CC-circuits and the expressive power of nilpotent algebras

Michael Kompatscher

Charles University Prague

06/09/2019

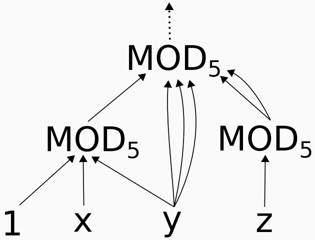
SSAOS19 - Karolinka

CC-circuits

CC-circuits

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

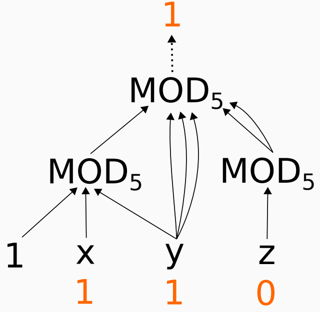
$$\text{MOD}_m(x_1, \dots, x_n) = \begin{cases} 1 \text{ if } \sum_i x_i \equiv 0 \mod m \\ 0 \text{ else.} \end{cases}$$



CC-circuits

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

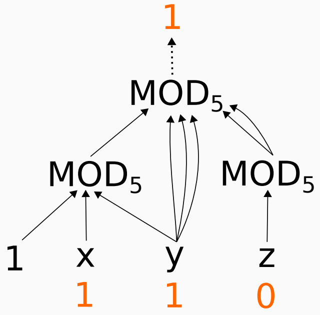
$$\mathrm{MOD}_m(x_1, \ldots, x_n) = \begin{cases} 1 \text{ if } \sum_i x_i \equiv 0 \mod m \\ 0 \text{ else.} \end{cases}$$



CC-circuits

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

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

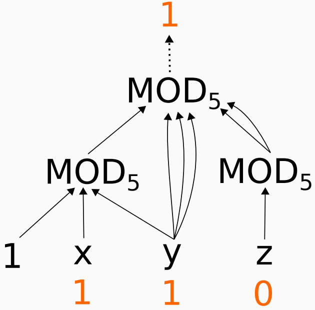


- Gates are of arbitrary fan-in

CC-circuits

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

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

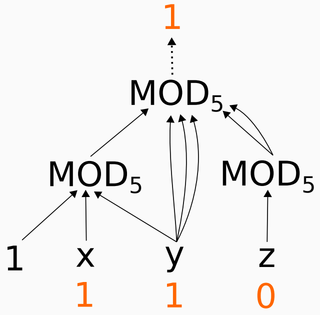


- Gates are of arbitrary fan-in
- Depth = longest path

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
- $CC[m]^+$-**circuit**: $\mathbb{Z}_m$-valued, also $+$-gates

A conjecture about CC-circuits

$\{\text{NEG}, \text{AND}, \text{OR}\}$-circuits of depth d need size $\Omega(e^{n^{\frac{1}{d-1}}})$ to compute $\text{MOD}_2(x_1, \ldots, x_n)$ (Håstad '87)

A conjecture about CC-circuits

$\{\mathrm{NEG}, \mathrm{AND}, \mathrm{OR}\}$-circuits of depth d need size $\Omega(e^{n^{\frac{1}{d-1}}})$ to compute $\mathrm{MOD}_2(x_1, \ldots, x_n)$ (Håstad '87)

Is also the converse true?

A conjecture about CC-circuits

$\{\mathrm{NEG}, \mathrm{AND}, \mathrm{OR}\}$-circuits of depth d need size $\Omega(e^{n^{\frac{1}{d-1}}})$ to compute $\mathrm{MOD}_2(x_1, \ldots, x_n)$ (Håstad '87)

Is also the converse true?

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

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

A conjecture about CC-circuits

$\{\mathrm{NEG}, \mathrm{AND}, \mathrm{OR}\}$-circuits of depth d need size $\Omega(e^{n^{\frac{1}{d-1}}})$ to compute $\mathrm{MOD}_2(x_1, \ldots, x_n)$ (Håstad '87)

Is also the converse true?

