Matrix Rigidity

Rigidity and circuit lower bounds

Sasha Golovnev

November 30, 2020

Circuit Complexity

Boolean Circuits

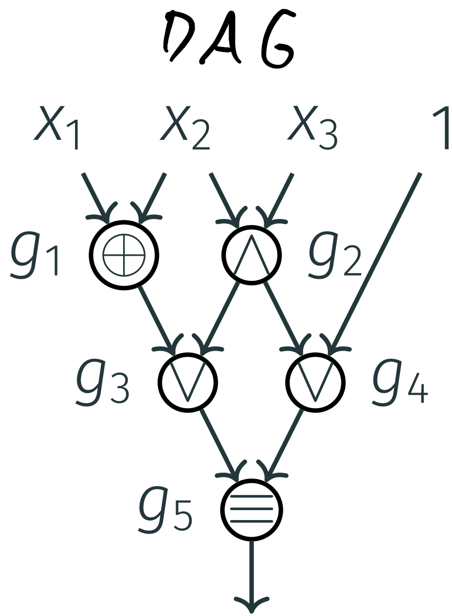
$$f\colon \{0,1\}^n \to \{0,1\}^n$$

$$\begin{aligned} g_1 &= x_1 \oplus x_2 \\ g_2 &= x_2 \wedge x_3 \\ g_3 &= g_1 \vee g_2 \\ g_4 &= g_2 \vee 1 \\ g_5 &= g_3 \equiv g_4 \end{aligned}$$

Boolean Circuits

$$f\colon \{0,1\}^n \to \{0,1\}^n$$

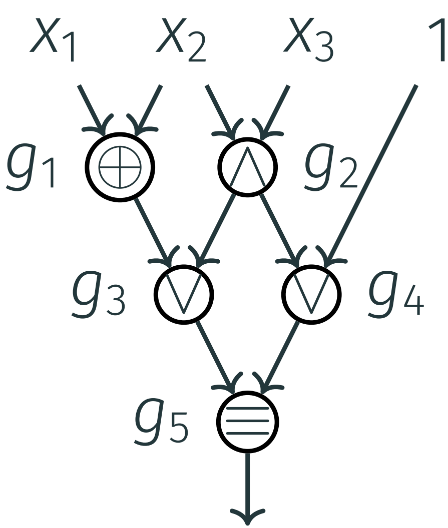
$$
\begin{aligned}
g_1 &= x_1 \oplus x_2 \\
g_2 &= x_2 \wedge x_3 \\
g_3 &= g_1 \vee g_2 \\
g_4 &= g_2 \vee 1 \\
g_5 &= g_3 \equiv g_4
\end{aligned}
$$



Boolean Circuits

$$f\colon \{0,1\}^n \to \{0,1\}^n$$

$$\begin{aligned} g_1 &= x_1 \oplus x_2 \\ g_2 &= x_2 \wedge x_3 \\ g_3 &= g_1 \vee g_2 \\ g_4 &= g_2 \vee 1 \\ g_5 &= g_3 \equiv g_4 \end{aligned}$$



Inputs:
$x_1, \ldots, x_n, 0, 1$

Gates:
binary functions

Fan-out:
unbounded

Exponential Bounds

Lower Bound [Sha1949]

Counting shows that almost all functions of n variables have circuit size at least

$$2^n .$$

Exponential Bounds

Lower Bound [Sha1949]

Counting shows that almost all functions of n variables have circuit size at least

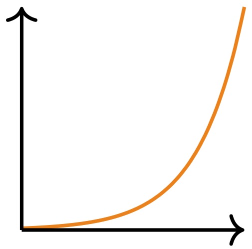
$$2^n .$$

Upper Bound [Lup1958]

Every function can be computed by a circuit of size

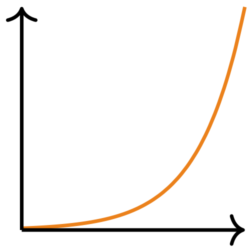
$$2^n .$$

Explicit Bounds



Most functions have exponential circuit complexity

Explicit Bounds

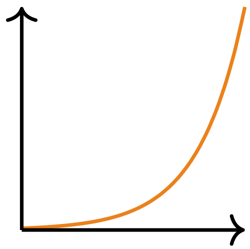


Most functions have exponential circuit complexity

$P \neq NP$

We want to prove super-polynomial lower bounds

Explicit Bounds

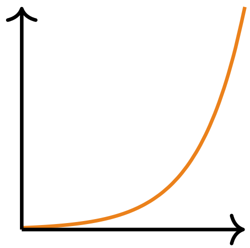


Most functions have exponential circuit complexity

$P \neq NP$

We want to prove super-polynomial lower bounds (for a function from **NP**)

