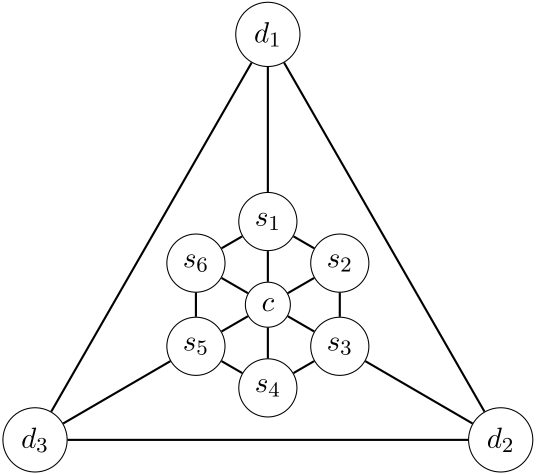
SOLVING EQUATIONS IN FINITE ALGEBRAS

Erhard Aichinger
Institute for Algebra
Austrian Science Fund FWF P29931

JOHANNES KEPLER UNIVERSITY LINZ

Using equation solving for: Graph coloring



Task: Color the 10 vertices of the graph with 3 colors.
No vertices connected by an edge may have the same color.

Algebraic task: Find
$c, s_1, \ldots, s_6, d_1, \ldots, d_3 \in \mathbb{R}$ such that
$c, s_1, \ldots, d_3 \in \{1, 2, 3\}$, and
$c \neq s_1, \ldots, d_2 \neq d_3$.

Using equation solving for: Graph coloring

Fact

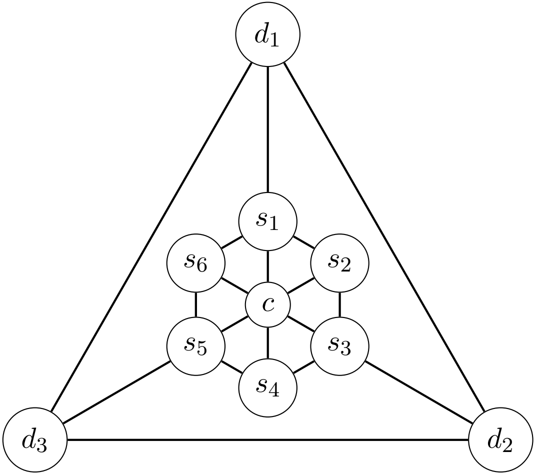
Let

$$
\begin{aligned}
p(x) &:= (x-1)(x-2)(x-3) = x^3 - 6x^2 + 11x - 6, \\
q(x,y) &:= \tfrac{p(x)-p(y)}{x-y} = x^2 + xy - 6x + y^2 - 6y + 11.
\end{aligned}
$$

Then:

- For all $z \in \mathbb{R}$: $z \in \{1,2,3\}$ iff $p(z) = 0$.
- For $(u,v) \in \{1,2,3\} \times \{1,2,3\}$, we have $u \neq v$ iff $q(x,y) = 0$.

Using equation solving for: Graph coloring



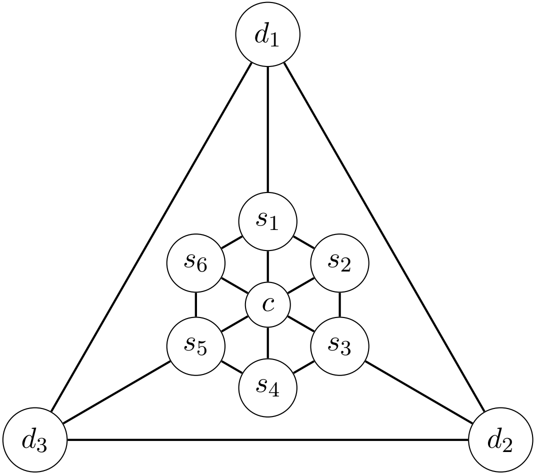
Algebraic task:

Solve

$p(c) = p(s_1) = \cdots = p(d_3) = 0,$

$q(c, s_1) = q(c, s_2) = \cdots q(d_2, d_3) = 0$.

Using equation solving for: Graph coloring



Algebraic task:

Solve

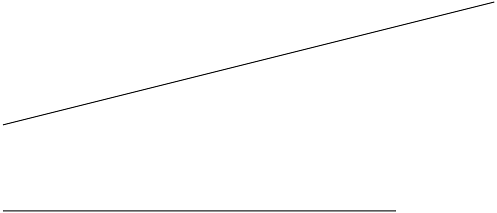
$p(c) = p(s_1) = \cdots = p(d_3) = 0,$

$q(c, s_1) = q(c, s_2) = \cdots q(d_2, d_3) = 0.$

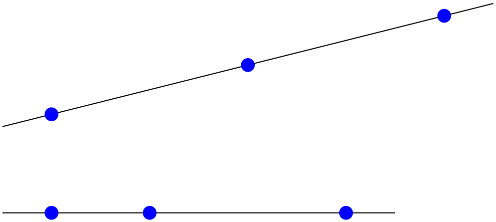
Solution of the algebraic task: The Gröbner basis of the system is $\{1\}$. (Mathematica, 40ms).

Conclusion: No coloring with 3 colors is possible.

