POLYNOMIAL MAPS ON SUPERNILPOTENT ALGEBRAS

Erhard Aichinger
Institute for Algebra
Austrian Science Fund FWF P29931

JOHANNES KEPLER
UNIVERSITY LINZ

Systems of polynomial equations

A system of polynomial equations

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

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?

Systems of polynomial equations

The general problem

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

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

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

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

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

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

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

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

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

Goals

- solve systems of equations over **nilpotent** algebras.
- discuss the meaning of **nilpotent** and **supernilpotent**.

Nilpotent and supernilpotent algebras

Nilpotency for groups and rings

- A group G is nilpotent if $\exists k \in \mathbb{N} : \underbrace{[G, [G, \ldots, [G, G] \ldots]]}_{k+1} = \{1_G\}$.
- 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

Nilpotent and supernilpotent universal algebras

Definition of nilpotency

Nilpotency is a property that can be seen from $(\mathsf{Con}(\mathbf{A}), \vee, \cap, [.,.])$, where $[.,.]$ is the term condition commutator.

$\mathbf{A}$ is nilpotent if $\exists k \in \mathbb{N} : \underbrace{[1_A, [1_A, \ldots, [1_A, 1_A] \ldots]]}_{k+1} = 0_A$.

Nilpotent and supernilpotent universal algebras

Definition of supernilpotency

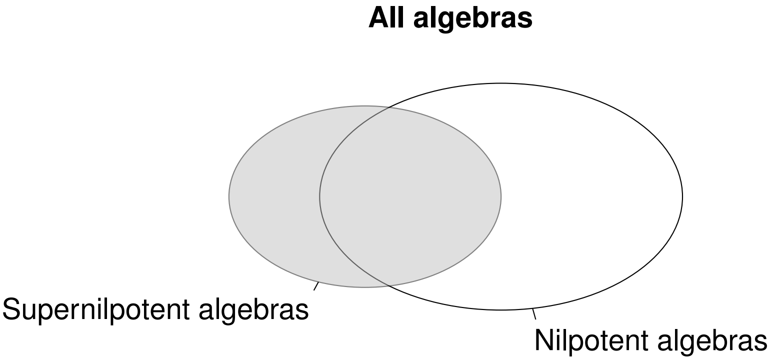
Supernilpotency is defined through a term condition:

$\mathbf{A}$ is 2-supernilpotent if for all terms t and for all vectors $\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3, \boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3$ from $\mathbf{A}$

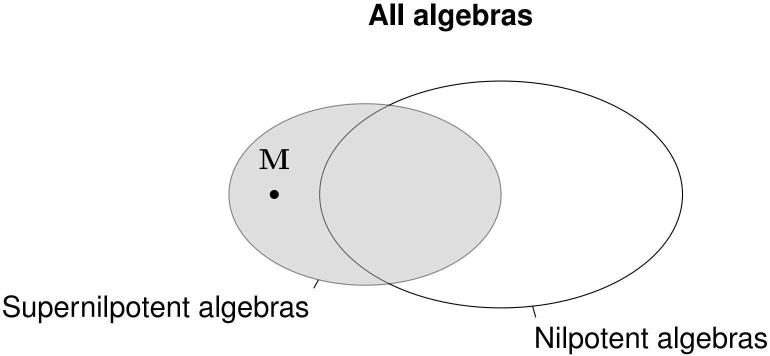
$$\left.\begin{array}{rcl} t^{\mathbf{A}}(\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3) & = & t^{\mathbf{A}}(\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{b}_3) \\ t^{\mathbf{A}}(\boldsymbol{a}_1, \boldsymbol{b}_2, \boldsymbol{a}_3) & = & t^{\mathbf{A}}(\boldsymbol{a}_1, \boldsymbol{b}_2, \boldsymbol{b}_3) \\ t^{\mathbf{A}}(\boldsymbol{b}_1, \boldsymbol{a}_2, \boldsymbol{a}_3) & = & t^{\mathbf{A}}(\boldsymbol{b}_1, \boldsymbol{a}_2, \boldsymbol{b}_3) \end{array}\right\} \Longrightarrow t^{\mathbf{A}}(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{a}_3) = t^{\mathbf{A}}(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3).$$

- k-supernilpotency is defined similarly through an infinite set of quasi-identities.
- Combinatorial description for finite algebras in cm varieties
  $\mathbf{A}$ is supernilpotent $\Longleftrightarrow \exists p \in \mathbb{R}[x]\ \forall n \in \mathbb{N}\ \ |\mathsf{Clo}_n(\mathbf{A})| \leq 2^{p(n)}$.

