Complexity of solving equations in finite algebras

Gábor Horváth

University of Debrecen, Hungary

July 20, 2015

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.

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.

Easy observations about rings

- $p_1 \approx p_2 \iff p_1 - p_2 \approx 0$
- $p_1 = p_2$ solvable $\iff p_1 - p_2 = 0$ solvable

solvability in P $\Longrightarrow$ equivalence in P

- $\mathcal{R} = \{r_0, r_1, \ldots, r_N\}$
- $r_0 = 0$
- $p(x) \not\approx 0 \iff p(x) = r_i$ solvable for some $1 \leq i$
- solving $p(x) = r_1$, solving $p(x) = r_2$, $\ldots$, solving $p(x) = r_N$ $\Longrightarrow$ deciding $p(x) \approx 0$

solvability in P over $\mathcal{R}$ $\Longrightarrow$ solvability in P over $\mathcal{R}/\mathcal{I}$

$f(x) = 0$ over $\mathcal{R}/\mathcal{I} \iff f(x) = r_i \in \mathcal{I}$ over $\mathcal{R}$

Easy observations about rings (cont.)

equivalence in P $\Longrightarrow$ equation solvability in P ???

- not in general
- Klíma: monoid M
  equivalence over M is in P
  equations solvability over M is NP-complete

Finite field $\mathcal{F}_q$

- $a \neq 0 \iff a^{q-1} = 1$
- $a = 0 \iff a^{q-1} \neq 1$
- $p(x) = 0$ is solvable $\iff p(x)^{q-1} \not\approx 1$

Easy observations about rings (cont.)

equivalence in P $\Longrightarrow$ equation solvability in P ???

- not in general
- Klíma: monoid M
  equivalence over M is in P
  equations solvability over M is NP-complete

Finite field $\mathcal{F}_q$

- $a \neq 0 \iff a^{q-1} = 1$
- $a = 0 \iff a^{q-1} \neq 1$
- $p(x) = 0$ is solvable $\iff p(x)^{q-1} \not\approx 1$
- $\begin{array}{rcl} p_1(x) & = & 0, \\ \vdots & \vdots & \vdots \\ p_k(x) & = & 0 \end{array}$ is solvable $\iff (p_1(x) \dots p_k(x))^{q-1} \not\approx 1$

Rings

Theorem (Hunt, Stearnes (1990), Burris, Lawrence (1993))

$\mathcal{R}$ is nilpotent $\Longrightarrow$ equivalence is in P

$\mathcal{R}$ is not nilpotent $\Longrightarrow$ equivalence, solvability is (co)NP-complete

Theorem (Horváth (2011))

$\mathcal{R}$ is nilpotent $\Longrightarrow$ solvability is in P

Rings

Theorem (Hunt, Stearnes (1990), Burris, Lawrence (1993))

$\mathcal{R}$ is nilpotent $\Longrightarrow$ equivalence is in P

$\mathcal{R}$ is not nilpotent $\Longrightarrow$ equivalence, solvability is (co)NP-complete

Theorem (Horváth (2011))

$\mathcal{R}$ is nilpotent $\Longrightarrow$ solvability is in P

Proof

Ramsey's theorem, running time:

$$n^{|\mathcal{R}|^{|\mathcal{R}|^{|\mathcal{R}|^{|\mathcal{R}|^{\cdots}}}}}$$

Rings

Theorem (Hunt, Stearnes (1990), Burris, Lawrence (1993))

$\mathcal{R}$ is nilpotent $\Longrightarrow$ equivalence is in P
$\mathcal{R}$ is not nilpotent $\Longrightarrow$ equivalence, solvability is (co)NP-complete

Theorem (Horváth (2011))

$\mathcal{R}$ is nilpotent $\Longrightarrow$ solvability is in P

Proof

Ramsey's theorem, running time:

$$n^{|\mathcal{R}|^{|\mathcal{R}|^{|\mathcal{R}|^{|\mathcal{R}|^{\cdots}}}}}$$

Theorem (Károlyi, Szabó (2015))

$\mathcal{R}$ is nilpotent $\Longrightarrow$ solvability is in P
(running time: $n^{|\mathcal{R}|\cdot k}$)

