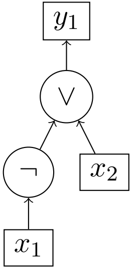
SOLVING SYSTEMS OF EQUATIONS IN SUPERNILPOTENT ALGEBRAS

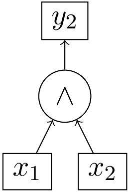
Erhard Aichinger
Institute for Algebra
Austrian Science Fund FWF P29931

JOHANNES KEPLER
UNIVERSITY LINZ

Problem

Given:





Asked:

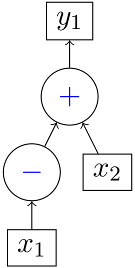
$$\exists x_1, x_2 \in \{0,1\} \quad : \quad y_1(x_1, x_2) \quad = \quad y_2(x_1, x_2),$$ or, equivalently,

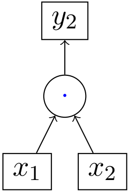
$$\exists x_1, x_2 \in \{0,1\} \quad : \quad (\neg x_1) \vee x_2 \quad = \quad x_1 \wedge x_2.$$

This is (equivalent to) CIRCUIT SAT =: CSAT($\mathbf{B}$), where $\mathbf{B} = (\{0,1\}; \vee, \wedge, \neg)$.

Problem for $(\mathbb{Z}_3; +, \cdot)$

Given:





Asked:

$$\exists x_1, x_2 \in \mathbb{Z}_3 \quad : \quad y_1(x_1, x_2) \quad = \quad y_2(x_1, x_2),$$ or, equivalently,

$$\exists x_1, x_2 \in \mathbb{Z}_3 \quad : \quad (-x_1) + x_2 \quad = \quad x_1 \cdot x_2.$$

This is CSAT$(\mathbb{Z}_3)$, where $\mathbb{Z}_3 = (\{[0]_3, [1]_3, [2]_3\}; +, \cdot, -)$.

Problems associated with an algebraic structure $\mathbf{A}$

With every finite algebraic structure of finite type $\mathbf{A} = (A; f_1, f_2, \ldots, f_m)$, we associate the decision problem

---

CSAT$(\mathbf{A})$

- **Given:** two circuits F, G with gates from
  - $\{f_1, \ldots, f_m\}$ (operations) and
  - $\{x_i : i \in \mathbb{N}\}$ (input)

  and one output each.
- **Asked:** Is there an assignment $x_i \mapsto a_i$ such that $F(a_1, a_2, \ldots) = G(a_1, a_2, \ldots)$?

For $\mathbf{A} := (\{0,1\}; \vee, \wedge, \neg)$, the problem CSAT$(\mathbf{A})$ is NP-complete.

For $\mathbf{A} := (\{0,1\}; +\bmod 2, 1) = (\mathbb{Z}_2; +, 1)$, the problem CSAT$(\mathbf{A})$ is in P.

Overview of the results

Two computational problems are associated with every algebra $\mathbf{A}$ and every $s \in \mathbb{N}$:

1. s-PolSysSat($\mathbf{A}$): Does a given system of s polynomial equations have a solution in $\mathbf{A}$?
2. s-SCSat($\mathbf{A}$): Given $2s$ circuits $f_1, g_1, \ldots, f_s, g_s$, is there an assignment $\boldsymbol{a}$ to the input variables such that $\bigwedge_{i=1}^{s} f_i(\boldsymbol{a}) = g_i(\boldsymbol{a})$?

We provide a polynomial time algorithm for these problems provided that

> $\mathbf{A}$ *is a supernilpotent algebra of finite type in a congruence modular variety.*

Overview of the results

Two computational problems are associated with every algebra $\mathbf{A}$ and every $s \in \mathbb{N}$:

1. s-PolSysSat($\mathbf{A}$): Does a given system of s polynomial equations have a solution in $\mathbf{A}$?
2. s-SCSat($\mathbf{A}$): Given $2s$ circuits $f_1, g_1, \ldots, f_s, g_s$, is there an assignment $\boldsymbol{a}$ to the input variables such that $\bigwedge_{i=1}^{s} f_i(\boldsymbol{a}) = g_i(\boldsymbol{a})$?

