The equivalence problem for nilpotent algebras

in congruence modular varieties

Michael Kompatscher
Charles University Prague

23.05.2019
BLAST2019 - University of Colorado Boulder

The equivalence problem

The equivalence problem for finite algebras

$\mathbf{A} = (A, f_1, \ldots, f_n)$... finite algebra

The equivalence problem for finite algebras

$\mathbf{A} = (A, f_1, \dots, f_n)$... finite algebra

Circuit equivalence problem CEQV($\mathbf{A}$)

INPUT: $p(x_1, \dots, x_n), q(x_1, \dots, x_n)$ polynomials, encoded by *circuits*

QUESTION: Does $\mathbf{A} \models p(x_1, \dots, x_n) \approx q(x_1, \dots, x_n)$?

The equivalence problem for finite algebras

$\mathbf{A} = (A, f_1, \ldots, f_n)$... finite algebra

Circuit equivalence problem CEQV($\mathbf{A}$)

INPUT: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ polynomials, encoded by *circuits*

QUESTION: Does $\mathbf{A} \models p(x_1, \ldots, x_n) \approx q(x_1, \ldots, x_n)$?

$\mathrm{CEQV}(\mathbf{A}) \in \mathrm{coNP}$

The equivalence problem for finite algebras

$\mathbf{A} = (A, f_1, \dots, f_n)$... finite algebra

Circuit equivalence problem CEQV($\mathbf{A}$)

INPUT: $p(x_1, \dots, x_n), q(x_1, \dots, x_n)$ polynomials, encoded by *circuits*

QUESTION: Does $\mathbf{A} \models p(x_1, \dots, x_n) \approx q(x_1, \dots, x_n)$?

CEQV($\mathbf{A}$) $\in$ coNP

Main question

What are criteria for tractability (P) or hardness (coNP-c)?

The equivalence problem for finite algebras

$\mathbf{A} = (A, f_1, \ldots, f_n)$... finite algebra

Circuit equivalence problem CEQV($\mathbf{A}$)

INPUT: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ polynomials, encoded by *circuits*
QUESTION: Does $\mathbf{A} \models p(x_1, \ldots, x_n) \approx q(x_1, \ldots, x_n)$?

CEQV($\mathbf{A}$) $\in$ coNP

Main question

What are criteria for tractability (P) or hardness (coNP-c)?

Why circuits?

The equivalence problem for finite algebras

$\mathbf{A} = (A, f_1, \ldots, f_n)$... finite algebra

Circuit equivalence problem CEQV($\mathbf{A}$)

INPUT: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ polynomials, encoded by *circuits*
QUESTION: Does $\mathbf{A} \models p(x_1, \ldots, x_n) \approx q(x_1, \ldots, x_n)$?

CEQV($\mathbf{A}$) $\in$ coNP

Main question

What are criteria for tractability (P) or hardness (coNP-c)?

Why circuits?

Pol($\mathbf{A}$)... clone of polynomials of $\mathbf{A}$

- Pol($\mathbf{A}$) $\subseteq$ Pol($\mathbf{A}'$) $\Rightarrow$ CEQV($\mathbf{A}$) $\leq$ CEQV($\mathbf{A}'$)

The equivalence problem for finite algebras

$\mathbf{A} = (A, f_1, \ldots, f_n)$... finite algebra

Circuit equivalence problem CEQV($\mathbf{A}$)

INPUT: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ polynomials, encoded by *circuits*
QUESTION: Does $\mathbf{A} \models p(x_1, \ldots, x_n) \approx q(x_1, \ldots, x_n)$?

CEQV($\mathbf{A}$) $\in$ coNP

Main question

What are criteria for tractability (P) or hardness (coNP-c)?

Why circuits?

Pol($\mathbf{A}$)... clone of polynomials of $\mathbf{A}$

- $\mathrm{Pol}(\mathbf{A}) \subseteq \mathrm{Pol}(\mathbf{A}') \Rightarrow \mathrm{CEQV}(\mathbf{A}) \leq \mathrm{CEQV}(\mathbf{A}')$
- If input encoded by strings ('PolEQV') $\rightarrow$ language sensitive.

The equivalence problem for finite algebras

$\mathbf{A} = (A, f_1, \dots, f_n)$... finite algebra

Circuit equivalence problem CEQV($\mathbf{A}$)

INPUT: $p(x_1, \dots, x_n), q(x_1, \dots, x_n)$ polynomials, encoded by *circuits*
QUESTION: Does $\mathbf{A} \models p(x_1, \dots, x_n) \approx q(x_1, \dots, x_n)$?

CEQV($\mathbf{A}$) $\in$ coNP

Main question

What are criteria for tractability (P) or hardness (coNP-c)?

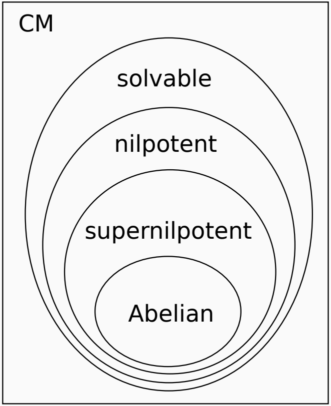
Why circuits?

Pol($\mathbf{A}$)... clone of polynomials of $\mathbf{A}$

- Pol($\mathbf{A}$) $\subseteq$ Pol($\mathbf{A}'$) $\Rightarrow$ CEQV($\mathbf{A}$) $\leq$ CEQV($\mathbf{A}'$)
- If input encoded by strings ('PolEQV') $\rightarrow$ language sensitive.
- (encoding not relevant in nilpotent case)

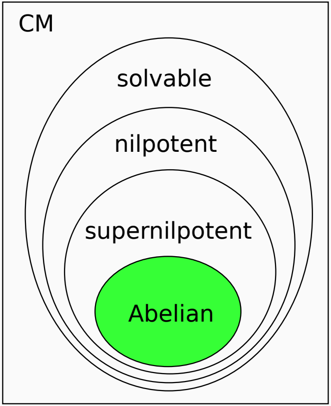
In congruence modular varieties

A... from congruence modular variety



In congruence modular varieties

A... from congruence modular variety

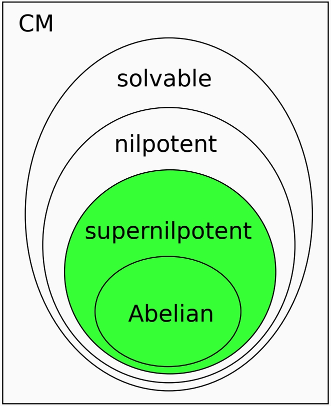


- **A** Abelian $\leftrightarrow$ module. CEQV(**A**) $\in$ P

  compute normal form $p(\bar{x}) \approx \alpha_0 + \sum_{i=1}^{n} \alpha_i x_i$

In congruence modular varieties

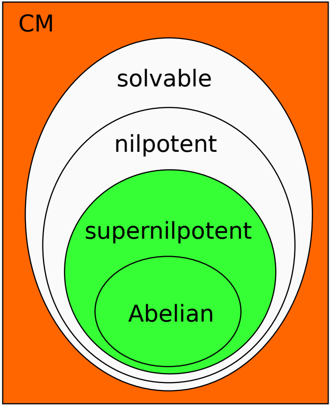
A... from congruence modular variety



- **A** Abelian $\leftrightarrow$ module. CEQV(**A**) $\in$ P
  compute normal form $p(\bar{x}) \approx \alpha_0 + \sum_{i=1}^{n} \alpha_i x_i$
- **A** k-supernilpotent. CEQV(**A**) $\in$ P:
  $p(x_1 \ldots, x_n) \approx 0$ iff $p(a_1 \ldots, a_n) = 0$, for all $\bar{a}$ with at most k-many $a_i \neq 0$
  (Aichinger, Mudrinski '10)

