CC-circuits and the expressive power of nilpotent algebras

Michael Kompatscher
CU Prague

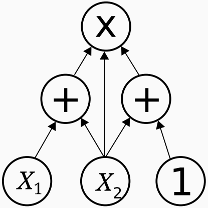
01/19/2020
Birkhoff seminar, CU Boulder

Circuits in Universal Algebra: Why?

Circuits

Definition

A circuit is finite directed acyclic graph, where every vertex ('gate') is labelled by an operation of arity corresponding to its in-degree ('fan-in').



- natural model of computation
- usually studied for Boolean values
- Circuit over an algebra $\mathbf{A} = (A, f_1, \ldots, f_n)$: labelled by basic operations f_i

Circuits over algebras

Circuits over an algebra $\mathbf{A} = (A, f_1, \ldots, f_n)$ encode the term operations over $\mathbf{A}$

Circuits over algebras

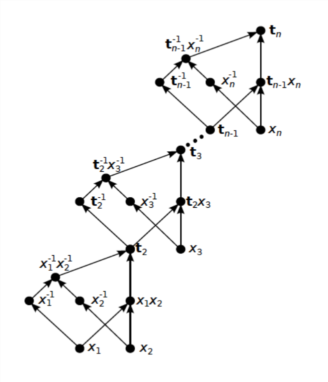
Circuits over an algebra $\mathbf{A} = (A, f_1, \ldots, f_n)$ encode the term operations over $\mathbf{A}$ - **and they are good at it!**

Circuits over algebras

Circuits over an algebra $\mathbf{A} = (A, f_1, \ldots, f_n)$ encode the term operations over $\mathbf{A}$ - **and they are good at it!**

Example

In $(A_4, \cdot, ^{-1})$, the operations $t_n(x_1, \ldots, x_n) = [\cdots[[x_1, x_2], x_3], \ldots, x_n]$ can be represented by circuits linear in n, corresponds to terms exponential in n.



© Idziak, Krzaczkowski

Circuits over algebras

Circuits over an algebra $\mathbf{A} = (A, f_1, \ldots, f_n)$ encode the term operations over $\mathbf{A}$ - **and they are good at it!**

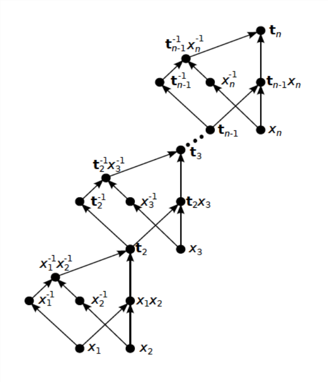
Example

In $(A_4, \cdot, ^{-1})$, the operations $t_n(x_1, \ldots, x_n) = [\cdots[[x_1, x_2], x_3], \ldots, x_n]$ can be represented by circuits linear in n, corresponds to terms exponential in n.

Encoding by circuits is

- more compact than encoding by terms
- stable under term equivalence

$\rightsquigarrow$ use in algorithmic problems.



Outline of this talk:

1. Circuit complexity and CC-circuits
2. Circuits over $\mathbf{A} \leftrightarrow$ CC-circuits
   for finite nilpotent $\mathbf{A}$ from CM varieties
3. Consequences in circuit complexity
4. Consequences for solving equations and checking identities
   in nilpotent algebras.

1) CC-circuits

Circuit complexity

Boolean circuits can be used to measure the complexity of $L \subseteq \{0,1\}^*$.

Basic idea

We say a family $(C_n)_{n \in \mathbb{N}}$ computes $L \subseteq \{0,1\}^*$ if $C_n(x_1, \dots, x_n) = 1 \leftrightarrow (x_1, \dots, x_n) \in L \cap \{0,1\}^n$. The complexity is measured by the size/depth of C_n.

Circuit complexity

Boolean circuits can be used to measure the complexity of $L \subseteq \{0,1\}^*$.

Basic idea

We say a family $(C_n)_{n\in\mathbb{N}}$ computes $L \subseteq \{0,1\}^*$ if $C_n(x_1,\ldots,x_n) = 1 \leftrightarrow (x_1,\ldots,x_n) \in L \cap \{0,1\}^n$. The complexity is measured by the size/depth of C_n.

Examples

Circuit complexity

Boolean circuits can be used to measure the complexity of $L \subseteq \{0,1\}^*$.

Basic idea

We say a family $(C_n)_{n\in\mathbb{N}}$ computes $L \subseteq \{0,1\}^*$ if $C_n(x_1,\ldots,x_n) = 1 \leftrightarrow (x_1,\ldots,x_n) \in L \cap \{0,1\}^n$. The complexity is measured by the size/depth of C_n.

Examples

- $P/poly$: Circuits over $(\{0,1\},\wedge,\vee,\neg)$ of polynomial size

Circuit complexity

Boolean circuits can be used to measure the complexity of $L \subseteq \{0,1\}^*$.

Basic idea

We say a family $(C_n)_{n \in \mathbb{N}}$ computes $L \subseteq \{0,1\}^*$ if $C_n(x_1, \ldots, x_n) = 1 \leftrightarrow (x_1, \ldots, x_n) \in L \cap \{0,1\}^n$. The complexity is measured by the size/depth of C_n.

Examples

- $P/poly$: Circuits over $(\{0,1\}, \wedge, \vee, \neg)$ of polynomial size
- NC: Circuits over $(\{0,1\}, \wedge, \vee, \neg)$ of polynomial size and depth $\leq \mathcal{O}(log^k(n))$

Circuit complexity

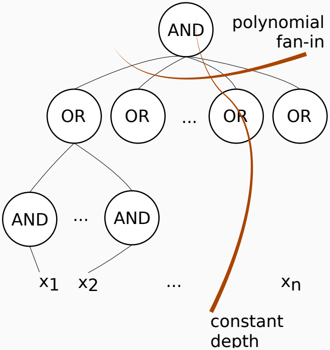
Boolean circuits can be used to measure the complexity of $L \subseteq \{0,1\}^*$.

Basic idea

We say a family $(C_n)_{n\in\mathbb{N}}$ computes $L \subseteq \{0,1\}^*$ if $C_n(x_1,\ldots,x_n) = 1 \leftrightarrow (x_1,\ldots,x_n) \in L \cap \{0,1\}^n$. The complexity is measured by the size/depth of C_n.

