Majority is incompressible by $\mathsf{AC}^0[p]$ circuits

Igor Carboni Oliveira

Columbia University

Joint work with Rahul Santhanam (Univ. Edinburgh)

Part 1
Background, Examples, and Motivation

Basic Definitions

AC^0_d circuits: polynomial size circuits of depth $\leq d$ containing unbounded fan-in AND, OR, NOT gates.

size = number of wires.

Basic Definitions

AC_d^0 circuits: polynomial size circuits of depth $\leq d$ containing unbounded fan-in AND, OR, NOT gates.

size = number of wires.

$\mathrm{AC}_d^0[p]$ circuits: allow mod_p gates in the previous model (p prime). We have $\mathrm{mod}_p(z_1, \ldots, z_m) = 1$ if and only if $p \mid \sum_j z_j$.

Basic Definitions

AC^0_d circuits: polynomial size circuits of depth $\leq d$ containing unbounded fan-in AND, OR, NOT gates.

size = number of wires.

$\mathrm{AC}^0_d[p]$ circuits: allow mod_p gates in the previous model (p prime).
We have $\mathrm{mod}_p(z_1, \ldots, z_m) = 1$ if and only if $p \mid \sum_j z_j$.

$\mathrm{Majority} = \{\mathrm{Majority}_n\}_{n \in \mathbb{N}}$, where $\mathrm{Majority}_n \colon \{0,1\}^n \to \{0,1\}$.

$\mathrm{Majority}_n(x_1, \ldots, x_n) = 1$ if and only if $\sum_i x_i \geq n/2$.

Basic Results

Razborov/Smolensky (1987).
If Majority is computed by $\mathrm{AC}^0_d[p]$ circuits then $d = \Omega(\log n / \log\log n)$.

Basic Results

Razborov/Smolensky (1987).
If Majority is computed by $AC^0_d[p]$ circuits then $d = \Omega(\log n / \log\log n)$.

This lower bound is optimal.

No explicit lower bounds for poly size circuits beyond depth $\log n / \log\log n$.

Basic Results

Razborov/Smolensky (1987).
If Majority is computed by $\mathrm{AC}^0_d[p]$ circuits then $d = \Omega(\log n / \log\log n)$.

This lower bound is optimal.

No explicit lower bounds for poly size circuits beyond depth $\log n / \log\log n$.

Technique does not generalize to modulo m gates, where $m = p \cdot q$.

As far as we know, it is possible that $\mathrm{NP} \subseteq \mathrm{AC}^0_3[6]$ (linear size).

This Talk

Understand structure of polynomial-size circuits with mod p gates computing **Majority.**

This Talk

Understand structure of polynomial-size circuits with mod p gates computing **Majority**.

Follows from the investigation of more general framework: "Interactive Compression Games".

Hybridizes computational complexity and communication complexity.

Example: Boolean circuits for symmetric functions

Idea. Boolean circuits can process $\log n$ bits very efficiently.
Every $f\colon \{0,1\}^{\log n} \to \{0,1\}$ computed by CNF/DNF of size n.

Circuit for $\text{Majority}_n(x)$. Computes $O(\log n)$-bit string counting #1's in x.

Example: Boolean circuits for symmetric functions

Idea. Boolean circuits can process $\log n$ bits very efficiently.
Every $f\colon \{0,1\}^{\log n} \to \{0,1\}$ computed by CNF/DNF of size n.

Circuit for $\text{Majority}_n(x)$. Computes $O(\log n)$-bit string counting #1's in x.

Partition input bits into $(\log n)$-bit blocks, produce $(\log\log n)$-bit strings from each block.

Example: Boolean circuits for symmetric functions

Idea. Boolean circuits can process $\log n$ bits very efficiently.
Every $f\colon \{0,1\}^{\log n} \to \{0,1\}$ computed by CNF/DNF of size n.

Circuit for $\text{Majority}_n(x)$. Computes $O(\log n)$-bit string counting #1's in x.

Partition input bits into $(\log n)$-bit blocks, produce $(\log \log n)$-bit strings from each block.

In each layer, reduces number of strings by a factor of roughly $\log n$.

Example: Boolean circuits for symmetric functions

Lemma. For every $d \geq 1$, we obtain an AC_d^0 circuit with $n/(\log n)^{(d-1)-o(1)}$ output wires encoding #1's in x.

n input bits processed in $O(\log_{\log n} n) = O(\log n / \log\log n)$ stages.

Example: Boolean circuits for symmetric functions

Lemma. For every $d \geq 1$, we obtain an AC^0_d circuit with $n/(\log n)^{(d-1)-o(1)}$ output wires encoding #1's in x.

n input bits processed in $O(\log_{\log n} n) = O(\log n/\log\log n)$ stages.

We will revisit this construction later in the talk.

Interactive Compression Games (Chattopadhyay and Santhanam, 2012)

Fix a circuit class $\mathcal{C}$ and a Boolean function f.
We define a communication game between Alice and Bob.

Alice knows the input $x \in \{0,1\}^n$, but her computations are limited to $\mathcal{C}$.

Bob is computationally unbounded, but has no access to x.

Interactive Compression Games (Chattopadhyay and Santhanam, 2012)

Fix a circuit class $\mathcal{C}$ and a Boolean function f.
We define a communication game between Alice and Bob.

