R}$, BUT
  Substitutions only from $\mathcal{S}$

$$f(x_1, \ldots, x_n) \stackrel{?}{\approx} 0, \qquad (x_i \in \mathcal{S})$$

$$f(x_1, \ldots, x_n) \stackrel{?}{=} 0, \qquad (x_i \in \mathcal{S})$$

Sigma problems with substitutions

Theorem (Horváth (2014))

$\mathcal{R}$ is a commutative ring, $\mathcal{S} \leq \mathcal{R}^\times$
$\Longrightarrow$ sigma equivalence with substitutions from $\mathcal{S}$ is in P

Proof.

Sigma problems with substitutions

Theorem (Horváth (2014))

$\mathcal{R}$ is a commutative ring, $\mathcal{S} \leq \mathcal{R}^\times$
$\Longrightarrow$ sigma equivalence with substitutions from $\mathcal{S}$ is in P

Proof.

$$\mathcal{R} \quad = \quad \mathcal{R}_1 \quad \oplus \quad \ldots \quad \oplus \quad \mathcal{R}_k \qquad\qquad \mathcal{R}_i \text{ local (Pierce)}$$

□

Sigma problems with substitutions

Theorem (Horváth (2014))

$\mathcal{R}$ is a commutative ring, $\mathcal{S} \leq \mathcal{R}^\times$
$\Longrightarrow$ sigma equivalence with substitutions from $\mathcal{S}$ is in P

Proof.

$$\mathcal{R}^\times = {\mathcal{R}_1}^\times \oplus \ldots \oplus {\mathcal{R}_k}^\times \qquad \mathcal{R}_i \text{ local (Pierce)}$$

□

Sigma problems with substitutions

Theorem (Horváth (2014))

$\mathcal{R}$ is a commutative ring, $\mathcal{S} \leq \mathcal{R}^\times$
$\Longrightarrow$ sigma equivalence with substitutions from $\mathcal{S}$ is in P

Proof.

$$\begin{array}{c} \mathcal{S} \\ \leq \\ \mathcal{R}^\times \end{array} \quad = \quad {\mathcal{R}_1}^\times \quad \oplus \quad \ldots \quad \oplus \quad {\mathcal{R}_k}^\times \qquad \begin{array}{l} \mathcal{R}_i \text{ local} \\ \text{(Pierce)} \end{array}$$

□

Sigma problems with substitutions

Theorem (Horváth (2014))

$\mathcal{R}$ is a commutative ring, $\mathcal{S} \leq \mathcal{R}^\times$
$\Longrightarrow$ sigma equivalence with substitutions from $\mathcal{S}$ is in P

Proof.

$$\begin{array}{ccccccccc} \mathcal{S} & & \mathcal{S}_1 & & \dots & & \mathcal{S}_k & & \\ \leq & & \leq & & \dots & & \leq & & \\ \mathcal{R}^\times & = & {\mathcal{R}_1}^\times & \oplus & \dots & \oplus & {\mathcal{R}_k}^\times & & \mathcal{R}_i \text{ local} \\ & & & & & & & & \text{(Pierce)} \end{array}$$

□

Sigma problems with substitutions

Theorem (Horváth (2014))

$\mathcal{R}$ is a commutative ring, $\mathcal{S} \leq \mathcal{R}^\times$
$\Longrightarrow$ sigma equivalence with substitutions from $\mathcal{S}$ is in P

Proof.

$$\begin{array}{ccccccccc} \mathcal{S} & & \mathcal{S}_1 & & \dots & & \mathcal{S}_k & & \\ \leq & & \leq & & \dots & & \leq & & \\ \mathcal{R}^\times & = & {\mathcal{R}_1}^\times & \oplus & \dots & \oplus & {\mathcal{R}_k}^\times & & \mathcal{R}_i \text{ local} \\ & & & & & & & & \text{(Pierce)} \end{array}$$

local rings ✓(similar proof as for $\mathcal{S} = \mathcal{R}$)

□

Sigma problems with substitutions

Theorem (Horváth (2014))