$\mathbb{Z}_2$ Equivalence is coNP-complete

$\mathbb{Z}_2$

Boolean-algebra $\mathcal{B}$

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

$\mathbb{Z}_2$

polynomial reduction to 3-SAT:

$$(x_1 \vee x_2 \vee x_3) \wedge (x_4 \vee x_5 \vee \bar{x}_6) \wedge \cdots \rightsquigarrow$$

$$((x_1 + x_2 + x_1x_2) + x_3 + x_3(x_1 + x_2 + x_1x_2)) \cdot$$
$$((x_4 + x_5 + x_4x_5) + (1 - x_6) + (1 - x_6)(x_4 + x_5 + x_4x_5)) \cdot \cdots \overset{?}{\approx} 0$$

Equation solvability

NP-complete: same

$\mathcal{M}_2(\mathbb{Z}_2)$ Equivalence is coNP-complete

$\mathcal{M}_2(\mathbb{Z}_2)$

$(AB - BA)^2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$

	$x \wedge y$	$\leftrightarrow$	$x \cdot y$	
Boolean-algebra $\mathcal{B}$	$x \vee y$	$\leftrightarrow$	$x + y + xy$	$\mathcal{M}_2(\mathbb{Z}_2)$
	$\bar{x}$	$\leftrightarrow$	$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) - x$	

polynomial reduction to 3-SAT:

$(x_1 \vee x_2 \vee x_3) \wedge (x_4 \vee x_5 \vee \bar{x}_6) \wedge \cdots \rightsquigarrow$

$$((x_1+x_2+x_1x_2)+x_3+x_3(x_1+x_2+x_1x_2)) \cdot$$
$$((x_4+x_5+x_4x_5)+(1-x_6)+(1-x_6)(x_4+x_5+x_4x_5)) \cdot \cdots \stackrel{?}{\approx} \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$$

$x_i = (a_ib_i - b_ia_i)^2$

Equation solvability

NP-complete: same

$\mathbb{Z}_2$ is not nilpotent $\Longrightarrow$ equivalence is coNP-complete ???

Something is fishy...

$x_i^2 \equiv x_i$ in $\mathbb{Z}_2 \Longrightarrow$ long division

everybody can do long division by $(x_i^2 - x_i)$:

$x_i^k \rightsquigarrow x_i$

$\mathbb{Z}_2$ is not nilpotent $\Longrightarrow$ equivalence is coNP-complete ???

Something is fishy...

$x_i^2 \equiv x_i$ in $\mathbb{Z}_2 \Longrightarrow$ long division

everybody can do long division by $(x_i^2 - x_i)$:

$x_i^k \rightsquigarrow x_i$

Example ($p(x_1, \ldots, x_n)$ sums of monomials)

$x_1 x_2^3 + x_1 + x_2 x_1 x_3 + x_{19}$

$(x_1 + x_2)^n$

$\mathbb{Z}_2$ is not nilpotent $\Longrightarrow$ equivalence is coNP-complete ???

Something is fishy...

$x_i^2 \equiv x_i$ in $\mathbb{Z}_2 \Longrightarrow$ long division

everybody can do long division by $(x_i^2 - x_i)$:

$x_i^k \rightsquigarrow x_i$

Example ($p(x_1, \ldots, x_n)$ sums of monomials)

$x_1 x_2^3 + x_1 + x_2 x_1 x_3 + x_{19}$

$(x_1 + x_2)^n$

sigma equivalence problem

sigma equation solvability problem

Sigma equivalence for rings

Theorem (Lawrence, Willard, 1997)

$\mathcal{R}/\mathcal{J}$ is commutative $\Longrightarrow$ sigma equivalence, solvability are in P
$\mathcal{R}/\mathcal{J}$ is not commutative $\Longrightarrow$ szigma equivalence, solvability are (co)NP-complete

Sigma equivalence for rings

Theorem (Lawrence, Willard, 1997)

$\mathcal{R}/\mathcal{J}$ is commutative $\Longrightarrow$ sigma equivalence, solvability are in P
$\mathcal{R}/\mathcal{J}$ is not commutative $\Longrightarrow$ szigma equivalence, solvability are (co)NP-complete

Sigma equivalence for rings

Conjecture (Lawrence, Willard (1997))

$\mathcal{R}/\mathcal{J}$ is commutative $\Longrightarrow$ sigma equivalence, solvability are in P
$\mathcal{R}/\mathcal{J}$ is not commutative $\Longrightarrow$ szigma equivalence, solvability are (co)NP-complete

Sigma equivalence for rings

Conjecture (Lawrence, Willard (1997))

$\mathcal{R}/\mathcal{J}$ is commutative $\Longrightarrow$ sigma equivalence, solvability are in P
$\mathcal{R}/\mathcal{J}$ is not commutative $\Longrightarrow$ szigma equivalence, solvability are (co)NP-complete