Alice knows the input $x \in \{0, 1\}^n$, but her computations are limited to $\mathcal{C}$.

Bob is computationally unbounded, but has no access to x.

Goal:

Players must interact in order to compute $f(x)$.
Minimize total number of bits sent by Alice.

Interactive Compression Games (Chattopadhyay and Santhanam, 2012)

Fix a circuit class $\mathcal{C}$ and a Boolean function f.
We define a communication game between Alice and Bob.

Alice knows the input $x \in \{0,1\}^n$, but her computations are limited to $\mathcal{C}$.

Bob is computationally unbounded, but has no access to x.

Goal:

Players must interact in order to compute $f(x)$.
Minimize total number of bits sent by Alice.

$f \notin \mathcal{C} \iff$ $\mathcal{C}$**-compression game for** f **is nontrivial.**

Interactive Compression Games

Formally:

A $\mathcal{C}$-bounded protocol $\Pi_n = \langle C^{(1)}, \ldots, C^{(r)}, f^{(1)}, \ldots, f^{(r-1)}, E_n \rangle$ with $r = r(n)$ rounds consists of a sequence of $\mathcal{C}$-circuits for Alice, a strategy for Bob, given by functions $f^{(1)}, \ldots, f^{(r-1)}$, and a set of accepting transcripts E_n.

Interactive Compression Games

Formally:

A $\mathcal{C}$-bounded protocol $\Pi_n = \langle C^{(1)}, \ldots, C^{(r)}, f^{(1)}, \ldots, f^{(r-1)}, E_n \rangle$ with $r = r(n)$ rounds consists of a sequence of $\mathcal{C}$-circuits for Alice, a strategy for Bob, given by functions $f^{(1)}, \ldots, f^{(r-1)}$, and a set of accepting transcripts E_n.

Every protocol Π_n has its signature$(\Pi_n) = (n, s_1, t_1, s_2, \ldots, t_{r-1}, s_r)$, which is the sequence corresponding to the input size $n = |x|$ and the length of the messages exchanged by Alice and Bob during the protocol.

Interactive Compression Games

Formally:
A $\mathcal{C}$-bounded protocol $\Pi_n = \langle C^{(1)}, \ldots, C^{(r)}, f^{(1)}, \ldots, f^{(r-1)}, E_n \rangle$ with $r = r(n)$ rounds consists of a sequence of $\mathcal{C}$-circuits for Alice, a strategy for Bob, given by functions $f^{(1)}, \ldots, f^{(r-1)}$, and a set of accepting transcripts E_n.

Every protocol Π_n has its signature$(\Pi_n) = (n, s_1, t_1, s_2, \ldots, t_{r-1}, s_r)$, which is the sequence corresponding to the input size $n = |x|$ and the length of the messages exchanged by Alice and Bob during the protocol.

Π_n solves the compression game of a function $h_n \colon \{0,1\}^n \to \{0,1\}$ if

$$h(x) = 1 \quad \Longleftrightarrow \quad \text{transcript}_{\Pi_n}(x) \in E_n.$$

Interactive Compression Games

Formally:
A $\mathcal{C}$-bounded protocol $\Pi_n = \langle C^{(1)}, \ldots, C^{(r)}, f^{(1)}, \ldots, f^{(r-1)}, E_n \rangle$ with $r = r(n)$ rounds consists of a sequence of $\mathcal{C}$-circuits for Alice, a strategy for Bob, given by functions $f^{(1)}, \ldots, f^{(r-1)}$, and a set of accepting transcripts E_n.

Every protocol Π_n has its signature$(\Pi_n) = (n, s_1, t_1, s_2, \ldots, t_{r-1}, s_r)$, which is the sequence corresponding to the input size $n = |x|$ and the length of the messages exchanged by Alice and Bob during the protocol.

Π_n solves the compression game of a function $h_n \colon \{0,1\}^n \to \{0,1\}$ if

$$h(x) = 1 \quad \Longleftrightarrow \quad \text{transcript}_{\Pi_n}(x) \in E_n.$$

Finally, we let cost$(\Pi_n) = s_1 + \ldots + s_r$.

Previous work

Harnik and Naor, 2006. “instance compression” (1-round compression), cryptographic application.

Previous work

Harnik and Naor, 2006. "instance compression" (1-round compression), cryptographic application.

Dubrov and Ishai, 2006. Lower bound for $\mathcal{C} = \mathrm{AC}^0$, $f =$ Parity, (1-round compression). Connection with non-Boolean PRGs.

Previous work

Harnik and Naor, 2006. “instance compression” (1-round compression), cryptographic application.

Dubrov and Ishai, 2006. Lower bound for $\mathcal{C} = \mathrm{AC}^0$, $f =$ Parity, (1-round compression). Connection with non-Boolean PRGs.

Bodlaender et al., 2008. Investigates problems without polynomial kernels.

Previous work

Harnik and Naor, 2006. "instance compression" (1-round compression), cryptographic application.

Dubrov and Ishai, 2006. Lower bound for $\mathcal{C} = \mathrm{AC}^0$, $f = \text{Parity}$, (1-round compression). Connection with non-Boolean PRGs.

Bodlaender et al., 2008. Investigates problems without polynomial kernels.

Fortnow and Santhanam, 2008. conditional lower bound for instance compression.

Previous work

Dell and van Melkebeek, 2010. $\mathcal{C}$ = polynomial time, f = d-CNF SAT (conditional lower bound).