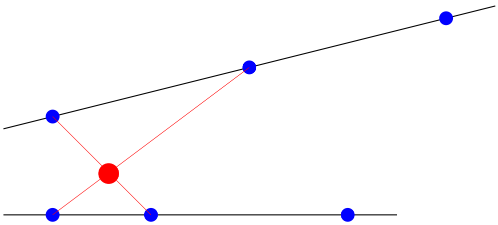
Using equation solving for: Geometrical Theorem Proving



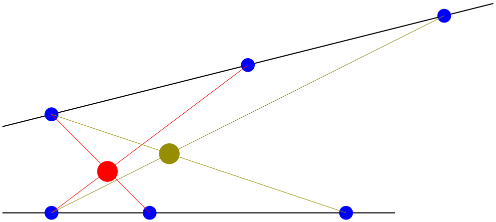
Using equation solving for: Geometrical Theorem Proving



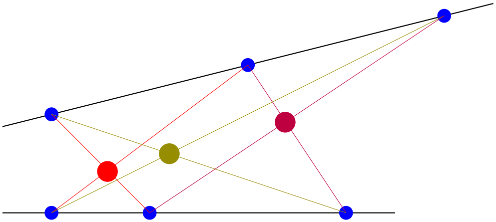
Using equation solving for: Geometrical Theorem Proving



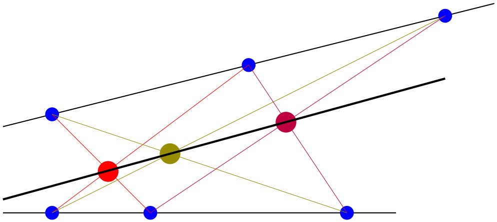
Using equation solving for: Geometrical Theorem Proving



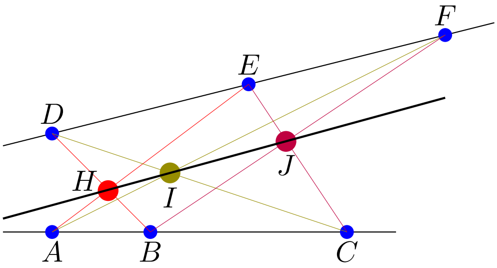
Using equation solving for: Geometrical Theorem Proving



Using equation solving for: Geometrical Theorem Proving



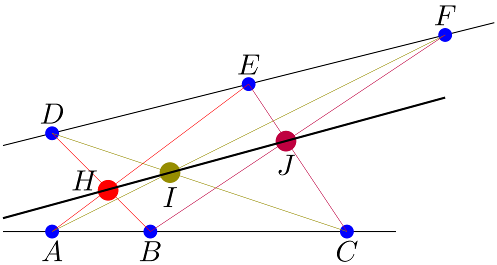
Using equation solving for: Geometrical Theorem Proving



Theorem (Pappus of Alexandria, $\sim$320)
Let $A, B, C, D, E, F, H, I, J$ points in the plane such that each of the following triples is collinear:
(A, B, C), (D, E, F), (A, H, E), (D, H, B), (D, I, C), (A, I, F), (E, J, C), (B, J, F).

Then (H, I, J) are collinear.

Using equation solving for: Geometrical Theorem Proving



Theorem (Pappus of Alexandria, $\sim$320)
Let $A, B, C, D, E, F, H, I, J$ points in the plane such that each of the following triples is collinear:
(A, B, C), (D, E, F), (A, H, E), (D, H, B), (D, I, C), (A, I, F), (E, J, C), (B, J, F).
Assume that (A, B, D) and (A, B, E) are not collinear.

Then (H, I, J) are collinear.

Using equation solving for: Geometrical Theorem Proving

Theorem. Suppose that (A, B, C), (D, E, F), (A, H, E), (D, H, B), (D, I, C), (A, I, F), (E, J, C), (B, J, F) are collinear, and that (A, B, D) and (A, B, E) are not collinear.
Then (H, I, J) is collinear.

Proof:

- We try to construct a counterexample.
- We coordinatize points with pairs of real numbers: $A = (a_1, a_2), \ldots, J = (j_1, j_2)$.
- $C(u_1, u_2, v_1, v_2, w_1, w_2) := \det(\begin{pmatrix} u_1 & u_2 & 1 \\ v_1 & v_2 & 1 \\ w_1 & w_2 & 1 \end{pmatrix}) = -u_2v_1 + u_1v_2 + u_2w_1 - v_2w_1 - u_1w_2 + v_1w_2$ has the property: $C(u_1, u_2, v_1, v_2, w_1, w_2) = 0$ iff $(\binom{u_1}{u_2}, \binom{v_1}{v_2}, \binom{w_1}{w_2})$ is collinear.

Using equation solving for: Geometrical Theorem Proving

Theorem. Suppose that (A, B, C), (D, E, F), (A, H, E), (D, H, B), (D, I, C), (A, I, F), (E, J, C), (B, J, F) are collinear, and that (A, B, D) and (A, B, E) are not collinear.
Then (H, I, J) is collinear.

Proof:

- A counterexample has to satisfy

$$\begin{aligned}
&C(a_1, a_2, b_1, b_2, c_1, c_2) = \cdots = C(b_1, b_2, j_1, j_2, f_1, f_2) = 0,\\
&C(a_1, a_2, b_1, b_2, d_1, d_2) \neq 0,\;\; C(a_1, a_2, b_1, b_2, e_1, e_2) \neq 0,\\
&C(h_1, h_2, i_1, i_2, j_1, j_2) \neq 0.
\end{aligned}$$

Using equation solving for: Geometrical Theorem Proving

Theorem. Suppose that (A, B, C), (D, E, F), (A, H, E), (D, H, B), (D, I, C), (A, I, F), (E, J, C), (B, J, F) are collinear, and that (A, B, D) and (A, B, E) are not collinear.
Then (H, I, J) is collinear.

Proof:

- A counterexample has to satisfy

$$
\begin{aligned}
&C(a_1, a_2, b_1, b_2, c_1, c_2) = \cdots = C(b_1, b_2, j_1, j_2, f_1, f_2) = 0, \\
&C(a_1, a_2, b_1, b_2, d_1, d_2) \cdot z_1 = 1,\ C(a_1, a_2, b_1, b_2, e_1, e_2) \neq 0, \\
&C(h_1, h_2, i_1, i_2, j_1, j_2) \neq 0.
\end{aligned}
$$

Using equation solving for: Geometrical Theorem Proving

Theorem. Suppose that (A, B, C), (D, E, F), (A, H, E), (D, H, B), (D, I, C), (A, I, F), (E, J, C), (B, J, F) are collinear, and that (A, B, D) and (A, B, E) are not collinear.
Then (H, I, J) is collinear.