Theorem (Szabó, Vértesi (2004, 2011))

$\mathcal{R}/\mathcal{J}$ is not commutative $\Longrightarrow$ sigma equivalence, solvability are (co)NP-complete

Sigma equivalence for rings

Conjecture (Lawrence, Willard (1997))

$\mathcal{R}/\mathcal{J}$ is commutative $\Longrightarrow$ sigma equivalence, solvability are in P
$\mathcal{R}/\mathcal{J}$ is not commutative $\Longrightarrow$ szigma equivalence, solvability are (co)NP-complete

Theorem (Szabó, Vértesi (2004, 2011))

$\mathcal{R}/\mathcal{J}$ is not commutative $\Longrightarrow$ sigma equivalence, solvability are (co)NP-complete

Theorem (Horváth (2012))

$\mathcal{R}$ is commutative $\Longrightarrow$ sigma equivalence is in P

Sigma equivalence for rings

Conjecture (Lawrence, Willard (1997))

$\mathcal{R}/\mathcal{J}$ is commutative $\Longrightarrow$ sigma equivalence, solvability are in P
$\mathcal{R}/\mathcal{J}$ is not commutative $\Longrightarrow$ szigma equivalence, solvability are (co)NP-complete

Theorem (Szabó, Vértesi (2004, 2011))

$\mathcal{R}/\mathcal{J}$ is not commutative $\Longrightarrow$ sigma equivalence, solvability are (co)NP-complete

Theorem (Horváth (2012))

$\mathcal{R}$ is commutative $\Longrightarrow$ sigma equivalence is in P

Theorem (Horváth, Lawrence, Willard (2015))

$\mathcal{R}/\mathcal{J}$ is commutative $\Longrightarrow$ sigma equivalence, solvability are in P

Commutative Rings

Theorem (Pierce)

$\mathcal{R}$ is a commutative ring $\Longrightarrow \mathcal{R} = \oplus \mathcal{R}_i \oplus \mathcal{N}$,
where $\mathcal{R}_i$ is local, $\mathcal{N}$ is nilpotent.

- Equivalence/solvability can be checked for components.
- Nilpotent case is easy (bounded substitution).
- Main case: local rings.

Local Rings

Definition

$\mathcal{R}$ is local iff there is a unique maximal ideal in $\mathcal{R}$.

Examples

- $\mathcal{F}_q$
- $\mathbb{Z}_{p^\alpha}$
- $\begin{bmatrix} \mathcal{F}_q & \mathcal{F}_q \\ 0 & 0 \end{bmatrix}$

Properties

- $\mathcal{J}$ is the unique maximal ideal
- $\mathcal{R}^* = \mathcal{R} \setminus \mathcal{J}$
- $\mathcal{R}/\mathcal{J} \simeq \mathcal{F}_q$ if $\mathcal{R}$ is commutative

Equivalence for $\mathbb{Z}_p$

$f(\bar{x}) \approx 0$?

$x_i^p - x_i \approx 0$

Lemma

$f \approx 0 \iff f = \sum_i g_i \cdot \left(x_i^p - x_i\right)$

dividing by $\left(x_i^p - x_i\right)$ is easy: decrease the exponents by $(p-1)$

works for every finite field $\mathcal{F}_q$

Equation solvability for $\mathcal{F}_q$

$f(x) = 0$ is solvable $\iff f(x)^{q-1} \not\approx 1$

can be calculated in $O(||f||^q)$ time

finding the solutions

$f(a_1, x_2, x_3, \ldots, x_n) = 0$ solvable?

Equation solvability for $\mathcal{F}_q$

$f(x) = 0$ is solvable $\iff f(x)^{q-1} \not\approx 1$

can be calculated in $O(||f||^q)$ time

finding the solutions

$f(a_1, x_2, x_3, \ldots, x_n) = 0$ solvable? NO

Equation solvability for $\mathcal{F}_q$

$f(x) = 0$ is solvable $\iff f(x)^{q-1} \not\approx 1$

can be calculated in $O(||f||^q)$ time

finding the solutions

$f(a_1, x_2, x_3, \ldots, x_n) = 0$ solvable? NO
$f(a_1', x_2, x_3, \ldots, x_n) = 0$ solvable?

