Addition is exponentially harder than counting for shallow monotone circuits

Igor Carboni Oliveira

University of Oxford

Joint work with **Xi Chen** and **Rocco Servedio**

We know a fair bit about monotone functions and monotone circuits (tight circuit lower bounds, etc).

Extending results from monotone to non-monotone circuits is quite challenging.

In this work we continue the investigation of monotonicity and the power of non-monotone operations in bounded-depth boolean circuits.

Summary:

Exponential versus polynomial weights in (monotone) threshold circuits.

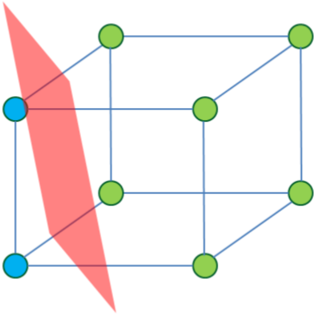
The power of negation gates in bounded-depth AND/OR/NOT circuits.

Part 1. Monotone threshold/majority circuits.

Weighted threshold functions

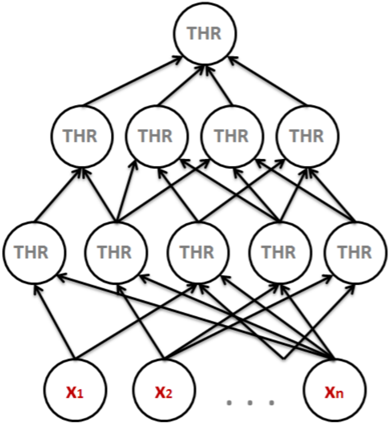
Def. $f\colon \{0,1\}^m \to \{0,1\}$ is a ***weighted threshold function*** if there are integers (**"weights"**) $w_1, \ldots, w_m$ and t such that

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



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?

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

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

Size of Majority Circuit: Total weight in the circuit, or equivalently, number of wires.

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]**.

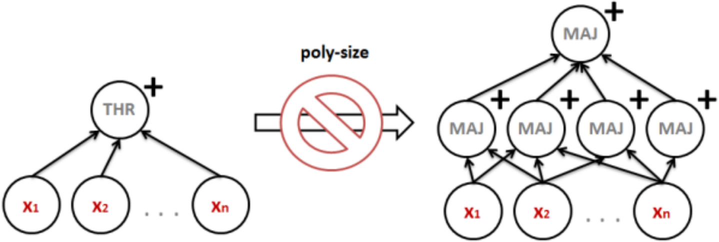
[Goldmann and Karpinski, 1993]

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

[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.

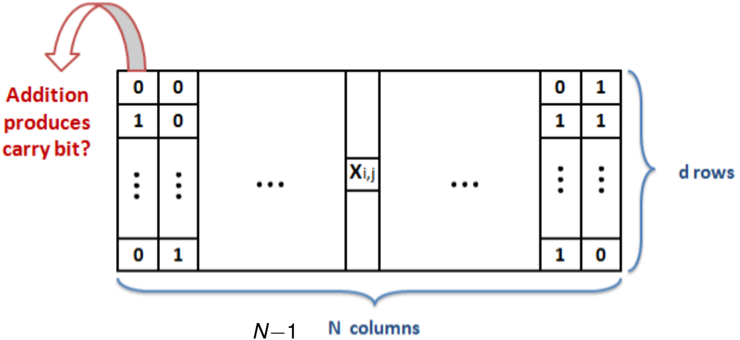
Solution to the question posed by Goldmann and Karpinski:

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

Our hard monotone threshold gate: $\text{Add}_{d,N}$

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

The lower bound



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

Theorem 1. For every fixed $d \geq 2$, any depth-d monotone MAJ circuit for $\text{Add}_{d,N}$ has size $2^{\Omega(N^{1/d})}$. There is a matching upper bound of the form $2^{O(N^{1/d})}$.

"And you do Addition?" the White Queen asked. "What's one and one and one and one and one and one and one and one and one and one?"

"I don't know," said Alice. "I lost count."

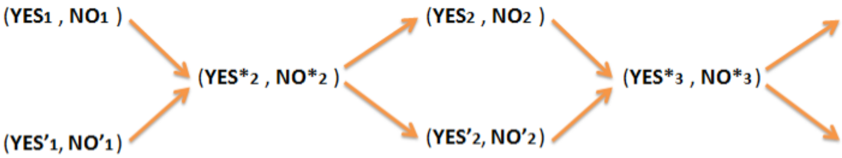
"She can't do Addition," the Red Queen interrupted.

— Lewis Carroll, *Through the Looking Glass*

In order for Alice to compute $\mathrm{Add}_{k,N}$
efficiently in small depth, she must count and **subtract** ones!