Proof:

- A counterexample has to satisfy

$$
\begin{aligned}
&C(a_1, a_2, b_1, b_2, c_1, c_2) = \cdots = C(b_1, b_2, j_1, j_2, f_1, f_2) = 0,\\
&C(a_1, a_2, b_1, b_2, d_1, d_2) \cdot z_1 = 1,\ C(a_1, a_2, b_1, b_2, e_1, e_2) \cdot z_2 = 1,\\
&C(h_1, h_2, i_1, i_2, j_1, j_2) \cdot z_3 = 1.
\end{aligned}
$$

- The theorem holds if and only if this **system of equations** has no solution in the real numbers.

Using equation solving for: Geometrical Theorem Proving

We use the computer algebra system “Mathematica”.

pappus.nb * - Wolfram Mathematica 12.0

File Edit Insert Format Cell Graphics Evaluation Palettes Window Help

In[40]:=
```
Collinear[P1_, P2_, P3_] := Det[{P1, P2, P3}];
AA = {a1, a2, 1}; BB = {b1, b2, 1}; CC = {c1, c2, 1};
DD = {d1, d2, 1}; EE = {e1, e2, 1}; FF = {f1, f2, 1};
HH = {h1, h2, 1}; II = {i1, i2, 1}; JJ = {j1, j2, 1};
TheSystem = {Collinear[AA, BB, CC], Collinear[DD, EE, FF], Collinear[AA, HH, EE], Collinear[DD, HH, BB],
  Collinear[DD, II, CC], Collinear[AA, II, FF], Collinear[EE, JJ, CC], Collinear[BB, JJ, FF],
  (*Non degenerate*)
  Collinear[AA, BB, DD] * z1 - 1, Collinear[AA, BB, EE] * z2 - 1,
  (*Conclusion*)
  Collinear[HH, II, JJ] * z3 - 1}
```

Out[44]=
```
{-a2 b1 + a1 b2 + a2 c1 - b2 c1 - a1 c2 + b1 c2,
 -d2 e1 + d1 e2 + d2 f1 - e2 f1 - d1 f2 + e1 f2, a2 e1 - a1 e2 - a2 h1 + e2 h1 + a1 h2 - e1 h2,
 -b2 d1 + b1 d2 + b2 h1 - d2 h1 - b1 h2 + d1 h2, -c2 d1 + c1 d2 + c2 i1 - d2 i1 - c1 i2 + d1 i2,
 a2 f1 - a1 f2 - a2 i1 + f2 i1 + a1 i2 - f1 i2, -c2 e1 + c1 e2 + c2 j1 - e2 j1 - c1 j2 + e1 j2,
 b2 f1 - b1 f2 - b2 j1 + f2 j1 + b1 j2 - f1 j2, -1 + (-a2 b1 + a1 b2 + a2 d1 - b2 d1 - a1 d2 + b1 d2) z1,
 -1 + (-a2 b1 + a1 b2 + a2 e1 - b2 e1 - a1 e2 + b1 e2) z2, -1 + (-h2 i1 + h1 i2 + h2 j1 - i2 j1 - h1 j2 + i1 j2) z3}
```

In[45]:=
```
GroebnerBasis [TheSystem] // Timing
```

Out[45]=
```
{2.02533, {1}}
```

absolute timing | extract time | extract result | clear cache first

200%

Using equation solving for: Geometrical Theorem Proving

Conclusions

- There is no counterexample to Pappus's Theorem, not even in the complex plane $\mathbb{C}^2$.
- Hence (this version) of Pappus's Theorem holds.
- Similar proofs for: Desargues, Ceva, Menelaus, ...
- **Algebraic** way to decide which first order formulae hold in the relational structure

$$\mathbf{L} = (\mathbb{C}^2, \text{IsCollinearTriple}(x, y, z))$$

  by **solving systems of polynomial equations**.
  What about **other axiomatizations** or **calculi** for this structure $\mathbf{L}$?

Using equation solving for: Boolean Satisfiability

Given: Equations over the algebraic structure $(\mathbf{B} = \{0, 1\}; \wedge, \vee, \neg, 0, 1)$, e. g.

$$\begin{aligned} x_1 \vee x_2 \vee x_3 &= 1 \\ x_2 \vee \neg x_3 &= 1 \\ x_1 \vee \neg x_3 &= 1. \end{aligned}$$

Asked: Does this system have a solution?

Using equation solving for: Boolean Satisfiability

Given: Equations over the algebraic structure $(\mathbf{B} = \{0,1\}; \wedge, \vee, \neg, 0, 1)$, e. g.

$$\begin{aligned} x_1 \vee x_2 \vee x_3 &= 1 \\ x_2 \vee \neg x_3 &= 1 \\ x_1 \vee \neg x_3 &= 1. \end{aligned}$$

Asked: Does this system have a solution?

Given: Equations over the algebraic structure $(\mathbb{F}_2 = \{0,1\}; +, \cdot, 0, 1)$,

$$\begin{aligned} x_1 + x_2 + x_3 + x_1x_2 + x_1x_3 & \\ +x_2x_3 + x_1x_2x_3 + 1 &= 0 \\ x_3 + x_2x_3 &= 0 \\ x_3 + x_1x_3 &= 0. \end{aligned}$$

Asked: Does this system have a solution?

Using equation solving for: Boolean Satisfiability

Given: Equations over the algebraic structure $(\mathbf{B} = \{0,1\}; \wedge, \vee, \neg, 0, 1)$, e. g.

$$\begin{aligned} x_1 \vee x_2 \vee x_3 &= 1 \\ x_2 \vee \neg x_3 &= 1 \\ x_1 \vee \neg x_3 &= 1. \end{aligned}$$

Asked: Does this system have a solution?

3SAT is known to be computationally hard (NP-complete).