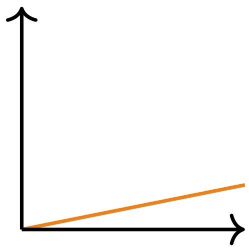
Explicit Bounds



Most functions have exponential circuit complexity

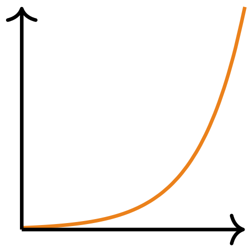
$P \neq NP$

We want to prove super-polynomial lower bounds (for a function from **NP**)



We can prove only $\approx 3n$ lower bounds

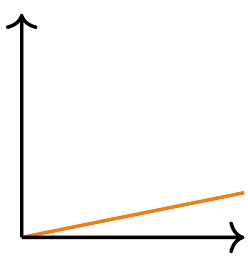
Explicit Bounds



Most functions have exponential circuit complexity

$P \neq NP$

We want to prove super-polynomial lower bounds (for a function from **NP**)



We can prove only $\approx 3n$ lower bounds (even for a function from $\mathbf{E}^{\mathbf{NP}}$)

Super-linear Circuit Lower Bounds?

- Two n-bit integers can be multiplied by a circuit of size $O(n \log n)$ [SS71,F07,HH19]

Super-linear Circuit Lower Bounds?

- Two n-bit integers can be multiplied by a circuit of size $O(n \log n)$ [SS71,F07,HH19]
- Discrete Fourier Transform of a sequence of length n can be computed by a circuit of size $O(n \log n)$

Super-linear Circuit Lower Bounds?

- Two n-bit integers can be multiplied by a circuit of size $O(n \log n)$ [SS71,F07,HH19]
- Discrete Fourier Transform of a sequence of length n can be computed by a circuit of size $O(n \log n)$
- Shifts, Permutations

Super-linear Circuit Lower Bounds?

- Two n-bit integers can be multiplied by a circuit of size $O(n \log n)$ [SS71,F07,HH19]
- Discrete Fourier Transform of a sequence of length n can be computed by a circuit of size $O(n \log n)$
- Shifts, Permutations
- NP-hard problems

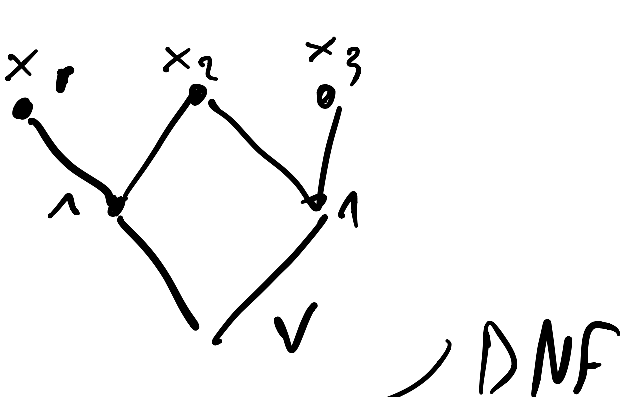
Super-linear Circuit Lower Bounds?

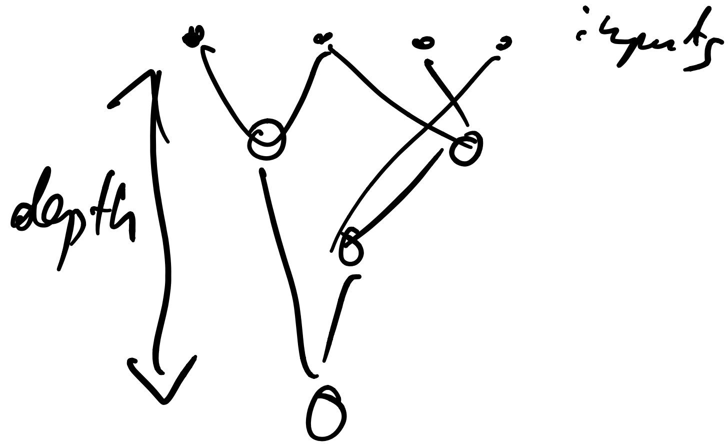
- Two n-bit integers can be multiplied by a circuit of size $O(n \log n)$ [SS71,F07,HH19]
- Discrete Fourier Transform of a sequence of length n can be computed by a circuit of size $O(n \log n)$
- Shifts, Permutations
- **NP**-hard problems
- . . .

