Addition is exponentially harder than counting for shallow monotone circuits

Igor Carboni Oliveira

Columbia University / Charles University in Prague

Joint work with **Xi Chen** (Columbia) and **Rocco Servedio** (Columbia)

What is this talk about?

1. Exponential weights in bounded-depth monotone majority circuits.

What is this talk about?

1. **Exponential weights in bounded-depth monotone majority circuits.**

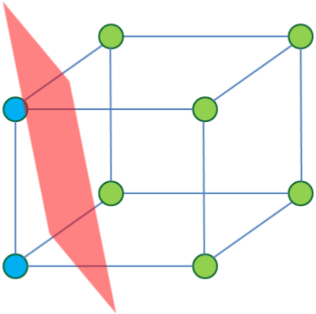
2. **The power of negation gates in bounded-depth AND/OR/NOT circuits.**

Part 1. Monotone majority circuits.

Weighted threshold functions

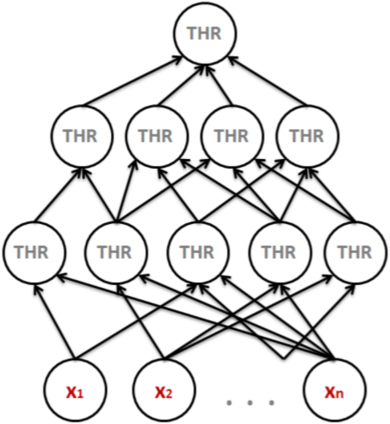
Def. $f\colon \{0,1\}^m \to \{0,1\}$ is a ***weighted threshold function*** if there are integers (**"weights"**) $w_1, \ldots, w_m$ and t such that

$$f(x) = 1 \quad \Leftrightarrow \quad \sum_{i=1}^{m} w_i x_i \geq t.$$



Threshold circuits: Definition

- Each internal gate computes a weighted threshold function.



- This circuit has **depth** 3 (# layers) and **size** 10 (# gates).

Threshold circuits: The frontier

Simple computational model whose power remains mysterious.

Open Problem. Can we solve **s-t-connectivity** using constant-depth polynomial size threshold circuits?

Threshold circuits: The frontier

Simple computational model whose power remains mysterious.

Open Problem. Can we solve **s-t-connectivity** using constant-depth polynomial size threshold circuits?

However, relative success in understanding the role of large weights in the gates of the circuit:

"Exponential weights vs. polynomial weights".

Threshold Circuits vs. Majority Circuits

◦ **Majority circuits:** “We care about the weights.”

Example: $3x_1 - 4x_3 + 2x_7 - x_2 \overset{?}{\geq} 5.$

The weight of this gate is $3 + 4 + 2 + 1 = 10$**.**

Threshold Circuits vs. Majority Circuits

◦ **Majority circuits:** "We care about the weights."

Example: $3x_1 - 4x_3 + 2x_7 - x_2 \;\geq^?\; 5.$

The weight of this gate is $3 + 4 + 2 + 1 = 10$**.**

Size of Majority Circuit: Total weight in the circuit.

Polynomial weight is sufficient

[Siu and Bruck, 1991] Poly-size bounded-depth threshold circuits simulated by poly-size bounded-depth majority circuits.

Polynomial weight is sufficient

[Siu and Bruck, 1991] Poly-size bounded-depth threshold circuits simulated by poly-size bounded-depth majority circuits.

[Goldmann, Hastad, and Razborov, 1992] depth-d threshold circuits simulated by depth-$(d+1)$ majority circuits.

Polynomial weight is sufficient

[Siu and Bruck, 1991] Poly-size bounded-depth threshold circuits simulated by poly-size bounded-depth majority circuits.

[Goldmann, Hastad, and Razborov, 1992] depth-d threshold circuits simulated by depth-$(d+1)$ majority circuits.

[Goldmann and Karpinski, 1993] Constructive simulation.

