# Violating Constant Degree Hypothesis Requires Breaking Symmetry

Piotr Kawałek & Armin Weiß

TU Wien, University of Stuttgart

STACS, 6 March 2025

European Research Council
Established by the European Commission

ERC Synergy Grant POCOCOP (GA 101071674)

# Circuit complexity

Language $L$ is in the complexity class $P/\text{poly}$ iff there is an infinite family of circuits (with one output wire)

$$C_1, C_2, C_3, \dots$$

such that:

1. $C_n$ has $n$ inputs and accepts (only) words of length $n$ of $L$
2. $C_n$ is of size $O(\text{poly}(n))$
3. $C_n$ computes over $\{0, 1\}$ and is built of gates $\wedge, \vee, \neg$.

# Circuit complexity

Language $L$ is in the complexity class $P/\text{poly}$ iff there is an infinite family of circuits (with one output wire)

$$C_1, C_2, C_3, \ldots$$

such that:

1. $C_n$ has $n$ inputs and accepts (only) words of length $n$ of $L$
2. $C_n$ is of size $O(\text{poly}(n))$
3. $C_n$ computes over $\{0, 1\}$ and is built of gates $\wedge, \vee, \neg$.

**Fact 1:** $P \subseteq P/\text{poly}$,

# Circuit complexity

Language $L$ is in the complexity class $P/\text{poly}$ iff there is an infinite family of circuits (with one output wire)

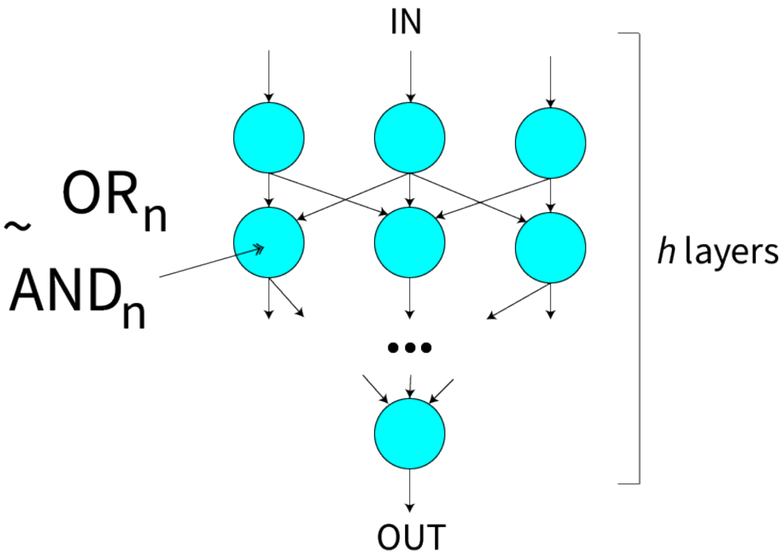
$$C_1, C_2, C_3, \ldots$$

such that:

1. $C_n$ has $n$ inputs and accepts (only) words of length $n$ of $L$
2. $C_n$ is of size $O(\text{poly}(n))$
3. $C_n$ computes over $\{0, 1\}$ and is built of gates $\wedge, \vee, \neg$.

**Fact 1:** $P \subseteq P/\text{poly}$,
**Fact 2:** $NP \subsetneq P/\text{poly} \implies P \neq NP$.

# $AC^0$-circuits



# Lower bounds we know

**Question 1:** Can we perform addition modulo 2 with small bounded-depth $\mathrm{AC}^0$-circuits?

# Lower bounds we know

**Question 1:** Can we perform addition modulo 2 with small bounded-depth $\mathrm{AC}^0$-circuits?

**Håstad'86:** $\mathrm{AC}^0$-circuits of height $h$ require size $2^{\Omega(n^{1/(h-1)})}$ to compute $\mathrm{PARITY}$.