Previous work

Dell and van Melkebeek, 2010. $\mathcal{C} =$ polynomial time, $f = d$-CNF SAT (conditional lower bound).

Faust et al., 2010. Application in leakage resilient cryptography.

Previous work

Dell and van Melkebeek, 2010. $\mathcal{C} =$ polynomial time, $f = d$-CNF SAT (conditional lower bound).

Faust et al., 2010. Application in leakage resilient cryptography.

Drucker, 2012. limitations of instance compression in the classical and quantum setting (conditional).

Previous work

Dell and van Melkebeek, 2010. $\mathcal{C} =$ polynomial time, $f = d$-CNF SAT (conditional lower bound).

Faust et al., 2010. Application in leakage resilient cryptography.

Drucker, 2012. limitations of instance compression in the classical and quantum setting (conditional).

Chattopadhyay and Santhanam, 2012. Optimal lower bound for $\mathcal{C} = \mathrm{AC}^0$, $f =$ Parity. Partial results for $\mathrm{AC}^0[p]$-compression.

Applications and Motivation

Results have found applications in cryptography, parameterized complexity theory, PCPs, circuit lower bounds.

Our main motivation:

Understand information bottlenecks in circuit lower bounds.

Understand structure of optimal circuits/algorithms.

Interactive Compression versus Computation

$\text{InnerProduct}_n(x, y) \stackrel{\text{def}}{=} \sum_i x_i \cdot y_i \pmod 2$.

Threshold gate: $\sum_j w_i z_i \geq^? t, \quad w_j, t \in \mathbb{R}$.

Proposition [HMPSP'93]. InnerProduct $\notin$ poly(n)-TH $\circ$ poly(n)-TH.

Interactive Compression versus Computation

$\text{InnerProduct}_n(x, y) \stackrel{\text{def}}{=} \sum_i x_i \cdot y_i \pmod 2$.

Threshold gate: $\sum_j w_i z_i \geq^? t, \quad w_j, t \in \mathbb{R}$.

Proposition [HMPSP'93]. InnerProduct $\notin$ poly(n)-TH $\circ$ poly(n)-TH.

On the other hand,

Proposition. There exists a (poly(n)-TH $\circ$ poly(n)-TH)-compression game for InnerProduct with $O(\log n)$ rounds and communication cost $O(\log n)$.

Interactive Compression versus Computation

Protocol.
Alice's circuits are of the form $C(x, y, v)$.

(first layer) C computes $z_i \stackrel{\text{def}}{=} x_i \wedge y_i$, for every $i \in [n]$.

(second layer) C outputs $\text{sign}(\sum_{i\in[n]} z_i - \sum_{i\in[n]} v_i)$.

Idea. Bob does all the work, and simulates a binary search in order to compute $\sum_i x_i \cdot y_i$.

Interactive Compression versus Computation

Protocol.
Alice's circuits are of the form $C(x, y, v)$.

(first layer) C computes $z_i \stackrel{\text{def}}{=} x_i \wedge y_i$, for every $i \in [n]$.

(second layer) C outputs $\text{sign}(\sum_{i \in [n]} z_i - \sum_{i \in [n]} v_i)$.

Idea. Bob does all the work, and simulates a binary search in order to compute $\sum_i x_i \cdot y_i$.

Bob sends $v = 0^{n/2} 1^{n/2}$:
bit computed by Alice reveals if $\sum_{i \in [n]} x_i \cdot y_i$ is at least $n/2$.

Interactive Compression versus Computation

Protocol.
Alice's circuits are of the form $C(x, y, v)$.

(first layer) C computes $z_i \stackrel{\text{def}}{=} x_i \wedge y_i$, for every $i \in [n]$.

(second layer) C outputs $\text{sign}(\sum_{i\in[n]} z_i - \sum_{i\in[n]} v_i)$.

Idea. Bob does all the work, and simulates a binary search in order to compute $\sum_i x_i \cdot y_i$.

Bob sends $v = 0^{n/2}1^{n/2}$:
bit computed by Alice reveals if $\sum_{i\in[n]} x_i \cdot y_i$ is at least $n/2$.

Bob sends string corresponding to the next step of the binary search, and so on.

Part 2: Main Results

Main Result

Razborov/Smolensky, 1987.
"Any $\mathsf{AC}^0_d[p]$-compression game for Majority requires nontrivial communication."

Main Result

Razborov/Smolensky, 1987.
"Any $\mathsf{AC}^0_d[p]$-compression game for Majority requires nontrivial communication."

Chattophadyay and Santhanam, 2012.
Any single-round $\mathsf{AC}^0_d[p]$-compression game for Majority requires communication $\sqrt{n}/(\log n)^{O(d)}$.

Main Result

[Theorem 1]. There exists a fixed constant $c \in \mathbb{N}$ such that, for each $d \in \mathbb{N}$, and every $n \in \mathbb{N}$ sufficiently large, the following holds.

1) Any $\mathsf{AC}^0_d[p]$-compression game for $\mathsf{Majority}_n$ (any number of rounds) has communication cost $\geq n/(\log n)^{2d+c}$.

Main Result

[Theorem 1]. There exists a fixed constant $c \in \mathbb{N}$ such that, for each $d \in \mathbb{N}$, and every $n \in \mathbb{N}$ sufficiently large, the following holds.