What We Can Prove

What We Can Prove

- Depth 2: CNF/DNF. Even $\oplus_n$ requires circuits of size $\Omega(2^n)$.





$(x_1 \wedge x_2) \vee (x_2 \wedge x_3)$

$\text{Parity}_n = x_1 \oplus x_2 \oplus \dots \oplus x_n$

What We Can Prove

- Depth 2: CNF/DNF. Even $\oplus_n$ requires circuits of size $\Omega(2^n)$.
- Constant depth d. Lower bounds $2^{n^{1/(d-1)}}$.

$d=3$ Lower bound $2^{\Omega(\sqrt{n})}$ – parity

What We Can Prove

- Depth 2: CNF/DNF. Even $\oplus_n$ requires circuits of size $\Omega(2^n)$.
- Constant depth d. Lower bounds $2^{n^{1/(d-1)}}$.
- Depth $1.9 \log n$. Know functions that cannot be computed.

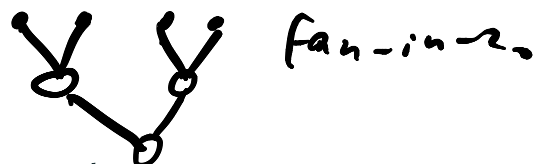
Explicit lower bounds

What We Can Prove

- Depth 2: CNF/DNF. Even $\oplus_n$ requires circuits of size $\Omega(2^n)$.

unbounded fan-in

- Constant depth d. Lower bounds $2^{n^{1/(d-1)}}$.
- Depth $1.9 \log n$. Know functions that cannot be computed.



- Depth $2 \log n$. Nothing better than $\approx 3n$.

Problem on the Frontier

Problem

Prove a lower bound of $10n$ against circuits of depth $10 \log n$.

Problem on the Frontier

Problem

Prove a lower bound of $10n$ against circuits of depth $10 \log n$.

More generally, a lower bound of $\omega(n)$ against circuits of depth $O(\log n)$.

Problem on the Frontier

Problem

Prove a lower bound of $10n$ against circuits of depth $10 \log n$.

More generally, a lower bound of $\omega(n)$ against circuits of depth $O(\log n)$.

Valiant [Val77] gives us an amazing tool to study such circuits.

Another Problem on the Frontier

Problem

Prove a lower bound of $\omega(n)$ against linear circuits of depth $O(\log n)$.

Another Problem on the Frontier

Problem

Prove a lower bound of $\omega(n)$ against linear circuits of depth $O(\log n)$.

Valiant's [Val77] tool for these circuits is even nicer!

Linear Circuits

$x \to Mx$

- A linear map computes Mx for input $x \in \mathbb{F}^n$ where $M \in \mathbb{F}^{m \times n}$

Linear Circuits

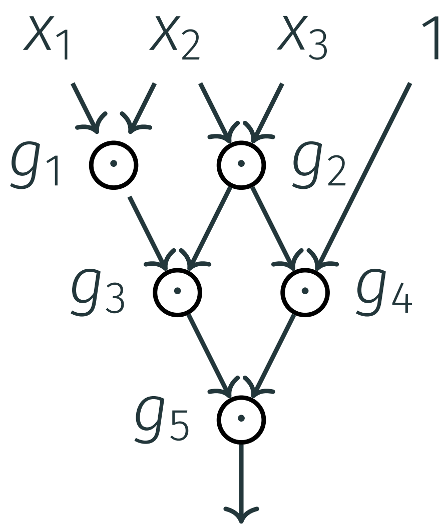
- A linear map computes Mx for input $x \in \mathbb{F}^n$ where $M \in \mathbb{F}^{m \times n}$
- A linear circuit only contains gates that, for inputs x and y, compute $\alpha x + \beta y$ for some $\alpha, \beta \in \mathbb{F}$