**Note 1:** Lower bound perfectly matches the naive contruction.

# Lower bounds we know

**Question 1:** Can we perform addition modulo 2 with small bounded-depth $\mathrm{AC}^0$-circuits?

**Håstad'86:** $\mathrm{AC}^0$-circuits of height $h$ require size $2^{\Omega(n^{1/(h-1)})}$ to compute $\mathrm{PARITY}$.

**Note 1:** Lower bound perfectly matches the naive contruction.

**Note 2:** The same lower bound holds if we replace parity with arbitrary $\mathrm{MOD}_m$ function (by the very same proof).

# Lower bounds we know

**Question 1:** Can we perform addition modulo 2 with small bounded-depth $\mathrm{AC}^0$-circuits?

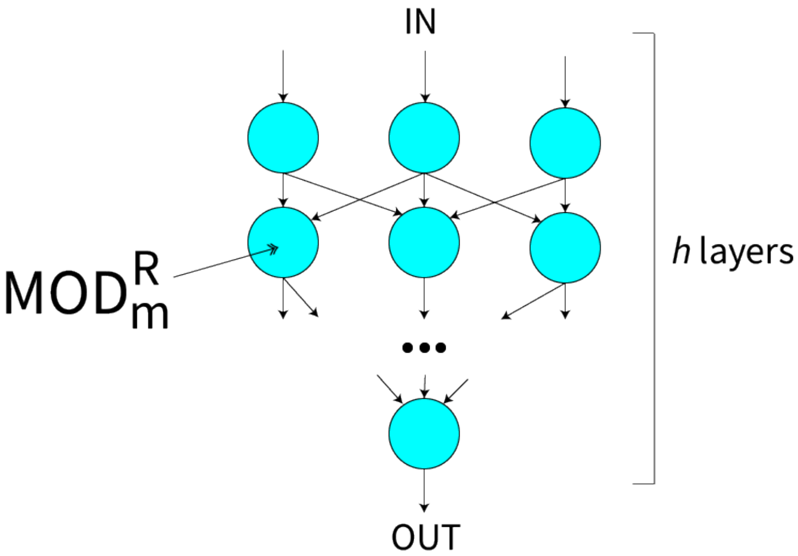
**Håstad'86:** $\mathrm{AC}^0$-circuits of height $h$ require size $2^{\Omega(n^{1/(h-1)})}$ to compute $\mathrm{PARITY}$.

**Note 1:** Lower bound perfectly matches the naive contruction.

**Note 2:** The same lower bound holds if we replace parity with arbitrary $\mathrm{MOD}_m$ function (by the very same proof).

**Dual question:** Can we represent Boolean operations like $\mathrm{AND}_n$ with small modulo counting circuits on bounded depth?

# $CC^0$-circuits



# Constructions

**Fact 1:** $\mathrm{CC}_h[p]$-circuits can encode only bounded arity *AND*.

# Constructions

**Fact 1:** $\mathrm{CC}_h[p]$-circuits can encode only bounded arity *AND*.

**Fact 2:** $\mathrm{MOD}_q \circ \mathrm{MOD}_p$-circuits can encode any function (for $p \neq q$). $\mathrm{AND}_n$ can be constructructed in size $O(p^n)$.

# Constructions

**Fact 1:** $\mathrm{CC}_h[p]$-circuits can encode only bounded arity *AND*.

**Fact 2:** $\mathrm{MOD}_q \circ \mathrm{MOD}_p$-circuits can encode any function (for $p \neq q$). $\mathrm{AND}_n$ can be constructructed in size $O(p^n)$.

**BBR'94:** $CC_3[m]$-circuits can encode $\mathrm{AND}_n$ in size $2^{O(n^{1/r})}$, where $r$ is the number of prime divisors of $m$.

# Constructions

**Fact 1:** $\mathrm{CC}_h[p]$-circuits can encode only bounded arity *AND*.

**Fact 2:** $\mathrm{MOD}_q \circ \mathrm{MOD}_p$-circuits can encode any function (for $p \neq q$). $\mathrm{AND}_n$ can be constructructed in size $O(p^n)$.