1) Any $\mathsf{AC}^0_d[p]$-compression game for Majority_n (any number of rounds) has communication cost $\geq n/(\log n)^{2d+c}$.

2) There exists a single-round $\mathsf{AC}^0_d[p]$-compression game for Majority_n with communication cost $\leq n/(\log n)^{d-c}$.

Lower bound against circuits with oracle gates

Theorem 1 implies that structure of Boolean circuit for Majority is essentially optimal.

Lower bound against circuits with oracle gates

Theorem 1 implies that structure of Boolean circuit for Majority is essentially optimal.

Circuits with oracle gates: several applications in theoretical computer science.

Lower bound against circuits with oracle gates

Theorem 1 implies that structure of Boolean circuit for Majority is essentially optimal.

Circuits with oracle gates: several applications in theoretical computer science.

Example:

[IW'97] $\exists f \in$ EXP that requires circuits of size $2^{\Omega(n)}$ then P $=$ BPP.

[KvM'99] $\exists f \in$ NE $\cap$ coNE that requires circuits with SAT-oracles of size $2^{\Omega(n)}$ then AM $=$ NP.

Lower bound against circuits with oracle gates

Lemma. Let C be a Boolean circuit over n variables from $\mathcal{C}_d(\text{poly}(n))$ augmented with oracle gates $f_i \colon \{0,1\}^{s_i} \to \{0,1\}^{t_i}$, where $i \in [r]$, for some $r = r(n)$.

Let $s = s_1 + \ldots + s_r$ be the total fan-in of these oracle gates, and $h \colon \{0,1\}^n \to \{0,1\}$ be the Boolean function computed by C.

Then h admits a $\mathcal{C}_d(\text{poly}(n))$-compression game with communication cost $c(n) \leq s$ consisting of at most $r + 1$ rounds.

Lower bound against circuits with oracle gates

Lemma. Let C be a Boolean circuit over n variables from $\mathcal{C}_d(\mathrm{poly}(n))$ augmented with oracle gates $f_i \colon \{0,1\}^{s_i} \to \{0,1\}^{t_i}$, where $i \in [r]$, for some $r = r(n)$.

Let $s = s_1 + \ldots + s_r$ be the total fan-in of these oracle gates, and $h \colon \{0,1\}^n \to \{0,1\}$ be the Boolean function computed by C.

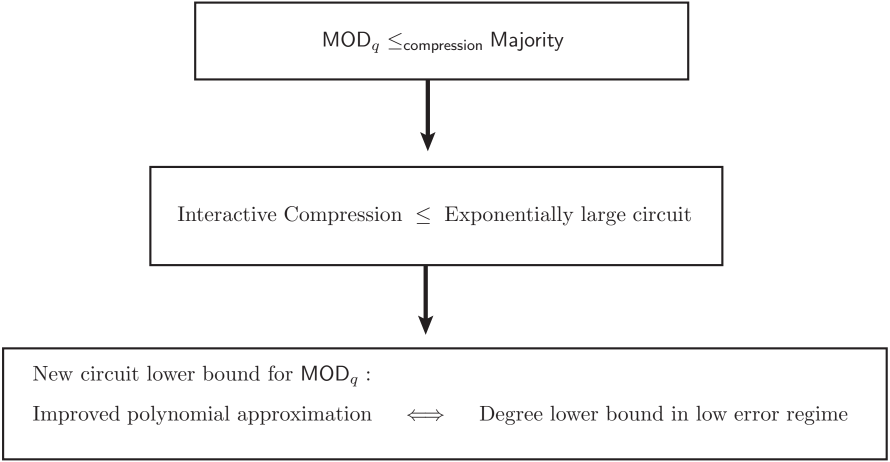
Then h admits a $\mathcal{C}_d(\mathrm{poly}(n))$-compression game with communication cost $c(n) \leq s$ consisting of at most $r + 1$ rounds.

Main lower bound holds for protocols with unlimited number of rounds:

Corollary. If Majority is computed by an $\mathrm{AC}^0_d[p]$ circuit with arbitrary oracle gates, then the total fan-in of the oracle gates is $\geq n/(\log n)^{2d+O(1)}$.

Sketch of the lower bound (Theorem 1)

Let $\mathcal{C} = \mathsf{AC}^0_d[p]$, and consider a fixed prime $q \neq p$.



Compressing symmetric functions using Majority

Lemma.
Let $h\colon \{0,1\}^n \to \{0,1\}$ be an arbitrary symmetric function, $\mathcal{C}$ be a circuit class, and $d \geq 1$.

Assume that the $\mathcal{C}_d(\text{poly}(n))$-compression game for Majority_n can be solved with cost $c(n)$ in $r(n)$ rounds.

Then the $\mathcal{C}_{d+O(1)}(\text{poly}(n))$-compression game for h can be solved with cost $c_h(n) = O(c(2n) \cdot \log n)$ in $r_h(n) = O(r(2n) \cdot \log n)$ rounds.

Compressing symmetric functions using Majority

Lemma.
Let $h\colon \{0,1\}^n \to \{0,1\}$ be an arbitrary symmetric function, $\mathcal{C}$ be a circuit class, and $d \geq 1$.

Assume that the $\mathcal{C}_d(\text{poly}(n))$-compression game for Majority_n can be solved with cost $c(n)$ in $r(n)$ rounds.