In congruence modular varieties

A... from congruence modular variety



- **A** Abelian $\leftrightarrow$ module. CEQV(**A**) $\in$ P

  compute normal form $p(\bar{x}) \approx \alpha_0 + \sum_{i=1}^{n} \alpha_i x_i$

- **A** k-supernilpotent. CEQV(**A**) $\in$ P:
  $p(x_1 \ldots, x_n) \approx 0$ iff $p(a_1 \ldots, a_n) = 0$, for all $\bar{a}$ with at most k-many $a_i \neq 0$

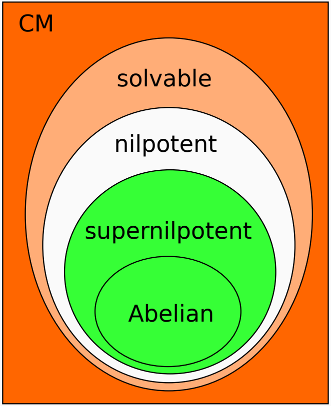
  (Aichinger, Mudrinski '10)

- **A** non-solvable: CEQV(**A**) $\in$ coNP-c

  (Idziak, Krzaczkowski '18)

In congruence modular varieties

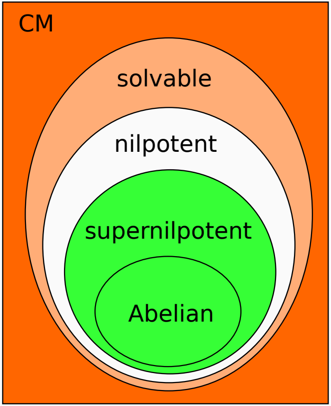
A... from congruence modular variety



- **A** Abelian $\leftrightarrow$ module. CEQV(**A**) $\in$ P
  compute normal form $p(\bar{x}) \approx \alpha_0 + \sum_{i=1}^{n} \alpha_i x_i$
- **A** k-supernilpotent. CEQV(**A**) $\in$ P:
  $p(x_1 \ldots, x_n) \approx 0$ iff $p(a_1 \ldots, a_n) = 0$, for all $\bar{a}$ with at most k-many $a_i \neq 0$
  (Aichinger, Mudrinski '10)
- **A** solvable, non-nilpotent:
  $\exists \theta$: CEQV(**A**/θ) $\in$ coNP-c
  (Idziak, Krzaczkowski '18)
- **A** non-solvable: CEQV(**A**) $\in$ coNP-c
  (Idziak, Krzaczkowski '18)

In congruence modular varieties

A... from congruence modular variety



- **A** Abelian $\leftrightarrow$ module. CEQV(**A**) $\in$ P

  compute normal form $p(\bar{x}) \approx \alpha_0 + \sum_{i=1}^{n} \alpha_i x_i$
- **A** k-supernilpotent. CEQV(**A**) $\in$ P:
  $p(x_1 \ldots, x_n) \approx 0$ iff $p(a_1 \ldots, a_n) = 0$, for all $\bar{a}$ with at most k-many $a_i \neq 0$

  (Aichinger, Mudrinski '10)
- **A nilpotent, not supernilpotent...?**
- **A** solvable, non-nilpotent:
  $\exists \theta$: CEQV(**A**$/\theta$) $\in$ coNP-c

  (Idziak, Krzaczkowski '18)
- **A** non-solvable: CEQV(**A**) $\in$ coNP-c

  (Idziak, Krzaczkowski '18)

Nilpotent algebras

The structure of nilpotent algebras

A... n-nilpotent from CM variety.

The structure of nilpotent algebras

A... n-nilpotent from CM variety.

Theorem (Freese, McKenzie)

The structure of nilpotent algebras

A... n-nilpotent from CM variety.

Theorem (Freese, McKenzie)

Then $\exists$ **L** Abelian, **U** is $(n-1)$-nilpotent, $A = L \times U$ and

$$f^{\mathbf{A}}((l_1, u_1), \ldots, (l_n, u_n)) = (f^{\mathbf{L}}(l_1, \ldots, l_n) + \hat{f}(u_1, \ldots, u_n), f^{\mathbf{U}}(u_1, \ldots, u_n)),$$

for all operations.

The structure of nilpotent algebras

A... n-nilpotent from CM variety.

Theorem (Freese, McKenzie)

Then $\exists$ **L** Abelian, **U** is $(n-1)$-nilpotent, $A = L \times U$ and

$$f^{\mathbf{A}}((l_1, u_1), \dots, (l_n, u_n)) = (f^{\mathbf{L}}(l_1, \dots, l_n) + \hat{f}(u_1, \dots, u_n), f^{\mathbf{U}}(u_1, \dots, u_n)),$$

for all operations. We write $\mathbf{A} = \mathbf{L} \otimes^T \mathbf{U}$.

The structure of nilpotent algebras

A... n-nilpotent from CM variety.

Theorem (Freese, McKenzie)

Then $\exists$ **L** Abelian, **U** is $(n-1)$-nilpotent, $A = L \times U$ and

$$f^{\mathbf{A}}((l_1, u_1), \ldots, (l_n, u_n)) = (f^{\mathbf{L}}(l_1, \ldots, l_n) + \hat{f}(u_1, \ldots, u_n), f^{\mathbf{U}}(u_1, \ldots, u_n)),$$

for all operations. We write $\mathbf{A} = \mathbf{L} \otimes^T \mathbf{U}$.

Corollary

Checking $\mathbf{A} \models p^{\mathbf{A}}(x_1, \ldots, x_n) \approx 0$ is equivalent to checking

The structure of nilpotent algebras

A... n-nilpotent from CM variety.

Theorem (Freese, McKenzie)

Then $\exists$ **L** Abelian, **U** is $(n-1)$-nilpotent, $A = L \times U$ and

$$f^{\mathbf{A}}((l_1, u_1), \ldots, (l_n, u_n)) = (f^{\mathbf{L}}(l_1, \ldots, l_n) + \hat{f}(u_1, \ldots, u_n), f^{\mathbf{U}}(u_1, \ldots, u_n)),$$

for all operations. We write $\mathbf{A} = \mathbf{L} \otimes^T \mathbf{U}$.

Corollary

Checking $\mathbf{A} \models p^{\mathbf{A}}(x_1, \ldots, x_n) \approx 0$ is equivalent to checking
$p^{\mathbf{U}}(u_1, \ldots, u_n) \approx 0$ in **U**
$p^{\mathbf{L}}(l_1, \ldots, l_n) \approx c$ in **L**
$\hat{p}(u_1, \ldots, u_n) \approx -c$ in **L**

The structure of nilpotent algebras

A... n-nilpotent from CM variety.