We provide a polynomial time algorithm for these problems provided that

> $\mathbf{A}$ *is a supernilpotent algebra of finite type in a congruence modular variety.*

Such algebras

Overview of the results

Two computational problems are associated with every algebra $\mathbf{A}$ and every $s \in \mathbb{N}$:

1. s-PolSysSat($\mathbf{A}$): Does a given system of s polynomial equations have a solution in $\mathbf{A}$?
2. s-SCSat($\mathbf{A}$): Given $2s$ circuits $f_1, g_1, \dots, f_s, g_s$, is there an assignment $\boldsymbol{a}$ to the input variables such that $\bigwedge_{i=1}^{s} f_i(\boldsymbol{a}) = g_i(\boldsymbol{a})$?

We provide a polynomial time algorithm for these problems provided that

> $\mathbf{A}$ *is a supernilpotent algebra of finite type in a congruence modular variety.*

Such algebras exist

Overview of the results

Two computational problems are associated with every algebra $\mathbf{A}$ and every $s \in \mathbb{N}$:

1. s-POLSYSSAT($\mathbf{A}$): Does a given system of s polynomial equations have a solution in $\mathbf{A}$?
2. s-SCSAT($\mathbf{A}$): Given $2s$ circuits $f_1, g_1, \ldots, f_s, g_s$, is there an assignment $\boldsymbol{a}$ to the input variables such that $\bigwedge_{i=1}^{s} f_i(\boldsymbol{a}) = g_i(\boldsymbol{a})$?

We provide a polynomial time algorithm for these problems provided that

> $\mathbf{A}$ *is a supernilpotent algebra of finite type in a congruence modular variety.*

Such algebras exist, have been studied

Overview of the results

Two computational problems are associated with every algebra $\mathbf{A}$ and every $s \in \mathbb{N}$:

1. s-PolSysSat($\mathbf{A}$): Does a given system of s polynomial equations have a solution in $\mathbf{A}$?
2. s-SCSat($\mathbf{A}$): Given $2s$ circuits $f_1, g_1, \ldots, f_s, g_s$, is there an assignment $\boldsymbol{a}$ to the input variables such that $\bigwedge_{i=1}^{s} f_i(\boldsymbol{a}) = g_i(\boldsymbol{a})$?

We provide a polynomial time algorithm for these problems provided that

> $\mathbf{A}$ *is a supernilpotent algebra of finite type in a congruence modular variety.*

Such algebras exist, have been studied, and include many familiar algebraic structures, such as nilpotent groups, nilpotent rings, and nilpotent loops of prime power order.

Which algebras are considered?

A supernilpotent algebra in a congruence modular variety is an algebra $\mathbf{A}$ that

1. has a Mal'cev operation $d(a,a,b) = d(b,b,a) = a$ among its term operations,
2. has a $k \in \mathbb{N}$ such that for all $n \geq k$, every n-ary polynomial function p, and all $a_1, b_1, \ldots, a_n, b_n \in A$,
   the value of
   $$p(b_1, \ldots, b_n)$$
   is determined by the $2^n - 1$ values
   $$p(a_1, \ldots, a_n), p(a_1, \ldots, a_{n-1}, b_n), \ldots, p(b_1, \ldots, b_{n-1}, a_n).$$
   ($2^n - 1$ vertices of a hypercube determine the remaining one.)

An instance of 2-PolSysSat(D_4)

A system of polynomial equations

$$\begin{aligned} D_4 &:= \langle a, b \mid a^4 = b^2 = 1, b * a = a^3 * b \rangle \\ \mathbf{D}_4 &:= (D_4; *). \end{aligned}$$

Then

$$\begin{aligned} x_1 * x_1 * b * x_2 * x_2 &\approx x_1 * a \\ x_1 * x_1 * b * x_2 * x_2 &\approx b * x_2 \end{aligned}$$

is a system of 2 polynomial equations over $\mathbf{D}_4$.