Nilpotency vs. supernilpotency

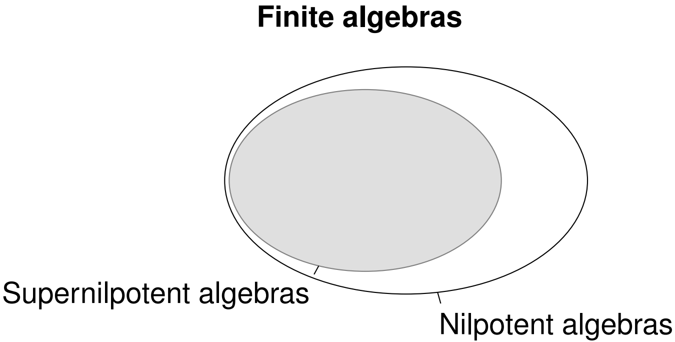


Nilpotency vs. supernilpotency



$\mathbf{M}$ ... [Moore Moorhead 2018]

Nilpotency vs. supernilpotency

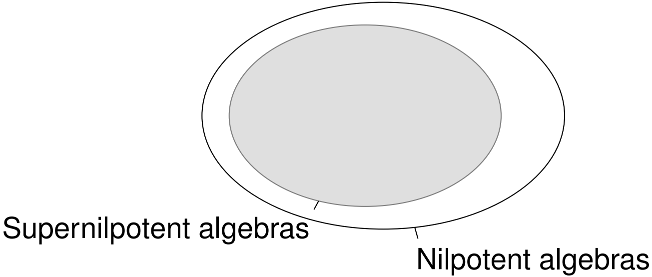


Theorem – announced by [Kearnes Szendrei 2018]

Every finite supernilpotent algebra is nilpotent.

Nilpotency vs. supernilpotency

Algebras in congruence modular varieties

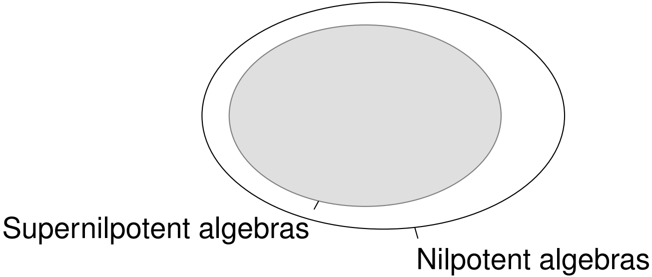


Theorem [Wires 2019]

Every supernilpotent algebra in a congruence modular variety is nilpotent.

Nilpotency vs. supernilpotency

Algebras in congruence permutable varieties

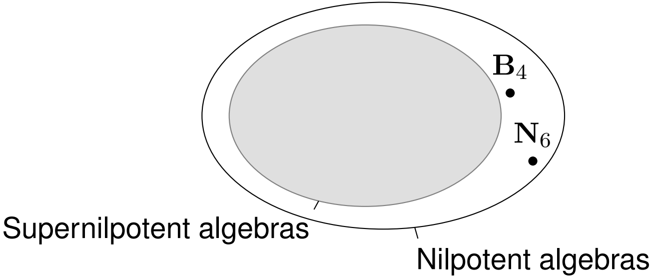


Theorem [EA Mudrinski 2010]

Every supernilpotent algebra in a congruence permutable variety is nilpotent.

