The equivalence problem for nilpotent algebras

in congruence modular varieties

Michael Kompatscher
Charles University Prague

22/06/2019
AAA98 - Dresden

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

$\mathbf{A} = (A, f_1, \ldots, f_n)$... 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 $\mathbf{A} \models p(x_1, \ldots, x_n) \approx q(x_1, \ldots, x_n)$?

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

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

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

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

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

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

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

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

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

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)?

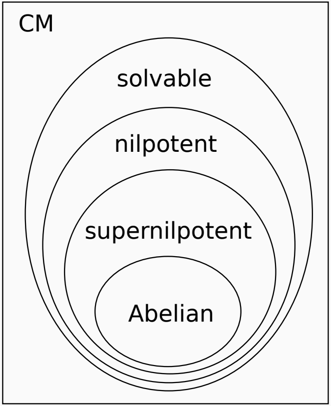
Why circuits?

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.
- (will set aside in this talk)

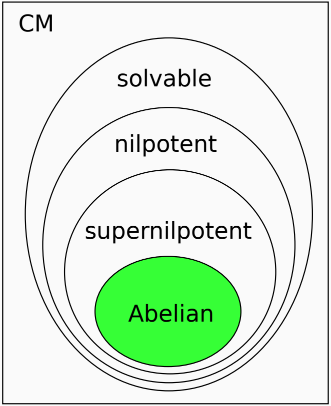
In congruence modular varieties

A... from congruence modular variety



In congruence modular varieties

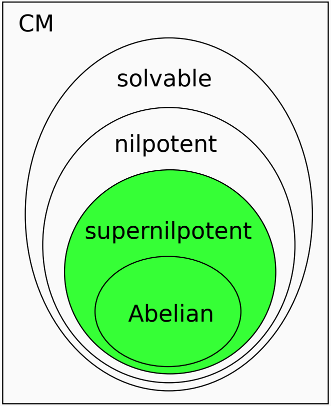
A... from congruence modular variety



- **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

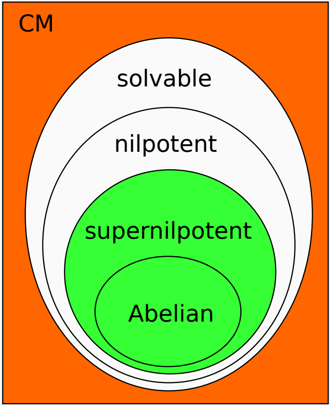
A... from congruence modular variety



- **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:
  $p(x_1 \dots, x_n) \approx 0$ iff $p(a_1 \dots, a_n) = 0$, 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 $a_i \neq 0$

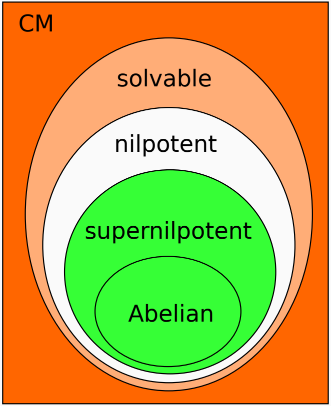
  (Aichinger, Mudrinski '10)

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

  (Idziak, Krzaczkowski '18)

In congruence modular varieties

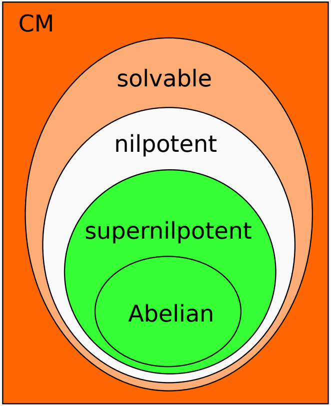
A... from congruence modular variety



- **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($\mathbf{A}/\theta$) $\in$ 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($\mathbf{A}/\theta$) $\in$ 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

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

for all operations.

