SOLVING SYSTEMS OF EQUATIONS OVER CERTAIN SOLVABLE GROUPS

Philipp Nuspl
Institute for Algebra
Austrian Science Fund FWF P29931

JOHANNES KEPLER
UNIVERSITY LINZ

Der Wissenschaftsfonds.

Problem

Let $(G, \cdot)$ be a finite group.

Definition

Given polynomials $t_1, \ldots, t_s$ over G we want to decide whether

$$\exists\, x = (x_1, \ldots, x_n) \in G^n \colon t_1(x) = \cdots = t_s(x) = 1.$$

- For fixed s the problem is called s-PolSysSat(G).
- For $s = 1$ the problem is called PolSat(G).
- Otherwise the problem is called PolSysSat(G).

Assumption: Each polynomial t over G is of the form

$$t = w_1 \cdot w_2 \cdots w_k \text{ where } w_j \in G \cup \{x_1, \ldots, x_n\}.$$

Motivation

Let $s \geq 2$. Why is s-PolSysSat interesting?

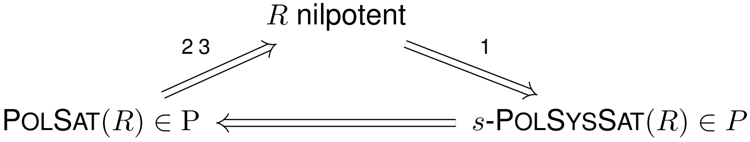
$$\textsc{PolSat} \overset{D}{<} s\text{-}\textsc{PolSysSat} \overset{D_4}{<} \textsc{PolSysSat}$$

with

- $D = (\{0,1\}, \wedge, \vee)$ (Gorazd and Krzaczkowski 2011),
- D_4 the dihedral group with 8 elements (Aichinger 2019).

Rings

If $\mathrm{P} \neq \mathrm{NP}$, then for rings R we have



[1] Aichinger 2019

[2] Burris and Lawrence 1993

[3] Horváth 2011

Known Results for Groups

	abelian	nilpotent	solvable	non-solvable
PolSat	P	P [1]	? [3] [4]	NPC [1]
s-PolSysSat	P	P [2]	?	NPC [1]
PolSysSat	P	NPC [1]	NPC [1]	NPC [1]

[1] Goldmann and Russell 1999

[2] Aichinger 2019

[3] Horváth 2015

[4] Horváth and Földvári 2018

Main Theorem

Theorem (Horváth and Szabó 2006)

For groups G of order $|G| = pq$ with primes p, q we have

$$\textsc{PolSat}(G) \in \mathrm{P}.$$

We will now prove:

Theorem

For groups G of order $|G| = pq$ with primes p, q we have

$$s\text{-}\textsc{PolSysSat}(G) \in \mathrm{P}.$$

Proof

Let G be finite group with $|G| = pq$ and $p \geq q$ primes.

- If $p = q$ or $q \nmid p - 1$, then G is abelian.
- Write $G = \mathbb{Z}_p \rtimes \mathbb{Z}_q$ with $q \mid p - 1$ and

$$\psi\colon (\mathbb{Z}_q, +) \to (\mathbb{Z}_p - \{0\}, \cdot) \cong \text{Aut}(\mathbb{Z}_p).$$

- Product of $(a_1, b_1), (a_2, b_2) \in G$ is given as

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 + \psi(b_1) \cdot a_2, b_1 + b_2).$$

- We want to solve a system over $G = \mathbb{Z}_p \rtimes \mathbb{Z}_q$:

$$
\begin{aligned}
t_1 &= (a_{1,1}, b_{1,1}) \cdot (a_{1,2}, b_{1,2}) \cdots (a_{1,k_1}, b_{1,k_1}) = (0,0), \\
&\vdots \\
t_s &= (a_{s,1}, b_{s,1}) \cdot (a_{s,2}, b_{s,2}) \cdots (a_{s,k_s}, b_{s,k_s}) = (0,0).
\end{aligned}
$$

- This is equivalent to:

$$
\left.
\begin{aligned}
a_{1,1} + \psi(b_{1,1})a_{1,2} + \psi(b_{1,1})\psi(b_{1,2})a_{1,3} + \cdots + \psi(b_{1,1})\psi(b_{1,2})\cdots\psi(b_{1,k_1-1})a_{1,k_1} &= 0, \\
&\vdots \\
a_{s,1} + \psi(b_{s,1})a_{s,2} + \psi(b_{s,1})\psi(b_{s,2})a_{s,3} + \cdots + \psi(b_{s,1})\psi(b_{s,2})\cdots\psi(b_{s,k_s-1})a_{s,k_s} &= 0,
\end{aligned}
\right\}
$$

$$
\left.
\begin{aligned}
b_{1,1} + b_{1,2} + \cdots + b_{1,k_1} &= 0, \\
&\vdots \\
b_{s,1} + b_{s,2} + \cdots + b_{s,k_s} &= 0.
\end{aligned}
\right\}
$$

Second part

- Solving linear system over $\mathbb{Z}_q$ with variables $\{y_1, \ldots, y_n\}$: Gaussian elimination.
- Solutions can be written parametrized by some variables $z_1, \ldots, z_k$ over $\mathbb{Z}_q$, i.e.

$$y_i = \sum_{j=1}^{k} c_{i,j} z_j + d_i \quad \text{for all } i = 1, \ldots, n$$

  with $c_{i,j}, d_i \in \mathbb{Z}_q$.
- Then

$$\psi(y_i) = \psi\left(\sum_{j=1}^{k} c_{i,j} z_j + d_i\right) = \psi(d_i) \prod_{j=1}^{k} \psi(z_j)^{c_{i,j}}.$$

- Use these in the first part of the system.