$\mathcal{R}$ is a commutative ring, $\mathcal{S} \leq \mathcal{R}^\times$
$\Longrightarrow$ sigma equivalence with substitutions from $\mathcal{S}$ is in P

Proof.

$$\begin{array}{ccccccccc} \mathcal{S} & & \mathcal{S}_1 & & \dots & & \mathcal{S}_k & & \\ \leq & & \leq & & \dots & & \leq & & \\ \mathcal{R}^\times & = & {\mathcal{R}_1}^\times & \oplus & \dots & \oplus & {\mathcal{R}_k}^\times & & \mathcal{R}_i \text{ local} \\ & & & & & & & & \text{(Pierce)} \end{array}$$

local rings ✓(similar proof as for $\mathcal{S} = \mathcal{R}$)
equivalence can be checked componentwise

□

Sigma problems with substitutions

Theorem (Horváth (2014))

$\mathcal{R}$ is a commutative ring, $\mathcal{S} \leq \mathcal{R}^\times$
$\Longrightarrow$ sigma equivalence with substitutions from $\mathcal{S}$ is in P

Proof.

$$\begin{array}{ccccccccc} \mathcal{S} & & \mathcal{S}_1 & & \dots & & \mathcal{S}_k & & \\ \leq & & \leq & & \dots & & \leq & & \\ \mathcal{R}^\times & = & {\mathcal{R}_1}^\times & \oplus & \dots & \oplus & {\mathcal{R}_k}^\times & & \mathcal{R}_i \text{ local} \\ & & & & & & & & \text{(Pierce)} \end{array}$$

local rings ✓(similar proof as for $\mathcal{S} = \mathcal{R}$)
equivalence can be checked componentwise
equation solvability can be checked componentwise □

Equation solvability componentwise?

Example

$\mathcal{R} = \mathbb{Z}_{12} = \mathbb{Z}_3 \oplus \mathbb{Z}_4$
$\mathcal{S} = \{1, -1\} = \{(1,1), (-1,-1)\}$

$$x + 5 = 0$$

No solutions over $\mathbb{Z}_{12}$ from $\{1, -1\}$, but
$x = 1$ is a solution in $\mathbb{Z}_3$
$x = -1$ is a solution in $\mathbb{Z}_4$

Trouble

$(1, -1) \in \mathcal{S}_1 \oplus \mathcal{S}_2$, but $(1, -1) \notin \mathcal{S}$

Sigma problems with substitutions

Theorem (Horváth (2014))

$\mathcal{R}$ is a commutative ring, $\mathcal{S} \leq \mathcal{R}^\times$
$\Longrightarrow$ sigma equivalencewith substitutions from $\mathcal{S}$ is in P

Proof.

$$\begin{array}{ccccccccc} \mathcal{S} & & \mathcal{S}_1 & & \dots & & \mathcal{S}_k & & \\ \leq & & \leq & & \dots & & \leq & & \\ \mathcal{R}^\times & = & \mathcal{R}_1^\times & \oplus & \dots & \oplus & \mathcal{R}_k^\times & & \mathcal{R}_i \text{ local} \\ & & & & & & & & \text{(Pierce)} \end{array}$$

local rings ✓(similar proof as for $\mathcal{S} = \mathcal{R}$)
equivalence can be checked componentwise
equation solvability can be checked componentwise □

Sigma problems with substitutions

Theorem (Horváth (2014))

$\mathcal{R}$ is a commutative ring, $\mathcal{S} \leq \mathcal{R}^\times$
$\Longrightarrow$ sigma equivalencewith substitutions from $\mathcal{S}$ is in P

Proof.

$$\begin{array}{ccccccc} \mathcal{S} & = & \mathcal{S}_1 & \oplus & \dots & \oplus & \mathcal{S}_k \\ \leq & & \leq & & \dots & & \leq \\ \mathcal{R}^\times & = & \mathcal{R}_1^\times & \oplus & \dots & \oplus & \mathcal{R}_k^\times \end{array} \qquad \mathcal{R}_i \text{ local (Pierce)}$$

local rings ✓(similar proof as for $\mathcal{S} = \mathcal{R}$)
equivalence can be checked componentwise
equation solvability can be checked componentwise □