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

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

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

A conjecture about CC-circuits

$\{\mathrm{NEG}, \mathrm{AND}, \mathrm{OR}\}$-circuits of depth d need size $\Omega(e^{n^{\frac{1}{d-1}}})$ to compute $\mathrm{MOD}_2(x_1, \ldots, x_n)$ (Håstad '87)

Is also the converse true?

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

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

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

A conjecture about CC-circuits

$\{\text{NEG}, \text{AND}, \text{OR}\}$-circuits of depth d need size $\Omega(e^{n^{\frac{1}{d-1}}})$ to compute $\text{MOD}_2(x_1, \ldots, x_n)$ (Håstad '87)

Is also the converse true?

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

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

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

A conjecture about CC-circuits

$\{\text{NEG}, \text{AND}, \text{OR}\}$-circuits of depth d need size $\Omega(e^{n^{\frac{1}{d-1}}})$ to compute $\text{MOD}_2(x_1, \ldots, x_n)$ (Håstad '87)

Is also the converse true?

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

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

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

A conjecture about CC-circuits

$\{\text{NEG}, \text{AND}, \text{OR}\}$-circuits of depth d need size $\Omega(e^{n^{\frac{1}{d-1}}})$ to compute $\text{MOD}_2(x_1, \ldots, x_n)$ (Håstad '87)

Is also the converse true?

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

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

- If p prime, $CC[p^k]$-circuits of depth d *cannot* compute AND of arity $\geq C(d)$ (BST '90)
- Otherwise they do (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)

Nilpotent algebras

The structure of nilpotent algebras

$\mathbf{A} = (A; f_1, \ldots, f_k)$ finite algebra
Polynomials of $\mathbf{A}$: $t(x_1, \ldots, x_n, a_1, \ldots, a_k)$: t term of $\mathbf{A}$, $a_i \in A$

The structure of nilpotent algebras

$\mathbf{A} = (A; f_1, \ldots, f_k)$ finite algebra
Polynomials of $\mathbf{A}$: $t(x_1, \ldots, x_n, a_1, \ldots, a_k)$: t term of $\mathbf{A}$, $a_i \in A$

Nilpotent algebras $\mathbf{A}$ are

The structure of nilpotent algebras

$\mathbf{A} = (A; f_1, \ldots, f_k)$ finite algebra
Polynomials of $\mathbf{A}$: $t(x_1, \ldots, x_n, a_1, \ldots, a_k)$: t term of $\mathbf{A}$, $a_i \in A$

Nilpotent algebras $\mathbf{A}$ are

- in general defined by "term condition" on congruences.

The structure of nilpotent algebras

$\mathbf{A} = (A; f_1, \ldots, f_k)$ finite algebra
Polynomials of $\mathbf{A}$: $t(x_1, \ldots, x_n, a_1, \ldots, a_k)$: t term of $\mathbf{A}$, $a_i \in A$

Nilpotent algebras $\mathbf{A}$ are

- in general defined by "term condition" on congruences.

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

The structure of nilpotent algebras

$\mathbf{A} = (A; f_1, \ldots, f_k)$ finite algebra
Polynomials of $\mathbf{A}$: $t(x_1, \ldots, x_n, a_1, \ldots, a_k)$: t term of $\mathbf{A}$, $a_i \in A$

Nilpotent algebras **A** are

- in general defined by "term condition" on congruences.

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

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

The structure of nilpotent algebras

$\mathbf{A} = (A; f_1, \ldots, f_k)$ finite algebra
Polynomials of $\mathbf{A}$: $t(x_1, \ldots, x_n, a_1, \ldots, a_k)$: t term of $\mathbf{A}$, $a_i \in A$

Nilpotent algebras $\mathbf{A}$ are

- in general defined by "term condition" on congruences.