Polynomial weight is sufficient

[Siu and Bruck, 1991] Poly-size bounded-depth threshold circuits simulated by poly-size bounded-depth majority circuits.

[Goldmann, Hastad, and Razborov, 1992] depth-d threshold circuits simulated by depth-$(d+1)$ majority circuits.

[Goldmann and Karpinski, 1993] Constructive simulation.

Simplification/better parameters:
[Hofmeister, 1996] and **[Amano and Maruoka, 2005]**.

[Goldmann and Karpinski, 1993]

"If original threshold circuit is **monotone** (positive weights), simulation yields majority circuits with **negative weights**."

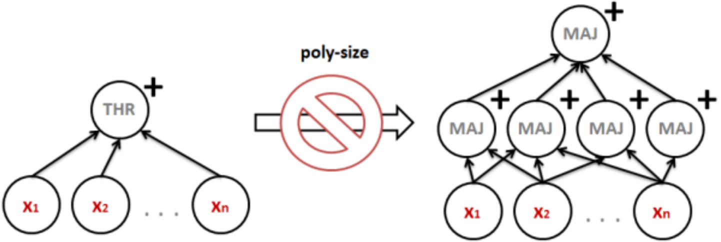
[Goldmann and Karpinski, 1993]

"If original threshold circuit is **monotone** (positive weights), simulation yields majority circuits with **negative weights.**"

[GK'93] Is there a monotone transformation?

(Question recently reiterated by J. Hastad, 2010 & 2014)

Previous Work [Hofmeister, 1992]



No efficient monotone simulation in depth **2**:
Total weight must be $2^{\Omega(\sqrt{n})}$.

Our first result.

Solution to question posed by Goldmann and Karpinski:

No efficient monotone simulation in any fixed depth $d \in \mathbb{N}$.

Our first result.

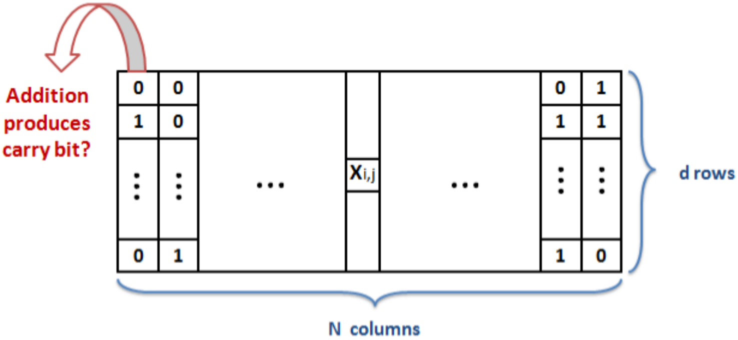
Solution to question posed by Goldmann and Karpinski:

No efficient monotone simulation in any fixed depth $d \in \mathbb{N}$.

Our hard monotone threshold gate: $U_{d,N}$

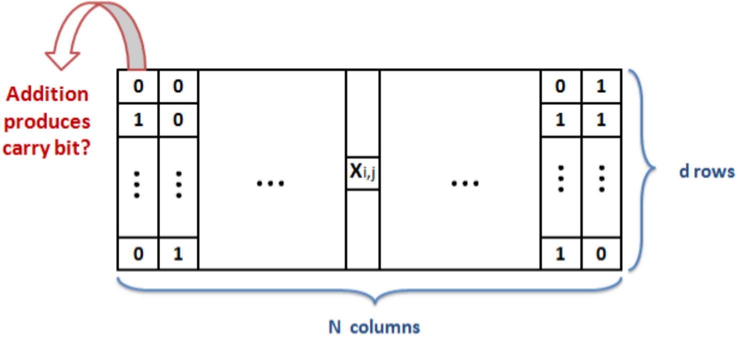
Checks if the addition of d natural numbers (each with N bits) is at least 2^N.

