SOLVING SYSTEMS OF EQUATIONS OF FIXED SIZE OVER FINITE GROUPS

Philipp Nuspl
Institute for Algebra
Austrian Science Fund FWF P29931

JOHANNES KEPLER
UNIVERSITY LINZ

FWF
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

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

Systems of fixed size

Why consider s-PolSysSat(G)?

$$\text{PolSat} < s\text{-PolSysSat} < \text{PolSysSat}$$

- For $D = (\{0,1\}, \wedge, \vee)$ we have PolSat$(D) \in \mathrm{P}$, but 2-PolSysSat$(D) \in \mathrm{NPC}$ (Gorazd and Krzaczkowski 2011, Schaefer 1978): V set of variables, $Y \subseteq V^3$:

$$\left.\begin{array}{l} \bigwedge\limits_{(x,y,z)\in Y} (x \vee y \vee z) = 1, \\ \bigvee\limits_{(x,y,z)\in Y} (x \wedge y \wedge z) = 0, \end{array}\right\} \Leftrightarrow \Big(\bigwedge_{(x,y,z)\in Y} (x \vee y \vee z)\Big) \wedge \Big(\bigwedge_{(x,y,z)\in Y} (\neg x \vee \neg y \vee \neg z)\Big) = 1.$$

- For the group S_3 we have s-PolSysSat$(S_3) \in \mathrm{P}$, but PolSysSat$(S_3) \in \mathrm{NPC}$.

Expanded polynomials

Let $\mathbb{F}_q$ be the finite field with q elements. A polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ is given in expanded form if f is given as

$$f(x_1, \ldots, x_n) = \sum_{0 \leq s_1, \ldots, s_n \leq q-1} c_{s_1,\ldots,s_n} x_1^{s_1} \cdots x_n^{s_n}$$

with $c_{s_1,\ldots,s_n} \in \mathbb{F}_q$, i.e.

- f is written as sum of monomials,
- all the exponents are in $\{0, \ldots, q-1\}$.

Equations over Finite Fields

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

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

Equations over Finite Fields

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

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

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

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

Let $f(x_1, \ldots, x_n) \coloneqq \prod_{i=1}^{s} \left(1 - f_i(x_1, \ldots, x_n)^{q-1}\right)$. Now

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

Known Results for Groups

	abelian	nilpotent	solvable	non-solvable
POLSAT	P	P [1]	?	NPC [1]
s-POLSYSSAT	P	P [2]	?	NPC [1]
POLSYSSAT	P	NPC [1]	NPC [1]	NPC [1]

Results for solvable non-nilpotent groups: POLSAT$(G) \in \mathrm{P}$ with

- $G = \mathbb{Z}_{2p^\alpha} \rtimes A$ for prime p and abelian group A, [3]
- $G = P \rtimes A$ for p-group P and abelian group A. [4]

---

[1] Goldmann and Russell 1999

[2] Aichinger 2019

[3] Horváth 2015

[4] Földvári and Horváth 2019

Equations over $\mathbb{Z}_p \rtimes \mathbb{Z}_q$

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

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

- 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:

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

Proof continued

- Second part is linear system over $\mathbb{Z}_q$. We can solve it by Gaussian elimination.
- Use these results in first part. Then we 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 $H \coloneqq \mathsf{Im}(\psi) \leq (\mathbb{Z}_p - \{0\}, \cdot)$.
- We know how to solve this in polynomial time.

Equations over $P \rtimes A$

Theorem (Földvári and Horváth 2019)

For groups $G = P \rtimes A$ where P is a p-group and A is abelian we have

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

Theorem

For groups $G = P \rtimes A$ where P is a p-group and A is abelian we have

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

Proof outline

- Multiplication of elements in $G = P \rtimes A$ can be expressed by polynomials over some field $\mathbb{F}_q$ (Földvári and Horváth 2019).
  - Use representation as polycyclic group.
- In polynomial time we can compute these polynomials in expanded form.
- For fixed group one equation over G yields n equations in expanded form over $\mathbb{F}_q$.
- Then s equations over G yield $s \cdot n$ equations in expanded form over $\mathbb{F}_q$.

Equations over $\mathbb{Z}_{2p^\alpha} \rtimes A$

Corollary

For groups $G = \mathbb{Z}_{2p^\alpha} \rtimes A$ where p is prime, $\alpha \in \mathbb{N}$ and A is abelian we have

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

Proof:

- If $p = 2$, then apply previous Theorem.
- If $p \neq 2$, then $\mathbb{Z}_{2p^\alpha} = \mathbb{Z}_2 \times \mathbb{Z}_{p^\alpha}$ and

$$(\mathbb{Z}_2 \times \mathbb{Z}_{p^\alpha}) \rtimes A \cong \mathbb{Z}_2 \times (\mathbb{Z}_{p^\alpha} \rtimes A).$$

References I

Aichinger, Erhard (2019). “Solving Systems of Equations in Supernilpotent Algebras”. In: 44th International Symposium on Mathematical Foundations of Computer Science (MFCS 2019). Vol. 138. Leibniz International Proceedings in Informatics (LIPIcs), 72:1–72:9. ISBN: 978-3-95977-117-7.

Földvári, Attila and Gábor Horváth (2019). “The Complexity of the Equation Solvability and Equivalence Problems over Finite Groups”. In: International Journal of Algebra and Computation.

Goldmann, Mikael and Alexander Russell (1999). “The complexity of solving equations over finite groups”. In: Proceedings. Fourteenth Annual IEEE Conference on Computational Complexity, pp. 80–86.

References II

Gorazd, Tomasz A. and Jacek Krzaczkowski (2011). “The Complexity of Problems Connected with Two-element Algebras”. In: Reports on Mathematical Logic 2011.Number 46.

Horváth, Gábor (2015). “The Complexity of the equivalence and equation solvability problems over meta-abelian groups”. In:

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

Schaefer, Thomas J. (1978). “The Complexity of Satisfiability Problems”. In: STOC. ACM, pp. 216–226.