Examples

- $P/poly$: Circuits over $(\{0,1\},\wedge,\vee,\neg)$ of polynomial size
- NC: Circuits over $(\{0,1\},\wedge,\vee,\neg)$ of polynomial size and depth $\leq \mathcal{O}(log^k(n))$
- AC^0: polynomial size, constant depth, but arbitrary fan-in



A result about AC^0-circuits

Theorem (Furst, Saxe, Sipser '84)

The parity language $\{x \in \{0,1\}^* : \sum_{i=1}^{n} x_i = 0 \mod 2\}$ is not in AC^0.

A result about AC^0-circuits

Theorem (Furst, Saxe, Sipser '84)
The parity language $\{x \in \{0,1\}^* : \sum_{i=1}^{n} x_i = 0 \mod 2\}$ is not in AC^0.

There exists even a strict lower bound!

Theorem (Håstad '87)
Circuits of depth d with $\{\mathrm{AND}, \mathrm{OR}, \mathrm{NEG}\}$-gates need size $\Omega(e^{n^{\frac{1}{d-1}}})$ to compute parity.

A result about AC^0-circuits

Theorem (Furst, Saxe, Sipser '84)

The parity language $\{x \in \{0,1\}^* : \sum_{i=1}^{n} x_i = 0 \mod 2\}$ is not in AC^0.

There exists even a strict lower bound!

Theorem (Håstad '87)

Circuits of depth d with $\{\mathrm{AND}, \mathrm{OR}, \mathrm{NEG}\}$-gates need size $\Omega(e^{n^{\frac{1}{d-1}}})$ to compute parity.

In essence: Logical gates are bad at counting.

A result about AC^0-circuits

Theorem (Furst, Saxe, Sipser '84)
The parity language $\{x \in \{0,1\}^* : \sum_{i=1}^{n} x_i = 0 \mod 2\}$ is not in AC^0.

There exists even a strict lower bound!

Theorem (Håstad '87)
Circuits of depth d with $\{\text{AND}, \text{OR}, \text{NEG}\}$-gates need size $\Omega(e^{n^{\frac{1}{d-1}}})$ to compute parity.

In essence: Logical gates are bad at counting.

Question:

- Are vice-versa counting gates bad at logic?
- What are circuits with 'counting gates'?

CC-circuits

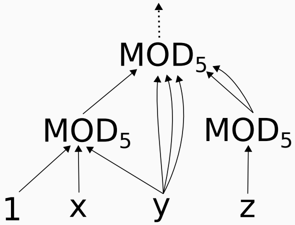
A $CC[m]$-**circuit** is a (Boolean) circuit, whose gates are MOD_m-gates:

$$\text{MOD}_m(x_1, \ldots, x_n) = \begin{cases} 1 \text{ if } \sum_i x_i \equiv 0 \mod m \\ 0 \text{ else.} \end{cases}$$

CC-circuits

A $CC[m]$-**circuit** is a (Boolean) circuit, whose gates are MOD_m-gates:

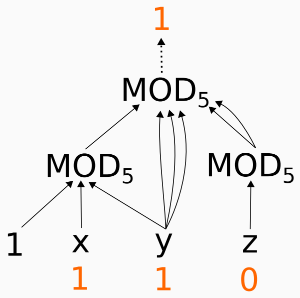
$$\text{MOD}_m(x_1, \ldots, x_n) = \begin{cases} 1 \text{ if } \sum_i x_i \equiv 0 \mod m \\ 0 \text{ else.} \end{cases}$$



CC-circuits

A $CC[m]$-**circuit** is a (Boolean) circuit, whose gates are MOD_m-gates:

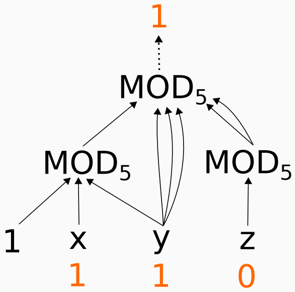
$$\text{MOD}_m(x_1, \ldots, x_n) = \begin{cases} 1 \text{ if } \sum_i x_i \equiv 0 \mod m \\ 0 \text{ else.} \end{cases}$$



CC-circuits

A $CC[m]$-**circuit** is a (Boolean) circuit, whose gates are MOD_m-gates:

$$\mathrm{MOD}_m(x_1, \dots, x_n) = \begin{cases} 1 \text{ if } \sum_i x_i \equiv 0 \mod m \\ 0 \text{ else.} \end{cases}$$

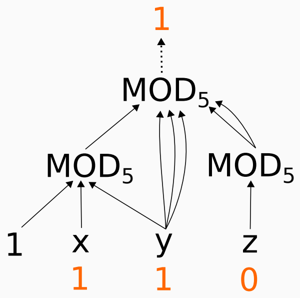


- Gates are of arbitrary fan-in

CC-circuits

A $CC[m]$-**circuit** is a (Boolean) circuit, whose gates are MOD_m-gates:

$$\text{MOD}_m(x_1, \ldots, x_n) = \begin{cases} 1 \text{ if } \sum_i x_i \equiv 0 \mod m \\ 0 \text{ else.} \end{cases}$$

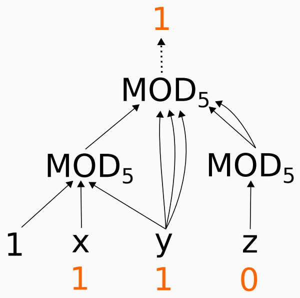


- Gates are of arbitrary fan-in
- Depth = longest path

CC-circuits

A $CC[m]$-**circuit** is a (Boolean) circuit, whose gates are MOD_m-gates:

$$\mathrm{MOD}_m(x_1, \ldots, x_n) = \begin{cases} 1 \text{ if } \sum_i x_i \equiv 0 \mod m \\ 0 \text{ else.} \end{cases}$$

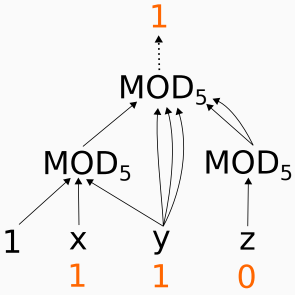


- Gates are of arbitrary fan-in
- Depth = longest path
- $CC^0[m]$: languages accepted by constant depth polynomial size $CC[m]$-circuits.