Nilpotency vs. supernilpotency

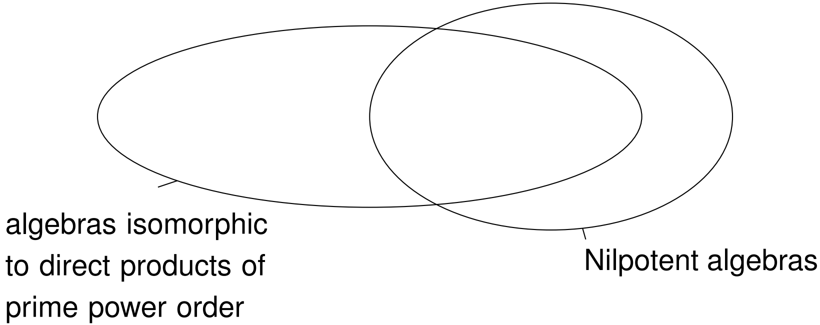
Algebras in congruence permutable varieties



$\mathbf{B}_4 = (\mathbb{Z}_4, +, 2x_1x_2, 2x_1x_2x_3, \ldots)$
$\mathbf{N}_6 = (\mathbb{Z}_6, +, (-1)^x)$.

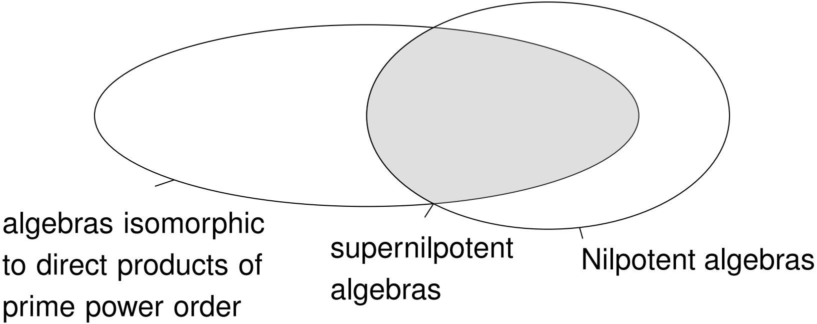
Nilpotency vs. supernilpotency

Algebras in cong. mod. varieties with fin. many basic operations



Nilpotency vs. supernilpotency

Algebras in cong. mod. varieties with fin. many basic operations

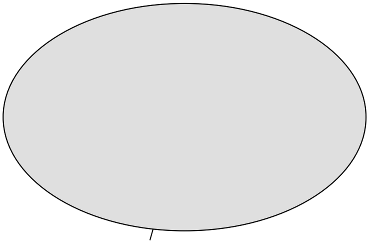


Theorem [Kearnes 1999], [Berman Blok 1987]

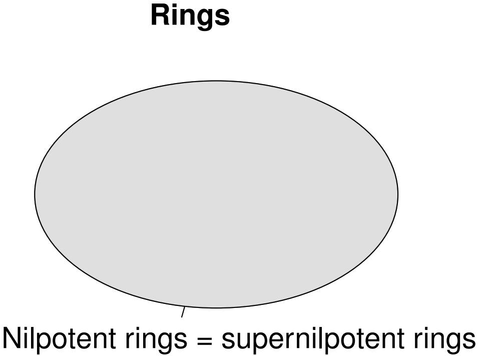
$\mathbf{A}$ in a cm variety, finitely many basic operations. Then $\mathbf{A}$ is supernilpotent $\iff$ $\mathbf{A}$ is nilpotent and isomorphic to a product of algebras of prime power order.

Nilpotency vs. supernilpotency

Groups



Nilpotency vs. supernilpotency



Next Goal

- How difficult is solving polynomial systems over supernilpotent algebras?

Systems of 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-PolSysSat$(\mathbf{A})$ is in P.

History

- $\mathbf{G}$ is a finite nilpotent group $\Rightarrow$ PolSat$(\mathbf{G}) \in \mathrm{P}$ [Horváth, 2011]
- $\mathbf{R}$ is a finite nilpotent ring $\Rightarrow$ PolSat$(\mathbf{R}) \in \mathrm{P}$ [Horváth, 2011]
- $\mathbf{A}$ is a finite supernilpotent algebra 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 [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 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.
- For nilpotent rings $\mathbf{A}$, a non-Ramsey $d_{\mathbf{A}}$ was found in [Károlyi and Szabó, 2015].
- Faster solutions of 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].

Next Goal

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

Nilpotent and supernilpotent algebras

Structure Theorem for nilpotent algebras of prime power order

[Berman Blok 1987], [Freese McKenzie 1987], [Hobby McKenzie 1988], [EA Mudrinski 2010], [EA 2018], [Wires 2019]

Let $\mathbf{A} = (A, (f_i)_{i \in I})$ be in a cm 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.