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

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** $\sim$ ✓ ($n-1$-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** $\sim \checkmark$ ($n-1$-nilpotent)
$p^{\mathbf{L}}(l_1, \ldots, l_n) \approx c$ in **L** $\checkmark$
$\hat{p}(u_1, \ldots, u_n) \approx -c$ 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

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

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** $\sim \checkmark$ ($n-1$-nilpotent)
$p^{\mathbf{L}}(l_1, \ldots, l_n) \approx c$ in **L** $\checkmark$
$\hat{p}(u_1, \ldots, u_n) \approx -c$ in **L**

- we need to analyze the expressions $\hat{p}$!
- Operations $\hat{p}\colon U^n \to L$ form a $(\mathbf{U}, \mathbf{L})$-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
$p((l_1, u_1), \dots, (l_n, u_n)) = (\alpha_0 + \sum_i \alpha_i l_i + \hat{p}(u_1, \dots, u_n), \beta_0 + \sum_i \beta_i u_i)$,

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

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

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

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

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 $\mathrm{CEQV}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f)) \in \mathrm{P}$

(compute normal form of p, and check if $= 0$)

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

Thus $\text{CEQV}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f)) \in \text{P}$

(compute normal form of p, and check if $= 0$)

Observation 1

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

Thus $\mathrm{CEQV}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f)) \in \mathrm{P}$

(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 $\mathrm{CEQV}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f)) \in \mathrm{P}$
(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 $\mathrm{CEQV}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f)) \in \mathrm{P}$

(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 $\mathrm{CEQV}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f)) \in \mathrm{P}$
(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 $\mathbf{L} = \mathbb{Z}_p$, $\mathbf{U} = \mathbb{Z}_q$:
$\mathrm{Pol}(\mathbf{A}) \leq \mathrm{Pol}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f))$

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

- **Question:** Can we find such canonical extension for every $\mathbf{L}$, $\mathbf{U}$?

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

Thus $\mathrm{CEQV}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f)) \in \mathrm{P}$

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

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

- **Question:** Can we find such canonical extension for every $\mathbf{L}$, $\mathbf{U}$?

Observation 2

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

Thus $\mathrm{CEQV}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f)) \in \mathrm{P}$
(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 $\mathbf{L} = \mathbb{Z}_p$, $\mathbf{U} = \mathbb{Z}_q$:
$\mathrm{Pol}(\mathbf{A}) \leq \mathrm{Pol}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f))$

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

- **Question:** Can we find such canonical extension for every $\mathbf{L}$, $\mathbf{U}$?

Observation 2

- Only finitely many identities used to compute normal form.

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

Thus $\mathrm{CEQV}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f)) \in \mathrm{P}$
(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 $\mathbf{L} = \mathbb{Z}_p$, $\mathbf{U} = \mathbb{Z}_q$:
$\mathrm{Pol}(\mathbf{A}) \leq \mathrm{Pol}((\mathbb{Z}_p \times \mathbb{Z}_q, +, (0,0), -, f))$

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

- **Question:** Can we find such canonical extension for every $\mathbf{L}$, $\mathbf{U}$?

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 $|U|$ of same characteristic)

Let $\mathbf{L} \otimes^T \mathbf{U} = (\mathbb{Z}_p \times \mathbb{Z}_p, +, (0,0), -, f)$,
$i : U \to L$ isomorphism
$\hat{f}(u_1, u_2, \ldots, u_{p-1}) = i(u_1 \cdot u_2 \cdots u_{p-1})$.

Example 2 ($|L|$ and $|U|$ of same characteristic)

Let $\mathbf{L} \otimes^T \mathbf{U} = (\mathbb{Z}_p \times \mathbb{Z}_p, +, (0,0), -, f)$,
$i : U \to L$ isomorphism
$\hat{f}(u_1, u_2, \ldots, u_{p-1}) = i(u_1 \cdot u_2 \cdots u_{p-1})$.

- $\hat{f}$ generates all unary maps $U \to L$ $\quad$ (by $u \mapsto \hat{f}(u-1, \ldots, u-(p-1))$)

Example 2 ($|L|$ and $|U|$ of same characteristic)

Let $\mathbf{L} \otimes^T \mathbf{U} = (\mathbb{Z}_p \times \mathbb{Z}_p, +, (0,0), -, f)$,
$i : U \to L$ isomorphism
$\hat{f}(u_1, u_2, \ldots, u_{p-1}) = i(u_1 \cdot u_2 \cdots u_{p-1})$.