Given: Equations over the algebraic structure $(\mathbb{F}_2 = \{0,1\}; +, \cdot, 0, 1)$,

$$\begin{aligned} x_1 + x_2 + x_3 + x_1x_2 + x_1x_3 & \\ +x_2x_3 + x_1x_2x_3 + 1 &= 0 \\ x_3 + x_2x_3 &= 0 \\ x_3 + x_1x_3 &= 0. \end{aligned}$$

Asked: Does this system have a solution?

Using equation solving for: Boolean Satisfiability

Given: Equations over the algebraic structure $(\mathbf{B} = \{0,1\}; \wedge, \vee, \neg, 0, 1)$, e. g.

$$\begin{aligned} x_1 \vee x_2 \vee x_3 &= 1 \\ x_2 \vee \neg x_3 &= 1 \\ x_1 \vee \neg x_3 &= 1. \end{aligned}$$

Asked: Does this system have a solution?

3SAT is known to be computationally hard (NP-complete).

Given: Equations over the algebraic structure $(\mathbb{F}_2 = \{0,1\}; +, \cdot, 0, 1)$,

$$\begin{aligned} x_1 + x_2 + x_3 + x_1x_2 + x_1x_3 & \\ +x_2x_3 + x_1x_2x_3 + 1 &= 0 \\ x_3 + x_2x_3 &= 0 \\ x_3 + x_1x_3 &= 0. \end{aligned}$$

Asked: Does this system have a solution?

Hence solving polynomial systems over $\mathbb{F}_2$ is also hard (NP-complete).

Solving equations over finite fields

Given: $f_1, \ldots, f_s \in \mathbb{F}_2[x_1, \ldots, x_N]$.
Asked: $\exists \boldsymbol{a} \in \mathbb{F}_2^N : f_1(\boldsymbol{a}) = \cdots = f_s(\boldsymbol{a}) = 0$.

Computational Complexity:

Restrictions	1 eqn.	s eqns.	none
none			
$f_1, \ldots, f_s$ in expanded form			
$\deg(f_i) \leq D$			

Solving equations over finite fields

Given: $f_1, \ldots, f_s \in \mathbb{F}_2[x_1, \ldots, x_N]$.
Asked: $\exists \boldsymbol{a} \in \mathbb{F}_2^N : f_1(\boldsymbol{a}) = \cdots = f_s(\boldsymbol{a}) = 0$.

Computational Complexity:

Restrictions	1 eqn.	s eqns.	none
none	NP-comp.	NP-comp.	NP-comp.
$f_1, \ldots, f_s$ in expanded form			NP-comp.
$\deg(f_i) \leq D$			NP-comp if $D \geq 2$.

Solving equations over finite fields

Given: $f_1, \ldots, f_s \in \mathbb{F}_2[x_1, \ldots, x_N]$.
Asked: $\exists \boldsymbol{a} \in \mathbb{F}_2^N : f_1(\boldsymbol{a}) = \cdots = f_s(\boldsymbol{a}) = 0$.

Computational Complexity:

Restrictions	1 eqn.	s eqns.	none
none	NP-comp.	NP-comp.	NP-comp.
$f_1, \ldots, f_s$ in expanded form	P		NP-comp.
$\deg(f_i) \leq D$			NP-comp if $D \geq 2$.

Solving equations over finite fields

Given: $f_1, \dots, f_s \in \mathbb{F}_2[x_1, \dots, x_N]$.
Asked: $\exists \boldsymbol{a} \in \mathbb{F}_2^N : f_1(\boldsymbol{a}) = \cdots = f_s(\boldsymbol{a}) = 0$.

Computational Complexity:

Restrictions	1 eqn.	s eqns.	none
none	NP-comp.	NP-comp.	NP-comp.
$f_1, \dots, f_s$ in expanded form	P	P	NP-comp.
$\deg(f_i) \leq D$			NP-comp if $D \geq 2$.

Solving equations over finite fields

Given: $f_1, \ldots, f_s \in \mathbb{F}_2[x_1, \ldots, x_N]$.
Asked: $\exists \boldsymbol{a} \in \mathbb{F}_2^N : f_1(\boldsymbol{a}) = \cdots = f_s(\boldsymbol{a}) = 0$.

Computational Complexity:

Restrictions	1 eqn.	s eqns.	none
none	NP-comp.	NP-comp.	NP-comp.
$f_1, \ldots, f_s$ in expanded form	P	P	NP-comp.
$\deg(f_i) \leq D$	P	P	NP-comp if $D \geq 2$.

Solving equations over finite fields

Given: $f_1, \dots, f_s \in \mathbb{F}_2[x_1, \dots, x_N]$.
Asked: $\exists \boldsymbol{a} \in \mathbb{F}_2^N : f_1(\boldsymbol{a}) = \cdots = f_s(\boldsymbol{a}) = 0$.

Computational Complexity:

Restrictions	1 eqn.	s eqns.	none
none	NP-comp.	NP-comp.	NP-comp.
$f_1, \dots, f_s$ in expanded form	P	P	NP-comp.
$\deg(f_i) \leq D$	P	P	NP-comp if $D \geq 2$.

Reason: If there is a solution, then there is one with many zeroes.

Solving equations over finite fields

We use Alon's Combinatorial Nullstellensatz with restricted variables.

Theorem [Brink, 2011]

Let $f_1, \dots, f_s \in \mathbb{F}_q[x_1, \dots, x_N]$, for all $i : \deg(f_i) \leq D$, $\boldsymbol{a} = (a_1, \dots, a_N) \in \mathbb{F}_q^N$. Suppose $N > (q-1)sD$.
If $f_1(\boldsymbol{a}) = \cdots = f_s(\boldsymbol{a}) = 0$, then the system has at least one more solution in $\{0, a_1\} \times \{0, a_2\} \times \cdots \times \{0, a_N\}$.

Solving equations over finite fields

Let $\boldsymbol{a} = (a_1, \dots, a_N) \in \mathbb{F}_q^N$, $U \subseteq \{1, \dots, N\}$. 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 $(a_1, a_2, a_3, a_4)^{(\{1,3\})} = (a_1, o, a_3, o)$.