Nilpotent and supernilpotent algebras

Structure Theorem for nilpotent algebras of prime power order

[Berman Blok 1987], [Freese McKenzie 1987], [Hobby McKenzie 1988], [EA Mudrinski 2010], [EA 2018], [Wires 2019]

Let $\mathbf{A} = (A, (f_i)_{i \in I})$ be in a cm 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 $(A, +) \cong (\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p, +)$.

Nilpotent and supernilpotent algebras

Structure Theorem for nilpotent algebras of prime power order

[Berman Blok 1987], [Freese McKenzie 1987], [Hobby McKenzie 1988], [EA Mudrinski 2010], [EA 2018], [Wires 2019]

Let $\mathbf{A} = (A, (f_i)_{i\in I})$ be in a cm 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 $\mathrm{Pol}(\mathbf{A}) \subseteq \{p^{\mathbf{F}} \mid n \in \mathbb{N}, p \in \mathbf{F}[x_1, \ldots, x_n], \mathrm{wid}(p) \leq K\}$.

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

Nilpotent and supernilpotent algebras

Structure Theorem for nilpotent algebras of prime power order

[Berman Blok 1987], [Freese McKenzie 1987], [Hobby McKenzie 1988], [EA Mudrinski 2010], [EA 2018], [Wires 2019]

Let $\mathbf{A} = (A, (f_i)_{i \in I})$ be in a cm 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 $\mathrm{Pol}(\mathbf{A}) \subseteq \{p^{\mathbf{F}} \mid n \in \mathbb{N}, p \in \mathbf{F}[x_1, \ldots, x_n], \mathrm{wid}(p) \leq K\}$.
- $\mathbf{A}$ has small free spectrum: $\exists p \in \mathbb{R}[x] : \forall n \in \mathbb{N} : |\mathrm{Clo}_n(\mathbf{A})| \leq 2^{p(n)}$.

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

Nilpotent and supernilpotent algebras

Structure Theorem for nilpotent algebras of prime power order

[Berman Blok 1987], [Freese McKenzie 1987], [Hobby McKenzie 1988], [EA Mudrinski 2010], [EA 2018], [Wires 2019]

Let $\mathbf{A} = (A, (f_i)_{i\in I})$ be in a cm 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 $\mathrm{Pol}(\mathbf{A}) \subseteq \{p^{\mathbf{F}} \mid n \in \mathbb{N}, p \in \mathbf{F}[x_1, \ldots, x_n], \mathrm{wid}(p) \leq K\}$.
- $\mathbf{A}$ has small free spectrum: $\exists p \in \mathbb{R}[x] : \forall n \in \mathbb{N} : |\mathrm{Clo}_n(\mathbf{A})| \leq 2^{p(n)}$.
- $\mathbf{A}$ is supernilpotent.

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

Nilpotent and supernilpotent algebras

Structure Theorem for nilpotent algebras of prime power order

[Berman Blok 1987], [Freese McKenzie 1987], [Hobby McKenzie 1988], [EA Mudrinski 2010], [EA 2018], [Wires 2019]

Let $\mathbf{A} = (A, (f_i)_{i \in I})$ be in a cm 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 $\mathrm{Pol}(\mathbf{A}) \subseteq \{p^{\mathbf{F}} \mid n \in \mathbb{N}, p \in \mathbf{F}[x_1, \dots, x_n], \mathrm{wid}(p) \leq K\}$.
- $\mathbf{A}$ has small free spectrum: $\exists p \in \mathbb{R}[x] : \forall n \in \mathbb{N} : |\mathrm{Clo}_n(\mathbf{A})| \leq 2^{p(n)}$.
- $\mathbf{A}$ is supernilpotent.
- $\mathbf{A}$ is K-supernilpotent.

