The complexity of the equivalence problem for commutative rings

Gábor Horváth

University of Debrecen, Hungary

joint work with Ross Willard and John Lawrence

24th June 2010

The equivalence (identity checking) problem

fixed finite algebra $\mathcal{A}$

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?

Equivalence for rings

Theorem (Hunt, Stearnes, Burris, Lawrence)

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

What happens for special input polynomials?

Sigma equivalence problem

- 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
- $f_1 \equiv f_2 \Longleftrightarrow f_1 - f_2 \equiv 0$

Sigma equivalence for finite rings

Conjecture (Lawrence, Willard)

$\mathcal{R}/\mathcal{J}$ is commutative $\Longrightarrow$ sigma equivalence is in P,
$\mathcal{R}/\mathcal{J}$ is not commutative $\Longrightarrow$ sigma equivalence is coNP-complete.

Theorem (Szabó, Vértesi)

$\mathcal{R}/\mathcal{J}$ is not commutative $\Longrightarrow$ sigma equivalence is coNP-complete.

What if $\mathcal{R}/\mathcal{J}$ is commutative?

Sigma equivalence for finite rings

Theorem (Horváth, Lawrence, Willard)

$\mathcal{R}$ is commutative $\Longrightarrow$ sigma equivalence is 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 can be checked for components.
- Nilpotent case is easy (bounded substitution).
- Main case: local rings.

Local Rings

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

Examples

- F_q
- Z_{p^α}
- $\begin{bmatrix} F_q & F_q \\ 0 & 0 \end{bmatrix}$

Properties

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

Z_p

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

$x_i^p - x_i \equiv 0$

Lemma

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

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

works for every finite field F_q

Z_9

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

- unique maximal ideal is (3)
- $Z_9/(3) = Z_3 = \{-1, 0, 1\}$ (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

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

$f_1(\bar{y}) \equiv 0$ in Z_3,
$f_2(\bar{y}, \bar{z}) \equiv 0$ in Z_3
Easy: divide by $(y_i^3 - y_i)$

Works for every Z_{p^α}

Generalize F_q and Z_{p^α}

F_q

- $q = p^d$
- $m(x)$ irreducible of degree d
- $F_q = Z_p[x]/(m(x)) = \mathbb{Z}[x]/(p, m(x))$

Generalize F_q and Z_{p^α}

F_q

- $q = p^d$
- $m(x)$ irreducible of degree d
- $F_q = Z_p[x]/(m(x)) = \mathbb{Z}[x]/(p, m(x))$

Z_{p^α}

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

Generalize F_q and Z_{p^α}

F_q

- $q = p^d$
- $m(x)$ irreducible of degree d
- $F_q = Z_p[x]/(m(x)) = \mathbb{Z}[x]/(p, m(x))$

Z_{p^α}

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

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

- $r \in \mathcal{R}$ 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 Z_9)
- $y^q \equiv y$ for $y \in S$, ...

Third example

$$\mathcal{R} = \begin{bmatrix} F_q & F_q \\ 0 & 0 \end{bmatrix}$$

- $F_q = \begin{bmatrix} F_q & 0 \\ 0 & 0 \end{bmatrix}$ is a subring
- $\mathcal{J} = \begin{bmatrix} 0 & F_q \\ 0 & 0 \end{bmatrix}$
- $\mathcal{R}$ is a 2-dimensional module over F_q: $\mathcal{R} = \begin{bmatrix} F_q & 0 \\ 0 & 0 \end{bmatrix} \oplus_m \begin{bmatrix} 0 & F_q \\ 0 & 0 \end{bmatrix}$
- check equivalence for each F_q-component

Local rings

Theorem (Raghavendran)

$\mathcal{R}$ local $\Longrightarrow$ there exists $\mathcal{R}_0 \leq \mathcal{R}$ Galois subring

Theorem (Raghavendran)

M module over Galois ring $\mathcal{R}_0$
$\Longrightarrow$ M is the direct sum of cyclic $\mathcal{R}_0$-modules

- $\mathcal{R}$ is a direct sum of cyclic $\mathcal{R}_0$-modules
- check equivalence for components separately
- each component: check equivalence for Galois ring $\mathcal{R}_0$

Noncommutative rings

Theorem (Horváth, Lawrence, Willard)

$\mathcal{R}$ is finite, $\mathcal{R}/\mathcal{J}$ can be lifted in the center
$\Longrightarrow$ sigma equivalence is in P

Open questions

Problem

$\mathcal{R}$ is finite, direct irreducible, $\mathcal{R}/\mathcal{J} = \oplus F_q$,
$\mathcal{R}/\mathcal{J}$ cannot be lifted in the center

Example

$$U_n(F_q) = \begin{bmatrix} F_q & F_q & F_q \\ 0 & F_q & F_q \\ 0 & 0 & F_q \end{bmatrix}$$