Theorem (Freese, McKenzie)

Then $\exists$ **L** Abelian, **U** is $(n-1)$-nilpotent, $A = L \times U$ and

$$f^{\mathbf{A}}((l_1, u_1), \dots, (l_n, u_n)) = (f^{\mathbf{L}}(l_1, \dots, l_n) + \hat{f}(u_1, \dots, u_n), f^{\mathbf{U}}(u_1, \dots, u_n)),$$

for all operations. We write $\mathbf{A} = \mathbf{L} \otimes^T \mathbf{U}$.

Corollary

Checking $\mathbf{A} \models p^{\mathbf{A}}(x_1, \dots, x_n) \approx 0$ is equivalent to checking
$p^{\mathbf{U}}(u_1, \dots, u_n) \approx 0$ in **U** ✓ ($n-1$-nilpotent)
$p^{\mathbf{L}}(l_1, \dots, l_n) \approx c$ in **L** ✓
$\hat{p}(u_1, \dots, u_n) \approx -c$ in **L**

The structure of nilpotent algebras

A... n-nilpotent from CM variety.

Theorem (Freese, McKenzie)

Then $\exists$ **L** Abelian, **U** is $(n-1)$-nilpotent, $A = L \times U$ and

$$f^{\mathbf{A}}((l_1, u_1), \ldots, (l_n, u_n)) = (f^{\mathbf{L}}(l_1, \ldots, l_n) + \hat{f}(u_1, \ldots, u_n), f^{\mathbf{U}}(u_1, \ldots, u_n)),$$

for all operations. We write $\mathbf{A} = \mathbf{L} \otimes^T \mathbf{U}$.

Corollary

Checking $\mathbf{A} \models p^{\mathbf{A}}(x_1, \ldots, x_n) \approx 0$ is equivalent to checking
$p^{\mathbf{U}}(u_1, \ldots, u_n) \approx 0$ in **U** ✓ ($n-1$-nilpotent)
$p^{\mathbf{L}}(l_1, \ldots, l_n) \approx c$ in **L** ✓
$\hat{p}(u_1, \ldots, u_n) \approx -c$ in **L**

we need to analyze the expressions $\hat{p}$!

The structure of nilpotent algebras

A... n-nilpotent from CM variety.

Theorem (Freese, McKenzie)

Then $\exists$ **L** Abelian, **U** is $(n-1)$-nilpotent, $A = L \times U$ and

$$f^{\mathbf{A}}((l_1, u_1), \dots, (l_n, u_n)) = (f^{\mathbf{L}}(l_1, \dots, l_n) + \hat{f}(u_1, \dots, u_n), f^{\mathbf{U}}(u_1, \dots, u_n)),$$

for all operations. We write $\mathbf{A} = \mathbf{L} \otimes^T \mathbf{U}$.

Corollary

Checking $\mathbf{A} \models p^{\mathbf{A}}(x_1, \dots, x_n) \approx 0$ is equivalent to checking
$p^{\mathbf{U}}(u_1, \dots, u_n) \approx 0$ in **U** ✓ ($n-1$-nilpotent)
$p^{\mathbf{L}}(l_1, \dots, l_n) \approx c$ in **L** ✓
$\hat{p}(u_1, \dots, u_n) \approx -c$ in **L**

we need to analyze the expressions $\hat{p}$!
Operations $\hat{p}\colon U^n \to L$ form an (**L**)-clonoid.

Example 1 ($|L|$ and $|U|$ coprime)

$$\mathbf{L} \otimes^T \mathbf{U} = (\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f) \text{ with } p \neq q,\ \hat{f}(u) = \begin{cases} 1 \text{ if } u = 0 \\ 0 \text{ else} \end{cases}$$

Example 1 ($|L|$ and $|U|$ coprime)

$$\mathbf{L} \otimes^T \mathbf{U} = (\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f) \text{ with } p \neq q,\ \hat{f}(u) = \begin{cases} 1 \text{ if } u = 0 \\ 0 \text{ else} \end{cases}$$

2-nilpotent, polynomials of form

Example 1 ($|L|$ and $|U|$ coprime)

$$\mathbf{L} \otimes^T \mathbf{U} = (\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f) \text{ with } p \neq q,\ \hat{f}(u) = \begin{cases} 1 \text{ if } u = 0 \\ 0 \text{ else} \end{cases}$$

2-nilpotent, polynomials of form
$p((l_1, u_1), \ldots, (l_n, u_n)) = (\alpha_0 + \sum_i \alpha_i l_i + \hat{p}(u_1, \ldots, u_n), \beta_0 + \sum_i \beta_i u_i)$,

Example 1 ($|L|$ and $|U|$ coprime)

$$\mathbf{L} \otimes^T \mathbf{U} = (\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f) \text{ with } p \neq q,\ \hat{f}(u) = \begin{cases} 1 \text{ if } u = 0 \\ 0 \text{ else} \end{cases}$$

2-nilpotent, polynomials of form
$p((l_1, u_1), \ldots, (l_n, u_n)) = (\alpha_0 + \sum_i \alpha_i l_i + \hat{p}(u_1, \ldots, u_n), \beta_0 + \sum_i \beta_i u_i)$,
$\hat{p}$ affine combination of $\hat{f}(\delta_0 + \sum \delta_i u_i)$

Example 1 ($|L|$ and $|U|$ coprime)

$$\mathbf{L} \otimes^T \mathbf{U} = (\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f) \text{ with } p \neq q,\ \hat{f}(u) = \begin{cases} 1 \text{ if } u = 0 \\ 0 \text{ else} \end{cases}$$

2-nilpotent, polynomials of form
$p((l_1, u_1), \dots, (l_n, u_n)) = (\alpha_0 + \sum_i \alpha_i l_i + \hat{p}(u_1, \dots, u_n), \beta_0 + \sum_i \beta_i u_i)$,
$\hat{p}$ affine combination of $\hat{f}(\delta_0 + \sum \delta_i u_i)$

Simplify $\hat{p}$ by:

- $\hat{f}(u) \approx \hat{f}(2u) \approx \cdots \approx \hat{f}((q-1)u)$
- $1 \approx \sum_{i=0}^{p-1} \hat{f}(u - i)$
- axioms for **L** and **U** (e.g. $p \cdot \hat{f}(u) \approx 0$, $\hat{f}(u + q \cdot u') \approx \hat{f}(u)$)

Example 1 ($|L|$ and $|U|$ coprime)

$$\mathbf{L} \otimes^T \mathbf{U} = (\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f) \text{ with } p \neq q,\ \hat{f}(u) = \begin{cases} 1 \text{ if } u = 0 \\ 0 \text{ else} \end{cases}$$

2-nilpotent, polynomials of form
$p((l_1, u_1), \ldots, (l_n, u_n)) = (\alpha_0 + \sum_i \alpha_i l_i + \hat{p}(u_1, \ldots, u_n), \beta_0 + \sum_i \beta_i u_i)$,
$\hat{p}$ affine combination of $\hat{f}(\delta_0 + \sum \delta_i u_i)$