E.g., $\mathbb{F} = \mathbb{F}_2$, $\oplus$

$x \to Mx$

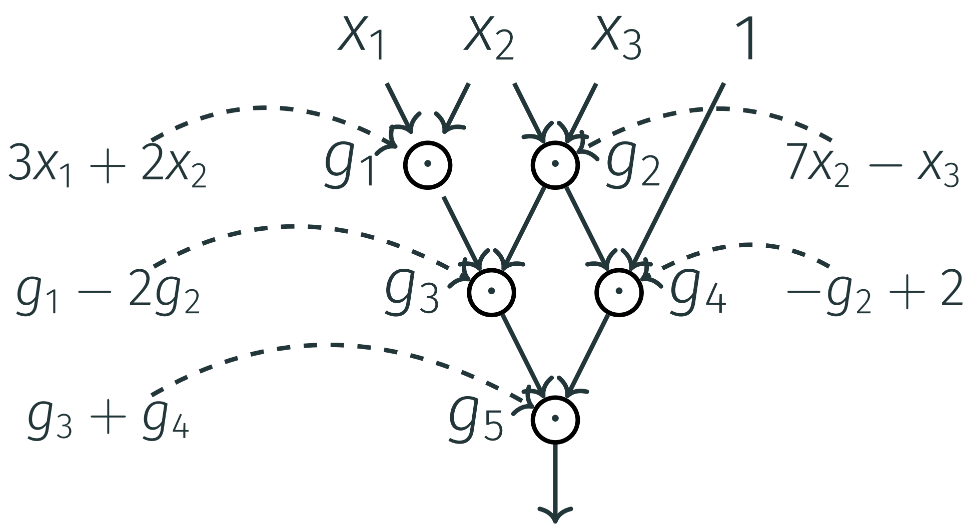
Linear Circuits

- A linear map computes Mx for input $x \in \mathbb{F}^n$ where $M \in \mathbb{F}^{m \times n}$
- A linear circuit only contains gates that, for inputs x and y, compute $\alpha x + \beta y$ for some $\alpha, \beta \in \mathbb{F}$



Linear Circuits

- A linear map computes Mx for input $x \in \mathbb{F}^n$ where $M \in \mathbb{F}^{m \times n}$
- A linear circuit only contains gates that, for inputs x and y, compute $\alpha x + \beta y$ for some $\alpha, \beta \in \mathbb{F}$

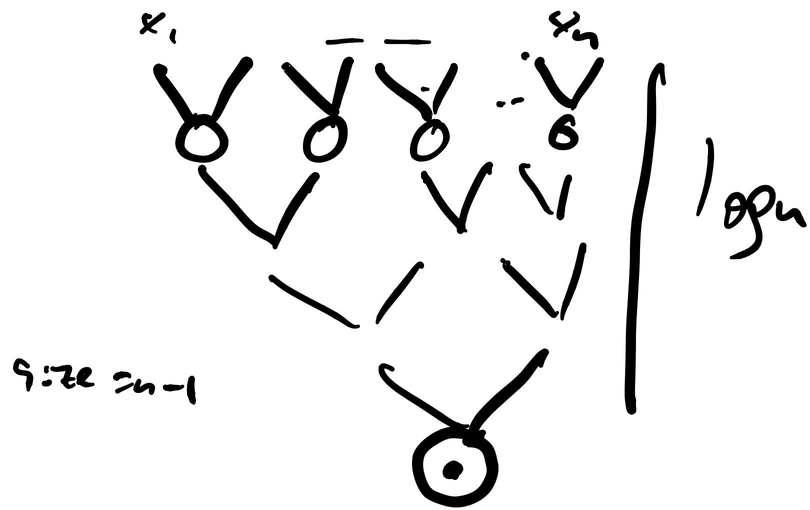


Complexity of Linear Operators

- Linear circuits compute only linear functions

Complexity of Linear Operators

- Linear circuits compute only linear functions
- We don't study linear functions with 1 output as they have circuit complexity $\leq n$ even in depth $\log n$



Complexity of Linear Operators

- Linear circuits compute only linear functions
- We don't study linear functions with 1 output as they have circuit complexity $\leq n$ even in depth $\log n$
- A random linear map with n outputs has complexity $n^2/\log n$

Complexity of Linear Operators

- Linear circuits compute only linear functions
- We don't study linear functions with 1 output as they have circuit complexity $\leq n$ even in depth $\log n$
- A random linear map with n outputs has complexity $n^2 / \log n$
- The best lower bound we can prove against linear circuits with n outputs is $3n - o(n)$

$\{0,1\}^n \to \{0,1\}^n$

Another Problem on the Frontier

Problem

Prove a lower bound of $\omega(n)$ *against linear circuits of depth* $O(\log n)$.

Another Problem on the Frontier

Problem

Prove a lower bound of $\omega(n)$ against linear circuits of depth $O(\log n)$.

- Incomparable to the previous problem (bounds against non-linear circuits):

Another Problem on the Frontier

Problem

Prove a lower bound of $\omega(n)$ against linear circuits of depth $O(\log n)$.