Equation solvability for $\mathcal{F}_q$

$f(x) = 0$ is solvable $\iff f(x)^{q-1} \not\approx 1$

can be calculated in $O(||f||^q)$ time

finding the solutions

$f(a_1, x_2, x_3, \ldots, x_n) = 0$ solvable? NO
$f(a_1', x_2, x_3, \ldots, x_n) = 0$ solvable? YES

Equation solvability for $\mathcal{F}_q$

$f(x) = 0$ is solvable $\iff f(x)^{q-1} \not\approx 1$

can be calculated in $O(||f||^q)$ time

finding the solutions

$f(a_1, x_2, x_3, \ldots, x_n) = 0$ solvable? NO
$f(a_1', x_2, x_3, \ldots, x_n) = 0$ solvable? YES
$f(a_1', a_2, x_3, \ldots, x_n) = 0$ solvable? etc.

Equation solvability for $\mathcal{F}_q$

$f(x) = 0$ is solvable $\iff f(x)^{q-1} \not\approx 1$

can be calculated in $O(||f||^q)$ time

finding the solutions

$f(a_1, x_2, x_3, \ldots, x_n) = 0$ solvable? NO
$f(a_1', x_2, x_3, \ldots, x_n) = 0$ solvable? YES
$f(a_1', a_2, x_3, \ldots, x_n) = 0$ solvable? etc.

Gergő Borus (2013)

implemented in Singular starting with version 3-1-6

Equivalence for $\mathbb{Z}_9$

Separate $\mathcal{R}/\mathcal{J}$ and $\mathcal{J}$

- unique maximal ideal is (3)
- $\mathbb{Z}_9/(3) = \mathbb{Z}_3 = \{-1, 0, 1\}$ (coset representation)
- $a = b + 3 \cdot c, \quad (b, c \in \{-1, 0, 1\})$
- $x_i = y_i + 3 \cdot z_i \quad (y_i, z_i \in \{-1, 0, 1\})$

Example

$x_1x_2x_3 = (y_1 + 3z_1) \cdot (y_2 + 3z_2) \cdot (y_3 + 3z_3) = y_1y_2y_3 +$
$3z_1y_2y_3 + 3y_1z_2y_3 + 3y_1y_2z_3 + 3^2z_1z_2y_3 + 3^2z_1y_2z_3 + 3^2y_1z_2z_3 +$
$3^3z_1z_2z_3$
$\Longrightarrow$ fast expansion, no exponential blowup

Equivalence for $\mathbb{Z}_9$ (cont.)

$$f(\bar{x}) = f_1(\bar{y}) + 3 \cdot f_2(\bar{y}, \bar{z}), \quad \bar{y}, \bar{z} \in \{-1, 0, 1\}$$

Check

$f_1(\bar{y}) \approx 0$ in $\mathbb{Z}_3 = \mathbb{Z}_9/(3)$,
$f_2(\bar{y}, \bar{z}) \approx 0$ in $\mathbb{Z}_3 = \{-1, 0, 1\}$.

divide by $(y_i^3 - y_i)$

$$f_1(\bar{y}) = \sum \underbrace{\left(y_i^3 - y_i\right) g_i(\bar{y})}_{\approx 0 \text{ in } \mathbb{Z}_9 \text{ !!!}} + g_0(\bar{y})$$

$f_1(\bar{y}) \approx 0$ in $\mathbb{Z}_9/(3) \iff g_0(\bar{y}) = 3 \cdot h_0(\bar{y}) \implies$ move it into f_2

Works for every $\mathbb{Z}_{p^\alpha}$

Equation solvability for $\mathbb{Z}_9$

$$f(\bar{x}) = f_1(\bar{y}) + 3 \cdot f_2(\bar{y}, \bar{z}), \quad \bar{y}, \bar{z} \in \{-1, 0, 1\}$$

Check

$f_1(\bar{y}) = 0$ in $\mathbb{Z}_3 = \mathbb{Z}_9/(3)$,
$f_2(\bar{y}, \bar{z}) = 0$ in $\mathbb{Z}_3 = \{-1, 0, 1\}$.

Equation solvability for $\mathbb{Z}_9$

$$f(\bar{x}) = f_1(\bar{y}) + 3 \cdot f_2(\bar{y}, \bar{z}), \quad \bar{y}, \bar{z} \in \{-1, 0, 1\}$$

Check

$f_1(\bar{y}) = 0$ in $\mathbb{Z}_3 = \mathbb{Z}_9/(3)$,
$f_2(\bar{y}, \bar{z}) = 0$ in $\mathbb{Z}_3 = \{-1, 0, 1\}$.

Trouble!