Question

Does the system have a solution inside D_4?

Comparison to other problems

Similar problems

- $\textsc{PolSat}(\mathbf{A}) = 1$-$\textsc{PolSysSat}(\mathbf{A})$.
- $\textsc{PolSysSat}(\mathbf{A})$ (no restriction on the number of equations).

Difficulties of these problems

$\textsc{PolSat}(\mathbf{A}) = 1$-$\textsc{PolSysSat}(\mathbf{A}) \leq 2$-$\textsc{PolSysSat}(\mathbf{A}) \leq \textsc{PolSysSat}(\mathbf{A})$

Comparison between these problems

One equation – two equations – arbitrary many equations

$\textsc{PolSat}(\mathbf{A}) = 1\text{-}\textsc{PolSysSat}(\mathbf{A}) \leq 2\text{-}\textsc{PolSysSat}(\mathbf{A}) \leq \textsc{PolSysSat}(\mathbf{A})$

One is easier than two is easier than arbitrary many equations

- $\mathbf{L} = (\{0,1\}; \vee, \wedge)$: $\textsc{PolSat}(\mathbf{L}) \in \mathrm{P}$ and $2\text{-}\textsc{PolSysSat}(\mathbf{L})$ is NP-complete [Gorazd, Krzaczkowsi 2011].
- $\textsc{PolSysSat}(\mathbf{D}_4)$ is NP-complete [Goldmann, Russell, 2002].
- We will prove that for every $s \in \mathbb{N}$:

$$s\text{-}\textsc{PolSysSat}(\mathbf{D}_4) \in \mathrm{P}.$$

Systems of equations over supernilpotent algebras

History

- $\mathbf{G}$ is a finite nilpotent group $\Rightarrow$ PolSat$(\mathbf{G}) \in \mathrm{P}$ [Goldmann, Russell, 2002] and [Horváth, 2011]
- $\mathbf{R}$ is a finite nilpotent ring $\Rightarrow$ PolSat$(\mathbf{R}) \in \mathrm{P}$ [Goldmann, Russell, 2002] and [Horváth, 2011]
- $\mathbf{A}$ is a finite supernilpotent algebra of finite type in a congruence modular variety $\Rightarrow$ PolSat$(\mathbf{A}) \in \mathrm{P}$ [Kompatscher, 2018]

Equations over supernilpotent algebras

Algorithms for one equation are based on:

Theorem [Goldmann, Russell, 2002; Horváth 2011; Kompatscher 2018]

Let $\mathbf{A}$ be a finite supernilpotent algebra in a cm variety, let $o \in A$. Then
$\exists d_{\mathbf{A}} \in \mathbb{N} \quad \forall n \in \mathbb{N} \ \ \forall \boldsymbol{a} \in A^n \ \ \forall f \in \mathrm{Pol}_n(\mathbf{A}) \quad \exists \boldsymbol{y} \in A^n \ :$

$$f(\boldsymbol{y}) = f(\boldsymbol{a}), \text{ and } \boldsymbol{y} \text{ has at most } d_{\mathbf{A}} \text{ entries different from } o.$$

Hence: if $f(\boldsymbol{x}) \approx b$ has a solution and $n \geq d_{\mathbf{A}}$, there is one in a hitting set C with

$$|C| \leq \binom{n}{d_{\mathbf{A}}} |A|^{d_{\mathbf{A}}}.$$

Equations over supernilpotent algebras

The exponent $d_{\mathbf{A}}$

- $d_{\mathbf{A}}$ is the degree of the polynomial bounding the “running time” of this algorithm.
- Horváth and Kompatscher obtain $d_{\mathbf{A}}$ by Ramsey’s Theorem.
- Faster solutions of $\textsc{PolSat}(\mathbf{A})$ for nilpotent groups and rings using structure theory: [Földvári, 2017 and 2018].