- Incomparable to the previous problem (bounds against non-linear circuits):
- Weaker computational model

Another Problem on the Frontier

Problem

Prove a lower bound of $\omega(n)$ against linear circuits of depth $O(\log n)$.

- Incomparable to the previous problem (bounds against non-linear circuits):
- Weaker computational model
- But fewer problems to prove lower bounds for.

Circuits and Rigidity

Rigidity Implies Circuit Lower Bounds

Theorem (Val77)

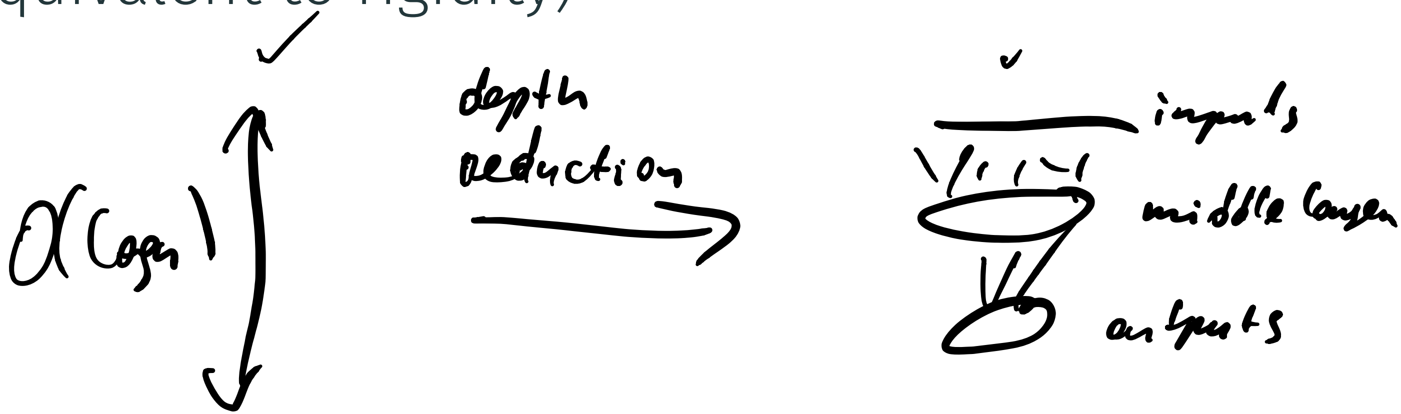
Let $\mathbb{F}$ be a field, and $A \in \mathbb{F}^{n \times n}$ be a family of matrices for $n \in \mathbb{N}$.

If $\mathcal{R}_A^{\mathbb{F}}(\varepsilon n) > n^{1+\delta}$ for constant $\varepsilon, \delta > 0$, then any $O(\log n)$-depth linear circuit computing $x \to Ax$ must be of size $\omega(n)$.

Rigidity for rank $n/100$ and sparsity $n^{1.01}$ implies super-linear log-depth circuit lower bounds

Depth Reductions

- The proof (see Lecture 1) reduces the depth of a circuit from $O(\log n)$ to 2 (and the latter is equivalent to rigidity)



Depth Reductions

- The proof (see Lecture 1) reduces the depth of a circuit from $O(\log n)$ to 2 (and the latter is equivalent to rigidity)
- The proof is graph-theoretic, and graph-theoretic proofs cannot go beyond $O(\log n)$ depth [Sch82, Sch83, Kla94]

Depth Reductions

- The proof (see Lecture 1) reduces the depth of a circuit from $O(\log n)$ to 2 (and the latter is equivalent to rigidity)
- The proof is graph-theoretic, and graph-theoretic proofs cannot go beyond $O(\log n)$ depth [Sch82, Sch83, Kla94]
- A non-graph-theoretic proof [GKW21] works for unbounded-depth circuits, but alas only for size $< 4n$

Unbounded-depth and Rigidity

Theorem (GKW21)

Let $\mathbb{F}$ be a field, and $A \in \mathbb{F}^{n \times n}$ be a family of matrices for $n \in \mathbb{N}$.

If $\mathcal{R}_A^{\mathbb{F}}(\varepsilon n) > 16n$, then any linear circuit computing $x \to Ax$ must be of size $\geq 4\varepsilon n$.