Simplify $\hat{p}$ by:

- $\hat{f}(u) \approx \hat{f}(2u) \approx \cdots \approx \hat{f}((q-1)u)$
- $1 \approx \sum_{i=0}^{p-1} \hat{f}(u - i)$
- axioms for $\mathbf{L}$ and $\mathbf{U}$ (e.g. $p \cdot \hat{f}(u) \approx 0$, $\hat{f}(u + q \cdot u') \approx \hat{f}(u)$)

$\rightarrow$ compute in **polynomial time** the representation:

$$\hat{p}(u_1, \ldots, u_n) \approx \gamma_0 + \sum \gamma_{\bar{\delta}} \cdot \hat{f}(1 + \sum \delta_i \cdot u_i)$$

Example 1 ($|L|$ and $|U|$ coprime)

$$\mathbf{L} \otimes^T \mathbf{U} = (\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f) \text{ with } p \neq q,\ \hat{f}(u) = \begin{cases} 1 \text{ if } u = 0 \\ 0 \text{ else} \end{cases}$$

2-nilpotent, polynomials of form
$p((l_1, u_1), \dots, (l_n, u_n)) = (\alpha_0 + \sum_i \alpha_i l_i + \hat{p}(u_1, \dots, u_n), \beta_0 + \sum_i \beta_i u_i)$,
$\hat{p}$ affine combination of $\hat{f}(\delta_0 + \sum \delta_i u_i)$

Simplify $\hat{p}$ by:

- $\hat{f}(u) \approx \hat{f}(2u) \approx \cdots \approx \hat{f}((q-1)u)$
- $1 \approx \sum_{i=0}^{p-1} \hat{f}(u - i)$
- axioms for **L** and **U** (e.g. $p \cdot \hat{f}(u) \approx 0$, $\hat{f}(u + q \cdot u') \approx \hat{f}(u)$)

$\rightarrow$ compute in **polynomial time** the representation:

$$\hat{p}(u_1, \dots, u_n) \approx \gamma_0 + \sum \gamma_{\bar{\delta}} \cdot \hat{f}(1 + \sum \delta_i \cdot u_i)$$

This is representation is **unique:**
$\{\hat{f}(1 + \sum_{i=1}^n \delta_i \cdot u_i)\} \cup \{1\}$ is a basis of the vector space $\mathbf{L}^{U^n}$ for every n.

Example 1 ($|L|$ and $|U|$ coprime)

Thus $\mathrm{CEQV}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f)) \in \mathrm{P}$:
To check $p(x_1, \dots, x_n) \approx 0$ compute normal form of p, and check if $= 0$.

Example 1 ($|L|$ and $|U|$ coprime)

Thus $\mathrm{CEQV}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f)) \in \mathrm{P}$:
To check $p(x_1, \ldots, x_n) \approx 0$ compute normal form of p, and check if $= 0$.

Observation 1

Example 1 ($|L|$ and $|U|$ coprime)

Thus $\mathrm{CEQV}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f)) \in \mathrm{P}$:
To check $p(x_1, \ldots, x_n) \approx 0$ compute normal form of p, and check if $= 0$.

Observation 1

- *all* operations $U^n \to L$ are generated by $\hat{f}$.

Example 1 ($|L|$ and $|U|$ coprime)

Thus $\mathrm{CEQV}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f)) \in \mathrm{P}$:
To check $p(x_1, \dots, x_n) \approx 0$ compute normal form of p, and check if $= 0$.

Observation 1

- *all* operations $U^n \to L$ are generated by $\hat{f}$.

$\Rightarrow$ For every 2-nilpotent $\mathbf{A}$ with $\mathbf{L} = \mathbb{Z}_p$, $\mathbf{U} = \mathbb{Z}_q$:
$\mathrm{Pol}(\mathbf{A}) \leq \mathrm{Pol}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f))$

Example 1 ($|L|$ and $|U|$ coprime)

Thus $\mathrm{CEQV}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f)) \in \mathrm{P}$:
To check $p(x_1, \ldots, x_n) \approx 0$ compute normal form of p, and check if $= 0$.

Observation 1

- *all* operations $U^n \to L$ are generated by $\hat{f}$.

$\Rightarrow$ For every 2-nilpotent $\mathbf{A}$ with $\mathbf{L} = \mathbb{Z}_p$, $\mathbf{U} = \mathbb{Z}_q$:
$\mathrm{Pol}(\mathbf{A}) \leq \mathrm{Pol}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f))$

$\Rightarrow$ $\mathrm{CEQV}(\mathbf{A}) \in \mathrm{P}$.

Example 1 ($|L|$ and $|U|$ coprime)

Thus $\mathrm{CEQV}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f)) \in \mathrm{P}$:
To check $p(x_1, \dots, x_n) \approx 0$ compute normal form of p, and check if $= 0$.

Observation 1

- *all* operations $U^n \to L$ are generated by $\hat{f}$.

$\Rightarrow$ For every 2-nilpotent $\mathbf{A}$ with $\mathbf{L} = \mathbb{Z}_p$, $\mathbf{U} = \mathbb{Z}_q$:
$\mathrm{Pol}(\mathbf{A}) \leq \mathrm{Pol}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f))$

$\Rightarrow$ $\mathrm{CEQV}(\mathbf{A}) \in \mathrm{P}$.

Observation 2

Example 1 ($|L|$ and $|U|$ coprime)

Thus $\mathrm{CEQV}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f)) \in \mathrm{P}$:
To check $p(x_1, \ldots, x_n) \approx 0$ compute normal form of p, and check if $= 0$.

Observation 1

- *all* operations $U^n \to L$ are generated by $\hat{f}$.

$\Rightarrow$ For every 2-nilpotent $\mathbf{A}$ with $\mathbf{L} = \mathbb{Z}_p$, $\mathbf{U} = \mathbb{Z}_q$:
$\mathrm{Pol}(\mathbf{A}) \leq \mathrm{Pol}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f))$

$\Rightarrow$ $\mathrm{CEQV}(\mathbf{A}) \in \mathrm{P}$.

Observation 2

- Only finitely many identities used to compute normal form.

Example 1 ($|L|$ and $|U|$ coprime)

Thus $\mathrm{CEQV}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f)) \in \mathrm{P}$:
To check $p(x_1, \ldots, x_n) \approx 0$ compute normal form of p, and check if $= 0$.

Observation 1

- *all* operations $U^n \to L$ are generated by $\hat{f}$.

$\Rightarrow$ For every 2-nilpotent $\mathbf{A}$ with $\mathbf{L} = \mathbb{Z}_p$, $\mathbf{U} = \mathbb{Z}_q$:
$\mathrm{Pol}(\mathbf{A}) \leq \mathrm{Pol}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f))$

$\Rightarrow$ $\mathrm{CEQV}(\mathbf{A}) \in \mathrm{P}$.

Observation 2

- Only finitely many identities used to compute normal form.

$\Rightarrow$ $(\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f)$ is finitely based.