CC-circuits

A $CC[m]$-**circuit** is a (Boolean) circuit, whose gates are MOD_m-gates:

$$\text{MOD}_m(x_1, \ldots, x_n) = \begin{cases} 1 \text{ if } \sum_i x_i \equiv 0 \mod m \\ 0 \text{ else.} \end{cases}$$



- Gates are of arbitrary fan-in
- Depth = longest path
- $CC^0[m]$: languages accepted by constant depth polynomial size $CC[m]$-circuits.
- $CC^0 = \bigcup_m CC^0[m]$

A conjecture about CC-circuits

Conjecture (McKenzie*, Péladeau, Therién...)

$\forall m, d$: $CC[m]$-circuits of depth d need size $\Omega(e^n)$ to compute $\text{AND}(x_1, \ldots, x_n)$.

*not the one you are thinking of!

A conjecture about CC-circuits

Conjecture (McKenzie*, Péladeau, Therién...)

$\forall m, d$: $CC[m]$-circuits of depth d need size $\Omega(e^n)$ to compute $\text{AND}(x_1, \ldots, x_n)$.

Weak version of conjecture: AND is not in CC^0.

*not the one you are thinking of!

A conjecture about CC-circuits

Conjecture (McKenzie*, Péladeau, Therién...)

$\forall m, d$: $CC[m]$-circuits of depth d need size $\Omega(e^n)$ to compute $\text{AND}(x_1, \ldots, x_n)$.

Weak version of conjecture: AND is not in CC^0.

What is known?

- For p prime, $CC[p^k]$-circuits of depth d *cannot* compute AND of big arity (BST '90)

*not the one you are thinking of!

A conjecture about CC-circuits

Conjecture (McKenzie*, Péladeau, Therién...)

$\forall m, d$: $CC[m]$-circuits of depth d need size $\Omega(e^n)$ to compute $\text{AND}(x_1, \ldots, x_n)$.

Weak version of conjecture: AND is not in CC^0.

What is known?

- For p prime, $CC[p^k]$-circuits of depth d *cannot* compute AND of big arity (BST '90)
- Otherwise they compute *all* functions (for $d \geq 2$),

*not the one you are thinking of!

A conjecture about CC-circuits

Conjecture (McKenzie*, Péladeau, Therién...)

$\forall m, d$: $CC[m]$-circuits of depth d need size $\Omega(e^n)$ to compute $\mathrm{AND}(x_1, \ldots, x_n)$.

Weak version of conjecture: AND is not in CC^0.

What is known?

- For p prime, $CC[p^k]$-circuits of depth d *cannot* compute AND of big arity (BST '90)
- Otherwise they compute *all* functions (for $d \geq 2$),
- true for $m = pq$, $d = 2$ (BST '90)

*not the one you are thinking of!

A conjecture about CC-circuits

Conjecture (McKenzie*, Péladeau, Therién...)

$\forall m, d$: $CC[m]$-circuits of depth d need size $\Omega(e^n)$ to compute $\text{AND}(x_1, \ldots, x_n)$.

Weak version of conjecture: AND is not in CC^0.

What is known?

- For p prime, $CC[p^k]$-circuits of depth d *cannot* compute AND of big arity (BST '90)
- Otherwise they compute *all* functions (for $d \geq 2$),
- true for $m = pq$, $d = 2$ (BST '90)
- open for $m = 6$, $d = 3$

*not the one you are thinking of!

A conjecture about CC-circuits

Conjecture (McKenzie*, Péladeau, Therién...)

$\forall m, d$: $CC[m]$-circuits of depth d need size $\Omega(e^n)$ to compute $\mathrm{AND}(x_1, \ldots, x_n)$.

Weak version of conjecture: AND is not in CC^0.

What is known?

- For p prime, $CC[p^k]$-circuits of depth d *cannot* compute AND of big arity (BST '90)
- Otherwise they compute *all* functions (for $d \geq 2$),
- true for $m = pq$, $d = 2$ (BST '90)
- open for $m = 6$, $d = 3$
- best known lower bounds in general are super-linear (CGPT '06)

*not the one you are thinking of!

Beyond Boolean

How about $\mathbb{Z}_m$-valued variants of $CC[m]$-circuits?

Beyond Boolean

How about $\mathbb{Z}_m$-valued variants of $CC[m]$-circuits?

Definition $CC^+[m]$**-circuits:**

- consist of MOD_m-gates and $+$-gates
- evaluated over $\mathbb{Z}_m$, not $\{0, 1\}$

Beyond Boolean

How about $\mathbb{Z}_m$-valued variants of $CC[m]$-circuits?

Definition $CC^+[m]$**-circuits:**

- consist of MOD_m-gates and $+$-gates
- evaluated over $\mathbb{Z}_m$, not $\{0, 1\}$

Definition

An operation f is called (0-)*absorbing* if
$f(0, x_2, \ldots, x_n) \approx f(x_1, 0, x_2, \ldots, x_n) \approx \cdots \approx f(x_1, \ldots, x_{n-1}, 0) \approx 0.$

Beyond Boolean

How about $\mathbb{Z}_m$-valued variants of $CC[m]$-circuits?