- $\hat{f}$ generates all unary maps $U \to L$ (by $u \mapsto \hat{f}(u-1, \ldots, u-(p-1))$)
- For $n \in \mathbb{N}$, the 'monomials' of degree $\leq p-1$
  $B_n = \{\hat{f}(1, \ldots, 1, u_{i_1}, \ldots, u_{i_k})\}$ form a basis for all $\hat{p}(u_1, \ldots, u_n)$

Example 2 ($|L|$ and $|U|$ of same characteristic)

Let $\mathbf{L} \otimes^T \mathbf{U} = (\mathbb{Z}_p \times \mathbb{Z}_p, +, (0,0), -, f)$,
$i : U \to L$ isomorphism
$\hat{f}(u_1, u_2, \ldots, u_{p-1}) = i(u_1 \cdot u_2 \cdots u_{p-1})$.

- $\hat{f}$ generates all unary maps $U \to L$ (by $u \mapsto \hat{f}(u-1, \ldots, u-(p-1))$)
- For $n \in \mathbb{N}$, the 'monomials' of degree $\leq p-1$ $B_n = \{\hat{f}(1, \ldots, 1, u_{i_1}, \ldots, u_{i_k})\}$ form a basis for all $\hat{p}(u_1, \ldots, u_n)$
- Normal form of $\hat{p}$ in B_n can be computed in polynomial time (distributivity of $\hat{f}$ over $+$)

Example 2 ($|L|$ and $|U|$ of same characteristic)

Let $\mathbf{L} \otimes^T \mathbf{U} = (\mathbb{Z}_p \times \mathbb{Z}_p, +, (0,0), -, f)$,
$i : U \to L$ isomorphism
$\hat{f}(u_1, u_2, \ldots, u_{p-1}) = i(u_1 \cdot u_2 \cdots u_{p-1})$.

- $\hat{f}$ generates all unary maps $U \to L$ (by $u \mapsto \hat{f}(u-1, \ldots, u-(p-1))$)
- For $n \in \mathbb{N}$, the 'monomials' of degree $\leq p-1$
  $B_n = \{\hat{f}(1, \ldots, 1, u_{i_1}, \ldots, u_{i_k})\}$ form a basis for all $\hat{p}(u_1, \ldots, u_n)$
- Normal form of $\hat{p}$ in B_n can be computed in polynomial time
  (distributivity of $\hat{f}$ over $+$)

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

Example 2 ($|L|$ and $|U|$ of same characteristic)

Let $\mathbf{L} \otimes^T \mathbf{U} = (\mathbb{Z}_p \times \mathbb{Z}_p, +, (0,0), -, f)$,
$i : U \to L$ isomorphism
$\hat{f}(u_1, u_2, \ldots, u_{p-1}) = i(u_1 \cdot u_2 \cdots u_{p-1})$.

- $\hat{f}$ generates all unary maps $U \to L$ (by $u \mapsto \hat{f}(u-1, \ldots, u-(p-1))$)
- For $n \in \mathbb{N}$, the 'monomials' of degree $\leq p-1$
  $B_n = \{\hat{f}(1, \ldots, 1, u_{i_1}, \ldots, u_{i_k})\}$ form a basis for all $\hat{p}(u_1, \ldots, u_n)$
- Normal form of $\hat{p}$ in B_n can be computed in polynomial time
  (distributivity of $\hat{f}$ over $+$)

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

Observe: All **A** with $\mathbf{L} = \mathbf{U} = \mathbb{Z}_p$ and **unary** operations reduce to this one. Analogous for *n*-**ary** operations.

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 idea

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 idea

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

2-nilpotent algebras

Theorem (Kawałek, MK, Krzaczkowski ’19)

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

Proof idea

1. Examples 1 generalizes to $\mathbf{U} = \mathbb{Z}_p^k$ and $\mathbf{L} = \mathbb{Z}_q^l$
2. Deal with products $\mathbf{U} = \mathbb{Z}_{p_1}^{k_1} \times \cdots \times \mathbb{Z}_{p_n}^{k_n}$ by adapting $\hat{f}$:
   $\hat{f}(u_1, \ldots, u_n) = 1$ if $\forall j : \pi_j(u_j) = 0$ and 0 else

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 idea

1. Examples 1 generalizes to $\mathbf{U} = \mathbb{Z}_p^k$ and $\mathbf{L} = \mathbb{Z}_q^l$
2. Deal with products $\mathbf{U} = \mathbb{Z}_{p_1}^{k_1} \times \cdots \times \mathbb{Z}_{p_n}^{k_n}$ by adapting $\hat{f}$:
   $\hat{f}(u_1, \ldots, u_n) = 1$ if $\forall j : \pi_j(u_j) = 0$ and 0 else
3. **Problem:** Non vector-spaces, e.g. $\mathbf{U} \cong \mathbb{Z}_9$, $\mathbf{L} \cong \mathbb{Z}_4$.