Example 2 ($|L|$ and $|U|$ not coprime)

Let $\mathbf{L} \otimes^T \mathbf{U} = (\mathbb{Z}_p \times \mathbb{Z}_p, +, (0,0), -, f)$, f binary

$$\hat{f}(u_1, u_2) = \begin{cases} 1 \text{ if } u_1 = u_2 = 0 \\ 0 \text{ else} \end{cases}$$

Example 2 ($|L|$ and $|U|$ not coprime)

Let $\mathbf{L} \otimes^T \mathbf{U} = (\mathbb{Z}_p \times \mathbb{Z}_p, +, (0,0), -, f)$, f binary

$$\hat{f}(u_1, u_2) = \begin{cases} 1 \text{ if } u_1 = u_2 = 0 \\ 0 \text{ else} \end{cases}$$

- Is 2-supernilpotent

Example 2 ($|L|$ and $|U|$ not coprime)

Let $\mathbf{L} \otimes^T \mathbf{U} = (\mathbb{Z}_p \times \mathbb{Z}_p, +, (0,0), -, f)$, f binary

$$\hat{f}(u_1, u_2) = \begin{cases} 1 \text{ if } u_1 = u_2 = 0 \\ 0 \text{ else} \end{cases}$$

- Is 2-supernilpotent
- Function $\hat{p}$ do not generate all $\mathbf{L}^{U^n} = \mathbb{Z}_p^{\mathbb{Z}_p^n}$
  (no nontrivial 0-absorbing operations of arity > 2)

Example 2 ($|L|$ and $|U|$ not coprime)

Let $\mathbf{L} \otimes^T \mathbf{U} = (\mathbb{Z}_p \times \mathbb{Z}_p, +, (0,0), -, f)$, f binary

$$\hat{f}(u_1, u_2) = \begin{cases} 1 \text{ if } u_1 = u_2 = 0 \\ 0 \text{ else} \end{cases}$$

- Is 2-supernilpotent
- Function $\hat{p}$ do not generate all $\mathbf{L}^{U^n} = \mathbb{Z}_p^{\mathbb{Z}_p^n}$ (no nontrivial 0-absorbing operations of arity > 2)
- But, for $n \geq 2$: $\{(u_1, \ldots, u_n) \mapsto \hat{f}(u_i - a_i, u_j - a_j) | i < j, a_i, a_j \in U\}$ is a basis generating all $\hat{p}(x_1, \ldots, x_n)$

Example 2 ($|L|$ and $|U|$ not coprime)

Let $\mathbf{L} \otimes^T \mathbf{U} = (\mathbb{Z}_p \times \mathbb{Z}_p, +, (0,0), -, f)$, f binary

$$\hat{f}(u_1, u_2) = \begin{cases} 1 \text{ if } u_1 = u_2 = 0 \\ 0 \text{ else} \end{cases}$$

- Is 2-supernilpotent
- Function $\hat{p}$ do not generate all $\mathbf{L}^{U^n} = \mathbb{Z}_p^{\mathbb{Z}_p^n}$
  (no nontrivial 0-absorbing operations of arity > 2)
- But, for $n \geq 2$: $\{(u_1, \ldots, u_n) \mapsto \hat{f}(u_i - a_i, u_j - a_j) | i < j, a_i, a_j \in U\}$
  is a basis generating all $\hat{p}(x_1, \ldots, x_n)$
- Normal form $\hat{p}(u_1, \ldots, u_n) \approx \sum \gamma \cdot \hat{f}(u_i - a_i, u_j - a_j)$
  can be computed in polynomial time

Example 2 ($|L|$ and $|U|$ not coprime)

Let $\mathbf{L} \otimes^T \mathbf{U} = (\mathbb{Z}_p \times \mathbb{Z}_p, +, (0,0), -, f)$, f binary

$$\hat{f}(u_1, u_2) = \begin{cases} 1 \text{ if } u_1 = u_2 = 0 \\ 0 \text{ else} \end{cases}$$

- Is 2-supernilpotent
- Function $\hat{p}$ do not generate all $\mathbf{L}^{U^n} = \mathbb{Z}_p^{\mathbb{Z}_p^n}$ (no nontrivial 0-absorbing operations of arity > 2)
- But, for $n \geq 2$: $\{(u_1, \ldots, u_n) \mapsto \hat{f}(u_i - a_i, u_j - a_j) | i < j, a_i, a_j \in U\}$ is a basis generating all $\hat{p}(x_1, \ldots, x_n)$
- Normal form $\hat{p}(u_1, \ldots, u_n) \approx \sum \gamma \cdot \hat{f}(u_i - a_i, u_j - a_j)$ can be computed in polynomial time

$\Rightarrow$ CEQV($\mathbf{L} \otimes^T \mathbf{U}$) $\in$ P

Example 2 ($|L|$ and $|U|$ not coprime)

Let $\mathbf{L} \otimes^T \mathbf{U} = (\mathbb{Z}_p \times \mathbb{Z}_p, +, (0,0), -, f)$, f binary

$$\hat{f}(u_1, u_2) = \begin{cases} 1 \text{ if } u_1 = u_2 = 0 \\ 0 \text{ else} \end{cases}$$

- Is 2-supernilpotent
- Function $\hat{p}$ do not generate all $\mathbf{L}^{U^n} = \mathbb{Z}_p^{\mathbb{Z}_p^n}$
  (no nontrivial 0-absorbing operations of arity > 2)
- But, for $n \geq 2$: $\{(u_1, \ldots, u_n) \mapsto \hat{f}(u_i - a_i, u_j - a_j) | i < j, a_i, a_j \in U\}$
  is a basis generating all $\hat{p}(x_1, \ldots, x_n)$
- Normal form $\hat{p}(u_1, \ldots, u_n) \approx \sum \gamma \cdot \hat{f}(u_i - a_i, u_j - a_j)$
  can be computed in polynomial time

$\Rightarrow$ CEQV($\mathbf{L} \otimes^T \mathbf{U}$) $\in$ P

Remark: All 2-supernilpotent algebras with $\mathbf{L} = \mathbf{U} = \mathbb{Z}_p$ reduce to this one.

CEQV **for 2-nilpotent algebras**

2-nilpotent algebras

Theorem (Kawałek, MK, Krzaczkowski ’19)

Let $\mathbf{A} = \mathbf{L} \otimes^{T} \mathbf{U}$ 2-nilpotent. Then $\mathrm{CEQV}(\mathbf{A}) \in \mathrm{P}$

2-nilpotent algebras

Theorem (Kawałek, MK, Krzaczkowski ’19)

Let $\mathbf{A} = \mathbf{L} \otimes^{T} \mathbf{U}$ 2-nilpotent. Then $\mathrm{CEQV}(\mathbf{A}) \in \mathrm{P}$

Proof steps

2-nilpotent algebras

Theorem (Kawałek, MK, Krzaczkowski '19)
Let $\mathbf{A} = \mathbf{L} \otimes^T \mathbf{U}$ 2-nilpotent. Then $\mathrm{CEQV}(\mathbf{A}) \in \mathrm{P}$

Proof steps

1. Example 1 generalizes to $\mathbf{L} = (\mathbb{Z}_q)^k$ and $\mathbf{U} = (\mathbb{Z}_p)^l$.

2-nilpotent algebras

Theorem (Kawałek, MK, Krzaczkowski '19)

Let $\mathbf{A} = \mathbf{L} \otimes^T \mathbf{U}$ 2-nilpotent. Then $\mathrm{CEQV}(\mathbf{A}) \in \mathrm{P}$

Proof steps

1. Example 1 generalizes to $\mathbf{L} = (\mathbb{Z}_q)^k$ and $\mathbf{U} = (\mathbb{Z}_p)^l$.
2. If $\mathbf{L} = (\mathbb{Z}_{q_1})^{i_1} \times \cdots \times (\mathbb{Z}_{q_n})^{i_n} \rightarrow$ decompose $\hat{p} = \pi_1 \hat{p} + \ldots + \pi_n \hat{p}$.