First part

We now have a system of polynomials over $\mathbb{Z}_p$ in expanded form with

- variables $a_{i,j}$ over $\mathbb{Z}_p$ and
- variables $\psi(b_{i,j})$ over $H := \text{Im}(\psi) \leq (\mathbb{Z}_p - \{0\}, \cdot)$.

Lemma

Let $H \leq (\mathbb{Z}_p - \{0\}, \cdot)$ with $|H| \geq 2$. Then there exists a linear polynomial $h(x_1, \ldots, x_k) \in \mathbb{Z}[x_1, \ldots, x_k]$ with $h(H^k) = \mathbb{Z}_p$ and $k = \lceil \log_2(p) \rceil$.

Rewrite

$$a_{i,j} \longleftrightarrow h\left(a_{i,j}^{(1)}, \ldots, a_{i,j}^{(k)}\right)$$

with new variables $a_{i,j}^{(l)}$ over H.

We have system of expanded polynomials over $\mathbb{Z}_p$ with variables over H.

Equations over Finite Fields

Given: $f_1, \ldots, f_s \in \mathbb{F}[x_1, \ldots, x_n] := \mathbb{Z}_p[x_1, \ldots, x_n]$.
Asked: $\exists\, x \in \mathbb{F}^n \colon f_1(x) = \cdots = f_s(x) = 0$.

	no restrictions	f_i in expanded form (σ problem)
PolSat	NPC (reduce 3-CNF)	P
s-PolSysSat	NPC	P
PolSysSat	NPC	NPC (reduce PolSat)

Systems over Finite Fields

Given: $f_1, \ldots, f_s \in \mathbb{F}[x_1, \ldots, x_n] := \mathbb{Z}_p[x_1, \ldots, x_n]$.
Asked: $\exists\, x \in \mathbb{F}^n \colon f_1(x) = \cdots = f_s(x) = 0$.

- For $f \in \mathbb{F}[x_1, \ldots, x_n]$ we have

$$\forall x \in \mathbb{F}^n \colon f(x) = 0 \iff f \in \text{Ideal}_{\mathbb{F}[x_1,\ldots,x_n]}\left(x_1^p - x_1, \ldots, x_n^p - x_n\right).$$

- Then we define

$$f(x_1, \ldots, x_n) := \prod_{i=1}^{s} \left(1 - f_i(x_1, \ldots, x_n)^{p-1}\right).$$

- Now we have

$$\forall x \in \mathbb{F}^n \colon f(x) = 0 \iff \neg\left(\exists x \in \mathbb{F}^n \colon f_1(x) = \cdots = f_s(x) = 0\right).$$

Systems over Finite Fields

Similarly we can generalize a result from Horváth and Szabó 2006:

Lemma

Let $H \leq (\mathbb{Z}_p - \{0\}, \cdot)$ be a multiplicative subgroup. If the $f_i \in \mathbb{Z}_p[x_1, \ldots, x_n]$ are given in expanded form we can decide in polynomial time whether

$$\exists\, x \in H^n \colon f_1(x) = \cdots = f_s(x) = 0.$$

References I

Aichinger, Erhard (2019). “Solving systems of equations in supernilpotent algebras”. In: arXiv:1901.07862.

Burris, Stanley and John Lawrence (1993). “The Equivalence Problem for Finite Rings”. In: Journal of Symbolic Computation 15.1, pp. 67 –71. ISSN: 0747-7171.

Goldmann, Mikael and Alexander Russell (1999). “The Complexity of Solving Equations over Finite Groups.”. In: IEEE Conference on Computational Complexity. IEEE Computer Society, pp. 80–86.

Gorazd, Tomasz A. and Jacek Krzaczkowski (2011). “The complexity of problems connected with two-element algebras”. In: Reports on Mathematical Logic 46, pp. 91–108.

References II

Horváth, Gábor (2011). “The complexity of the equivalence and equation solvability problems over nilpotent rings and groups”. In: Algebra universalis 66.4, pp. 391–403.

– (2015). “The complexity of the equivalence and equation solvability problems over meta-Abelian groups”. In: Journal of Algebra 433.

Horváth, Gábor and Attila Földvári (2018). “The complexity of the equation solvability and equivalence problems over finite groups”. In: manuscript.

Horváth, Gábor and Csaba A. Szabó (2006). “The Complexity of Checking Identities over Finite Groups”. In: IJAC 16.5, pp. 931–940.