Equations over supernilpotent algebras

The exponent $d_{\mathbf{A}}$

- $d_{\mathbf{A}}$ is the degree of the polynomial bounding the "running time" of this algorithm.
- Horváth and Kompatscher obtain $d_{\mathbf{A}}$ by Ramsey's Theorem.
- For nilpotent rings $\mathbf{A}$, a non-Ramsey $d_{\mathbf{A}}$ was found in [Károlyi and Szabó, 2015].
- Faster solutions of $\textsc{PolSat}(\mathbf{A})$ for nilpotent groups and rings using structure theory: [Földvári, 2017 and 2018].

Systems of equations over supernilpotent algebras

Our contribution:

1. We improve the exponent $d_{\mathbf{A}}$ and obtain $d_{\mathbf{A}} := |A|^{\log_2(\mu)+\log_2(|A|)+1}$.
2. We generalize from 1 equation to s equations.

The main techniques are:

1. A description of supernilpotent algebras using the arithmetic of polynomials over finite fields ("Coordinatization").

2. An argument used by [Károlyi Szabó 2015] for solving equations in finite nilpotent rings. They use additive combinatorics and Alon's Combinatorial Nullstellensatz.

Systems of equations over supernilpotent algebras

Our contribution:

1. We improve the exponent $d_{\mathbf{A}}$ and obtain $d_{\mathbf{A}} := |A|^{\log_2(\mu)+\log_2(|A|)+1}$.
2. We generalize from 1 equation to s equations.

The main techniques are:

1. A description of supernilpotent algebras using the arithmetic of polynomials over finite fields (“Coordinatization”). Mainly done in [EA 2019, Bounding the free spectrum . . .].
2. An argument used by [Károlyi Szabó 2015] for solving equations in finite nilpotent rings. They use additive combinatorics and Alon’s Combinatorial Nullstellensatz.

Systems of equations over supernilpotent algebras

Our contribution:

1. We improve the exponent $d_{\mathbf{A}}$ and obtain $d_{\mathbf{A}} := |A|^{\log_2(\mu)+\log_2(|A|)+1}$.
2. We generalize from 1 equation to s equations.

The main techniques are:

1. A description of supernilpotent algebras using the arithmetic of polynomials over finite fields ("Coordinatization"). Mainly done in [EA 2019, Bounding the free spectrum . . .].
2. An argument used by [Károlyi Szabó 2015] for solving equations in finite nilpotent rings. They use additive combinatorics and Alon's Combinatorial Nullstellensatz. Generalized and presented in [EA 2019, MFCS 44].

Replacing arguments with 0

Definition

Let $o \in A$, $\boldsymbol{a} = (a_1, \ldots, a_n) \in A^n$, $U \subseteq \{1, \ldots, n\}$. Then

$$\boldsymbol{a}^{(U)}(i) = \begin{cases} a_i & \text{if} \quad i \in U, \\ o & \text{if} \quad i \notin U. \end{cases}$$

Hence $(a_1, a_2, a_3, a_4)^{(\{1,3\})} = (a_1, o, a_3, o)$.

A property of polynomial systems (prime power order)

Theorem [EA 2019], [Károlyi Szabó 2015]

Let $\mathbf{A}$ be in a cm variety with $|A| = p^\alpha = q$, let μ be maximal arity of the basic operations, let o be an element of A, $K := (\mu(p^\alpha - 1))^{\alpha-1}$. Let

$$\begin{aligned} u_1(x_1,\dots,x_n) &\approx v_1(x_1,\dots,x_n) \\ &\vdots \\ u_s(x_1,\dots,x_n) &\approx v_s(x_1,\dots,x_n) \end{aligned}$$

be a polynomial system over $\mathbf{A}$.