Then the $\mathcal{C}_{d+O(1)}(\text{poly}(n))$-compression game for h can be solved with cost $c_h(n) = O(c(2n) \cdot \log n)$ in $r_h(n) = O(r(2n) \cdot \log n)$ rounds.

Proof sketch.
1) Compression for Majority implies compression for Th_k.
2) Alice and Bob perform a binary search.

From interactive compression to very large circuits

Proposition.

If there exists a $\mathcal{C}_d(\text{poly}(n))$-compression game for f_n with cost $c(n)$, then there exist circuits $C_1, \ldots, C_T$ from $\mathcal{C}_{d+O(1)}(\text{poly}(n))$, where

$$T \leq 2^{c(n)},$$

such that $\forall x \in \{0,1\}^n$,

$$f_n(x) = \bigvee_{i \in [T]} C_i(x).$$

From interactive compression to very large circuits

Proposition.

If there exists a $\mathcal{C}_d(\text{poly}(n))$-compression game for f_n with cost $c(n)$, then there exist circuits $C_1, \ldots, C_T$ from $\mathcal{C}_{d+O(1)}(\text{poly}(n))$, where

$$T \leq 2^{c(n)},$$

such that $\forall x \in \{0,1\}^n$,

$$f_n(x) = \bigvee_{i \in [T]} C_i(x).$$

Proof sketch. Each circuit C_i checks whether the interaction induced by x leads to the i-th accepting transcript.

From interactive compression to very large circuits

Proposition.

If there exists a $\mathcal{C}_d(\text{poly}(n))$-compression game for f_n with cost $c(n)$, then there exist circuits $C_1, \ldots, C_T$ from $\mathcal{C}_{d+O(1)}(\text{poly}(n))$, where

$$T \leq 2^{c(n)},$$

such that $\forall x \in \{0,1\}^n$,

$$f_n(x) = \bigvee_{i \in [T]} C_i(x).$$

Proof sketch. Each circuit C_i checks whether the interaction induced by x leads to the i-th accepting transcript.

Depth blow-up is minimal: "Parallel simulation of all rounds".

The difficulty of analyzing very large circuits

Goal.
Lower bound against circuits of depth $d + O(1)$ and size $\geq 2^{c(n)}$.
Want to set $c(n) \approx n/\text{poly}(\log n)$.

The difficulty of analyzing very large circuits

Goal.
Lower bound against circuits of depth $d + O(1)$ and size $\geq 2^{c(n)}$.
Want to set $c(n) \approx n/\text{poly}(\log n)$.

Problem.
No explicit lower bounds for depth-d circuits of size $2^{\omega(n^{1/(d-1)})}$.

The difficulty of analyzing very large circuits

Goal.
Lower bound against circuits of depth $d + O(1)$ and size $\geq 2^{c(n)}$.
Want to set $c(n) \approx n/\text{poly}(\log n)$.

Problem.
No explicit lower bounds for depth-d circuits of size $2^{\omega(n^{1/(d-1)})}$.
(Actually, MOD_q admits depth-d circuits of size $\lll 2^{n/\text{poly}(\log n)}$).

The difficulty of analyzing very large circuits

Goal.
Lower bound against circuits of depth $d + O(1)$ and size $\geq 2^{c(n)}$.
Want to set $c(n) \approx n/\text{poly}(\log n)$.

Problem.
No explicit lower bounds for depth-d circuits of size $2^{\omega(n^{1/(d-1)})}$.
(Actually, MOD_q admits depth-d circuits of size $\lll 2^{n/\text{poly}(\log n)}$).

Idea.

$$f_n(x) = \dot{\bigvee_{i \in [T]}} C_i(x).$$

Initial function is a disjoint union of (poly-size) circuits C_i.

If $f(x) = 1$ then exactly one circuit evaluates to 1.

From interactive compression to very large circuits

Proposition (updated)

If there exists a $\mathcal{C}_d(\text{poly}(n))$-compression game for f_n with cost $c(n)$, then there exist circuits $C_1, \ldots, C_T$ from $\mathcal{C}_{d+O(1)}(\text{poly}(n))$, where

$$T \leq 2^{c(n)},$$

such that $\forall x \in \{0,1\}^n$,

$$f_n(x) = \dot{\bigvee_{i \in [T]}} C_i(x) \quad \textbf{(“uniqueness property”)}$$

New circuit lower bound for MOD_q

Proposition.
For every $d \geq 1$, if we have

$$\text{MOD}_q(x_1, \ldots, x_n) = \dot{\bigvee}_{i \in [T]} C_i(x_1, \ldots, x_n),$$

where each C_i is an $\text{AC}^0_d[p]$ circuit, then

$$T \geq 2^{n/(\log n)^{2d+O(1)}}.$$

New circuit lower bound for MOD_q

Proposition.
For every $d \geq 1$, if we have

$$\mathrm{MOD}_q(x_1, \ldots, x_n) = \dot{\bigvee}_{i \in [T]} C_i(x_1, \ldots, x_n),$$

where each C_i is an $\mathrm{AC}^0_d[p]$ circuit, then

$$T \geq 2^{n/(\log n)^{2d+O(1)}}.$$

Proof sketch.
Polynomial approximation method in the very low error regime.