2-nilpotent algebras

Theorem (Kawałek, MK, Krzaczkowski '19)

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

Proof idea

1. Examples 1 generalizes to $\mathbf{U} = \mathbb{Z}_p^k$ and $\mathbf{L} = \mathbb{Z}_q^l$
2. Deal with products $\mathbf{U} = \mathbb{Z}_{p_1}^{k_1} \times \cdots \times \mathbb{Z}_{p_n}^{k_n}$ by adapting $\hat{f}$:
   $\hat{f}(u_1, \ldots, u_n) = 1$ if $\forall j : \pi_j(u_j) = 0$ and 0 else
3. **Problem:** Non vector-spaces, e.g. $\mathbf{U} \cong \mathbb{Z}_9$, $\mathbf{L} \cong \mathbb{Z}_4$.
4. $\rightarrow$ **different approach:** 'systematic summing'

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 idea

1. Examples 1 generalizes to $\mathbf{U} = \mathbb{Z}_p^k$ and $\mathbf{L} = \mathbb{Z}_q^l$
2. Deal with products $\mathbf{U} = \mathbb{Z}_{p_1}^{k_1} \times \cdots \times \mathbb{Z}_{p_n}^{k_n}$ by adapting $\hat{f}$: $\hat{f}(u_1, \ldots, u_n) = 1$ if $\forall j : \pi_j(u_j) = 0$ and 0 else
3. **Problem:** Non vector-spaces, e.g. $\mathbf{U} \cong \mathbb{Z}_9$, $\mathbf{L} \cong \mathbb{Z}_4$.
4. $\to$ **different approach:** 'systematic summing'
5. E.g. $\hat{f}(u+1) + \hat{f}(u+v) + \hat{f}(u+4v) \approx const$

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 idea

1. Examples 1 generalizes to $\mathbf{U} = \mathbb{Z}_p^k$ and $\mathbf{L} = \mathbb{Z}_q^l$
2. Deal with products $\mathbf{U} = \mathbb{Z}_{p_1}^{k_1} \times \dots \times \mathbb{Z}_{p_n}^{k_n}$ by adapting $\hat{f}$: $\hat{f}(u_1, \dots, u_n) = 1$ if $\forall j : \pi_j(u_j) = 0$ and 0 else
3. **Problem:** Non vector-spaces, e.g. $\mathbf{U} \cong \mathbb{Z}_9$, $\mathbf{L} \cong \mathbb{Z}_4$.
4. $\rightarrow$ **different approach:** 'systematic summing'
5. E.g. $\hat{f}(u+1) + \hat{f}(u+v) + \hat{f}(u+4v) \approx const$

$\Rightarrow$ $\sum_{a=1}^{9}(\hat{f}(u+1) + \hat{f}(u+a) + \hat{f}(u+4a)) \approx \hat{f}(u+1) + 1 + 1 \approx const$

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 idea

1. Examples 1 generalizes to $\mathbf{U} = \mathbb{Z}_p^k$ and $\mathbf{L} = \mathbb{Z}_q^l$
2. Deal with products $\mathbf{U} = \mathbb{Z}_{p_1}^{k_1} \times \cdots \times \mathbb{Z}_{p_n}^{k_n}$ by adapting $\hat{f}$:
   $\hat{f}(u_1, \ldots, u_n) = 1$ if $\forall j : \pi_j(u_j) = 0$ and 0 else
3. **Problem:** Non vector-spaces, e.g. $\mathbf{U} \cong \mathbb{Z}_9$, $\mathbf{L} \cong \mathbb{Z}_4$.
4. $\rightarrow$ **different approach:** 'systematic summing'
5. E.g. $\hat{f}(u+1) + \hat{f}(u+v) + \hat{f}(u+4v) \approx \mathit{const}$

$\Rightarrow$ $\sum_{a=1}^{9} (\hat{f}(u+1) + \hat{f}(u+a) + \hat{f}(u+4a)) \approx \hat{f}(u+1) + 1 + 1 \approx \mathit{const}$

Problem

Specific for abelian $\mathbf{U}$. Are we stuck in general?

