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 \( \mathcal{A} \)

\[ t_1 \equiv t_2 \iff \forall a_1, \ldots, a_n \in \mathcal{A} \]
\[ t_1(a_1, \ldots, a_n) = t_2(a_1, \ldots, a_n) \]

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)

R is nilpotent \implies equivalence is in P,
R is not nilpotent \implies equivalence is coNP-complete.

What happens for special input polynomials?

Sigma equivalence problem

- 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
- \( f_1 \equiv f_2 \iff f_1 - f_2 \equiv 0 \)
Sigma equivalence for finite rings

Conjecture (Lawrence, Willard)
\[ \mathcal{R}/\mathcal{J} \text{ is commutative} \implies \text{sigma equivalence is in P}, \]
\[ \mathcal{R}/\mathcal{J} \text{ is not commutative} \implies \text{sigma equivalence is coNP-complete}. \]

Theorem (Szabó, Vértesi)
\[ \mathcal{R}/\mathcal{J} \text{ is not commutative} \implies \text{sigma equivalence is coNP-complete}. \]

What if \( \mathcal{R}/\mathcal{J} \) is commutative?
Sigma equivalence for finite rings

Theorem (Horváth, Lawrence, Willard)

\( \mathcal{R} \text{ is commutative} \implies \text{sigma equivalence is in } P \)
Commutative Rings

Theorem (Pierce)

$\mathcal{R}$ is a commutative ring $\iff \mathcal{R} = \bigoplus \mathcal{R}_i \oplus \mathcal{N}$, 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

- \( F_q \)
- \( Z_{p^\alpha} \)
- \[
\begin{bmatrix}
F_q & F_q \\
0 & 0
\end{bmatrix}
\]

Properties

- \( \mathcal{J} \) is the unique maximal ideal
- \( \mathcal{R}^* = \mathcal{R} \setminus \mathcal{J} \)
- \( \mathcal{R}/\mathcal{J} \cong F_q \) if \( \mathcal{R} \) is commutative
Lemma

\[ f \equiv 0 \iff f = \sum_i g_i \cdot (x_i^p - x_i) \]

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

works for every finite field \( F_q \)
Separate \( \mathcal{R}/\mathcal{I} \) and \( \mathcal{I} \)

- 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

\[
x_1 x_2 x_3 = (y_1 + 3z_1) \cdot (y_2 + 3z_2) \cdot (y_3 + 3z_3) = y_1 y_2 y_3 + 3z_1 y_2 y_3 + 3y_1 z_2 y_3 + 3^2 z_1 z_2 y_3 + 3^2 z_1 y_2 z_3 + 3^2 y_1 z_2 z_3 + 3^3 z_1 z_2 z_3
\]

\( \Rightarrow \) 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 $Z_p^{\alpha}$
Generalize $F_q$ and $\mathbb{Z}_{p^\alpha}$

**$F_q$**

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

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

**$Z_{p^\alpha}$**
- $Z_{p^\alpha} = \mathbb{Z}/(p^\alpha)$
Generalize $F_q$ and $Z_{p^\alpha}$

**$F_q$**

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

**$Z_{p^\alpha}$**

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

**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
- \( \text{char } \mathcal{R} = p^\alpha \)
- \( |\mathcal{R}| = q^\alpha \)
- \( \mathcal{J} = (p) \)
- \( \mathcal{R}/\mathcal{J} = F_q \)

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 \( \mathbb{Z}_9 \)\)
- \( y^q \equiv y \) for \( y \in S, \ldots \)
Third example

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

- \( F_q = \begin{bmatrix} F_q \\ 0 \\ 0 \end{bmatrix} \) 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)

\( \mathcal{R} \text{ local} \implies \text{there exists } \mathcal{R}_0 \leq \mathcal{R} \text{ Galois subring} \)

Theorem (Raghavendran)

\( M \text{ module over Galois ring } \mathcal{R}_0 \implies M \text{ is the direct sum of cyclic } \mathcal{R}_0\text{-modules} \)

- \( \mathcal{R} \) is a direct sum of cyclic \( \mathcal{R}_0\)-modules
- check equivalence for components separately
- each component: check equivalence for Galois ring \( \mathcal{R}_0 \)
Theorem (Horváth, Lawrence, Willard)

\( \mathcal{R} \) is finite, \( \mathcal{R}/J \) can be lifted in the center

\[ \implies \text{sigma equivalence is in } P \]
Open questions

Problem

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

Example

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