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, $A = L \times U$:

The structure of nilpotent algebras

$\mathbf{A} = (A; f_1, \ldots, f_k)$ finite algebra
Polynomials of $\mathbf{A}$: $t(x_1, \ldots, x_n, a_1, \ldots, a_k)$: t term of $\mathbf{A}$, $a_i \in A$

Nilpotent algebras $\mathbf{A}$ are

- in general defined by "term condition" on congruences.

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, $A = L \times U$:

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

The structure of nilpotent algebras

$\mathbf{A} = (A; f_1, \ldots, f_k)$ finite algebra
Polynomials of $\mathbf{A}$: $t(x_1, \ldots, x_n, a_1, \ldots, a_k)$: t term of $\mathbf{A}$, $a_i \in A$

Nilpotent algebras $\mathbf{A}$ are

- in general defined by "term condition" on congruences.

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, $A = L \times U$:

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

Also true for polynomials of $\mathbf{A}$

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

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

Example: Extended abelian groups

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

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

A is 2-nilpotent. Polynomial e.g.:

Example: Extended abelian groups

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

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

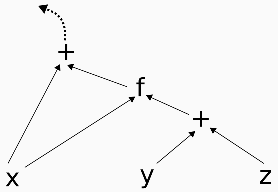
$\mathbf{A}$ is 2-nilpotent. Polynomial e.g.:
$x + f(x, y + z) = (x_1 + \hat{f}(x_2, y_2 + z_2), x_2)$

Example: Extended abelian groups

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

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

$\mathbf{A}$ 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

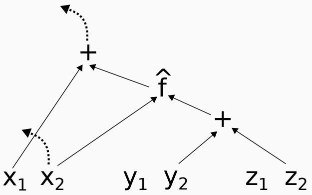


Example: Extended abelian groups

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

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

$\mathbf{A}$ 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



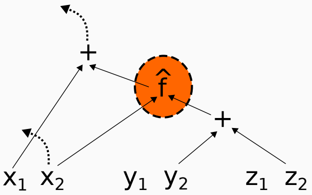
Example: Extended abelian groups

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

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

$\mathbf{A}$ 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

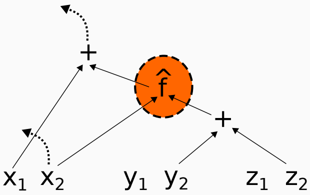


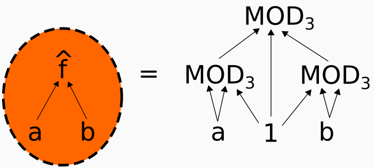
Example: Extended abelian groups

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

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

$\mathbf{A}$ 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



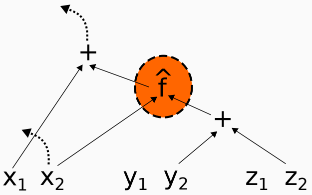


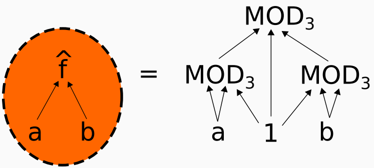
Example: Extended abelian groups

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

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

$\mathbf{A}$ 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





$\Rightarrow$ polynomials of $\mathbf{A}$ can be rewritten in p-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 $\mathbf{A}$ 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.

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 $\mathbf{A}$ 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.

$\rightarrow$ 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)

- 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)

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

Consequences

Conjecture (*) in nilpotent algebras

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

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

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

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: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ polynomials

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

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

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

INPUT: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ polynomials

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: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ polynomials

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

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

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

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: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ polynomials

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

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

Question

What is the complexity for nilpotent $\mathbf{A}$?

Circuit equivalence

Observation 1 (MK '19)

Assume (**) holds for **A** nilpotent.
Then CEQV(**A**) and CSAT(**A**) can be solved in $\mathcal{O}(n^{\log(n)})$.