Corollary [Károlyi and Szabó, 2015]

Let $f_1, \dots, f_s \in \mathbb{F}_q[x_1, \dots, x_N]$, for all $i : \deg(f_i) \leq D$, let $\boldsymbol{a} = (a_1, \dots, a_N) \in \mathbb{F}_q^N$.

If $f_1(\boldsymbol{a}) = \dots = f_s(\boldsymbol{a}) = 0$, then

$$\exists U \subseteq \{1, \dots, N\} : |U| \leq (q-1)sD \text{ and } f_1(\boldsymbol{a}^{(U)}) = \dots = f_s(\boldsymbol{a}^{(U)}) = 0.$$

Solving equations over finite fields

Problem: $\textsc{PolSysSat}(\mathbb{F}_2)$ with bounded degree D and fixed number s of equations.
Given: $f_1, \ldots, f_s \in \mathbb{F}_2[x_1, \ldots, x_N]$ of degree $\leq D$.
Asked: $\exists \boldsymbol{a} \in \mathbb{F}_2^N : f_1(\boldsymbol{a}) = \cdots = f_s(\boldsymbol{a}) = 0$.

Let wt$(\boldsymbol{a})$ be the number of indices with nonzero entries in $\boldsymbol{a}$.

It is sufficient to seach inside $R = \{\boldsymbol{a} \in \mathbb{F}_2^N \ : \ \text{wt}(\boldsymbol{a}) \leq sD\}$. Since

$$|R| \leq \binom{N}{sD} 2^{sD} \in O(N^{sD}) \text{ (when } s, D \text{ are fixed)},$$

this gives a polynomial time algorithm.

Equations over groups and algebras: problem statement

A system of polynomial equations over the dihedral group

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

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?

Equations over groups and algebras: problem statement

The general problem

Let $s \in \mathbb{N}$, and let $\mathbf{A} = (A; f_1, \dots, f_n)$ be a finite algebra. The decision problem s-PolSysSat($\mathbf{A}$) is:

Given: $2s$ polynomial terms $f_1, g_1, \dots, f_s, g_s$ over $\mathbf{A}$.

Asked: Does the system $f_1 \approx g_1, \dots, f_s \approx g_s$ have a solution in $\mathbf{A}$?

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

Let $s \in \mathbb{N}$. Then s-PolSysSat($\mathbf{A}$) $\in \mathrm{NP}$.

Equations over groups and algebras: comparison

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

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

Equations over groups and algebras: complexity

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 [Larose and Zádori 2006].
- We will prove that for every $s \in \mathbb{N}$:

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

Equation over finite p-groups

Goal: solve systems of equations over groups of prime power order.

Let G be a finite group with $|G| = p^n$, $p \in \mathbb{P}$, $n \geq 2$. Then

1. G is nilpotent of class $\leq n - 1$.
2. Equivalently, the lower central series $G_0 := G$, $G_i := [G, G_{i-1}]$ for $i \in \mathbb{N}$ satisfies $G_{n-1} = \{1_G\}$.

Equations over finite p-groups

- For every algebraic structure $\mathbf{A} = (A; f_1, f_2, \ldots)$, one can define its polynomial functions.
- They are those functions that can be represented by terms, using possibly constants from A.
- On a group $(G, *)$ with $a, b \in G$, the function $f : G^3 \to G$ defined by

$$f(x, y, z) := a * x * z * b * y * b * y * z * x * z * z * a$$

  for $x, y, z \in G$ is a polynomial function of $(G, *)$
- We will try to find a field $\mathbf{F}$ so that we can represent f by $p \in \mathbf{F}[x_1, \ldots, x_n]$.

$$f(x, y, z) = a_1\, x^3 y^2 + a_2\, x^2 z^4 + \ldots .$$

Equations over finite p-groups

We will now explain the method for solving systems from

- EA. Solving systems of equations in supernilpotent algebras. ArXiv e-prints (2019).

This method is based on

- G. Károlyi and C. Szabó, Evaluation of Polynomials over Finite Rings via Additive Combinatorics, ArXiv e-prints (2018).

The generalization from rings to other structures, such as groups, uses the coordinatization method for nilpotent algebras, which is Theorem 4.2 of

- EA, Bounding the free spectrum of nilpotent algebras of prime power order, Israel Journal of Mathematics (2019).

Equations over finite p-groups: Coordinatization

Theorem [EA, 2019]

Let $(G, *)$ be a group with $|G| = p^\alpha$. Let $K := (2(p^\alpha - 1))^{\alpha-1}$. Then there are binary operations $+$, $\cdot$ on G such that

- $\mathbf{F} := (G, +, \cdot)$ is a field,

Equations over finite p-groups: Coordinatization

Theorem [EA, 2019]

Let $(G, *)$ be a group with $|G| = p^\alpha$. Let $K := (2(p^\alpha - 1))^{\alpha-1}$. Then there are binary operations $+$, $\cdot$ on G such that

- $\mathbf{F} := (G, +, \cdot)$ is a field,
- For every $n \in \mathbb{N}$ and every polynomial function $f : G^n \to G$, there is $p \in \mathbf{F}[x_1, \ldots, x_n]$ such that
    1. f is the function induced by p,

Equations over finite p-groups: Coordinatization

Theorem [EA, 2019]

Let $(G, *)$ be a group with $|G| = p^\alpha$. Let $K := (2(p^\alpha - 1))^{\alpha-1}$. Then there are binary operations $+$, $\cdot$ on G such that

- $\mathbf{F} := (G, +, \cdot)$ is a field,
- For every $n \in \mathbb{N}$ and every polynomial function $f : G^n \to G$, there is $p \in \mathbf{F}[x_1, \ldots, x_n]$ such that
  1. f is the function induced by p,
  2. In its expanded form, every monomial of p contains at most K variables. Hence $\mathrm{width}(p) \leq K$.