If $R_A^{\mathbb{F}_2}(0.99n) > 16n$

$\Rightarrow$ $x \to Ax$ requires circuits of size

$4 \cdot 0.99n > 3.9n$

Rigidity for rank $0.99n$ and sparsity $16n$ implies circuit lower bound of $3.9n$

Comparison

Valiant

If $\mathcal{R}_A^{\mathbb{F}}(\varepsilon n) > n^{1+\delta}$, then A requires log-depth circuits of size $\omega(n)$

Comparison

If $\mathcal{R}_A^{\mathbb{F}}(\varepsilon n) > n^{1+\delta}$, then A requires log-depth circuits of size $\omega(n)$

If $\mathcal{R}_A^{\mathbb{F}}(0.99n) > 16n$, then A requires unbounded-depth circuits of size $3.9n$

Comparison

If $\mathcal{R}_A^{\mathbb{F}}(\varepsilon n) > n^{1+\delta}$, then A requires log-depth circuits of size $\omega(n)$

If $\mathcal{R}_A^{\mathbb{F}}(0.99n) > 16n$, then A requires unbounded-depth circuits of size $3.9n$

Best known explicit rigidity lower bound:

$\mathcal{R}_A^{\mathbb{F}}(r) \geq \Omega(\frac{n^2}{r} \log \frac{n}{r})$

$16n \gg \mathcal{R}_A^{\mathbb{F}_2}(0.99n) > \Omega(n)$

For a random / non-explicit we have

$\mathcal{R}_A^{\mathbb{F}_2}(0.99n) > \Omega(n^2)$

Main Result

Theorem

For every matrix $M \in \mathbb{F}_2^{m \times n}$ of circuit complexity s,

$$\mathcal{R}_M^{\mathbb{F}_2}(\lfloor s/4 \rfloor) \le 16m.$$

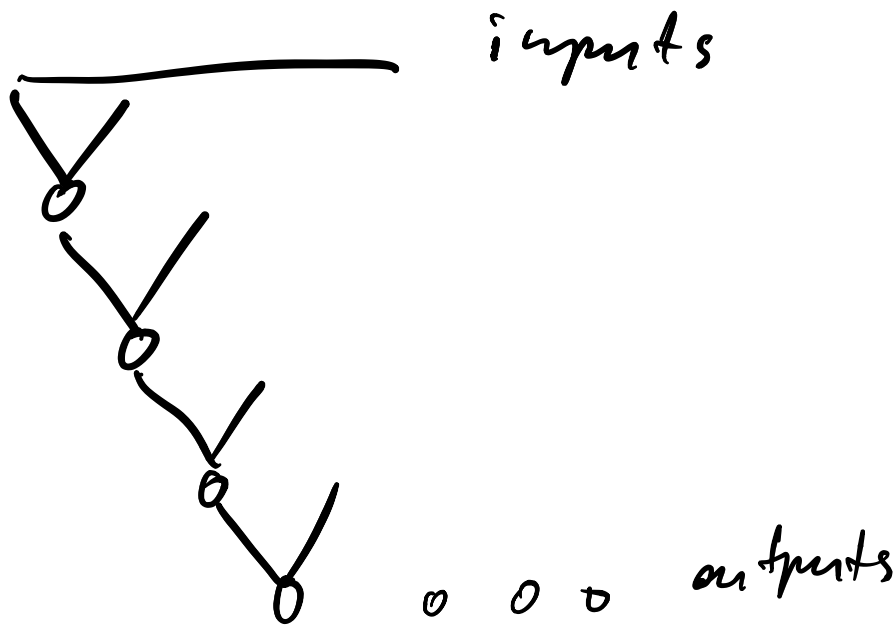
m=n

$R(\varepsilon n) > 16n \Rightarrow$ circuits of size $> 4\varepsilon n$

Base case: if depth of the circuit (depth of all outputs) ≤ 4

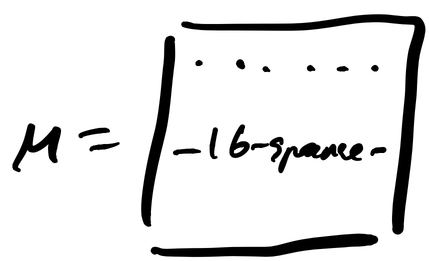
$\Rightarrow \|M\|_0 \leq 16n$

$\Rightarrow M = S + 0$



Every outputs depends on ≤ 16 inputs.