$\mathrm{wid}(p) \dots$ maximal number of variables in one monomial

Nilpotent and supernilpotent algebras

Structure Theorem for nilpotent algebras of prime power order

[Berman Blok 1987], [Freese McKenzie 1987], [Hobby McKenzie 1988], [EA Mudrinski 2010], [EA 2018], [Wires 2019]

Let $\mathbf{A} = (A, (f_i)_{i \in I})$ be in a cm 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 $\mathrm{Pol}(\mathbf{A}) \subseteq \{p^{\mathbf{F}} \mid n \in \mathbb{N}, p \in \mathbf{F}[x_1, \ldots, x_n], \mathrm{wid}(p) \leq K\}$.
- $\mathbf{A}$ has small free spectrum: $\exists p \in \mathbb{R}[x] : \forall n \in \mathbb{N} : |\mathrm{Clo}_n(\mathbf{A})| \leq 2^{p(n)}$.
- $\mathbf{A}$ is supernilpotent.
- $\mathbf{A}$ is K-supernilpotent.

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

Nilpotent and supernilpotent algebras

Structure Theorem for nilpotent algebras of prime power order

[Berman Blok 1987], [Freese McKenzie 1987], [Hobby McKenzie 1988], [EA Mudrinski 2010], [EA 2018], [Wires 2019]

Let $\mathbf{A} = (A, (f_i)_{i \in I})$ be in a cm 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 $\mathrm{Pol}(\mathbf{A}) \subseteq \{p^{\mathbf{F}} \mid n \in \mathbb{N}, p \in \mathbf{F}[x_1, \ldots, x_n], \mathrm{wid}(p) \leq K\}$.
- $\mathbf{A}$ has small free spectrum: $\exists p \in \mathbb{R}[x] : \forall n \in \mathbb{N} : |\mathrm{Clo}_n(\mathbf{A})| \leq 2^{p(n)}$.
- $\mathbf{A}$ is supernilpotent.
- $\mathbf{A}$ is K-supernilpotent.

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

Next Goal

- solve polynomial systems over supernilpotent algebras of prime power order.

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 2018], [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.

Proof:

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

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 $\leq K$.

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 $\leq K$.
- $\prod_{i=1}^{s}(1 - f_i(\boldsymbol{a})^{q-1}) \neq 0$.

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 $Q(\boldsymbol{a}) \neq 0$.

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 $Q(\boldsymbol{a}) \neq 0$.
- $\mathrm{rem}(Q(\boldsymbol{x}), \langle x_1^q - x, \ldots, x_n^q - x\rangle)$ has width $\leq Ks(q-1)$.

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 $Q(\boldsymbol{a}) \neq 0$.
- $\mathrm{rem}(Q(\boldsymbol{x}), \langle x_1^q - x, \ldots, x_n^q - x\rangle)$ has width $\leq Ks(q-1)$.
- "Hence" there is U with $|U| \leq Ks(q-1)$ and $Q(\boldsymbol{a}^{(U)}) \neq 0$.

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 $Q(\boldsymbol{a}) \neq 0$.
- $\mathrm{rem}(Q(\boldsymbol{x}), \langle x_1^q - x, \ldots, x_n^q - x\rangle)$ 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.

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 $Q(\boldsymbol{a}) \neq 0$.
- $\mathrm{rem}(Q(\boldsymbol{x}), \langle x_1^q - x, \ldots, x_n^q - x\rangle)$ 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.

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 $Q(\boldsymbol{a}) \neq 0$.
- $\mathrm{rem}(Q(\boldsymbol{x}), \langle x_1^q - x, \ldots, x_n^q - x\rangle)$ 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

$Ks\alpha(p-1) \leq Ks(q-1) = Ks(p^{\alpha} - 1)$.

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

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

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

Let $\boldsymbol{a} \in A^n$ 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.

Next Goal

- Drop “prime power order” restriction.

Supernilpotent algebras

Theorem [Kearnes 1999]

Every finite supernilpotent algebra in a cm variety is a direct product of supernilpotent algebras of prime power order.

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 $F \in \mathrm{Pol}_{n,s}(\mathbf{A})$ 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-$\textsc{PolSysSat}(\mathbf{A})$ using at most $c_{\mathbf{A}} \cdot n^e$ evaluations of the system, where n is the number of variables.

Next Goal

- Relate to “circuit satisfiability”.

Circuit satisfiability

Definition [Idziak Krzaczkowski 2018]

Problem $\mathrm{SC}\textsc{sat}(\mathbf{A})$.

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-$\mathrm{SC}\textsc{sat}(\mathbf{A})$: $2s$ 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].)