The width of a polynomial $p \in \mathbf{F}[x_1, \ldots, x_n]$ is the maximal number of variables in one monomial. (The word “width” was suggested by C. Raab.)

Equations over finite p-groups

Theorem [EA 2018], [Károlyi Szabó 2015]

Let G be a group with $|G| = p^\alpha = q$, and let $K := (2(p^\alpha - 1))^{\alpha-1}$. Let

$$\begin{array}{rcl} u_1(x_1, \ldots, x_n) & \approx & v_1(x_1, \ldots, x_n) \\ & \vdots & \\ u_s(x_1, \ldots, x_n) & \approx & v_s(x_1, \ldots, x_n) \end{array}$$

be a polynomial system over G.

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

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

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

Equations over finite p-groups

Proof:

- Using the coordinatization, our system is $f_1(\boldsymbol{x}) \approx \cdots \approx f_s(\boldsymbol{x}) \approx 0$ with $f_i \in \mathbf{F}[x_1, \ldots, x_n]$.

Equations over finite p-groups

Proof:

- Using the coordinatization, our system is $f_1(\boldsymbol{x}) \approx \cdots \approx f_s(\boldsymbol{x}) \approx 0$ with $f_i \in \mathbf{F}[x_1, \ldots, x_n]$.
- All f_i's have width $\leq K$.

Equations over finite p-groups

Proof:

- Using the coordinatization, our system is $f_1(\boldsymbol{x}) \approx \cdots \approx f_s(\boldsymbol{x}) \approx 0$ with $f_i \in \mathbf{F}[x_1, \ldots, x_n]$.
- All f_i's have width $\leq K$.
- $\prod_{i=1}^{s}(1 - f_i(\boldsymbol{a})^{q-1}) \neq 0$.

Equations over finite p-groups

Proof:

- Using the coordinatization, our system is $f_1(\boldsymbol{x}) \approx \cdots \approx f_s(\boldsymbol{x}) \approx 0$ with $f_i \in \mathbf{F}[x_1, \ldots, x_n]$.
- All f_i's have width $\leq K$.
- $\prod_{i=1}^{s}(1 - f_i(\boldsymbol{a})^{q-1}) \neq 0$.
- $Q(\boldsymbol{x}) = \prod_{i=1}^{s}(1 - f_i(\boldsymbol{x})^{q-1})$ has width $\leq Ks(q-1)$ and $Q(\boldsymbol{a}) \neq 0$.

Equations over finite p-groups

Proof:

- Using the coordinatization, our system is $f_1(\boldsymbol{x}) \approx \cdots \approx f_s(\boldsymbol{x}) \approx 0$ with $f_i \in \mathbf{F}[x_1, \ldots, x_n]$.
- All f_i's have width $\leq K$.
- $\prod_{i=1}^{s}(1 - f_i(\boldsymbol{a})^{q-1}) \neq 0$.
- $Q(\boldsymbol{x}) = \prod_{i=1}^{s}(1 - f_i(\boldsymbol{x})^{q-1})$ has width $\leq Ks(q-1)$ and $Q(\boldsymbol{a}) \neq 0$.
- $\mathrm{rem}(Q(\boldsymbol{x}), \langle x_1^q - x_1, \ldots, x_n^q - x_n \rangle)$ has width $\leq Ks(q-1)$.

Equations over finite p-groups

Proof:

- Using the coordinatization, our system is $f_1(\boldsymbol{x}) \approx \cdots \approx f_s(\boldsymbol{x}) \approx 0$ with $f_i \in \mathbf{F}[x_1, \ldots, x_n]$.
- All f_i's have width $\leq K$.
- $\prod_{i=1}^{s}(1 - f_i(\boldsymbol{a})^{q-1}) \neq 0$.
- $Q(\boldsymbol{x}) = \prod_{i=1}^{s}(1 - f_i(\boldsymbol{x})^{q-1})$ has width $\leq Ks(q-1)$ and $Q(\boldsymbol{a}) \neq 0$.
- $\mathrm{rem}(Q(\boldsymbol{x}), \langle x_1^q - x_1, \ldots, x_n^q - x_n \rangle)$ has width $\leq Ks(q-1)$.
- “Hence” there is U with $|U| \leq Ks(q-1)$ and $Q(\boldsymbol{a}^{(U)}) \neq 0$.

Equations over finite p-groups

Proof:

- Using the coordinatization, our system is $f_1(\boldsymbol{x}) \approx \cdots \approx f_s(\boldsymbol{x}) \approx 0$ with $f_i \in \mathbf{F}[x_1, \ldots, x_n]$.
- All f_i's have width $\leq K$.
- $\prod_{i=1}^{s}(1 - f_i(\boldsymbol{a})^{q-1}) \neq 0$.
- $Q(\boldsymbol{x}) = \prod_{i=1}^{s}(1 - f_i(\boldsymbol{x})^{q-1})$ has width $\leq Ks(q-1)$ and $Q(\boldsymbol{a}) \neq 0$.
- $\mathrm{rem}(Q(\boldsymbol{x}), \langle x_1^q - x_1, \ldots, x_n^q - x_n \rangle)$ has width $\leq Ks(q-1)$.
- "Hence" there is U with $|U| \leq Ks(q-1)$ and $Q(\boldsymbol{a}^{(U)}) \neq 0$.
- Then $\boldsymbol{a}^{(U)}$ is a solution.

Equations over finite p-groups

Proof:

- Using the coordinatization, our system is $f_1(\boldsymbol{x}) \approx \cdots \approx f_s(\boldsymbol{x}) \approx 0$ with $f_i \in \mathbf{F}[x_1, \dots, x_n]$.
- All f_i's have width $\leq K$.
- $\prod_{i=1}^{s}(1 - f_i(\boldsymbol{a})^{q-1}) \neq 0$.
- $Q(\boldsymbol{x}) = \prod_{i=1}^{s}(1 - f_i(\boldsymbol{x})^{q-1})$ has width $\leq Ks(q-1)$ and $Q(\boldsymbol{a}) \neq 0$.
- $\operatorname{rem}(Q(\boldsymbol{x}), \langle x_1^q - x_1, \dots, x_n^q - x_n \rangle)$ has width $\leq Ks(q-1)$.
- “Hence” there is U with $|U| \leq Ks(q-1)$ and $Q(\boldsymbol{a}^{(U)}) \neq 0$.
- Then $\boldsymbol{a}^{(U)}$ is a solution.