$x \rightarrow Mx$

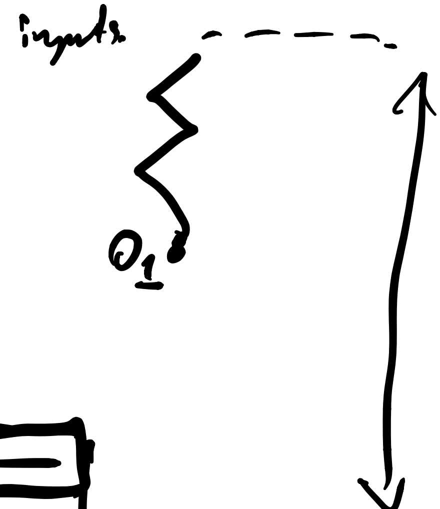


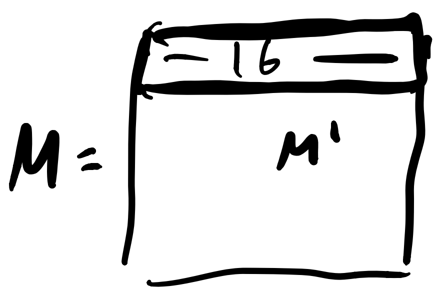
$\Rightarrow \|M\|_0 \le 16n$

$|R_M(O)| \le 16n$

Ind step:

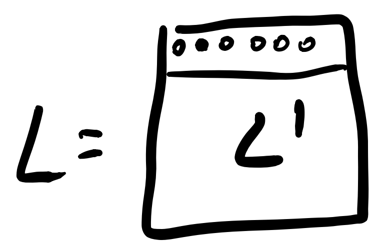
Case 1. If $\exists$ output of depth ≤ 4





$M' = S' + L'$

$M = S + L$



Remaining case:

All outputs have high depth.

Lin fn $G = x_1 \oplus x_3 \oplus x_7$

IF $G = 0$ then

$C(x) = C'(x)$ where $\text{size}(C') \le \text{size}(C) - 4$.

$C' : x \to M'x$

By ind hyp.,

$M' = S' + L'$

$\|S'\|_0 \le 16n$

$$\text{Rk}(L') \le \frac{\text{size}(C')}{4} = \frac{\text{size}(C)}{4} - 1$$

$M = S + L$; $S = S'$

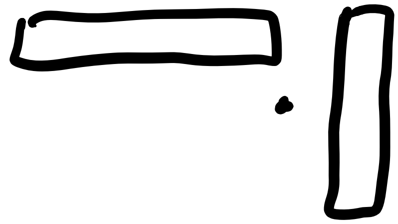
$$\text{Rk}(L) \le \text{Rk}(L') + 1 \le \frac{\text{size}(C)}{4}$$

IF $x_1 \oplus x_3 \oplus x_7 = 0$ $\Rightarrow$ $Mx = M'x$

$\Rightarrow (M - M')x = 0 \quad \forall x$

1. $M = M'$

2. $(M - M')_x = x_1 \oplus x_3 \oplus x_7$

$M = M' +$ 

$$M = M' + A, \quad rk(A) \le 1$$

$$M = M' + A = S + L$$

$$L = L' + \Delta$$

$$rk(L) \le rk(L') + 1 \le \frac{size(C)}{4}$$

One Step

Claim

Let $\mathcal{C}$ be an optimal linear circuit computing $M \in \{0,1\}^{m \times n}$ such that no output gate of $\mathcal{C}$ has depth smaller than 5. Then there is a gate G in $\mathcal{C}$ and a linear circuit $\mathcal{C}'$ computing a matrix $M' \in \{0,1\}^{m \times n}$ with the properties:

- $s(\mathcal{C}') \leq s(\mathcal{C}) - 4$, and
- for every $x \in \{0,1\}^n$,
  if $G(x) = 0$ then $\mathcal{C}(x) = \mathcal{C}'(x)$.

Claim

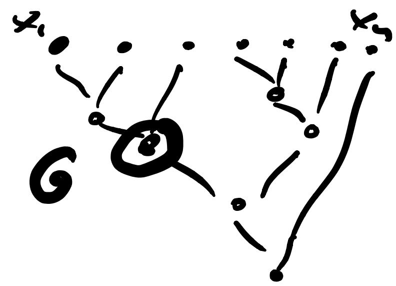
Let $\mathcal{C}$ be an optimal linear circuit computing $M \in \{0,1\}^{m\times n}$ such that no output gate of $\mathcal{C}$ has depth smaller than 5. Then there is a gate G in $\mathcal{C}$ and a linear circuit $\mathcal{C}'$ computing a matrix $M' \in \{0,1\}^{m\times n}$ with the properties:

- $s(\mathcal{C}') \leq s(\mathcal{C}) - 4$, and
- for every $x \in \{0,1\}^n$, if $G(x) = 0$ then $\mathcal{C}(x) = \mathcal{C}'(x)$.