New circuit lower bound for MOD_q

Proposition.
For every $d \geq 1$, if we have

$$\mathrm{MOD}_q(x_1, \ldots, x_n) = \dot{\bigvee}_{i \in [T]} C_i(x_1, \ldots, x_n),$$

where each C_i is an $\mathrm{AC}^0_d[p]$ circuit, then

$$T \geq 2^{n/(\log n)^{2d+O(1)}}.$$

Proof sketch.
Polynomial approximation method in the very low error regime.

(Razborov/Smolensky's lower bound: optimized when $\varepsilon = \Omega(1)$.)

Improved approximation by $\mathbb{F}_p$ polynomials

Polynomial approximation method + Uniqueness:

Claim. If each C_i can be δ-approximated by an $\mathbb{F}_p$ polynomial P_i, then

$$Q(x) \stackrel{\text{def}}{=} \sum_{i \in [T]} P_i(x) \qquad \textbf{(Recall: } f = \dot{\bigvee}_{i \in [T]} C_i)$$

is an $\varepsilon = T \cdot \delta$ approximator for f.

Improved approximation by $\mathbb{F}_p$ polynomials

Polynomial approximation method + Uniqueness:

Claim. If each C_i can be δ-approximated by an $\mathbb{F}_p$ polynomial P_i, then

$$Q(x) \stackrel{\text{def}}{=} \sum_{i \in [T]} P_i(x) \qquad \textbf{(Recall: } f = \dot{\bigvee}_{i \in [T]} C_i)$$

is an $\varepsilon = T \cdot \delta$ approximator for f.

Reason.
In general, several P_i's correct on x can cause "$\bigvee$" to be wrong ($\mathbb{F}_p$).
Uniqueness $\implies$ can take union bound over bad inputs only.

Improved approximation by $\mathbb{F}_p$ polynomials

Polynomial approximation method + Uniqueness:

Claim. If each C_i can be δ-approximated by an $\mathbb{F}_p$ polynomial P_i, then

$$Q(x) \stackrel{\text{def}}{=} \sum_{i \in [T]} P_i(x) \qquad \textbf{(Recall: } f = \dot{\bigvee}_{i \in [T]} C_i)$$

is an $\varepsilon = T \cdot \delta$ approximator for f.

Reason.
In general, several P_i's correct on x can cause "$\bigvee$" to be wrong ($\mathbb{F}_p$).
Uniqueness $\implies$ can take union bound over bad inputs only.

Important. Degree of Q at most degree of P_i's.

Improved approximation by $\mathbb{F}_p$ polynomials

Polynomial approximation method + Uniqueness:

Claim. If each C_i can be δ-approximated by an $\mathbb{F}_p$ polynomial P_i, then

$$Q(x) \stackrel{\text{def}}{=} \sum_{i \in [T]} P_i(x) \qquad \textbf{(Recall: } f = \dot{\bigvee}_{i \in [T]} C_i)$$

is an $\varepsilon = T \cdot \delta$ approximator for f.

Reason.
In general, several P_i's correct on x can cause "$\bigvee$" to be wrong ($\mathbb{F}_p$).
Uniqueness $\implies$ can take union bound over bad inputs only.

Important. Degree of Q at most degree of P_i's.

Problem: how to control error and degree simultaneously?

The low error regime in the approximation method

Razborov/Smolensky, 1987 (polynomial approximation)
For every $\delta(n) > 0$, any $\mathsf{AC}^0_d[p]$ admits a δ-error probabilistic polynomial $\mathbf{P}(x_1, \ldots, x_n) \in \mathbb{F}_p[x_1, \ldots, x_n]$ of degree $(O(\log n + \log(1/\delta)))^d$.

The low error regime in the approximation method

Razborov/Smolensky, 1987 (polynomial approximation)
For every $\delta(n) > 0$, any $\mathsf{AC}^0_d[p]$ admits a δ-error probabilistic polynomial $\mathbf{P}(x_1, \ldots, x_n) \in \mathbb{F}_p[x_1, \ldots, x_n]$ of degree $(O(\log n + \log(1/\delta)))^d$.

Kopparty and Srinivasan, 2012 (extension)

$(O(\log n))^d \cdot \log(1/\delta)$ **instead of** $(O(\log n + \log(1/\delta)))^d$.

The low error regime in the approximation method

Razborov/Smolensky, 1987 (polynomial approximation)
For every $\delta(n) > 0$, any $\mathrm{AC}^0_d[p]$ admits a δ-error probabilistic polynomial $\mathbf{P}(x_1, \ldots, x_n) \in \mathbb{F}_p[x_1, \ldots, x_n]$ of degree $(O(\log n + \log(1/\delta)))^d$.

Kopparty and Srinivasan, 2012 (extension)

$(O(\log n))^d \cdot \log(1/\delta)$ **instead of** $(O(\log n + \log(1/\delta)))^d$**.**

Razborov/Smolensky + folklore, 1987 (lower bound for all ε)
For every $\varepsilon(n) \in [2^{-.001n}, 1/100q]$, any $Q(x_1, \ldots, x_n) \in \mathbb{F}_p[x_1, \ldots, x_n]$ that ε-approximates MOD_q (uniform distribution) has degree

$$\Omega\left(\sqrt{n \cdot \log(1/\varepsilon)}\right).$$

Finishing the proof

Suppose $\mathrm{MOD}_q(x_1, \ldots, x_n) = \dot{\bigvee}_{i \in [T]} C_i(x_1, \ldots, x_n)$.