Let $\boldsymbol{a} \in A^n$ be a solution of this system. Then there is $U \subseteq \{1,\dots,n\}$ with

$$|U| \leq Ks\alpha(p-1)$$

such that $\boldsymbol{a}^{(U)}$ is a solution.

We can drop the prime power order restriction:

Theorem [EA 2019]

Let $\mathbf{A}$ be supernilpotent in a cm variety with all basic operations of arity $\leq \mu$. Let $F : A^n \to A^s$ with $F \in (\mathrm{Pol}_n(\mathbf{A}))^s$ be a polynomial map, and let $z \in A$.

Then

$\forall \boldsymbol{a} \in A^n \; \exists \boldsymbol{y} \in A^n$ such that

$$F(\boldsymbol{y}) = F(\boldsymbol{a}) \text{ and } \#\{j \in \underline{n} : \boldsymbol{y}(j) \neq z\} \leq s|A|^{\log_2(\mu)+\log_2(|A|)+1}.$$

Complexity of solving polynomial systems

Theorem [EA 2018]

Let $\mathbf{A}$ be a finite supernilpotent algebra in a congruence modular variety, and let $s \in \mathbb{N}$. Let

$$e := s|A|^{\log_2(\mu)+\log_2(|A|)+1}.$$

Then there exist $c_{\mathbf{A}} \in \mathbb{N}$ and an algorithm that decides s-PolSysSat$(\mathbf{A})$ using at most $c_{\mathbf{A}} \cdot n^e$ evaluations of the system, where n is the number of variables.

Circuit satisfiability

Definition [Idziak Krzaczkowski 2018]

Problem SCSAT($\mathbf{A}$).

Given: An even number of "circuits" $f_1, g_1, \dots, f_m, g_m$ whose gates are taken from the basic operations on $\mathbf{A}$ with n input variables.

Asked: $\exists \boldsymbol{a} \in A^n : f_1(\boldsymbol{a}) = g_1(\boldsymbol{a}), \dots, f_m(\boldsymbol{a}) = g_m(\boldsymbol{a})$.

A restriction to the input

s-SCSAT($\mathbf{A}$) : $2s$ circuits.

Circuit satisfiability

Theorem (Complexity of circuit satisfaction)

Let $\mathbf{A}$ be a finite algebra of finite type in a cm variety.

- SCSAT$(\mathbf{A}) \in \mathrm{P}$ if $\mathbf{A}$ is abelian [Larose Zádori 2006].
- SCSAT$(\mathbf{A})$ is NP-complete if $\mathbf{A}$ is not abelian [Larose Zádori 2006].
- $\mathbf{A}$ is supernilpotent $\Rightarrow$ 1-SCSAT$(\mathbf{A}) \in \mathrm{P}$ [Goldmann Russell Horváth Kompatscher 2018].
- $\mathbf{A}$ has no homomorphic image $\mathbf{A}'$ for which 1-SCSAT$(\mathbf{A}')$ is NP-complete $\Rightarrow$ $\mathbf{A} \cong \mathbf{N} \times \mathbf{D}$ with $\mathbf{N}$ nilpotent and $\mathbf{D}$ is a subdirect product of 2-element algebras that are polynomially equivalent to the two-element lattice. [Idziak Krzaczkowski 2017].

Complexity of s-SCSAT$(\mathbf{A})$

Theorem [EA 2019]

Let $\mathbf{A}$ be a finite algebra in a cm variety, $s \in \mathbb{N}$.

- $\mathbf{A}$ supernilpotent $\Rightarrow$ s-SCSAT$(\mathbf{A}) \in \mathrm{P}$.
- $\mathbf{A}$ has no homomorphic image $\mathbf{A}'$ for which 2-SCSAT$(\mathbf{A}')$ is NP-complete $\Rightarrow$ $\mathbf{A}$ is nilpotent.
  (Corollary of [Gorazd Krzaczkowski 2011] and [Idziak Krzaczkowski 2017].)