$f_1(\bar{y})$ can attain 3 or -3 in $\mathbb{Z}_9$, not only 0

Equation solvability for $\mathbb{Z}_9$

$$f(\bar{x}) = f_1(\bar{y}) + 3 \cdot f_2(\bar{y}, \bar{z}), \quad \bar{y}, \bar{z} \in \{-1, 0, 1\}$$

Check

$f_1(\bar{y}) = 0$ in $\mathbb{Z}_3 = \mathbb{Z}_9/(3)$,

$f_2(\bar{y}, \bar{z}) = 0$ in $\mathbb{Z}_3 = \{-1, 0, 1\}$.

Trouble!

$f_1(\bar{y})$ can attain 3 or -3 in $\mathbb{Z}_9$, not only 0

Example ($a^3 \in \{-1, 0, 1\}$ for every $a \in \mathbb{Z}_9$ and $a^3 - a \in (3)$)

Equation solvability for $\mathbb{Z}_9$

$$f(\bar{x}) = f_1(\bar{y}) + 3 \cdot f_2(\bar{y}, \bar{z}), \quad \bar{y}, \bar{z} \in \{-1, 0, 1\}$$

Check

$f_1(\bar{y}) = 0$ in $\mathbb{Z}_3 = \mathbb{Z}_9/(3)$,

$f_2(\bar{y}, \bar{z}) = 0$ in $\mathbb{Z}_3 = \{-1, 0, 1\}$.

Trouble!

$f_1(\bar{y})$ can attain 3 or -3 in $\mathbb{Z}_9$, not only 0

Example ($a^3 \in \{-1, 0, 1\}$ for every $a \in \mathbb{Z}_9$ and $a^3 - a \in (3)$)

$f_1(\bar{y}) = y_1^2 + y_2 y_3$

Equation solvability for $\mathbb{Z}_9$

$f(\bar{x}) = f_1(\bar{y}) + 3 \cdot f_2(\bar{y}, \bar{z}), \quad \bar{y}, \bar{z} \in \{-1, 0, 1\}$

Check

$f_1(\bar{y}) = 0$ in $\mathbb{Z}_3 = \mathbb{Z}_9/(3)$,
$f_2(\bar{y}, \bar{z}) = 0$ in $\mathbb{Z}_3 = \{-1, 0, 1\}$.

Trouble!

$f_1(\bar{y})$ can attain 3 or -3 in $\mathbb{Z}_9$, not only 0

Example ($a^3 \in \{-1, 0, 1\}$ for every $a \in \mathbb{Z}_9$ and $a^3 - a \in (3)$)

$f_1(\bar{y}) = y_1^2 + y_2 y_3$
$f_1(\bar{y})^3 = y_1^6 + y_2^3 y_3^3 + 3y_1^4 y_2 y_3 + 3y_1^2 y_2^2 y_3^2 \approx$
$y_1^2 + y_2 y_3 + 3\left(y_1^4 y_2 y_3 + y_1^2 y_2^2 y_3^2\right)$

Equation solvability for $\mathbb{Z}_9$

$$f(\bar{x}) = f_1(\bar{y}) + 3 \cdot f_2(\bar{y}, \bar{z}), \quad \bar{y}, \bar{z} \in \{-1, 0, 1\}$$

Check

$f_1(\bar{y}) = 0$ in $\mathbb{Z}_3 = \mathbb{Z}_9/(3)$,
$f_2(\bar{y}, \bar{z}) = 0$ in $\mathbb{Z}_3 = \{-1, 0, 1\}$.

Trouble!

$f_1(\bar{y})$ can attain 3 or -3 in $\mathbb{Z}_9$, not only 0

Example ($a^3 \in \{-1, 0, 1\}$ for every $a \in \mathbb{Z}_9$ and $a^3 - a \in (3)$)

$f_1(\bar{y}) = y_1^2 + y_2 y_3$
$f_1(\bar{y})^3 = y_1^6 + y_2^3 y_3^3 + 3y_1^4 y_2 y_3 + 3y_1^2 y_2^2 y_3^2 \approx$
$y_1^2 + y_2 y_3 + 3\left(y_1^4 y_2 y_3 + y_1^2 y_2^2 y_3^2\right)$
$f_1(\bar{y})^3 \approx f_1(\bar{y}) + 3g(\bar{y})$

Equation solvability for $\mathbb{Z}_9$

$$f(\bar{x}) = f_1(\bar{y}) + 3 \cdot f_2(\bar{y}, \bar{z}), \quad \bar{y}, \bar{z} \in \{-1, 0, 1\}$$

Check

$f_1(\bar{y}) = 0$ in $\mathbb{Z}_3 = \mathbb{Z}_9/(3)$,
$f_2(\bar{y}, \bar{z}) = 0$ in $\mathbb{Z}_3 = \{-1, 0, 1\}$.