**BBR'94:** $CC_3[m]$-circuits can encode $\mathrm{AND}_n$ in size $2^{O(n^{1/r})}$, where $r$ is the number of prime divisors of $m$.

Smart recursive application of the above construction gives a $\mathrm{CC}_h[m]$- representation of $\mathrm{AND}_n$ of size

$$\approx 2^{O(n^{1/(h-1)r})}$$

(Idziak, Kawałek, Krzaczkowski'22, Chapman, Williams'22)

# Lower bounds

**We know almost nothing!** Only slightly superlinear lower bounds are known (for $\mathrm{CC}_h[m]$-circuit computing $\mathrm{AND}_n$) and only for the number of wires (Chattopadhyay et al. FOCS'06).

# Lower bounds

**We know almost nothing!** Only slightly superlinear lower bounds are known (for $\mathrm{CC}_h[m]$-circuit computing $\mathrm{AND}_n$) and only for the number of wires (Chattopadhyay et al. FOCS'06).

**Fact:** We know that $\mathrm{MOD}_q \circ \mathrm{MOD}_m$ circuits computing $\mathrm{AND}_n$ need size $\Omega(c^n)$ (Barrington, Straubing, Thérien'90).

# Lower bounds

**We know almost nothing!** Only slightly superlinear lower bounds are known (for $\mathrm{CC}_h[m]$-circuit computing $\mathrm{AND}_n$) and only for the number of wires (Chattopadhyay et al. FOCS'06).

**Fact:** We know that $\mathrm{MOD}_q \circ \mathrm{MOD}_m$ circuits computing $\mathrm{AND}_n$ need size $\Omega(c^n)$ (Barrington, Straubing, Thérien'90).

In particular we do not know:

1. much about $\mathrm{MOD}_6 \circ \mathrm{MOD}_6$-circuits,

# Lower bounds

**We know almost nothing!** Only slightly superlinear lower bounds are known (for $\mathrm{CC}_h[m]$-circuit computing $\mathrm{AND}_n$) and only for the number of wires (Chattopadhyay et al. FOCS'06).

**Fact:** We know that $\mathrm{MOD}_q \circ \mathrm{MOD}_m$ circuits computing $\mathrm{AND}_n$ need size $\Omega(c^n)$ (Barrington, Straubing, Thérien'90).

In particular we do not know:

1. much about $\mathrm{MOD}_6 \circ \mathrm{MOD}_6$-circuits,
2. much about $\mathrm{MOD}_{q \cdot r} \circ \mathrm{MOD}_p$-circuits, for 3 different primes $p, q, r$,

# Lower bounds

**We know almost nothing!** Only slightly superlinear lower bounds are known (for $\mathrm{CC}_h[m]$-circuit computing $\mathrm{AND}_n$) and only for the number of wires (Chattopadhyay et al. FOCS'06).

**Fact:** We know that $\mathrm{MOD}_q \circ \mathrm{MOD}_m$ circuits computing $\mathrm{AND}_n$ need size $\Omega(c^n)$ (Barrington, Straubing, Thérien'90).

In particular we do not know:

1. much about $\mathrm{MOD}_6 \circ \mathrm{MOD}_6$-circuits,
2. much about $\mathrm{MOD}_{q \cdot r} \circ \mathrm{MOD}_p$-circuits, for 3 different primes $p, q, r$,
3. much about $\mathrm{MOD}_q \circ \mathrm{MOD}_p \circ \mathrm{AND}_d$-circuits.

# Lower bounds

**We know almost nothing!** Only slightly superlinear lower bounds are known (for $\mathrm{CC}_h[m]$-circuit computing $\mathrm{AND}_n$) and only for the number of wires (Chattopadhyay et al. FOCS'06).