Finishing the proof

Suppose $\text{MOD}_q(x_1, \ldots, x_n) = \dot{\bigvee}_{i \in [T]} C_i(x_1, \ldots, x_n)$.

We $\delta \stackrel{\text{def}}{=} \varepsilon / T$ approximate each C_i, getting a $T \cdot \delta = \varepsilon$ approximator:

$$\begin{aligned} \text{degree} &\leq (\log n)^d \cdot \log(1/\delta) \\ &= (\log n)^d (\log T + \log(1/\varepsilon)). \end{aligned}$$

Finishing the proof

Suppose $\text{MOD}_q(x_1, \ldots, x_n) = \dot{\bigvee}_{i \in [T]} C_i(x_1, \ldots, x_n)$.

We $\delta \stackrel{\text{def}}{=} \varepsilon / T$ approximate each C_i, getting a $T \cdot \delta = \varepsilon$ approximator:

$$\begin{aligned} \text{degree} \quad &\leq \quad (\log n)^d \cdot \log(1/\delta) \\ &= \quad (\log n)^d (\log T + \log(1/\varepsilon)). \end{aligned}$$

Using the degree lower bound, for any $\varepsilon \in [2^{-.001n}, 1/100q]$,

$$\sqrt{n \cdot \log(1/\varepsilon)} \quad \leq \quad \text{degree}.$$

Finishing the proof

Suppose $\text{MOD}_q(x_1, \ldots, x_n) = \dot{\bigvee}_{i \in [T]} C_i(x_1, \ldots, x_n)$.

We $\delta \stackrel{\text{def}}{=} \varepsilon / T$ approximate each C_i, getting a $T \cdot \delta = \varepsilon$ approximator:

$$\begin{aligned} \text{degree} \quad &\leq \quad (\log n)^d \cdot \log(1/\delta) \\ &= \quad (\log n)^d (\log T + \log(1/\varepsilon)). \end{aligned}$$

Using the degree lower bound, for any $\varepsilon \in [2^{-.001n}, 1/100q]$,

$$\sqrt{n \cdot \log(1/\varepsilon)} \quad \leq \quad \text{degree}.$$

Therefore,

$$\log T \quad \geq \quad \frac{\sqrt{n \cdot log(1/\varepsilon)} - (\log n)^d \cdot \log(1/\varepsilon)}{(\log n)^d},$$

Finishing the proof

Suppose $\mathrm{MOD}_q(x_1, \ldots, x_n) = \dot{\bigvee}_{i \in [T]} C_i(x_1, \ldots, x_n)$.

We $\delta \stackrel{\text{def}}{=} \varepsilon / T$ approximate each C_i, getting a $T \cdot \delta = \varepsilon$ approximator:

$$\begin{aligned} \text{degree} \quad &\leq \quad (\log n)^d \cdot \log(1/\delta) \\ &= \quad (\log n)^d (\log T + \log(1/\varepsilon)). \end{aligned}$$

Using the degree lower bound, for any $\varepsilon \in [2^{-.001n}, 1/100q]$,

$$\sqrt{n \cdot \log(1/\varepsilon)} \quad \leq \quad \text{degree}.$$

Therefore,

$$\log T \quad \geq \quad \frac{\sqrt{n \cdot log(1/\varepsilon)} - (\log n)^d \cdot \log(1/\varepsilon)}{(\log n)^d},$$

which is maximized when $\varepsilon = \exp\left(- n/(4(\log n)^{2d}) \right)$.

Observation

To obtain $\mathrm{AC}^0_d[p]$ circuit size lower bounds for MOD_q:

Polynomial approximation method with ε as large as possible.

Observation

To obtain $\mathrm{AC}^0_d[p]$ circuit size lower bounds for MOD_q:

Polynomial approximation method with ε as large as possible.

To understand structure of optimal polynomial size circuits up to depth $\approx \log n / \log\log n$:

Polynomial approximation method in the very low error regime.

Round complexity in $\mathcal{C}$-compression games

$AC^0[p]$ lower bound: holds for any number of rounds.

$AC^0[p]$ upper bound: single-round compression.

Power of interaction in compression games?

Round complexity in $\mathcal{C}$-compression games

$AC^0[p]$ lower bound: holds for any number of rounds.

$AC^0[p]$ upper bound: single-round compression.

Power of interaction in compression games?

Chattopadhyay and Santhanam, 2012:
For every fixed r, there is a Boolean function on n variables that admits AC^0-bounded protocols with r rounds and cost $O(n^{1/r})$, but for which any correct AC^0-bounded $(r-1)$-round protocol has cost $\Omega(n^{2/r-o(1)})$.

Round complexity in $\mathcal{C}$-compression games

$AC^0[p]$ lower bound: holds for any number of rounds.

$AC^0[p]$ upper bound: single-round compression.

Power of interaction in compression games?

Chattopadhyay and Santhanam, 2012:
For every fixed r, there is a Boolean function on n variables that admits AC^0-bounded protocols with r rounds and cost $O(n^{1/r})$, but for which any correct AC^0-bounded $(r-1)$-round protocol has cost $\Omega(n^{2/r-o(1)})$.

$\Longrightarrow$ Quadratic gap, dependence on r not very satisfactory.

The power of interaction in AC^0-compression games

[Theorem 2].