Definition $CC^+[m]$**-circuits:**

- consist of MOD_m-gates and $+$-gates
- evaluated over $\mathbb{Z}_m$, not $\{0, 1\}$

Definition

An operation f is called (0-)*absorbing* if
$f(0, x_2, \ldots, x_n) \approx f(x_1, 0, x_2, \ldots, x_n) \approx \cdots \approx f(x_1, \ldots, x_{n-1}, 0) \approx 0.$

Lemma (MK '19)

$CC^+[m]$-circuit		$CC[m]$-circuit
non-trivial absorbing, depth d	$\rightarrow$	computing AND, depth d
non-trivial absorbing, depth $d+1$	$\leftarrow$	computing AND, depth d

$\rightarrow$... linear time computation

2) Nilpotent algebras

The structure of nilpotent algebras

$\mathbf{A} = (A; f_1, \ldots, f_k)$ finite algebra

The structure of nilpotent algebras

$\mathbf{A} = (A; f_1, \ldots, f_k)$ finite algebra

Nilpotency of $\mathbf{A}$ is

The structure of nilpotent algebras

$\mathbf{A} = (A; f_1, \ldots, f_k)$ finite algebra

Nilpotency of $\mathbf{A}$ is

- in general defined by the term condition commutator
  $[\cdots[1_A, 1_A], \ldots 1_A] = 0_A$

The structure of nilpotent algebras

$\mathbf{A} = (A; f_1, \ldots, f_k)$ finite algebra

Nilpotency of $\mathbf{A}$ is

- in general defined by the term condition commutator $[\cdots[1_A, 1_A], \ldots 1_A] = 0_A$

in *congruence modular varieties* (**Freese, McKenzie***):

*Yes, that's him!

The structure of nilpotent algebras

$\mathbf{A} = (A; f_1, \dots, f_k)$ finite algebra

Nilpotency of **A** is

- in general defined by the term condition commutator $[\cdots[1_A, 1_A], \dots 1_A] = 0_A$

in *congruence modular varieties* (**Freese, McKenzie***):

- **A** is **Abelian** $\Leftrightarrow$ polynomially equivalent to a module

*Yes, that's him!

The structure of nilpotent algebras

$\mathbf{A} = (A; f_1, \ldots, f_k)$ finite algebra

Nilpotency of $\mathbf{A}$ is

- in general defined by the term condition commutator $[\cdots[1_A, 1_A], \ldots 1_A] = 0_A$

in *congruence modular varieties* (**Freese, McKenzie***):

- $\mathbf{A}$ is **Abelian** $\Leftrightarrow$ polynomially equivalent to a module
- $\mathbf{A}$ is n-**nilpotent** $\Leftrightarrow \exists\, \mathbf{L}$ Abelian, $\mathbf{U}$ is $(n-1)$-nilpotent, $A = L \times U$:

*Yes, that's him!

The structure of nilpotent algebras

$\mathbf{A} = (A; f_1, \dots, f_k)$ finite algebra

Nilpotency of $\mathbf{A}$ is

- in general defined by the term condition commutator $[\cdots[1_A, 1_A], \dots 1_A] = 0_A$

in *congruence modular varieties* (**Freese, McKenzie***):

- $\mathbf{A}$ is **Abelian** $\Leftrightarrow$ polynomially equivalent to a module
- $\mathbf{A}$ is n-**nilpotent** $\Leftrightarrow \exists$ $\mathbf{L}$ Abelian, $\mathbf{U}$ is $(n-1)$-nilpotent, $A = L \times U$:

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

*Yes, that's him!

The structure of nilpotent algebras

$\mathbf{A} = (A; f_1, \dots, f_k)$ finite algebra

Nilpotency of $\mathbf{A}$ is

- in general defined by the term condition commutator $[\cdots[1_A, 1_A], \dots 1_A] = 0_A$

in *congruence modular varieties* (**Freese, McKenzie***):

- $\mathbf{A}$ is **Abelian** $\Leftrightarrow$ polynomially equivalent to a module
- $\mathbf{A}$ is n-**nilpotent** $\Leftrightarrow \exists$ $\mathbf{L}$ Abelian, $\mathbf{U}$ is $(n-1)$-nilpotent, $A = L \times U$:

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

Also true for polynomial operations of $\mathbf{A}$

*Yes, that's him!

Encoding CC^+-circuits in nilpotent algebras

$CC^+[m]$-circuits of bounded depth can be encoded in a nilpotent algebra in the following sense:

Encoding CC^+-circuits in nilpotent algebras

$CC^+[m]$-circuits of bounded depth can be encoded in a nilpotent algebra in the following sense:

Proposition (MK '19)

$\forall m, d \in \mathbb{N}\ \exists (d+1)$-nilpotent algebra **B**, s.t.

- **B** contains the group $(B, +) = \mathbb{Z}_m^{d+1}$
- for every $CC[m]^+$-circuit C of depth d,
  $\exists$ circuit C' over **B** with
  $C'(x_1, \ldots, x_n) = (C(\pi_{d+1}(x_1), \ldots, \pi_{d+1}(x_n)), 0, \ldots, 0)$.

Encoding CC^+-circuits in nilpotent algebras

$CC^+[m]$-circuits of bounded depth can be encoded in a nilpotent algebra in the following sense:

Proposition (MK '19)

$\forall m, d \in \mathbb{N}\ \exists (d+1)$-nilpotent algebra $\mathbf{B}$, s.t.

- $\mathbf{B}$ contains the group $(B, +) = \mathbb{Z}_m^{d+1}$
- for every $CC[m]^+$-circuit C of depth d,
  $\exists$ circuit C' over $\mathbf{B}$ with
  $C'(x_1, \ldots, x_n) = (C(\pi_{d+1}(x_1), \ldots, \pi_{d+1}(x_n)), 0, \ldots, 0)$.

(Proof sketch on blackboard.)

Encoding CC^+-circuits in nilpotent algebras

$CC^+[m]$-circuits of bounded depth can be encoded in a nilpotent algebra in the following sense:

Proposition (MK '19)

$\forall m, d \in \mathbb{N}\ \exists (d+1)$-nilpotent algebra **B**, s.t.

- **B** contains the group $(B, +) = \mathbb{Z}_m^{d+1}$
- for every $CC[m]^+$-circuit C of depth d,
  $\exists$ circuit C' over **B** with
  $C'(x_1, \ldots, x_n) = (C(\pi_{d+1}(x_1), \ldots, \pi_{d+1}(x_n)), 0, \ldots, 0)$.

(Proof sketch on blackboard.)

Question

What about the opposite direction?