Our approach: pairs of pairs of distributions

We inductively construct distributions that are “hard” for deeper and deeper circuits.



YES$_\ell^\star$ distrib. support. over strings in $\{0,1\}^{\ell \times N_\ell}$ with sum $\geq 2^{N_\ell}$.
NO$_\ell^\star$ distrib. support. over strings in $\{0,1\}^{\ell \times N_\ell}$ with sum $< 2^{N_\ell}$.

Main Lemma. For each $2 \leq \ell \leq d$, every “small” depth-ℓ monotone MAJ circuit C satisfies:

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

Each $x_{\text{yes}} \sim \text{YES}_1$ looks like:

$$\begin{array}{cccccc|c|ccccc} 1 & 0 & 0 & 1 & \cdots & 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & 0 & \cdots & 1 & 1 & 0 & 0 & \cdots & 0 & 0 \end{array}$$

Each $y_{\text{no}} \sim \text{NO}_1$ looks like:

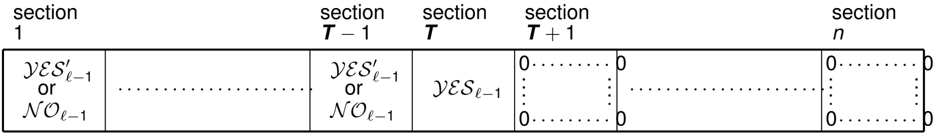
$$\begin{array}{cccccccccccc} 0 & 1 & 0 & 0 & \cdots & 1 & 1 & 0 & 1 & \cdots & 1 & 0 \\ 1 & 0 & 1 & 1 & \cdots & 0 & 0 & 1 & 0 & \cdots & 0 & 1 \end{array}$$

Each $x_{\text{yes}} \sim \text{YES}'_1$ looks like:

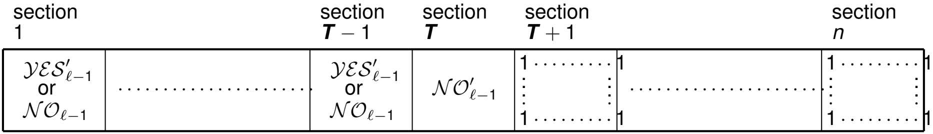
$$\begin{array}{cccccccccccc} 1 & 0 & 0 & 1 & \cdots & 0 & 1 & 0 & 1 & \cdots & 0 & 1 \\ 0 & 1 & 1 & 0 & \cdots & 1 & 0 & 1 & 0 & \cdots & 1 & 0 \end{array}$$

Each $y_{\text{no}} \sim \text{NO}'_1$ looks like:

$$\begin{array}{cccccc|c|ccccc} 1 & 0 & 0 & 1 & \cdots & 0 & 0 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 1 & 0 & \cdots & 1 & 0 & 1 & 1 & \cdots & 1 & 1 \end{array}$$



$\boldsymbol{x} \sim \mathcal{YES}^*_\ell$



$\boldsymbol{x} \sim \mathcal{NO}^*_\ell$

○ As we proceed, new distributions increase number of rows and columns in the support.

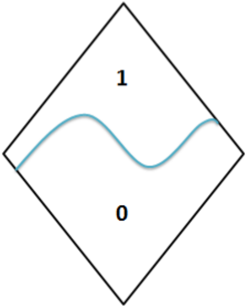
○ We have to maintain careful control over the properties of each pair of distributions.

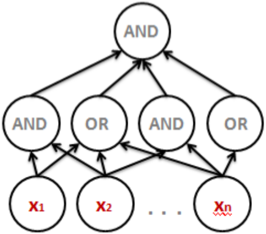
○ Proof of **Main Lemma** is by induction, considers three pairs of distributions, and is reasonably technical.

Part 2. Monotonicity and AC^0 circuits.

Monotone Complexity

Semantics vs. syntax:





Monotone Functions “ = ” Monotone Circuits

The Ajtai-Gurevich Theorem (1987)

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?

Similar 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);
- For every $d \geq 1$, f_n requires depth-d **monotone** MAJ circuits of size $2^{\widetilde{\Omega}(n^{1/d})}$.

∘ **Exponential separation and depth-3 upper bound;**
∘ **Hardness against** MAJ **gates instead of** AND/OR **gates.**

Proof. AC^0 upper bound for the addition function $\mathrm{Add}_{k,N}$ with $k = k(N) \to \infty$. □

A related problem.

Our result is essentially optimal in some aspects.

But I don't know the answer to the following question.

"Super Ajtai-Gurevich." Is there a monotone function in AC^0 that is not in monotone-P/poly?

(It is known that the addition function $\mathrm{Add}_{N,N}$ is in monNC^2.)

Thank you.