The lower bound



$$U_{d,N}: \quad \sum_{j=0}^{N-1} 2^j (x_{1,j} + \ldots + x_{d,j}) \overset{?}{\geq} 2^N$$

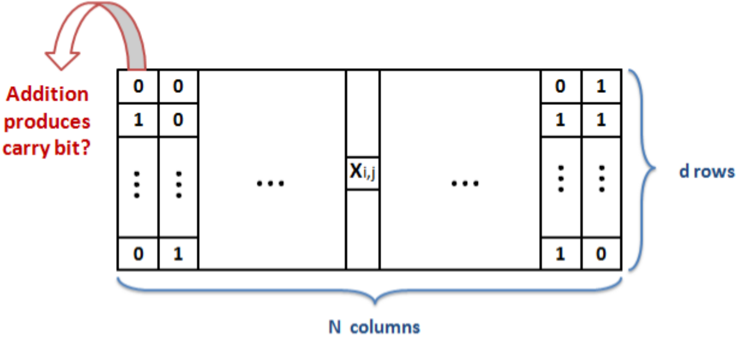
The lower bound



$$U_{d,N}: \quad \sum_{j=0}^{N-1} 2^j (x_{1,j} + \ldots + x_{d,j}) \overset{?}{\geq} 2^N$$

Theorem 1. Any depth-d monotone MAJ circuit for $U_{d,N}$ has size $2^{\Omega(N^{1/d})}$.

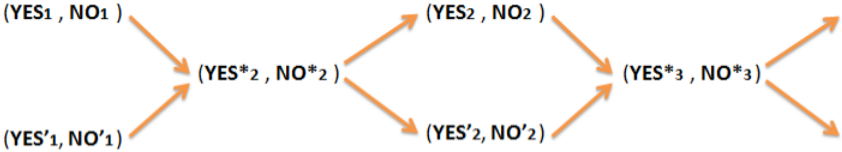
The lower bound



$$U_{d,N}: \quad \sum_{j=0}^{N-1} 2^j (x_{1,j} + \ldots + x_{d,j}) \overset{?}{\geq} 2^N$$

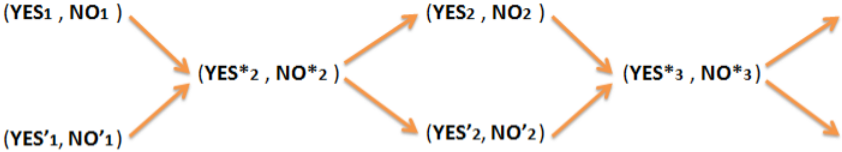
Theorem 1. Any depth-d monotone MAJ circuit for $U_{d,N}$ has size $2^{\Omega(N^{1/d})}$. Furthermore, there is a matching upper bound.

Our approach: pairs of pairs of distributions



Intuition: **YES*** distrib. supported over strings with sum $\geq 2^N$.
NO* distrib. supported over strings with sum $< 2^N$.

Our approach: pairs of pairs of distributions



Intuition: **YES*** distrib. supported over strings with sum $\geq 2^N$.
NO* distrib. supported over strings with sum $< 2^N$.

Inductive Lemma. $\forall \ell \leq d$ any "small" depth-ℓ MAJ circuit $\mathcal{C}$ satisfies:

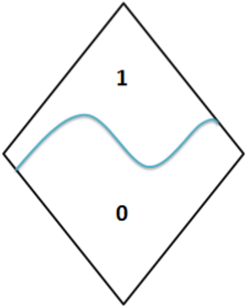
$$\Pr[\mathcal{C}(\mathrm{YES}^\star_\ell) = 1] + \Pr[\mathcal{C}(\mathrm{NO}^\star_\ell) = 0] \; < \; 1 + \frac{10^\ell}{10^d}.$$

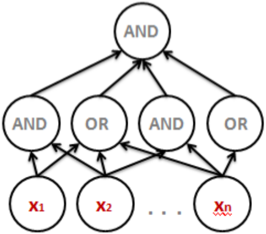
(Proof explores monotonicity and low weight in a crucial way.)