AAA (Aichinger's awesome augmentations)

Coordinatisation of nilpotent algebras

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.

Coordinatisation of nilpotent algebras

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.

CEQV($\mathbf{A}$) $\leq$ CEQV(($\mathbf{A}, +, 0, -$))

Coordinatisation of nilpotent algebras

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

Coordinatisation of nilpotent algebras

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.

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

Remark

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

Outline

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

Plan of attack

Outline

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

Plan of attack

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

Outline

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

Plan of attack

1. $\mathbf{A} = \mathbf{L} \otimes^T \mathbf{U}$
2. Extend **A** by $\hat{f}$ (that canonically generates subspaces of $\mathbf{L}^{U^n}$)

Outline

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

Plan of attack

1. $\mathbf{A} = \mathbf{L} \otimes^T \mathbf{U}$
2. Extend $\mathbf{A}$ by $\hat{f}$ (that canonically generates subspaces of $\mathbf{L}^{U^n}$)
3. Extension is finitely based

Outline

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

Plan of attack

1. $\mathbf{A} = \mathbf{L} \otimes^T \mathbf{U}$
2. Extend **A** by $\hat{f}$ (that canonically generates subspaces of $\mathbf{L}^{U^n}$)
3. Extension is finitely based
4. Computing a normal form of $\hat{p}(u_1, \ldots, u_n)$ in $\hat{f}$ is possible

Outline

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

Plan of attack

1. $\mathbf{A} = \mathbf{L} \otimes^T \mathbf{U}$
2. Extend **A** by $\hat{f}$ (that canonically generates subspaces of $\mathbf{L}^{U^n}$)
3. Extension is finitely based
4. Computing a normal form of $\hat{p}(u_1, \ldots, u_n)$ in $\hat{f}$ is possible

If **U** is abelian (4) can be done in P. But in general?

Example

Example (simplified)

$\mathbf{A} = (\mathbb{Z}_2 \times (\mathbb{Z}_3 \times \mathbb{Z}_5), +, f_2, f_3)$, with

$f_2((x_2, x_3, x_5)) = (1, 0, 0)$ if $x_3 = 0$

$f_3((x_2, x_3, x_5)) = (0, 1, 0)$ if $x_5 = 0$

Example

Example (simplified)

$\mathbf{A} = (\mathbb{Z}_2 \times (\mathbb{Z}_3 \times \mathbb{Z}_5), +, f_2, f_3)$, with
$f_2((x_2, x_3, x_5)) = (1, 0, 0)$ if $x_3 = 0$
$f_3((x_2, x_3, x_5)) = (0, 1, 0)$ if $x_5 = 0$

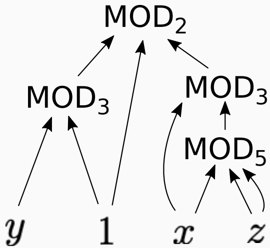
$p(x, y) \approx f_2(1 + y) + f_2(x + f_3(x + 2z))$; corresponds to the circuit

Example

Example (simplified)

$\mathbf{A} = (\mathbb{Z}_2 \times (\mathbb{Z}_3 \times \mathbb{Z}_5), +, f_2, f_3)$, with
$f_2((x_2, x_3, x_5)) = (1, 0, 0)$ if $x_3 = 0$
$f_3((x_2, x_3, x_5)) = (0, 1, 0)$ if $x_5 = 0$

$p(x, y) \approx f_2(1 + y) + f_2(x + f_3(x + 2z))$; corresponds to the circuit



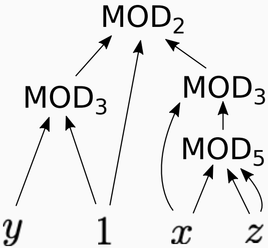
- MOD_n outputs 1
  iff input sums to 0 $\mod n$

Example

Example (simplified)

$\mathbf{A} = (\mathbb{Z}_2 \times (\mathbb{Z}_3 \times \mathbb{Z}_5), +, f_2, f_3)$, with
$f_2((x_2, x_3, x_5)) = (1, 0, 0)$ if $x_3 = 0$
$f_3((x_2, x_3, x_5)) = (0, 1, 0)$ if $x_5 = 0$