Let $r \geq 2$ and $\varepsilon > 0$ be fixed parameters. There is an explicit family of functions $f = \{f_n\}_{n \in \mathbb{N}}$ with the following properties:

- There exists an $AC^0_2(n)$-bounded protocol Π_n for f_n with r rounds and cost $c(n) \leq n^{\varepsilon}$, for every $n \geq n_f$, where n_f is a fixed constant that depends on f.

The power of interaction in AC^0-compression games

[Theorem 2].

Let $r \geq 2$ and $\varepsilon > 0$ be fixed parameters. There is an explicit family of functions $f = \{f_n\}_{n \in \mathbb{N}}$ with the following properties:

- There exists an $AC^0_2(n)$-bounded protocol Π_n for f_n with r rounds and cost $c(n) \leq n^{\varepsilon}$, for every $n \geq n_f$, where n_f is a fixed constant that depends on f.

- Any $AC^0(\text{poly}(n))$-bounded protocol Π for f with $r - 1$ rounds has cost $c(n) \geq n^{1-\varepsilon}$, for every $n \geq n_\Pi$, where n_Π is a fixed constant that depends on Π.

Hard function for round-limited protocols

Function $f_n \colon \{0,1\}^n \to \{0,1\}$, where $n \stackrel{\text{def}}{=} m + \ell \cdot r \cdot m$.

"Pointer Jumping Problem". Uses a function $h = \{h_t\}_{t \in \mathbb{N}}$ that is hard for AC^0.

Hard function for round-limited protocols

Function $f_n \colon \{0,1\}^n \to \{0,1\}$, where $n \stackrel{\text{def}}{=} m + \ell \cdot r \cdot m$.

"Pointer Jumping Problem". Uses a function $h = \{h_t\}_{t \in \mathbb{N}}$ that is hard for AC^0.

Intuition:

Upper bound: $r + 1$ rounds with communication $(1 + r) \cdot m$.
Lower bound: r rounds require communication at least $\ell \cdot m^{1-o(1)}$.

Appropriate setting of parameters induces gap: n^{ε} versus $n^{1-\varepsilon}$.

Hard function for round-limited protocols

Function $f_n \colon \{0,1\}^n \to \{0,1\}$, where $n \stackrel{\text{def}}{=} m + \ell \cdot r \cdot m$.

"Pointer Jumping Problem". Uses a function $h = \{h_t\}_{t \in \mathbb{N}}$ that is hard for AC^0.

Intuition:

Upper bound: $r + 1$ rounds with communication $(1 + r) \cdot m$.
Lower bound: r rounds require communication at least $\ell \cdot m^{1-o(1)}$.

Appropriate setting of parameters induces gap: n^{ε} versus $n^{1-\varepsilon}$.

Proof relies on a round elimination argument via random restrictions, together with an appropriate induction hypothesis.

Part 3: Open Problems

Open Problem 1: Round separation for $AC^0[p]$-compression games?

As far as we know, single-round $AC^0[p]$ protocols are as powerful as k-round protocols.

(Our technique for $AC^0[p]$ is insensitive to the # of rounds.)

Problem. Prove a "round separation theorem" for $AC^0[p]$-compression games.

Open Problem 2: Lower bounds for randomized $AC^0[p]$-compression games?

The randomized $AC^0[p]$-compression complexity of Majority remains open.

Reason: proof explores very low error regime in the polynomial approximation method (initial error probability is not tolerated).

Open Problem 2: Lower bounds for randomized AC^0[p]-compression games?

The randomized $AC^0[p]$-compression complexity of Majority remains open.

Reason: proof explores very low error regime in the polynomial approximation method (initial error probability is not tolerated).

Problem. Settle the randomized $AC^0[p]$-compression complexity of Majority.

Open Problem 2: Lower bounds for randomized $AC^0[p]$-compression games?

The randomized $AC^0[p]$-compression complexity of Majority remains open.

Reason: proof explores very low error regime in the polynomial approximation method (initial error probability is not tolerated).

Problem. Settle the randomized $AC^0[p]$-compression complexity of Majority.

Remark. Communication cost is $n/(\log n)^{\Theta(d)}$ for randomized AC^0_d-compression games (Chattopadhyay and Santhanam, 2012).

Open Problem 3: Power of modulo m gates in interactive compression?

Unconditional lower bounds:

Circuit class	**Hard function**	**Incompressibility (depth d)**
AC^0	Parity	$CC(\text{Parity}_n) \geq n / \log^{O(d)} n$
$AC^0[p]$	Majority	$CC(\text{Majority}_n) \geq n / \log^{O(d)} n$
$AC^0[m]$	NEXP, Majority (?)	$CC(\text{Majority}_n) = ?$

Open Problem 3: Power of modulo m gates in interactive compression?

Unconditional lower bounds:

Circuit class	Hard function	Incompressibility (depth d)
AC^0	Parity	$CC(Parity_n) \geq n/\log^{O(d)} n$
$AC^0[p]$	Majority	$CC(Majority_n) \geq n/\log^{O(d)} n$
$AC^0[m]$	NEXP, Majority (?)	$CC(Majority_n) = ?$

Question. Are there randomized $AC^0[m]$-compression games for Majority with communication cost $n^{1-\varepsilon}$?

This result would shed more light on the hardness of proving lower bounds against circuits with modulo m gates.

Thank you!