**Fact:** We know that $\mathrm{MOD}_q \circ \mathrm{MOD}_m$ circuits computing $\mathrm{AND}_n$ need size $\Omega(c^n)$ (Barrington, Straubing, Thérien'90).

In particular we do not know:

1. much about $\mathrm{MOD}_6 \circ \mathrm{MOD}_6$-circuits,
2. much about $\mathrm{MOD}_{q \cdot r} \circ \mathrm{MOD}_p$-circuits, for 3 different primes $p, q, r$,
3. much about $\mathrm{MOD}_q \circ \mathrm{MOD}_p \circ \mathrm{AND}_d$-circuits.

**It is consistent with our knowledge that all this kinds of circuits can solve NP-complete problems in polynomial size!**

# Constant Degree Hypothesis

**Conjecture by**
**Barrington, Straubing, Thérien 1990**

There is an absolute constant $c > 0$
such that any $\mathrm{MOD}_q \circ \mathrm{MOD}_m \circ \mathrm{AND}_d$
circuit computing $\mathrm{AND}_n$
requires size at least $\Omega(c^n)$.

**Here:** $q$ is a prime number, $m$ is an integer, $d$ is a fixed constant (i.e. d=2), $n$ is a (large) integer.

# Constant Degree Hypothesis

**Conjecture by**
**Barrington, Straubing, Thérien 1990**

There is an absolute constant $c > 0$
such that any $\mathrm{MOD}_q \circ \mathrm{MOD}_p \circ \mathrm{AND}_d$
circuit computing $\mathrm{AND}_n$
requires size at least $\Omega(c^n)$.

**Here:** $q$ is a prime number, $p$ is a prime, $d$ is a fixed constant (i.e. d=2), $n$ is a (large) integer.

# Polynomial Equivalence Problem

$\textsc{PolEqv}(\mathbf{G})$ - on the input we get an equation, i.e. two expressions over $G$

$$\mathbf{e}_1(x_1, \ldots, x_n) = \mathbf{e}_2(x_1, \ldots, x_n)$$

and we want to check that it is an identity, i.e. it is satisfied for all $(x_1, x_2, \ldots, x_n) \in G^n$.

# Polynomial Equivalence Problem

$\textsc{PolEqv}(\mathbf{G})$ - on the input we get an equation, i.e. two expressions over $G$

$$\mathbf{e}_1(x_1, \ldots, x_n) = \mathbf{e}_2(x_1, \ldots, x_n)$$

and we want to check that it is an identity, i.e. it is satisfied for all $(x_1, x_2, \ldots, x_n) \in G^n$.

**Example 1:** $x + y = y + x$ and $x + x + x = 0$ are identities in $\mathbb{Z}_3$. .

# Polynomial Equivalence Problem

$\textsc{PolEqv}(\mathbf{G})$ - on the input we get an equation, i.e. two expressions over $G$

$$\mathbf{e}_1(x_1, \dots, x_n) = \mathbf{e}_2(x_1, \dots, x_n)$$

and we want to check that it is an identity, i.e. it is satisfied for all $(x_1, x_2, \dots, x_n) \in G^n$.

**Example 1:** $x + y = y + x$ and $x + x + x = 0$ are identities in $\mathbb{Z}_3$. .

**Example 2:** $xy = yx$ is not an identity in $\mathbf{D}_5$.
What about $(xy)^{-1}yxzx^{-1} = (zxy^{-1})^{-1}xy$?

# Relating $\textsc{PolEqv}$ to CDH

**Theorem (Idziak, PK, Krzaczkowski, Weiß, ICALP'22)**

For a finite group $\mathbf{G}$ the problem $\textsc{PolEqv}(\mathbf{G})$ is

1. co-NP-complete when $\mathbf{G}$ is nonsolvable,
2. not in P (RP) when $\mathbf{G}$ has supernilpotent rank $\geqslant 3$ assuming ETH (rETH),
3. in RP when $\mathbf{G}$ has supernilpotent rank $= 2$ assuming Constant Degree Hypothesis.