Example: Extended abelian groups

$\mathbf{A} = (\mathbb{Z}_3 \times \mathbb{Z}_3, +, f(x, y))$ with

Example: Extended abelian groups

$\mathbf{A} = (\mathbb{Z}_3 \times \mathbb{Z}_3, +, f(x, y))$ with

$$f((x_1, x_2), (y_1, y_2)) = (\hat{f}(x_2, y_2), 0) = \begin{cases} (1, 0) \text{ if } x_2 = y_2 = 1 \\ (0, 0) \text{ else} \end{cases}$$

Example: Extended abelian groups

$\mathbf{A} = (\mathbb{Z}_3 \times \mathbb{Z}_3, +, f(x, y))$ with

$$f((x_1, x_2), (y_1, y_2)) = (\hat{f}(x_2, y_2), 0) = \begin{cases} (1, 0) \text{ if } x_2 = y_2 = 1 \\ (0, 0) \text{ else} \end{cases}$$

$\mathbf{A}$ is 2-nilpotent. Polynomial e.g.:

Example: Extended abelian groups

$\mathbf{A} = (\mathbb{Z}_3 \times \mathbb{Z}_3, +, f(x, y))$ with

$$f((x_1, x_2), (y_1, y_2)) = (\hat{f}(x_2, y_2), 0) = \begin{cases} (1, 0) \text{ if } x_2 = y_2 = 1 \\ (0, 0) \text{ else} \end{cases}$$

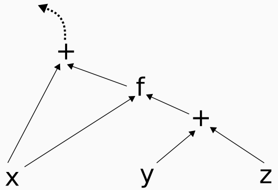
$\mathbf{A}$ is 2-nilpotent. Polynomial e.g.:
$x + f(x, y + z) = (x_1 + \hat{f}(x_2, y_2 + z_2), x_2)$

Example: Extended abelian groups

$\mathbf{A} = (\mathbb{Z}_3 \times \mathbb{Z}_3, +, f(x, y))$ with

$$f((x_1, x_2), (y_1, y_2)) = (\hat{f}(x_2, y_2), 0) = \begin{cases} (1, 0) \text{ if } x_2 = y_2 = 1 \\ (0, 0) \text{ else} \end{cases}$$

$\mathbf{A}$ is 2-nilpotent. Polynomial e.g.:
$x + f(x, y + z) = (x_1 + \hat{f}(x_2, y_2 + z_2), x_2)$ corresponds to the circuit

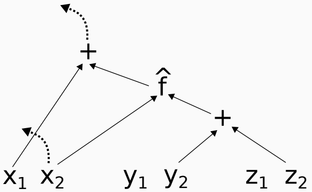


Example: Extended abelian groups

$\mathbf{A} = (\mathbb{Z}_3 \times \mathbb{Z}_3, +, f(x, y))$ with

$$f((x_1, x_2), (y_1, y_2)) = (\hat{f}(x_2, y_2), 0) = \begin{cases} (1, 0) \text{ if } x_2 = y_2 = 1 \\ (0, 0) \text{ else} \end{cases}$$

$\mathbf{A}$ is 2-nilpotent. Polynomial e.g.:
$x + f(x, y + z) = (x_1 + \hat{f}(x_2, y_2 + z_2), x_2)$ corresponds to the circuit

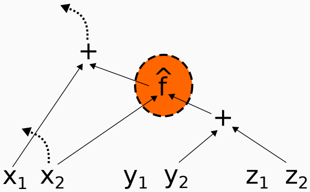


Example: Extended abelian groups

$\mathbf{A} = (\mathbb{Z}_3 \times \mathbb{Z}_3, +, f(x,y))$ with

$$f((x_1,x_2),(y_1,y_2)) = (\hat{f}(x_2,y_2),0) = \begin{cases}(1,0) \text{ if } x_2 = y_2 = 1 \\ (0,0) \text{ else}\end{cases}$$

$\mathbf{A}$ is 2-nilpotent. Polynomial e.g.:
$x + f(x, y+z) = (x_1 + \hat{f}(x_2, y_2 + z_2), x_2)$ corresponds to the circuit

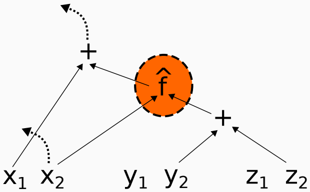


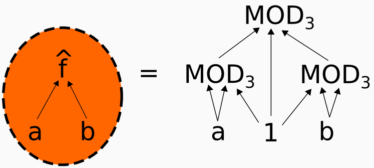
Example: Extended abelian groups

$\mathbf{A} = (\mathbb{Z}_3 \times \mathbb{Z}_3, +, f(x,y))$ with

$$f((x_1,x_2),(y_1,y_2)) = (\hat{f}(x_2,y_2),0) = \begin{cases}(1,0) \text{ if } x_2 = y_2 = 1 \\ (0,0) \text{ else}\end{cases}$$

$\mathbf{A}$ is 2-nilpotent. Polynomial e.g.:
$x + f(x, y+z) = (x_1 + \hat{f}(x_2, y_2+z_2), x_2)$ corresponds to the circuit



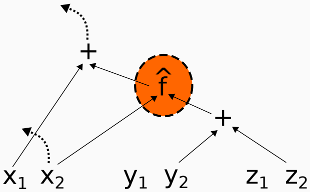


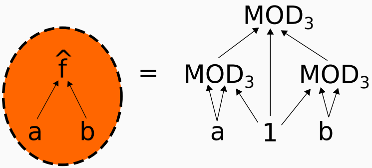
Example: Extended abelian groups

$\mathbf{A} = (\mathbb{Z}_3 \times \mathbb{Z}_3, +, f(x, y))$ with

$$f((x_1, x_2), (y_1, y_2)) = (\hat{f}(x_2, y_2), 0) = \begin{cases} (1,0) \text{ if } x_2 = y_2 = 1 \\ (0,0) \text{ else} \end{cases}$$

$\mathbf{A}$ is 2-nilpotent. Polynomial e.g.:
$x + f(x, y + z) = (x_1 + \hat{f}(x_2, y_2 + z_2), x_2)$ corresponds to the circuit





⇒ similarly all polynomials of **A** can be rewritten in polynomial time to $CC[3]^+$-circuits of depth 3

Coordinatisation of nilpotent algebras

Example works because of abelian group operations.

Coordinatisation of nilpotent algebras

Example works because of abelian group operations.

Theorem (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

Example works because of abelian group operations.

Theorem (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.

$\rightarrow$ wlog work only in Aichinger's extended groups

Coordinatisation of nilpotent algebras

Example works because of abelian group operations.