Equations over finite p-groups

Proof:

- Using the coordinatization, our system is $f_1(\boldsymbol{x}) \approx \cdots \approx f_s(\boldsymbol{x}) \approx 0$ with $f_i \in \mathbf{F}[x_1, \ldots, x_n]$.
- All f_i's have width $\leq K$.
- $\prod_{i=1}^{s}(1 - f_i(\boldsymbol{a})^{q-1}) \neq 0$.
- $Q(\boldsymbol{x}) = \prod_{i=1}^{s}(1 - f_i(\boldsymbol{x})^{q-1})$ has width $\leq Ks(q-1)$ and $Q(\boldsymbol{a}) \neq 0$.
- $\mathrm{rem}(Q(\boldsymbol{x}), \langle x_1^q - x_1, \ldots, x_n^q - x_n \rangle)$ has width $\leq Ks(q-1)$.
- "Hence" there is U with $|U| \leq Ks(q-1)$ and $Q(\boldsymbol{a}^{(U)}) \neq 0$.
- Then $\boldsymbol{a}^{(U)}$ is a solution.

Remark: This proves $|U| \leq Ks(q-1) = Ks(p^\alpha - 1)$. For the stronger $|U| \leq Ks\alpha(p-1)$, we would need more concepts.

Equations over finite p-groups: complexity

Theorem [EA 2019]

Let $\mathbf{G}$ be a finite nilpotent group, modular variety, and let $s \in \mathbb{N}$. Let

$$e := s|G|^{\log_2(|G|)+2}.$$

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

For $s = 1$, a polynomial time method with a better (smaller) exponent was given by [Földvári, 2017] using the structure theory of p-groups.

Equations over arbitrary algebras

Observation:

- We have solved systems over finite nilpotent groups.
- [Károlyi and Szabó, 2015] use similar methods for finite nilpotent rings.
- [Kompatscher, 2018] solves 1 equation over finite supernilpotent algebras in congruence modular varieties.
- We will therefore look at the problem from universal algebra.

Equations over arbitrary algebras

- An algebraic structure or (universal) algebra is a first order structure $\mathbf{A} = (A; f_1, f_2 \ldots)$ with only function symbols.
- Theorems for all algebraic structures:
  - Homomorphism theorems $\mathbf{A}/\ker(h) \cong \mathrm{Im}(h)$.

Equations over arbitrary algebras

- An algebraic structure or (universal) algebra is a first order structure $\mathbf{A} = (A; f_1, f_2 \ldots)$ with only function symbols.
- Theorems for all algebraic structures:
  - Homomorphism theorems $\mathbf{A}/\ker(h) \cong \mathrm{Im}(h)$.
  - HSP-Theorem of Equational logic:
    $\mathrm{Mod}(\{\varphi = (\forall \boldsymbol{x} : s(\boldsymbol{x}) \approx t(\boldsymbol{x})) \mid \mathbf{A} \models \varphi\}) =$ class of all homomorphic images of subalgebras of direct powers of $\mathbf{A}$

Equations over arbitrary algebras

- An algebraic structure or (universal) algebra is a first order structure $\mathbf{A} = (A; f_1, f_2 \ldots)$ with only function symbols.
- Theorems for all algebraic structures:
  - Homomorphism theorems $\mathbf{A}/\ker(h) \cong \mathrm{Im}(h)$.
  - HSP-Theorem of Equational logic:
    $\mathrm{Mod}(\{\varphi = (\forall \boldsymbol{x} : s(\boldsymbol{x}) \approx t(\boldsymbol{x})) \mid \mathbf{A} \models \varphi\}) =$ class of all homomorphic images of subalgebras of direct powers of $\mathbf{A} = \mathrm{HSP}(\mathbf{A})$. [Birkhoff 1935]

Equations over arbitrary algebras: Structure Theory

Structure Theorems for classes of algebras:

- Algebras in congruence modular varieties: Each algebra in $\mathrm{HSP}(\mathbf{A})$ has a lattice of congruence relations that satisfies the modular law

$$x \leq z \to (x \vee y) \wedge z = x \vee (y \wedge z).$$

- The following varieties are congruence modular:
  - R-modules,

Equations over arbitrary algebras: Structure Theory

Structure Theorems for classes of algebras:

- Algebras in congruence modular varieties: Each algebra in $\mathrm{HSP}(\mathbf{A})$ has a lattice of congruence relations that satisfies the modular law

$$x \leq z \to (x \vee y) \wedge z = x \vee (y \wedge z).$$

- The following varieties are congruence modular:
  - R-modules, rings, nearrings, groups, loops, quasigroups,

Equations over arbitrary algebras: Structure Theory

Structure Theorems for classes of algebras:

- Algebras in congruence modular varieties: Each algebra in $\mathrm{HSP}(\mathbf{A})$ has a lattice of congruence relations that satisfies the modular law

$$x \leq z \to (x \vee y) \wedge z = x \vee (y \wedge z).$$

- The following varieties are congruence modular:
  - R-modules, rings, nearrings, groups, loops, quasigroups, (but not: semigroups),

Equations over arbitrary algebras: Structure Theory

Structure Theorems for classes of algebras:

- Algebras in congruence modular varieties: Each algebra in $\mathrm{HSP}(\mathbf{A})$ has a lattice of congruence relations that satisfies the modular law

$$x \leq z \rightarrow (x \vee y) \wedge z = x \vee (y \wedge z).$$

- The following varieties are congruence modular:
  - R-modules, rings, nearrings, groups, loops, quasigroups, (but not: semigroups), lattices.
  - All finite algebras with few subpowers [Berman, Idziak, Marković, McKenzie, Valeriote, Willard, TAMS, 2010]:

$$\exists p \in \mathbb{R}[x] \ \forall n \in \mathbb{N} : \text{number of subalgebras of } \mathbf{A}^n \leq 2^{p(n)}.$$

Equations over arbitrary algebras: Structure Theory

For algebras in congruence modular varieties, we have the following notions:

- commutators, generalizing the commutator subgroup $[A, B] = \langle \{a^{-1}b^{-1}ab \mid a \in A, b \in B\} \rangle$ of $A, B \trianglelefteq G$. (Commutator Theory, [Smith 1976], [Freese McKenzie 1987])
- abelian algebras: can be coordinatized by a ring module. [Gumm 1983]
- nilpotent and solvable algebras.