Sigma problems with substitutions

Theorem (Horváth (2014))

$\mathcal{R}$ is a commutative ring, $\mathcal{S} \leq \mathcal{R}^\times$
$\Longrightarrow$ sigma equivalencewith substitutions from $\mathcal{S}$ is in P

Proof.

$$\begin{array}{ccccccc} \mathcal{S} & = & \mathcal{S}_1 & \oplus & \dots & \oplus & \mathcal{S}_k \\ \leq & & \leq & & \dots & & \leq \\ \mathcal{R}^\times & = & \mathcal{R}_1^\times & \oplus & \dots & \oplus & \mathcal{R}_k^\times \end{array} \qquad \mathcal{R}_i \text{ local (Pierce)}$$

local rings ✓(similar proof as for $\mathcal{S} = \mathcal{R}$)
equivalence can be checked componentwise
equation solvability can be checked componentwise ✓ □

Sigma problems with substitutions

Theorem (Horváth (2014))

$\mathcal{R}$ is a commutative ring, $\mathcal{S} \leq \mathcal{R}^\times$
$\Longrightarrow$ sigma equivalencewith substitutions from $\mathcal{S}$ is in P
$\mathcal{S} = \mathcal{S}_1 \oplus \cdots \oplus \mathcal{S}_k$
$\Longrightarrow$ sigma equation solvability with substitutions from $\mathcal{S}$ is in P

Proof.

$$\begin{array}{ccccccc} \mathcal{S} & = & \mathcal{S}_1 & \oplus & \dots & \oplus & \mathcal{S}_k \\ \leq & & \leq & & \dots & & \leq \\ \mathcal{R}^\times & = & \mathcal{R}_1^\times & \oplus & \dots & \oplus & \mathcal{R}_k^\times \end{array} \qquad \mathcal{R}_i \text{ local (Pierce)}$$

local rings ✓(similar proof as for $\mathcal{S} = \mathcal{R}$)
equivalence can be checked componentwise
equation solvability can be checked componentwise ✓ □

Open questions

Rings (sigma problems, substitutions from $\mathcal{S}$)

- $\mathcal{R}$ is not commutative
- equation solvability for $\mathcal{S} \neq \mathcal{S}_1 \oplus \cdots \oplus \mathcal{S}_k$

Groups

- $S_4 = S_3 \rtimes V$, S_3 is not Abelian
- $SL_2(3) = Q \rtimes Z_3$, Q is not Abelian
- $U(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^{\times}$, $U(3, \mathbb{Z}_3)$ is not Abelian
- $D_{12} = Z_{12} \rtimes Z_2$ ($\mathcal{R} = \mathbb{Z}_{12}$, $\mathcal{S} \neq \mathcal{S}_1 \oplus \mathcal{S}_2$)
- $Z_3 \rtimes Q$ (equation solvability)
- $(Z_2 \times Z_2 \times Z_3) \rtimes Z_2$ (equation solvability)

Open questions

Rings (sigma problems, substitutions from $\mathcal{S}$)

- $\mathcal{R}$ is not commutative
- equation solvability for $\mathcal{S} \neq \mathcal{S}_1 \oplus \cdots \oplus \mathcal{S}_k$

Groups

- $S_4 = S_3 \rtimes V$, S_3 is not Abelian
- $SL_2(3) = Q \rtimes Z_3$, Q is not Abelian
- $U(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^\times$, $U(3, \mathbb{Z}_3)$ is not Abelian
- $D_{12} = Z_{12} \rtimes Z_2$ ($\mathcal{R} = \mathbb{Z}_{12}$, $\mathcal{S} \neq \mathcal{S}_1 \oplus \mathcal{S}_2$)
- $Z_3 \rtimes Q$ (equation solvability)
- $(Z_2 \times Z_2 \times Z_3) \rtimes Z_2$ (equation solvability)

Theorem (Földvári (2014))

$SL_2(3)$, $U(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^\times \Longrightarrow$ *problems are in P.*