C:

$s(C) = s$

$C: x \to Mx$



If $G = 0$, then I have a smaller ckt.

$G = x_1 \oplus x_3 \oplus x_7$

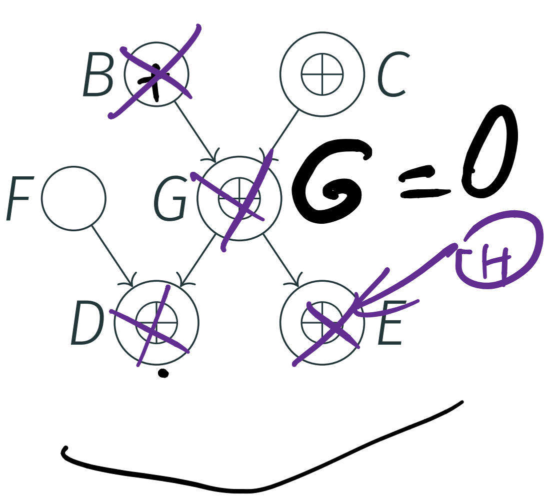
x_1	x_3	x_7	G	G
0	0	0	0	
0	0	1		1
0	1	0		
0	1	1	0	
1	0	0		1
1	0	1	0	
1	1	0	0	
1	1	1		1

Then $C' : x \to M'x$

1. $G = 0 \Rightarrow C(x) = C'(x)$
2. $s(C') \leq s(C) - 4$

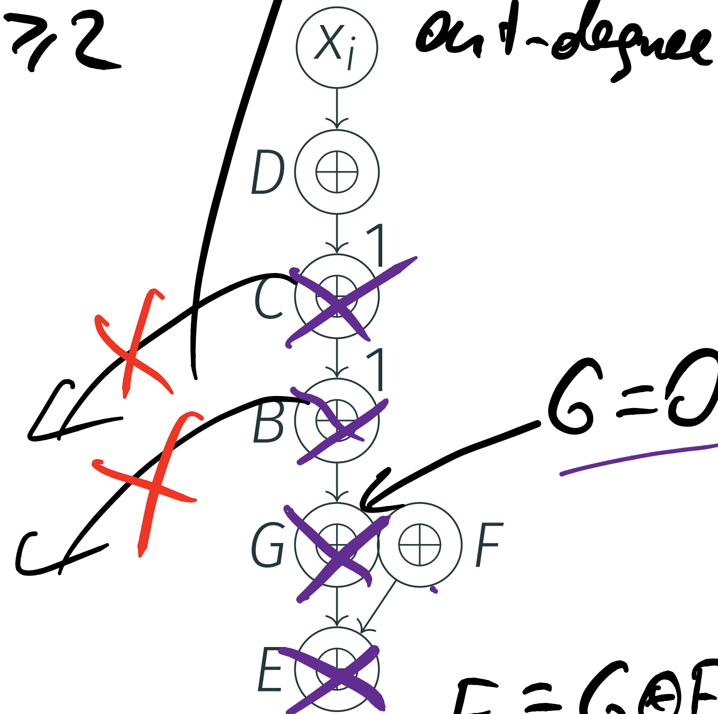
PROOF

$\exists$ gate G at depth $\{2,3,4\}$ s.t. out-degree$(G) \geq 2$



Case 1

$\forall$ gates depth $\{2,3,4\}$ have out-degree $= 1$



Case 2

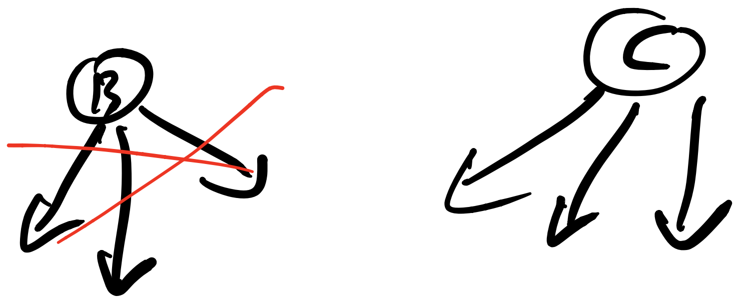
$E = G \oplus F$

$G = 0$

$E \equiv F$

Case 1: I don't need gate B.

$$B \equiv C$$



$$F \oplus G = D$$

But $G = 0 \Rightarrow F = D$

Removed B, G, D, E