# Relating $\textsc{PolEqv}$ to CDH

**Theorem (Idziak, PK, Krzaczkowski, Weiß, ICALP'22)**

For a finite group $\mathbf{G}$ the problem $\textsc{PolEqv}(\mathbf{G})$ is

1. co-NP-complete when $\mathbf{G}$ is nonsolvable,
2. not in P (RP) when $\mathbf{G}$ has supernilpotent rank $\geqslant 3$ assuming ETH (rETH),
3. in RP when $\mathbf{G}$ has supernilpotent rank $= 2$ assuming Constant Degree Hypothesis.

CDH holds iff
$\textsc{PolEqv}(\mathbf{G})$ is in RP for all the groups $\mathbf{G}$
with supernilpotent rank $= 2$ (unless rETH fails).

# Rewriting expressions to circuits

The reason for this 3 cases is:

1. expressions over nonsolvable group can "interpret" any $NC^1$ circuits, so we get co-NP-complete equivalence here.
2. expressions over supernilpotent rank 3 groups can "interpret" some height 3 $\mathrm{CC}$-circuits, which enables subexpotential encoding of $\mathrm{AND}_n$, and in turn subexpotential encoding of 3-CNF forumlas.
3. expressions over supernilpotent rank 2 groups can be rewritten to $\mathrm{MOD}_q \circ \mathrm{MOD}_m \circ \mathrm{AND}_d$ circuits.

# Constant Degree Hypothesis

**Conjecture by**
**Barrington, Straubing, Thérien 1990**

There is an absolute constant $c > 0$
such that any $\mathrm{MOD}_q \circ \mathrm{MOD}_p \circ \mathrm{AND}_d$
circuit computing $\mathrm{AND}_n$
requires size at least $\Omega(c^n)$.

**Here:** $q$ is a prime number, $p$ is a prime, $d$ is a fixed constant (i.e. d=2), $n$ is a (large) integer.

# Prior work

**Grolmusz, Tardos 2000**

$\mathrm{MOD}_q \circ \mathrm{MOD}_p \circ \mathrm{AND}_d$ - circuit computing $\mathrm{AND}_n$ requires size $\Omega(c^n)$ for some absolute constant $c$, **when the number of $\mathrm{AND}_d$ gates wired to one $\mathrm{MOD}_p$ gate is at most $o(n^2/\log n)$.**

# Prior work

**Grolmusz, Tardos 2000**

$\mathrm{MOD}_q \circ \mathrm{MOD}_p \circ \mathrm{AND}_d$ - circuit computing $\mathrm{AND}_n$ requires size $\Omega(c^n)$ for some absolute constant $c$, **when the number of AND$_d$ gates wired to one MOD$_p$ gate is at most $o(n^2/\log n)$.**

**Grolmusz, Tardos 2000; Straubing, Thérien 2000**

The only symmetric functions computed by $\mathrm{MOD}_q \circ \mathrm{MOD}_p$ - circuits of size $s$ have period $p \cdot q^k$, where $q^k \in \Theta(\log s)$.

# Prior work

## Grolmusz, Tardos 2000

$\mathrm{MOD}_q \circ \mathrm{MOD}_p \circ \mathrm{AND}_d$ - circuit computing $\mathrm{AND}_n$ requires size $\Omega(c^n)$ for some absolute constant $c$, **when the number of AND$_d$ gates wired to one MOD$_p$ gate is at most $o(n^2/\log n)$.**

## Grolmusz, Tardos 2000; Straubing, Thérien 2000

The only symmetric functions computed by $\mathrm{MOD}_q \circ \mathrm{MOD}_p$ - circuits of size $s$ have period $p \cdot q^k$, where $q^k \in \Theta(\log s)$.