2-nilpotent algebras

Theorem (Kawałek, MK, Krzaczkowski '19)

Let $\mathbf{A} = \mathbf{L} \otimes^T \mathbf{U}$ 2-nilpotent. Then $\mathrm{CEQV}(\mathbf{A}) \in \mathrm{P}$

Proof steps

1. Example 1 generalizes to $\mathbf{L} = (\mathbb{Z}_q)^k$ and $\mathbf{U} = (\mathbb{Z}_p)^l$.
2. If $\mathbf{L} = (\mathbb{Z}_{q_1})^{i_1} \times \cdots \times (\mathbb{Z}_{q_n})^{i_n} \to$ decompose $\hat{p} = \pi_1 \hat{p} + \ldots + \pi_n \hat{p}$.
3. $\mathbf{U} = (\mathbb{Z}_{p_1})^{i_1} \times \cdots \times (\mathbb{Z}_{p_n})^{i_n}$, $\mathbf{L} = (\mathbb{Z}_q)^l \to$ modify generating function:
$$\hat{f}(u_1, \ldots, u_n) = \begin{cases} 1 \text{ if } \pi_j(u_j) = 0 \text{ for } j = 1, \ldots, n \\ 0 \text{ else} \end{cases}$$

2-nilpotent algebras

Theorem (Kawałek, MK, Krzaczkowski '19)
Let $\mathbf{A} = \mathbf{L} \otimes^T \mathbf{U}$ 2-nilpotent. Then $\mathrm{CEQV}(\mathbf{A}) \in \mathrm{P}$

Proof steps

1. Example 1 generalizes to $\mathbf{L} = (\mathbb{Z}_q)^k$ and $\mathbf{U} = (\mathbb{Z}_p)^l$.
2. If $\mathbf{L} = (\mathbb{Z}_{q_1})^{i_1} \times \cdots \times (\mathbb{Z}_{q_n})^{i_n} \to$ decompose $\hat{p} = \pi_1 \hat{p} + \ldots + \pi_n \hat{p}$.
3. $\mathbf{U} = (\mathbb{Z}_{p_1})^{i_1} \times \cdots \times (\mathbb{Z}_{p_n})^{i_n}$, $\mathbf{L} = (\mathbb{Z}_q)^l \to$ modify generating function:
   $$\hat{f}(u_1, \ldots, u_n) = \begin{cases} 1 \text{ if } \pi_j(u_j) = 0 \text{ for } j = 1, \ldots, n \\ 0 \text{ else} \end{cases}$$
4. $\mathbf{U} = (\mathbb{Z}_{p_1})^{i_1} \times \cdots \times (\mathbb{Z}_{p_n})^{i_n} \times (\mathbb{Z}_q)^k$, $\mathbf{L} = (\mathbb{Z}_q)^l$
   mix coprime and supernilpotent approach

2-nilpotent algebras

Theorem (Kawałek, MK, Krzaczkowski '19)
Let $\mathbf{A} = \mathbf{L} \otimes^T \mathbf{U}$ 2-nilpotent. Then $\mathrm{CEQV}(\mathbf{A}) \in \mathrm{P}$

Proof steps

1. Example 1 generalizes to $\mathbf{L} = (\mathbb{Z}_q)^k$ and $\mathbf{U} = (\mathbb{Z}_p)^l$.
2. If $\mathbf{L} = (\mathbb{Z}_{q_1})^{i_1} \times \cdots \times (\mathbb{Z}_{q_n})^{i_n} \to$ decompose $\hat{p} = \pi_1 \hat{p} + \ldots + \pi_n \hat{p}$.
3. $\mathbf{U} = (\mathbb{Z}_{p_1})^{i_1} \times \cdots \times (\mathbb{Z}_{p_n})^{i_n}$, $\mathbf{L} = (\mathbb{Z}_q)^l \to$ modify generating function:
   $$\hat{f}(u_1, \ldots, u_n) = \begin{cases} 1 \text{ if } \pi_j(u_j) = 0 \text{ for } j = 1, \ldots, n \\ 0 \text{ else} \end{cases}$$
4. $\mathbf{U} = (\mathbb{Z}_{p_1})^{i_1} \times \cdots \times (\mathbb{Z}_{p_n})^{i_n} \times (\mathbb{Z}_q)^k$, $\mathbf{L} = (\mathbb{Z}_q)^l$
   mix coprime and supernilpotent approach
5. **Major problem:** Non vector-spaces, e.g. $\mathbf{U} \cong \mathbb{Z}_9$ $\mathbf{L} \cong \mathbb{Z}_4$. How to find normal form of $\mathbf{L}^{U^n}$? $\to$ **different approach**

A different approach

Example: $\mathbf{U} = \mathbb{Z}_9$ $\mathbf{L} = \mathbb{Z}_4$.
Let $\hat{f}(u) = 1$ if $u = 0$ and $\hat{f}(u) = 0$ else.

- Check $\hat{f}(u+1) + \hat{f}(u+v) + \hat{f}(u+4v) \approx const$

A different approach

Example: $\mathbf{U} = \mathbb{Z}_9$ $\mathbf{L} = \mathbb{Z}_4$.
Let $\hat{f}(u) = 1$ if $u = 0$ and $\hat{f}(u) = 0$ else.

- Check $\hat{f}(u+1) + \hat{f}(u+v) + \hat{f}(u+4v) \approx \mathit{const}$
- Idea: reduce to subterms by 'systematic summing':

A different approach

Example: $\mathbf{U} = \mathbb{Z}_9$ $\mathbf{L} = \mathbb{Z}_4$.
Let $\hat{f}(u) = 1$ if $u = 0$ and $\hat{f}(u) = 0$ else.

- Check $\hat{f}(u+1) + \hat{f}(u+v) + \hat{f}(u+4v) \approx const$
- Idea: reduce to subterms by 'systematic summing':
- $\sum_{a=1}^{9}(\hat{f}(u+1) + \hat{f}(u+a) + \hat{f}(u+4a)) \approx 9\hat{f}(u+1) + 1 + 1 \approx const$

A different approach

Example: $\mathbf{U} = \mathbb{Z}_9$ $\mathbf{L} = \mathbb{Z}_4$.
Let $\hat{f}(u) = 1$ if $u = 0$ and $\hat{f}(u) = 0$ else.