Theorem (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.

$\rightarrow$ wlog 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.

Main result

A... finite nilpotent algebra (from CM variety)

Main result

A... finite nilpotent algebra (from CM variety)
$|A| = \prod_{i=1}^{k} p_i^{j_i}$

Main result

A... finite nilpotent algebra (from CM variety)
$|A| = \prod_{i=1}^{k} p_i^{j_i}$
$m := \prod_{i=1}^{k} p_i$

Main result

A... finite nilpotent algebra (from CM variety)
$|A| = \prod_{i=1}^{k} p_i^{j_i}$
$m := \prod_{i=1}^{k} p_i$

Theorem (MK '19)

- $\forall d, m$: $\exists (d+1)$ nilpotent **B**, such that $CC[m]^{+}$-circuits of depth d can be encoded as polynomials over **B** in polynomial time.

Main result

A... finite nilpotent algebra (from CM variety)
$|A| = \prod_{i=1}^{k} p_i^{j_i}$
$m := \prod_{i=1}^{k} p_i$

Theorem (MK '19)

- $\forall d, m$: $\exists (d+1)$ nilpotent **B**, such that $CC[m]^+$-circuits of depth d can be encoded as polynomials over **B** in polynomial time.
- Every polynomial over **A** can be rewritten in polynomial time to a $CC[m]^+$-circuit of depth $\leq C(\mathbf{A})$.

Main result

A... finite nilpotent algebra (from CM variety)
$|A| = \prod_{i=1}^{k} p_i^{j_i}$
$m := \prod_{i=1}^{k} p_i$

Theorem (MK '19)

- $\forall d, m$: $\exists (d+1)$ nilpotent $\mathbf{B}$, such that $CC[m]^+$-circuits of depth d can be encoded as polynomials over $\mathbf{B}$ in polynomial time.
- Every polynomial over $\mathbf{A}$ can be rewritten in polynomial time to a $CC[m]^+$-circuit of depth $\leq C(\mathbf{A})$.
- If m is not prime power, then $C(\mathbf{A})$ is linear in $\log_2 |A|$.

3) Consequences on CC-circuits

Conjecture (*) in nilpotent algebras

An operation $f : A^n \to A$ is called 0-**absorbing** iff
$f(0, x_2, \dots, x_n) \approx f(x_1, 0, x_2, \dots, x_n) \approx \dots \approx f(x_1, \dots, x_{n-1}, 0) \approx 0$.

CC-circuits	in nilpotent algebra **A**
Conjecture (*) Bounded depth $CC[m]$-circuits need size $\Omega(e^n)$ to compute AND. **Theorem (BST '90)** Bounded depth $CC[p^k]$-circuits cannot compute AND of arity $\geq C(d)$ **Theorem (BST '90)** Conjecture (*) is true for $m = pq$ and depth 2	

Conjecture (*) in nilpotent algebras

An operation $f : A^n \to A$ is called 0-**absorbing** iff
$f(0, x_2, \ldots, x_n) \approx f(x_1, 0, x_2, \ldots, x_n) \approx \cdots \approx f(x_1, \ldots, x_{n-1}, 0) \approx 0$.

CC-circuits	in nilpotent algebra **A**
Conjecture (*) Bounded depth $CC[m]$-circuits need size $\Omega(e^n)$ to compute AND. **Theorem (BST '90)** Bounded depth $CC[p^k]$-circuits cannot compute AND of arity $\geq C(d)$ **Theorem (BST '90)** Conjecture (*) is true for $m = pq$ and depth 2	

Conjecture (*) in nilpotent algebras

An operation $f : A^n \to A$ is called 0-**absorbing** iff
$f(0, x_2, \ldots, x_n) \approx f(x_1, 0, x_2, \ldots, x_n) \approx \cdots \approx f(x_1, \ldots, x_{n-1}, 0) \approx 0$.

CC-circuits	in nilpotent algebra **A**
Conjecture (*) Bounded depth $CC[m]$-circuits need size $\Omega(e^n)$ to compute AND. **Theorem (BST '90)** Bounded depth $CC[p^k]$-circuits cannot compute AND of arity $\geq C(d)$ **Theorem (BST '90)** Conjecture (*) is true for $m = pq$ and depth 2	**Conjecture (**) (Aichinger '19)** Non-trivial absorbing circuits over **A** of arity n have size $\Omega(e^n)$.

Conjecture (*) in nilpotent algebras

An operation $f : A^n \to A$ is called 0-**absorbing** iff
$f(0, x_2, \dots, x_n) \approx f(x_1, 0, x_2, \dots, x_n) \approx \dots \approx f(x_1, \dots, x_{n-1}, 0) \approx 0$.

CC-circuits	in nilpotent algebra **A**
Conjecture (*) Bounded depth $CC[m]$-circuits need size $\Omega(e^n)$ to compute AND.	**Conjecture (**) (Aichinger '19)** Non-trivial absorbing circuits over **A** of arity n have size $\Omega(e^n)$.
Theorem (BST '90) Bounded depth $CC[p^k]$-circuits cannot compute AND of arity $\geq C(d)$	**Theorem (Aichinger, Mudrinski '10)** **A** with $\lvert A \rvert = p^k$ has only trivial absorbing circuits of arity $\geq C(\mathbf{A})$
Theorem (BST '90) Conjecture (*) is true for $m = pq$ and depth 2	

Conjecture (*) in nilpotent algebras

An operation $f : A^n \to A$ is called 0-**absorbing** iff
$f(0, x_2, \dots, x_n) \approx f(x_1, 0, x_2, \dots, x_n) \approx \dots \approx f(x_1, \dots, x_{n-1}, 0) \approx 0$.

CC-circuits	in nilpotent algebra **A**
Conjecture (*) Bounded depth $CC[m]$-circuits need size $\Omega(e^n)$ to compute AND.	**Conjecture (**) (Aichinger '19)** Non-trivial absorbing circuits over **A** of arity n have size $\Omega(e^n)$.
Theorem (BST '90) Bounded depth $CC[p^k]$-circuits cannot compute AND of arity $\geq C(d)$	**Theorem (Aichinger, Mudrinski '10)** **A** with $\lvert A\rvert = p^k$ has only trivial absorbing circuits of arity $\geq C(\mathbf{A})$
Theorem (BST '90) Conjecture (*) is true for $m = pq$ and depth 2	**(Idziak, Kawałek, Krzaczkowski '18)** (**) is true for certain 2-nilpotent **A** with $\lvert A\rvert = p^k q^l$

Remark

There exists another algebraic characterization of CC^0 by NUDFA (non-uniform deterministic finite automata) over monoids.