Trouble!

$f_1(\bar{y})$ can attain 3 or -3 in $\mathbb{Z}_9$, not only 0

Example ($a^3 \in \{-1, 0, 1\}$ for every $a \in \mathbb{Z}_9$ and $a^3 - a \in (3)$)

$f_1(\bar{y}) = y_1^2 + y_2 y_3$
$f_1(\bar{y})^3 = y_1^6 + y_2^3 y_3^3 + 3y_1^4 y_2 y_3 + 3y_1^2 y_2^2 y_3^2 \approx$
$y_1^2 + y_2 y_3 + 3\left(y_1^4 y_2 y_3 + y_1^2 y_2^2 y_3^2\right)$
$f_1(\bar{y})^3 \approx f_1(\bar{y}) + 3g(\bar{y})$
$f_1(\bar{y}) \approx f_1(\bar{y})^3 - 3g(\bar{y})$ AND $f_1(\bar{y})^3 \in \{-1, 0, 1\}$

Equation solvability for $\mathbb{Z}_9$ (cont.)

$$f(\bar{x}) = f_1(\bar{y}) + 3 \cdot f_2(\bar{y}, \bar{z}), \quad \bar{y}, \bar{z} \in \{-1, 0, 1\}$$
$$f(\bar{x}) = f_1(\bar{y})^3 + 3 \cdot (f_2(\bar{y}, \bar{z}) - g(\bar{y})), \quad \bar{y}, \bar{z} \in \{-1, 0, 1\}$$

$$\overbrace{f_1(\bar{y})^3}^{\in\{-1,0,1\}} + \overbrace{3 \cdot (f_2(\bar{y}, \bar{z}) - g(\bar{y}))}^{\in\{-3,0,3\}} = 0 \text{ in } \mathbb{Z}_9$$

$$\Updownarrow$$

$$f_1(\bar{y})^3 = 0 \text{ in } \mathbb{Z}_9$$
$$3 \cdot (f_2(\bar{y}, \bar{z}) - g(\bar{y})) = 0 \text{ in } \mathbb{Z}_9$$

$$\Updownarrow$$

$$f_1(\bar{y}) = 0 \text{ in } \mathbb{Z}_9/(3) = \mathbb{Z}_3$$
$$f_2(\bar{y}, \bar{z}) - g(\bar{y}) = 0 \text{ in } \{-1, 0, 1\} = \mathbb{Z}_3$$

Works for every $\mathbb{Z}_{p^\alpha}$

Generalize $\mathcal{F}_q$ and $\mathbb{Z}_{p^\alpha}$

$\mathcal{F}_q$

- $q = p^d$
- $m(x)$ irreducible of degree d
- $\mathcal{F}_q = \mathbb{Z}_p[x]/(m(x)) = \mathbb{Z}[x]/(p, m(x))$

Generalize $\mathcal{F}_q$ and $\mathbb{Z}_{p^\alpha}$

$\mathcal{F}_q$

- $q = p^d$
- $m(x)$ irreducible of degree d
- $\mathcal{F}_q = \mathbb{Z}_p[x]/(m(x)) = \mathbb{Z}[x]/(p, m(x))$

$\mathbb{Z}_{p^\alpha}$

- $\mathbb{Z}_{p^\alpha} = \mathbb{Z}/(p^\alpha)$

Generalize $\mathcal{F}_q$ and $\mathbb{Z}_{p^\alpha}$

$\mathcal{F}_q$

- $q = p^d$
- $m(x)$ irreducible of degree d
- $\mathcal{F}_q = \mathbb{Z}_p[x]/(m(x)) = \mathbb{Z}[x]/(p, m(x))$

$\mathbb{Z}_{p^\alpha}$

- $\mathbb{Z}_{p^\alpha} = \mathbb{Z}/(p^\alpha)$

Galois Ring

- $\mathcal{GR}(p^\alpha, q) = \mathbb{Z}[x]/(p^\alpha, m(x))$

Galois Rings

$\mathcal{R} = \mathcal{GR}(p^\alpha, q) = \mathbb{Z}[x]/(p^\alpha, m(x))$

- Raghavendran, Wilson
- $\operatorname{char} \mathcal{R} = p^\alpha$
- $|\mathcal{R}| = q^\alpha$
- $\mathcal{J} = (p)$
- $\mathcal{R}/\mathcal{J} = F_q$

Equivalence, equation solvability

- $r \in \mathcal{R}$ of order $(q-1)$
- $S = \{0, 1, r, r^2, \ldots, r^{q-2}\}$ is a coset representation for $\mathcal{R}/\mathcal{J}$ ($S = \{0, 1, -1\}$ for $\mathbb{Z}_9$)
- $y^q \approx y$ for $y \in S$, $a^{q^n} \in S$ for $a \in \mathcal{R}$, ...