- Check $\hat{f}(u+1) + \hat{f}(u+v) + \hat{f}(u+4v) \approx const$
- Idea: reduce to subterms by 'systematic summing':
- $\sum_{a=1}^{9}(\hat{f}(u+1) + \hat{f}(u+a) + \hat{f}(u+4a)) \approx 9\hat{f}(u+1) + 1 + 1 \approx const$

$\Rightarrow$ $\hat{f}(u+1) \approx const \Rightarrow \hat{f}(u+v) + \hat{f}(u+4v) \approx const$

A different approach

Example: $\mathbf{U} = \mathbb{Z}_9$ $\mathbf{L} = \mathbb{Z}_4$.
Let $\hat{f}(u) = 1$ if $u = 0$ and $\hat{f}(u) = 0$ else.

- Check $\hat{f}(u+1) + \hat{f}(u+v) + \hat{f}(u+4v) \approx \mathit{const}$
- Idea: reduce to subterms by 'systematic summing':
- $\sum_{a=1}^{9}(\hat{f}(u+1) + \hat{f}(u+a) + \hat{f}(u+4a)) \approx 9\hat{f}(u+1) + 1 + 1 \approx \mathit{const}$

$\Rightarrow$ $\hat{f}(u+1) \approx \mathit{const} \Rightarrow \hat{f}(u+v) + \hat{f}(u+4v) \approx \mathit{const}$

- $\hat{f}(u+v) + \hat{f}(u+4v) \approx \mathit{const}$ does not decompose, but reduce to $\mathbb{Z}_3$

A different approach

Example: $\mathbf{U} = \mathbb{Z}_9$ $\mathbf{L} = \mathbb{Z}_4$.
Let $\hat{f}(u) = 1$ if $u = 0$ and $\hat{f}(u) = 0$ else.

- Check $\hat{f}(u+1) + \hat{f}(u+v) + \hat{f}(u+4v) \approx \mathit{const}$
- Idea: reduce to subterms by 'systematic summing':
- $\sum_{a=1}^{9}(\hat{f}(u+1) + \hat{f}(u+a) + \hat{f}(u+4a)) \approx 9\hat{f}(u+1) + 1 + 1 \approx \mathit{const}$

$\Rightarrow$ $\hat{f}(u+1) \approx \mathit{const} \Rightarrow \hat{f}(u+v) + \hat{f}(u+4v) \approx \mathit{const}$

- $\hat{f}(u+v) + \hat{f}(u+4v) \approx \mathit{const}$ does not decompose, but reduce to $\mathbb{Z}_3$
- $\hat{f}(u+v) + \hat{f}((u+v)+3v) \approx 0 \Leftrightarrow \hat{f}(3w) + \hat{f}(3w+3v) \approx 0$

A different approach

Example: $\mathbf{U} = \mathbb{Z}_9$ $\mathbf{L} = \mathbb{Z}_4$.
Let $\hat{f}(u) = 1$ if $u = 0$ and $\hat{f}(u) = 0$ else.

- Check $\hat{f}(u+1) + \hat{f}(u+v) + \hat{f}(u+4v) \approx const$
- Idea: reduce to subterms by 'systematic summing':
- $\sum_{a=1}^{9}(\hat{f}(u+1) + \hat{f}(u+a) + \hat{f}(u+4a)) \approx 9\hat{f}(u+1) + 1 + 1 \approx const$

$\Rightarrow$ $\hat{f}(u+1) \approx const \Rightarrow \hat{f}(u+v) + \hat{f}(u+4v) \approx const$

- $\hat{f}(u+v) + \hat{f}(u+4v) \approx const$ does not decompose, but reduce to $\mathbb{Z}_3$
- $\hat{f}(u+v) + \hat{f}((u+v) + 3v) \approx 0 \Leftrightarrow \hat{f}(3w) + \hat{f}(3w + 3v) \approx 0$

Downsides

A different approach

Example: $\mathbf{U} = \mathbb{Z}_9$ $\mathbf{L} = \mathbb{Z}_4$.
Let $\hat{f}(u) = 1$ if $u = 0$ and $\hat{f}(u) = 0$ else.

- Check $\hat{f}(u+1) + \hat{f}(u+v) + \hat{f}(u+4v) \approx const$
- Idea: reduce to subterms by 'systematic summing':
- $\sum_{a=1}^{9}(\hat{f}(u+1) + \hat{f}(u+a) + \hat{f}(u+4a)) \approx 9\hat{f}(u+1) + 1 + 1 \approx const$

$\Rightarrow$ $\hat{f}(u+1) \approx const \Rightarrow \hat{f}(u+v) + \hat{f}(u+4v) \approx const$

- $\hat{f}(u+v) + \hat{f}(u+4v) \approx const$ does not decompose, but reduce to $\mathbb{Z}_3$
- $\hat{f}(u+v) + \hat{f}((u+v)+3v) \approx 0 \Leftrightarrow \hat{f}(3w) + \hat{f}(3w+3v) \approx 0$

Downsides

- For arbitrary abelian **U**,**L** very technical

A different approach

Example: $\mathbf{U} = \mathbb{Z}_9$ $\mathbf{L} = \mathbb{Z}_4$.
Let $\hat{f}(u) = 1$ if $u = 0$ and $\hat{f}(u) = 0$ else.

- Check $\hat{f}(u+1) + \hat{f}(u+v) + \hat{f}(u+4v) \approx const$
- Idea: reduce to subterms by 'systematic summing':
- $\sum_{a=1}^{9}(\hat{f}(u+1) + \hat{f}(u+a) + \hat{f}(u+4a)) \approx 9\hat{f}(u+1) + 1 + 1 \approx const$

$\Rightarrow$ $\hat{f}(u+1) \approx const \Rightarrow \hat{f}(u+v) + \hat{f}(u+4v) \approx const$

- $\hat{f}(u+v) + \hat{f}(u+4v) \approx const$ does not decompose, but reduce to $\mathbb{Z}_3$
- $\hat{f}(u+v) + \hat{f}((u+v)+3v) \approx 0 \Leftrightarrow \hat{f}(3w) + \hat{f}(3w+3v) \approx 0$

Downsides

- For arbitrary abelian **U**,**L** very technical
- How to generalize to $n-1$-nilpotent **U**?

A very helpful extension

Aichinger coordinatisation

Proposition (Aichinger '18)

Let **A** be nilpotent, $|A| = p_1^{i_1} \cdot p_2^{i_2} \cdots p_m^{i_m}$. Then there are operations $+, 0, -$ such that

Aichinger coordinatisation

Proposition (Aichinger '18)

Let **A** be nilpotent, $|A| = p_1^{i_1} \cdot p_2^{i_2} \cdots p_m^{i_m}$. Then there are operations $+$,0,$-$ such that

- $(A, +, 0, -) \cong \mathbb{Z}_{p_1}^{i_1} \times \cdots \times \mathbb{Z}_{p_m}^{i_m}$

Aichinger coordinatisation

Proposition (Aichinger '18)

Let **A** be nilpotent, $|A| = p_1^{i_1} \cdot p_2^{i_2} \cdots p_m^{i_m}$. Then there are operations $+$,0,$-$ such that

- $(A, +, 0, -) \cong \mathbb{Z}_{p_1}^{i_1} \times \cdots \times \mathbb{Z}_{p_m}^{i_m}$
- $(\mathbf{A}, +, 0, -)$ is still nilpotent.