Theorem (Barrington, Straubing, Therien '90)

$L \in$ complexity class	$\leftrightarrow$	L accepted by a NUDFA over M
AC^0	$\leftrightarrow$	M aperiodic monoid
CC^0	$\leftrightarrow$	M solvable group
ACC^0	$\leftrightarrow$	M solvable monoid
NC^1	$\leftrightarrow$	M non-solvable group

4) Consequences on CSAT and CEQV

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: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ circuits over $\mathbf{A}$

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: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ circuits over $\mathbf{A}$

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

Circuit Satisfaction Problem CSAT($\mathbf{A}$)

INPUT: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ circuits over $\mathbf{A}$

QUESTION: Does $p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n)$ have a solution in $\mathbf{A}$?

The equivalence problem for finite algebras

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

Circuit Equivalence Problem CEQV($\mathbf{A}$)

INPUT: $p(x_1, \dots, x_n), q(x_1, \dots, x_n)$ circuits over $\mathbf{A}$

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

Circuit Satisfaction Problem CSAT($\mathbf{A}$)

INPUT: $p(x_1, \dots, x_n), q(x_1, \dots, x_n)$ circuits over $\mathbf{A}$

QUESTION: Does $p(x_1, \dots, x_n) = q(x_1, \dots, x_n)$ have a solution in $\mathbf{A}$?

CEQV($\mathbf{A}$) $\in$ coNP, CSAT($\mathbf{A}$) $\in$ NP

In general the complexity is widely unclassified.

The equivalence problem for finite algebras

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

Circuit Equivalence Problem CEQV(**A**)

INPUT: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ circuits over **A**

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

Circuit Satisfaction Problem CSAT(**A**)

INPUT: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ circuits over **A**

QUESTION: Does $p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n)$ have a solution in **A**?

CEQV(**A**) $\in$ coNP, CSAT(**A**) $\in$ NP

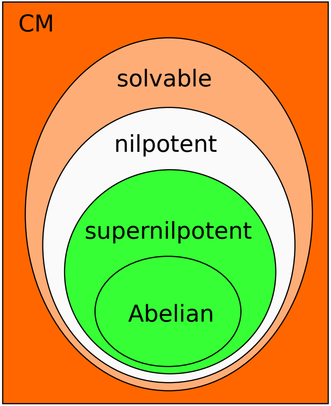
In general the complexity is widely unclassified.

Question

What is the complexity for nilpotent **A** from CM varieties?

In congruence modular varieties

A... from congruence modular variety:



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

For CSAT the picture is similar (modulo products with DL algebras).

Circuit equivalence

Observation 1 (MK ’19)

Assume Conjecture (**) holds for **A** nilpotent.
Then CEQV(**A**) and CSAT(**A**) can be solved in quasipolynomial time.

Proof idea:

Circuit equivalence

Observation 1 (MK '19)

Assume Conjecture (**) holds for $\mathbf{A}$ nilpotent.
Then CEQV($\mathbf{A}$) and CSAT($\mathbf{A}$) can be solved in quasipolynomial time.

Proof idea:

- Let $C(\bar{x}) \approx 0$ be an input to CEQV($\mathbf{A}$).

Circuit equivalence

Observation 1 (MK '19)

Assume Conjecture (**) holds for $\mathbf{A}$ nilpotent.
Then CEQV($\mathbf{A}$) and CSAT($\mathbf{A}$) can be solved in quasipolynomial time.

Proof idea:

- Let $C(\bar{x}) \approx 0$ be an input to CEQV($\mathbf{A}$).
- Assume $\exists \bar{a} : C(\bar{a}) \neq 0$.

Circuit equivalence

Observation 1 (MK '19)

Assume Conjecture (**) holds for $\mathbf{A}$ nilpotent.
Then CEQV($\mathbf{A}$) and CSAT($\mathbf{A}$) can be solved in quasipolynomial time.

Proof idea:

- Let $C(\bar{x}) \approx 0$ be an input to CEQV($\mathbf{A}$).
- Assume $\exists \bar{a} : C(\bar{a}) \neq 0$.
- Take $\bar{a}$ with minimal number k of $a_i \neq 0$, wlog.
  $\bar{a} = (a_1, \ldots, a_k, 0, \ldots, 0)$

Circuit equivalence

Observation 1 (MK '19)

Assume Conjecture (**) holds for **A** nilpotent.
Then CEQV(**A**) and CSAT(**A**) can be solved in quasipolynomial time.

Proof idea:

- Let $C(\bar{x}) \approx 0$ be an input to CEQV(**A**).
- Assume $\exists \bar{a} : C(\bar{a}) \neq 0$.
- Take $\bar{a}$ with minimal number k of $a_i \neq 0$, wlog.
  $\bar{a} = (a_1, \ldots, a_k, 0, \ldots, 0)$
- Then $C'(x_1, \ldots, x_k) = C(x_1, \ldots, x_k, 0, 0, \ldots, 0)$ is 0-absorbing.

Circuit equivalence

Observation 1 (MK '19)

Assume Conjecture (**) holds for **A** nilpotent.
Then CEQV(**A**) and CSAT(**A**) can be solved in quasipolynomial time.

Proof idea:

- Let $C(\bar{x}) \approx 0$ be an input to CEQV(**A**).
- Assume $\exists \bar{a} : C(\bar{a}) \neq 0$.
- Take $\bar{a}$ with minimal number k of $a_i \neq 0$, wlog. $\bar{a} = (a_1, \ldots, a_k, 0, \ldots, 0)$
- Then $C'(x_1, \ldots, x_k) = C(x_1, \ldots, x_k, 0, 0, \ldots, 0)$ is 0-absorbing.
- Conjecture $(**) \Rightarrow k \leq \log(|C|)$

Circuit equivalence

Observation 1 (MK '19)

Assume Conjecture (**) holds for **A** nilpotent.
Then CEQV(**A**) and CSAT(**A**) can be solved in quasipolynomial time.