Equations over arbitrary algebras: Structure Theory

Nilpotency for groups and rings

- A group G is nilpotent if $\exists k \in \mathbb{N} : \underbrace{[G, [G, \dots, [G, G] \dots]]}_{k+1} = \{1_G\}$.
- A ring R is nilpotent if $\exists k \in \mathbb{N} : R \models x_1 x_2 \cdots x_{k+1} \approx 0$.

Nilpotency for universal algebras

Nilpotency has been generalized in two ways to arbitrary algebras: there are

- nilpotent, and
- supernilpotent

algebras.

Equations over supernilpotent algebras

- How difficult is solving polynomial systems over supernilpotent algebras?

Equations over supernilpotent algebras

History

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

Equations over supernilpotent algebras

Algorithms for one equation are based on:

Theorem [Horváth 2011, Kompatscher 2018]

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

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

Hence: if $f(\boldsymbol{x}) \approx b$ has a solution and $n \geq d_{\mathbf{A}}$, there is one in a 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 that bounds 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].

Equations over supernilpotent algebras

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

- $d_{\mathbf{A}}$ is the degree of the polynomial that bounds 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].

Equations over supernilpotent algebras

Technique:

- Coordinatization of a finite nilpotent algebra of prime power order using a finite field.

Equations over nilpotent algebras

Theorem. (Coordinatization of nilpotent algebras, [EA 2019]).
Let $\mathbf{A} = (A, (f_i)_{i \in I})$ be in a congruence modular variety, $|A| = p^\alpha$, with all fundamental operations of arity at most μ. Let $K := (\mu(p^\alpha - 1))^{\alpha-1}$. TFAE:

- $\mathbf{A}$ is nilpotent.

Equations over nilpotent algebras

Theorem. (Coordinatization of nilpotent algebras, [EA 2019]).
Let $\mathbf{A} = (A, (f_i)_{i\in I})$ be in a congruence modular variety, $|A| = p^\alpha$, with all fundamental operations of arity at most μ. Let $K := (\mu(p^\alpha - 1))^{\alpha-1}$. TFAE:

- $\mathbf{A}$ is nilpotent.
- There is a binary $+$ on A such that

$$\mathbf{A}' = (A, +, (f_i)_{i\in I})$$

  is nilpotent and $(A, +) \cong (\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p, +)$.

Equations over nilpotent algebras

Theorem. (Coordinatization of nilpotent algebras, [EA 2019]).
Let $\mathbf{A} = (A, (f_i)_{i \in I})$ be in a congruence modular variety, $|A| = p^\alpha$, with all fundamental operations of arity at most μ. Let $K := (\mu(p^\alpha - 1))^{\alpha - 1}$. TFAE:

- $\mathbf{A}$ is nilpotent.
- There is a binary $+$ on A such that
$$\mathbf{A}' = (A, +, (f_i)_{i \in I})$$
is nilpotent and $(A, +) \cong (\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p, +)$.
- There is a field $\mathbf{F} := (A, +, \cdot)$ such that
Pol$(\mathbf{A}) \subseteq \{p^{\mathbf{F}} \mid n \in \mathbb{N}, p \in \mathbf{F}[x_1, \ldots, x_n], \mathrm{width}(p) \leq K\}$.

Equations over nilpotent algebras

Theorem. (Coordinatization of nilpotent algebras, [EA 2019]).
Let $\mathbf{A} = (A, (f_i)_{i \in I})$ be in a congruence modular variety, $|A| = p^\alpha$, with all fundamental operations of arity at most μ. Let $K := (\mu(p^\alpha - 1))^{\alpha - 1}$. TFAE:

- $\mathbf{A}$ is nilpotent.
- There is a binary $+$ on A such that

$$\mathbf{A}' = (A, +, (f_i)_{i \in I})$$

  is nilpotent and $(A, +) \cong (\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p, +)$.
- There is a field $\mathbf{F} := (A, +, \cdot)$ such that
  Pol$(\mathbf{A}) \subseteq \{p^{\mathbf{F}} \mid n \in \mathbb{N}, p \in \mathbf{F}[x_1, \ldots, x_n], \mathrm{width}(p) \leq K\}$.

$\mathrm{width}(p) \ldots$ maximal number of variables in one monomial.

Equations over supernilpotent algebras

Theorem [EA 2019]

Let $\mathbf{A}$ be a finite supernilpotent algebra in a congruence modular variety, and let $s \in \mathbb{N}$. Then s-$\textsc{PolSysSat}(\mathbf{A})$ is in P.

For

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

we use $c_{\mathbf{A}} \cdot n^e$ evaluations of the system, where n is the number of variables.

Improvement with respect to previous results:

- systems of $s > 1$ equations.
- For $s = 1$: Ramsey $d_{\mathbf{A}}$ replaced with $s|A|^{\log_2(\mu)+\log_2(|A|)+1}$ for arbitrary supernilpotent algebras in cm varieties.

Next Goal

- Relate to “circuit satisfiability”.

Circuit satisfiability

Definition [Idziak Krzaczkowski 2018]

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

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

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

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].)