$p(x, y) \approx f_2(1 + y) + f_2(x + f_3(x + 2z))$; corresponds to the circuit



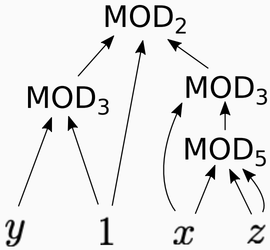
- MOD_n outputs 1
  iff input sums to 0 mod n
- (Boolean) circuits only using MOD_n
  gates are called *$CC[n]$-circuits*

Example

Example (simplified)

$\mathbf{A} = (\mathbb{Z}_2 \times (\mathbb{Z}_3 \times \mathbb{Z}_5), +, f_2, f_3)$, with
$f_2((x_2, x_3, x_5)) = (1, 0, 0)$ if $x_3 = 0$
$f_3((x_2, x_3, x_5)) = (0, 1, 0)$ if $x_5 = 0$

$p(x, y) \approx f_2(1 + y) + f_2(x + f_3(x + 2z))$; corresponds to the circuit



- MOD_n outputs 1 iff input sums to 0 mod n
- (Boolean) circuits only using MOD_n gates are called *CC[n]-circuits*
- CEQV(**A**) reduces to check if $CC[30]$-circuits of depth 3 are ≈ 0

Open questions

A... finite nilpotent, from a CM variety

Proposition (MK)

CEQV(**A**) can be reduced to checking equivalence of $CC[n]$ circuits of depth at most k, for some n, k (and vice versa).

Open questions

A... finite nilpotent, from a CM variety

Proposition (MK)

CEQV(**A**) can be reduced to checking equivalence of $CC[n]$ circuits of depth at most k, for some n, k (and vice versa).

Question

What is the complexity of $CC[n]_k - \mathrm{EQV}$?

Open questions

A... finite nilpotent, from a CM variety

Proposition (MK)

CEQV(**A**) can be reduced to checking equivalence of $CC[n]$ circuits of depth at most k, for some n, k (and vice versa).

Question

What is the complexity of $CC[n]_k - \mathrm{EQV}$?

Conjecture (Barrington, Straubing, Therien '90)

$CC[n]_k$ circuits need size $\mathcal{O}(c^s)$ to compute AND_s.

Open questions

A... finite nilpotent, from a CM variety

Proposition (MK)

CEQV(**A**) can be reduced to checking equivalence of $CC[n]$ circuits of depth at most k, for some n, k (and vice versa).

Question

What is the complexity of $CC[n]_k - \text{EQV}$?

Conjecture (Barrington, Straubing, Therien '90)

$CC[n]_k$ circuits need size $\mathcal{O}(c^s)$ to compute AND_s.

- Conjecture true $\Rightarrow$ $CC[n]_k - \text{EQV}$ decidable in $\mathcal{O}(|C|^{\log(|C|)})$

Open questions

A... finite nilpotent, from a CM variety

Proposition (MK)

CEQV(**A**) can be reduced to checking equivalence of $CC[n]$ circuits of depth at most k, for some n, k (and vice versa).

Question

What is the complexity of $CC[n]_k - \mathrm{EQV}$?

Conjecture (Barrington, Straubing, Therien '90)

$CC[n]_k$ circuits need size $\mathcal{O}(c^s)$ to compute AND_s.

- Conjecture true $\Rightarrow CC[n]_k - \mathrm{EQV}$ decidable in $\mathcal{O}(|C|^{\log(|C|)})$
- If AND_s-circuits computable in P $\Rightarrow CC[n]_k - \mathrm{EQV} \in$ coNP-c

Open questions

A... finite nilpotent, from a CM variety

Proposition (MK)

CEQV(**A**) can be reduced to checking equivalence of $CC[n]$ circuits of depth at most k, for some n, k (and vice versa).

Question

What is the complexity of $CC[n]_k - \text{EQV}$?

Conjecture (Barrington, Straubing, Therien '90)

$CC[n]_k$ circuits need size $\mathcal{O}(c^s)$ to compute AND_s.

- Conjecture true $\Rightarrow CC[n]_k - \text{EQV}$ decidable in $\mathcal{O}(|C|^{\log(|C|)})$
- If AND_s-circuits computable in P $\Rightarrow CC[n]_k - \text{EQV} \in \text{coNP-c}$

Question 2

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

Thank you!