Proof idea:

- Let $C(\bar{x}) \approx 0$ be an input to CEQV(**A**).
- Assume $\exists \bar{a} : C(\bar{a}) \neq 0$.
- Take $\bar{a}$ with minimal number k of $a_i \neq 0$, wlog. $\bar{a} = (a_1, \ldots, a_k, 0, \ldots, 0)$
- Then $C'(x_1, \ldots, x_k) = C(x_1, \ldots, x_k, 0, 0, \ldots, 0)$ is 0-absorbing.
- Conjecture $(**) \Rightarrow k \leq \log(|C|)$
- evaluate q at all tuples with 'support' $\log(|C|)$ in time $\mathcal{O}(|C|^{\log(|C|)})$

Circuit equivalence

Observation 1 (MK '19)

Assume Conjecture (**) holds for **A** nilpotent.
Then CEQV(**A**) and CSAT(**A**) can be solved in quasipolynomial time.

Proof idea:

- Let $C(\bar{x}) \approx 0$ be an input to CEQV(**A**).
- Assume $\exists \bar{a} : C(\bar{a}) \neq 0$.
- Take $\bar{a}$ with minimal number k of $a_i \neq 0$, wlog.
  $\bar{a} = (a_1, \ldots, a_k, 0, \ldots, 0)$
- Then $C'(x_1, \ldots, x_k) = C(x_1, \ldots, x_k, 0, 0, \ldots, 0)$ is 0-absorbing.
- Conjecture $(**) \Rightarrow k \leq \log(|C|)$
- evaluate q at all tuples with 'support' $\log(|C|)$ in time $\mathcal{O}(|C|^{\log(|C|)})$

Note that for $|A| = p^j$: $k \leq const$
$\Rightarrow$ polynomial time algorithm for prime powers / supernilpotent.
(Aichinger, Mudrinski '10)

On the contrary

Assume $\exists (C_n)_{n \in \mathbb{N}}$

- $CC[m]$-circuits of depth d,

On the contrary

Assume $\exists (C_n)_{n \in \mathbb{N}}$

- $CC[m]$-circuits of depth d,
- *enumerable* in polynomial time,

On the contrary

Assume $\exists (C_n)_{n \in \mathbb{N}}$

- $CC[m]$-circuits of depth d,
- *enumerable* in polynomial time,
- computing AND (AND is in 'uniform CC^0').

On the contrary

Assume $\exists(C_n)_{n\in\mathbb{N}}$

- $CC[m]$-circuits of depth d,
- *enumerable* in polynomial time,
- computing AND (AND is in 'uniform CC^0').

Observation 2 (MK '19)

Then $\exists\mathbf{B}$ nilpotent CEQV($\mathbf{B}$) $\in$ coNP-c and CSAT($\mathbf{B}$) $\in$ NP-c.

On the contrary

Assume $\exists (C_n)_{n \in \mathbb{N}}$

- $CC[m]$-circuits of depth d,
- *enumerable* in polynomial time,
- computing AND (AND is in 'uniform CC^0').

Observation 2 (MK '19)

Then $\exists \mathbf{B}$ nilpotent CEQV($\mathbf{B}$) $\in$ coNP-c and CSAT($\mathbf{B}$) $\in$ NP-c.

Conclusion

Complexity of CEQV($\mathbf{A}$), CSAT($\mathbf{A}$) for nilpotent $\mathbf{A}$ is correlated to the expressive power of CC-circuits.

Caution!

Caution!

- Falsehood of the conjecture does not implies hardness (non-uniform vs. uniform circuits).
- There can be better algorithms (semantic vs. syntactic approach):

Caution!

Caution!

- Falsehood of the conjecture does not implies hardness (non-uniform vs. uniform circuits).
- There can be better algorithms (semantic vs. syntactic approach):

Theorem (Idziak, Kawałek, Krzaczkowski ’18)

For every $\mathbf{A} = \mathbf{L} \otimes^{T} \mathbf{U}$ such that $\mathbf{L}$ and $\mathbf{U}$ are polynomially equivalent to finite vector spaces $\mathrm{CEQV}(\mathbf{A}) \in \mathrm{P}$ and $\mathrm{CSAT}(\mathbf{A}) \in \mathrm{P}$.

Caution!

Caution!

- Falsehood of the conjecture does not implies hardness (non-uniform vs. uniform circuits).
- There can be better algorithms (semantic vs. syntactic approach):

Theorem (Idziak, Kawałek, Krzaczkowski '18)

For every $\mathbf{A} = \mathbf{L} \otimes^T \mathbf{U}$ such that $\mathbf{L}$ and $\mathbf{U}$ are polynomially equivalent to finite vector spaces $\mathrm{CEQV}(\mathbf{A}) \in \mathrm{P}$ and $\mathrm{CSAT}(\mathbf{A}) \in \mathrm{P}$.

Theorem (Kawałek, Kompatscher, Krzaczkowski $\sim$'19)

For *every* $\mathbf{A}$ finite 2-nilpotent from a CM variety $\mathrm{CEQV}(\mathbf{A}) \in \mathrm{P}$.

Caution!

- Falsehood of the conjecture does not implies hardness (non-uniform vs. uniform circuits).
- There can be better algorithms (semantic vs. syntactic approach):

Theorem (Idziak, Kawałek, Krzaczkowski '18)

For every $\mathbf{A} = \mathbf{L} \otimes^T \mathbf{U}$ such that $\mathbf{L}$ and $\mathbf{U}$ are polynomially equivalent to finite vector spaces $\mathrm{CEQV}(\mathbf{A}) \in \mathrm{P}$ and $\mathrm{CSAT}(\mathbf{A}) \in \mathrm{P}$.

Theorem (Kawałek, Kompatscher, Krzaczkowski $\sim$'19)

For *every* $\mathbf{A}$ finite 2-nilpotent from a CM variety $\mathrm{CEQV}(\mathbf{A}) \in \mathrm{P}$.

(This is all we know, despite bold claims made at BLAST'19)

Thank you!