Third example

$\mathcal{R} = \begin{bmatrix} \mathcal{F}_q & \mathcal{F}_q \\ 0 & 0 \end{bmatrix}$ is a local ring

- $\mathcal{F}_q = \begin{bmatrix} \mathcal{F}_q & 0 \\ 0 & 0 \end{bmatrix}$ is a subring
- $\mathcal{R}$ is a 2-dimensional module over $\mathcal{F}_q$

  $\mathcal{R} = \begin{bmatrix} \mathcal{F}_q & 0 \\ 0 & 0 \end{bmatrix} \oplus_m \begin{bmatrix} 0 & \mathcal{F}_q \\ 0 & 0 \end{bmatrix}$
- check equivalence/equation solvability for each component

Local rings

$\mathcal{R}$ is a local ring

- $\mathcal{GR}$ is a subring
- $\mathcal{R}$ is a module over $\mathcal{GR}$

  $\mathcal{R}$ is the sum of cyclic $\mathcal{GR}$-modules
- check equivalence/equation solvability for each component

Semigroups, monoids

- Seif, Szabó (2003, 2006)
- Klíma (2002, 2004, 2007, 2009, 2010, 2012)
- Tesson (2003)
- Kisielewicz (2004)
- Seif (2005)
- Plescheva, Vértesi (2006)
- Kitaev, Seif (2008)
- Almeida, Volkov, Goldberg (2009)
- Szabó, Vértesi (2004, 2004, 2010)
- ...

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 (2011))

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

Meta-Abelian groups

Theorem (Horváth, Szabó (2006, 2012), Horváth (2015))

$G = A \rtimes B$, 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, 2012), Horváth (2015))

$G = A \rtimes B$, 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, 2012), Horváth (2015))

$G = A \rtimes B$, 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, 2012), Horváth (2015))

$G = A \rtimes B$, 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, 2012), Horváth (2015))

$G = A \rtimes B$, 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, 2012), Horváth (2015))

$G = A \rtimes B$, 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 (2015))

$\mathcal{R}$ 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 (2015))

$\mathcal{R}$ 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 (2015))

$\mathcal{R}$ 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 (2015))

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

Proof.

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

□

Sigma problems with substitutions

Theorem (Horváth (2015))

$\mathcal{R}$ 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 (2015))

$\mathcal{R}$ 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 (2015))

$\mathcal{R}$ 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 (2015))

$\mathcal{R}$ 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 (2015))

$\mathcal{R}$ 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 □

Sigma problems with substitutions

Theorem (Horváth (2015))

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

Proof.

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

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 (2015))

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

Proof.

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

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 (2015))

$\mathcal{R}$ is a commutative ring, $\mathcal{S} \leq \mathcal{R}^\times$
$\Longrightarrow$ sigma equivalence with 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.

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

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

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

- $S_4 = V \rtimes S_3$, $\mathcal{R} = \mathbb{Z}^{2\times 2}$ is not commutative, $\mathcal{S} = \mathcal{R}^\times$
- $SL_2(3) = Q \rtimes Z_3$, Q is not Abelian
- $U(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^\times$, $U(3, \mathbb{Z}_3)$ is not Abelian
- $D_{12} = Z_{12} \rtimes Z_2$ ($\mathcal{R} = \mathbb{Z}_{12}$, $\mathcal{S} \neq \mathcal{S}_1 \oplus \mathcal{S}_2$) (equation solvability)
- $Z_3 \rtimes Q$ (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

- $S_4 = V \rtimes S_3$, $\mathcal{R} = \mathbb{Z}^{2\times 2}$ is not commutative, $\mathcal{S} = \mathcal{R}^{\times}$
- $SL_2(3) = Q \rtimes Z_3$, Q is not Abelian
- $U(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^{\times}$, $U(3, \mathbb{Z}_3)$ is not Abelian
- $D_{12} = Z_{12} \rtimes Z_2$ ($\mathcal{R} = \mathbb{Z}_{12}$, $\mathcal{S} \neq \mathcal{S}_1 \oplus \mathcal{S}_2$) (equation solvability)
- $Z_3 \rtimes Q$ (equation solvability)
- $(Z_2 \times Z_2 \times Z_3) \rtimes Z_2$ (equation solvability)