Part 2. Monotonicity and AC^0 circuits.

Monotone Complexity

Semantics vs. syntax:





Monotone Functions “ = ” Monotone Circuits

The Ajtai-Gurevich Theorem (1987)

◦ Motivated by question in Finite Model Theory.

There is **monotone** $g_n \colon \{0,1\}^n \to \{0,1\}$ such that:

- $g \in \mathrm{AC}^0$;
- g_n requires **monotone** AC^0 circuits of size $n^{\omega(1)}$.

The Ajtai-Gurevich Theorem (1987)

◦ Motivated by question in Finite Model Theory.

There is **monotone** $g_n \colon \{0,1\}^n \to \{0,1\}$ such that:

- $g \in \mathrm{AC}^0$;
- g_n requires **monotone** AC^0 circuits of size $n^{\omega(1)}$.

"Negations can speed-up the bounded-depth computation of monotone functions."

The Ajtai-Gurevich Theorem (1987)

◦ Motivated by question in Finite Model Theory.

There is **monotone** $g_n \colon \{0,1\}^n \to \{0,1\}$ such that:

- $g \in \mathrm{AC}^0$;
- g_n requires **monotone** AC^0 circuits of size $n^{\omega(1)}$.

"Negations can speed-up the bounded-depth computation of monotone functions."

Obs.: g_n computed by monotone AC^0 circuits of size $n^{O(\log n)}$.

Question.

Is there an **exponential** speed-up in bounded-depth?

Question.

Is there an **exponential** speed-up in bounded-depth?

(Analogous question for **arbitrary** circuits answered positively **[Tardos, 1988]**.)

Our second result.

Theorem 2. There is a **monotone** $f_n \colon \{0,1\}^n \to \{0,1\}$ s.t.:

- $f \in \mathrm{AC}^0$ (f_n computed in depth 3);
- f_n requires depth-d **monotone** MAJ circuits of size $2^{\widetilde{\Omega}(n^{1/d})}$.

Our second result.

Theorem 2. There is a **monotone** $f_n \colon \{0,1\}^n \to \{0,1\}$ s.t.:

- $f \in \mathsf{AC}^0$ (f_n computed in depth 3);
- f_n requires depth-d **monotone** MAJ circuits of size $2^{\widetilde{\Omega}(n^{1/d})}$.

◦ **Exponential separation;**
◦ **Hardness against** MAJ **gates instead of** AND/OR **gates.**

Our second result.

Theorem 2. There is a **monotone** $f_n \colon \{0,1\}^n \to \{0,1\}$ s.t.:

- $f \in \mathsf{AC}^0$ (f_n computed in depth 3);
- f_n requires depth-d **monotone** MAJ circuits of size $2^{\widetilde{\Omega}(n^{1/d})}$.

◦ **Exponential separation;**
◦ **Hardness against** MAJ **gates instead of** AND/OR **gates.**

Proof. Upper bound for our addition function $U_{k,N}$. □

Concluding Remarks

Addition function $U_{k,N}$: monotone bounded-depth circuits are *exponentially weaker*.

Concluding Remarks

Addition function $U_{k,N}$**:** monotone bounded-depth circuits are *exponentially weaker*.

Small-distance connectivity STCONN($k(n)$)**:** Recent work showing that monotone bounded-depth circuits are *essentially optimal*.

Concluding Remarks

Addition function $U_{k,N}$**:** monotone bounded-depth circuits are *exponentially weaker*.

Small-distance connectivity STCONN($k(n)$)**:** Recent work showing that monotone bounded-depth circuits are *essentially optimal*.

An interesting direction:

Formulation of a general theory to explain when non-monotone operations speed-up the computation of monotone functions (in bounded-depth complexity).

Thank you!