**Corollary:** as $\mathrm{AND}_n$ function has no nontrivial periods it must have a large symmetric representation.

# Periods of symmetric functions

If function $f : \{0,1\}^n \longrightarrow \{0,1\}$ is symmetric we can define

$$f(k) := f(1^k\ 0^{n-k})$$

period of $f$ is any integer $r$ with $0 \leqslant r \leqslant n-1$ and

$$f(k) = f(k+r)$$

for all $k$ satisfying $0 \leqslant k \leqslant n-r$.

# Constant Degree Hypothesis

**Theorem**

There is an absolute constant $c > 0$
such that any **symmetric** $\mathrm{MOD}_q \circ \mathrm{MOD}_p \circ \mathrm{AND}_d$
circuit computing $\mathrm{AND}_n$
requires size at least $\Omega(c^n)$.

**Here:** $p, q$ are prime numbers, $d$ is a fixed constant (i.e. d=2), $n$ is a (large) integer.

# Why symmetric?

Two reasons to consider symmetric circuits here:

1. It is natural to believe that optimal representation of a symmetric function is symmetric (or close to symmetric).

# Why symmetric?

Two reasons to consider symmetric circuits here:

1. It is natural to believe that optimal representation of a symmetric function is symmetric (or close to symmetric).
2. Surprising Barrington et. al. construction of $CC_3[m]$ circuits for $\mathrm{AND}_n$ produces symmetric circuits.

# Symmetric circuits are periodic

**PK, Armin Weiß, 2025**

Let $p$ and $q$ be primes and $n \geqslant 13$ and let $1 \leqslant d \leqslant n$.
Then any function computed by an $n$-input symmetric $\mathrm{MOD}_q \circ \mathrm{MOD}_p \circ \mathrm{AND}_d$ circuit of size $s < 2^{n/9}$ has a period $p^{k_p} q^{k_q}$ given that $p^{k_p} > d$ and $q^{k_q} > \log s + 1$.

# Symmetric circuits are periodic

**PK, Armin Weiß, 2025**

Let $p$ and $q$ be primes and $n \geqslant 13$ and let $1 \leqslant d \leqslant n$.
Then any function computed by an $n$-input symmetric $\mathrm{MOD}_q \circ \mathrm{MOD}_p \circ \mathrm{AND}_d$ circuit of size $s < 2^{n/9}$ has a period $p^{k_p} q^{k_q}$ given that $p^{k_p} > d$ and $q^{k_q} > \log s + 1$.

**Corollary:** as $\mathrm{AND}_n$ function has no nontrivial periods it must have a large symmetric representation.

# Symmetric circuits are periodic

**PK, Armin Weiß, 2025**

Let $p$ and $q$ be primes and $n \geqslant 13$ and let $1 \leqslant d \leqslant n$.
Then any function computed by an $n$-input symmetric $\mathrm{MOD}_q \circ \mathrm{MOD}_p \circ \mathrm{AND}_d$ circuit of size $s < 2^{n/9}$ has a period $p^{k_p} q^{k_q}$ given that $p^{k_p} > d$ and $q^{k_q} > \log s + 1$.

**Corollary:** as $\mathrm{AND}_n$ function has no nontrivial periods it must have a large symmetric representation.

**Fact:** we provide a construction matching the proven lower bounds.

# Symmetric circuits are periodic

**PK, Armin Weiß, 2025**

Let $p$ and $q$ be primes and $n \geqslant 13$ and let $1 \leqslant d \leqslant n$. Then any function computed by an $n$-input symmetric $\mathrm{MOD}_q \circ \mathrm{MOD}_p \circ \mathrm{AND}_d$ circuit of size $s < 2^{n/9}$ has a period $p^{k_p} q^{k_q}$ given that $p^{k_p} > d$ and $q^{k_q} > \log s + 1$.

**Corollary:** as $\mathrm{AND}_n$ function has no nontrivial periods it must have a large symmetric representation.

**Fact:** we provide a construction matching the proven lower bounds.

**Thank you!**