Theorem (Földvári (2015))

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

$U(3,\mathcal{F}_3) \rtimes \mathcal{F}_3^\times$

$$U(3,\mathcal{F}_3)\rtimes\mathcal{F}_3^\times = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & h & c \\ 0 & 0 & 1 \end{pmatrix} : a,b,c \in \mathbb{F}_3, h \in \mathbb{F}_3^\times \right\} \leq T(3,\mathcal{F}_3)$$

Matrix multiplication in $U(3,\mathcal{F}_3) \rtimes \mathcal{F}_3^\times$:

$$\begin{pmatrix} 1 & a_1 & b_1 \\ 0 & h_1 & c_1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a_2 & b_2 \\ 0 & h_2 & c_2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a_2 + h_2 a_1 & b_2 + a_1 c_2 + b_1 \\ 0 & h_1 h_2 & h_1 c_2 + c_1 \\ 0 & 0 & 1 \end{pmatrix}$$

Solvability in $U(3, \mathcal{F}_3) \rtimes \mathcal{F}_3^\times$

- question: $T = T_1 T_2 \dots T_n = 1$, substitute
$$T_k = \begin{pmatrix} 1 & u_k & v_k \\ 0 & y_k & w_k \\ 0 & 0 & 1 \end{pmatrix}$$
- matrix multiplication:

$$u = \sum_{k=1}^{n} u_k \prod_{i=k+1}^{n} y_i$$

$$w = \sum_{k=1}^{n} \prod_{i=1}^{k-1} y_i w_k$$

$$v = \sum_{k=1}^{n} v_k + \sum_{k=2}^{n} \sum_{l=1}^{k-1} u_l \prod_{i=l+1}^{k-1} y_i w_k$$

$$y = \prod_{k=1}^{n} y_k$$

- sigma equation solvablity over $\mathcal{F}_3$ is in P

Semipattern group

$$\left\{ \begin{pmatrix} x & 0 & 0 & b \\ 0 & 1 & c & d \\ 0 & 0 & y & 0 \\ 0 & 0 & 0 & z \end{pmatrix} : a, b, c, d \in \mathbb{F}_q; x \in H_1; y, z \in H_2 \right\} \leq T(4, \mathbb{F}_q)$$

Theorem (Attila Földvári (2015))

semipattern groups $\Longrightarrow$ *equivalence, solvability is in P*

Corollary (Attila Földvári (2015))

$\mathcal{R}$ *is upper triangular matrix ring* $\Longrightarrow$ *sigma equivalence, solvability is in P*

Nilpotent rings

Theorem (Wilson (1973))

$\mathcal{R}$ is nilpotent, $\operatorname{char}\mathcal{R} = p^\alpha \Longrightarrow$ *$\mathcal{R}$ is a homomorphic image of*

$$\begin{pmatrix} (p) & * & * \\ \vdots & \ddots & * \\ (p) & \dots & (p) \end{pmatrix},$$

where elements are from $\mathbb{Z}_{p^\alpha}$

Corollary (Attila Földvári (2015))

$\mathcal{R}$ is nilpotent $\Longrightarrow$ equivalence, solvablity is in P
(futásidő: $\sim n^{|\mathcal{R}|\log|\mathcal{R}|}$*)*

Real 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

- $S_4 = V \rtimes S_3$, $\mathcal{R} = \mathbb{Z}^{2\times 2}$ is not commutative, $\mathcal{S} = \mathcal{R}^\times$
- $D_{12} = Z_{12} \rtimes Z_2$ ($\mathcal{R} = \mathbb{Z}_{12}$, $\mathcal{S} \neq \mathcal{S}_1 \oplus \mathcal{S}_2$) (equation solvability)
- $Z_3 \rtimes Q$ (equation solvability)
- $(Z_2 \times Z_2 \times Z_3) \rtimes Z_2$ (equation solvability)

Other algebras

- semigroups, monoids: a lot
- nearrings: ??? (general/sigma problems, substitutions from $\mathcal{S}$)
- general algebras: ???

Acknowledgements

This research was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences, by the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318202, and by the Hungarian Scientific Research Fund (OTKA) grant no. K109185.