Proof sketch:

Circuit equivalence

Observation 1 (MK '19)

Assume (**) holds for $\mathbf{A}$ nilpotent.
Then CEQV($\mathbf{A}$) and CSAT($\mathbf{A}$) can be solved in $\mathcal{O}(n^{\log(n)})$.

Proof sketch:

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

Circuit equivalence

Observation 1 (MK '19)

Assume (**) holds for $\mathbf{A}$ nilpotent.
Then CEQV($\mathbf{A}$) and CSAT($\mathbf{A}$) can be solved in $\mathcal{O}(n^{\log(n)})$.

Proof sketch:

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

Circuit equivalence

Observation 1 (MK '19)

Assume (**) holds for **A** nilpotent.
Then CEQV(**A**) and CSAT(**A**) can be solved in $\mathcal{O}(n^{\log(n)})$.

Proof sketch:

- Let $q(\bar{x}) \approx 0$ be an input to CEQV(**A**).
- Assume $\exists \bar{a} : q(\bar{a}) \neq 0$.
- 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 (**) holds for $\mathbf{A}$ nilpotent.
Then CEQV($\mathbf{A}$) and CSAT($\mathbf{A}$) can be solved in $\mathcal{O}(n^{\log(n)})$.

Proof sketch:

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

Circuit equivalence

Observation 1 (MK '19)

Assume (**) holds for $\mathbf{A}$ nilpotent.
Then CEQV($\mathbf{A}$) and CSAT($\mathbf{A}$) can be solved in $\mathcal{O}(n^{\log(n)})$.

Proof sketch:

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

Circuit equivalence

Observation 1 (MK '19)

Assume (**) holds for $\mathbf{A}$ nilpotent.
Then CEQV($\mathbf{A}$) and CSAT($\mathbf{A}$) can be solved in $\mathcal{O}(n^{\log(n)})$.

Proof sketch:

- Let $q(\bar{x}) \approx 0$ be an input to CEQV($\mathbf{A}$).
- Assume $\exists \bar{a} : q(\bar{a}) \neq 0$.
- Take $\bar{a}$ with minimal number k of $a_i \neq 0$, wlog. $\bar{a} = (a_1, \ldots, a_k, 0, \ldots, 0)$
- Then $t(x_1, \ldots, x_k) = q(x_1, \ldots, x_k, 0, 0, \ldots, 0)$ is 0-absorbing.
- $(**) \Rightarrow k \leq \log(|q|)$
- evaluate q at all tuples with 'support' $\log(|q|)$ in time $\mathcal{O}(|q|^{\log(|q|)})$

Circuit equivalence

Observation 1 (MK '19)

Assume (**) holds for **A** nilpotent.
Then CEQV(**A**) and CSAT(**A**) can be solved in $\mathcal{O}(n^{\log(n)})$.

Proof sketch:

- Let $q(\bar{x}) \approx 0$ be an input to CEQV(**A**).
- Assume $\exists \bar{a} : q(\bar{a}) \neq 0$.
- Take $\bar{a}$ with minimal number k of $a_i \neq 0$, wlog.
  $\bar{a} = (a_1, \ldots, a_k, 0, \ldots, 0)$
- Then $t(x_1, \ldots, x_k) = q(x_1, \ldots, x_k, 0, 0, \ldots, 0)$ is 0-absorbing.
- $(**) \Rightarrow k \leq \log(|q|)$
- evaluate q at all tuples with 'support' $\log(|q|)$ in time $\mathcal{O}(|q|^{\log(|q|)})$

Note that for $|A| = p^j$: $k \leq const$
$\Rightarrow$ polynomial time algorithm. **(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,
- computing AND,

On the contrary

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

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

On the contrary

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

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

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,
- computing AND,
- *enumerable* in polynomial time.

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.

On the contrary

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

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

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! $\exists$ 2-nilpotent algebras $\mathbf{A}$ such that CEQV($\mathbf{A}$) $\in$ P, but not with 'testing' algorithm. (**Idziak, Kawałek, Krzaczkowski; MK, 18**)

Thank you!