Aichinger coordinatisation

Proposition (Aichinger '18)

Let $\mathbf{A}$ be nilpotent, $|A| = p_1^{i_1} \cdot p_2^{i_2} \cdots p_m^{i_m}$. Then there are operations $+$,0,$-$ such that

- $(A, +, 0, -) \cong \mathbb{Z}_{p_1}^{i_1} \times \cdots \times \mathbb{Z}_{p_m}^{i_m}$
- $(\mathbf{A}, +, 0, -)$ is still nilpotent.

$\mathrm{CEQV}(\mathbf{A}) \leq \mathrm{CEQV}((\mathbf{A}, +, 0, -))$
$\rightarrow$ work only in Aichinger's extended groups

Aichinger coordinatisation

Proposition (Aichinger '18)

Let $\mathbf{A}$ be nilpotent, $|A| = p_1^{i_1} \cdot p_2^{i_2} \cdots p_m^{i_m}$. Then there are operations $+,0,-$ such that

- $(A, +, 0, -) \cong \mathbb{Z}_{p_1}^{i_1} \times \cdots \times \mathbb{Z}_{p_m}^{i_m}$
- $(\mathbf{A}, +, 0, -)$ is still nilpotent.

$\mathrm{CEQV}(\mathbf{A}) \leq \mathrm{CEQV}((\mathbf{A}, +, 0, -))$
$\rightarrow$ work only in Aichinger's extended groups

Remark

The degree of nilpotence might increase (but $\leq \log_2(|A|)$).
E.g. $(\mathbb{Z}_4, +)$ Abelian, but $(\mathbb{Z}_4, +, +_V)$ is 2-nilpotent.

Summary

A... *n*-nilpotent, extension of a group $\mathbb{Z}_{p_1}^{i_1} \times \cdots \times \mathbb{Z}_{p_m}^{i_m}$

Summary

A... n-nilpotent, extension of a group $\mathbb{Z}_{p_1}^{i_1} \times \cdots \times \mathbb{Z}_{p_m}^{i_m}$

- $\mathbf{A} = \mathbf{L} \otimes^T \mathbf{U}$

Summary

$\mathbf{A}$... n-nilpotent, extension of a group $\mathbb{Z}_{p_1}^{i_1} \times \cdots \times \mathbb{Z}_{p_m}^{i_m}$

- $\mathbf{A} = \mathbf{L} \otimes^T \mathbf{U}$
- $p^{\mathbf{A}}(x_1, \ldots, x_n) \approx 0$ holds iff $\begin{cases} p^{\mathbf{U}}(u_1, \ldots, u_n) \approx 0 \\ p^{\mathbf{L}}(l_1, \ldots, l_n) \approx c \\ \hat{p}(u_1, \ldots, u_n) \approx -c \end{cases}$

Summary

A... n-nilpotent, extension of a group $\mathbb{Z}_{p_1}^{i_1} \times \cdots \times \mathbb{Z}_{p_m}^{i_m}$

- $\mathbf{A} = \mathbf{L} \otimes^T \mathbf{U}$
- $p^{\mathbf{A}}(x_1, \ldots, x_n) \approx 0$ holds iff $\begin{cases} p^{\mathbf{U}}(u_1, \ldots, u_n) \approx 0 \\ p^{\mathbf{L}}(l_1, \ldots, l_n) \approx c \\ \hat{p}(u_1, \ldots, u_n) \approx -c \end{cases}$
- Extend **A** by f's, such that $\hat{f}$ generates feasible subspace of $\mathbf{L}^{U^n}$

Summary

A... n-nilpotent, extension of a group $\mathbb{Z}_{p_1}^{i_1} \times \cdots \times \mathbb{Z}_{p_m}^{i_m}$

- $\mathbf{A} = \mathbf{L} \otimes^T \mathbf{U}$
- $p^{\mathbf{A}}(x_1, \ldots, x_n) \approx 0$ holds iff $\begin{cases} p^{\mathbf{U}}(u_1, \ldots, u_n) \approx 0 \\ p^{\mathbf{L}}(l_1, \ldots, l_n) \approx c \\ \hat{p}(u_1, \ldots, u_n) \approx -c \end{cases}$
- Extend **A** by f's, such that $\hat{f}$ generates feasible subspace of $\mathbf{L}^{U^n}$
- compute normal form of $\hat{p}(u_1, \ldots, u_n)$ using $\hat{f}$

Summary

A... n-nilpotent, extension of a group $\mathbb{Z}_{p_1}^{i_1} \times \cdots \times \mathbb{Z}_{p_m}^{i_m}$

- $\mathbf{A} = \mathbf{L} \otimes^T \mathbf{U}$
- $p^{\mathbf{A}}(x_1, \ldots, x_n) \approx 0$ holds iff $\begin{cases} p^{\mathbf{U}}(u_1, \ldots, u_n) \approx 0 \\ p^{\mathbf{L}}(l_1, \ldots, l_n) \approx c \\ \hat{p}(u_1, \ldots, u_n) \approx -c \end{cases}$
- Extend **A** by f's, such that $\hat{f}$ generates feasible subspace of $\mathbf{L}^{U^n}$
- compute normal form of $\hat{p}(u_1, \ldots, u_n)$ using $\hat{f}$

$\Rightarrow$ CEQV(**A**) $\leq$ CEQV(**U**) in polynomial time

Summary

A... n-nilpotent, extension of a group $\mathbb{Z}_{p_1}^{i_1} \times \cdots \times \mathbb{Z}_{p_m}^{i_m}$

- $\mathbf{A} = \mathbf{L} \otimes^T \mathbf{U}$
- $p^{\mathbf{A}}(x_1, \ldots, x_n) \approx 0$ holds iff $\begin{cases} p^{\mathbf{U}}(u_1, \ldots, u_n) \approx 0 \\ p^{\mathbf{L}}(l_1, \ldots, l_n) \approx c \\ \hat{p}(u_1, \ldots, u_n) \approx -c \end{cases}$
- Extend **A** by f's, such that $\hat{f}$ generates feasible subspace of $\mathbf{L}^{U^n}$
- compute normal form of $\hat{p}(u_1, \ldots, u_n)$ using $\hat{f}$

$\Rightarrow$ CEQV(**A**) $\leq$ CEQV(**U**) in polynomial time

By induction on n:

Theorem (MK)

Let **A** be n-nilpotent. Then CEQV(**A**) $\in$ P.

Open questions

A... finite nilpotent, from a CM variety

Open questions

A... finite nilpotent, from a CM variety

Question

By our proof **A** has a finitely based nilpotent extension.

Is **A** *itself* finitely based?

Open questions

A... finite nilpotent, from a CM variety

Question

By our proof **A** has a finitely based nilpotent extension.
Is **A** *itself* finitely based?

Question

Is the equation/circuit solvability problem of **A** in P?

The end

Thank you!