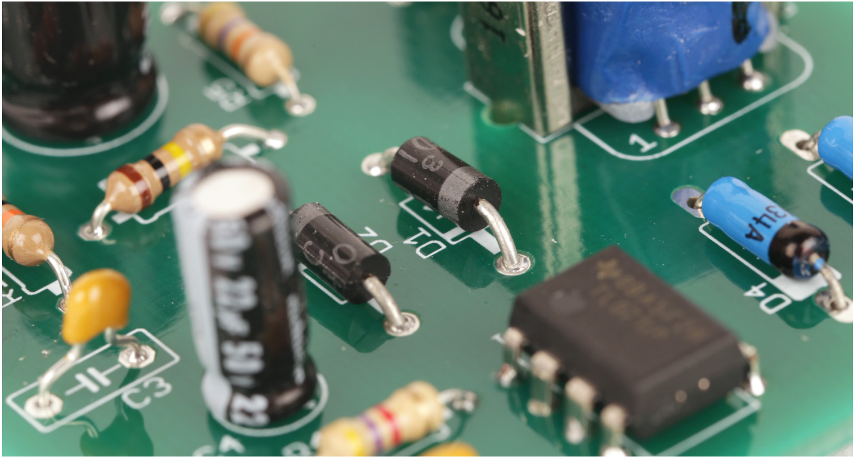
Gems of TCS

Circuit Complexity

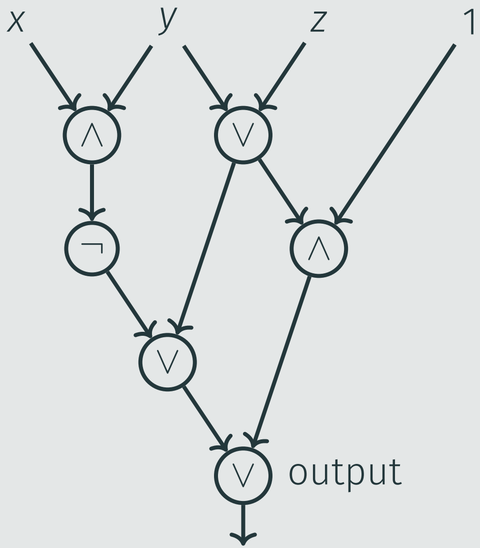
Sasha Golovnev

October 19, 2022



C3
D2
D1
D4

Circuit



Definition

A circuit is a directed acyclic graph of in-degree at most 2. Nodes of in-degree 0 are called inputs and are marked by Boolean variables and constants. Nodes of in-degree 1 and 2 are called gates: gates of in-degree 1 are labeled with NOT, gates of in-degree 2 are labeled with AND or OR. One of the sinks is marked as output.

Boolean Circuits

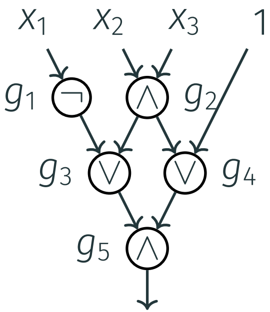
$$f\colon \{0,1\}^n \to \{0,1\}$$

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

Boolean Circuits

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

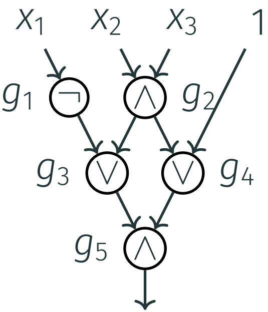
$$\begin{aligned} g_1 &= \neg x_1 \\ g_2 &= x_2 \wedge x_3 \\ g_3 &= g_1 \vee g_2 \\ g_4 &= g_2 \vee 1 \\ g_5 &= g_3 \wedge g_4 \end{aligned}$$



Boolean Circuits

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

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



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

Gates:
AND, OR, NOT

Fan-out:
unbounded

Depth:
unbounded

Exponential Bounds

Lower Bound [Sha1949]

Almost all functions of n variables have circuit size

$$\geq 2^n/n$$

Exponential Bounds

Lower Bound [Sha1949]

Almost all functions of n variables have circuit size

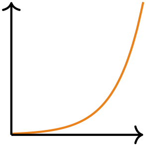
$$\geq 2^n/n$$

Upper Bound [Lup1958]

Any function can be computed by a circuit of size

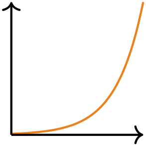
$$\leq 2^n/n$$

Explicit Bounds



Most functions have exponential circuit complexity

Explicit Bounds

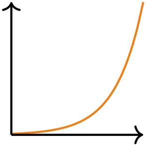


Most functions have exponential circuit complexity

$$P \neq NP$$

We want to prove super-polynomial lower bounds

Explicit Bounds

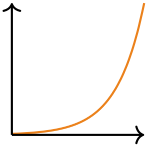


Most functions have exponential circuit complexity

$P \neq NP$

We want to prove superpolynomial lower bounds (for a function from **NP**)

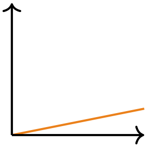
Explicit Bounds



Most functions have exponential circuit complexity

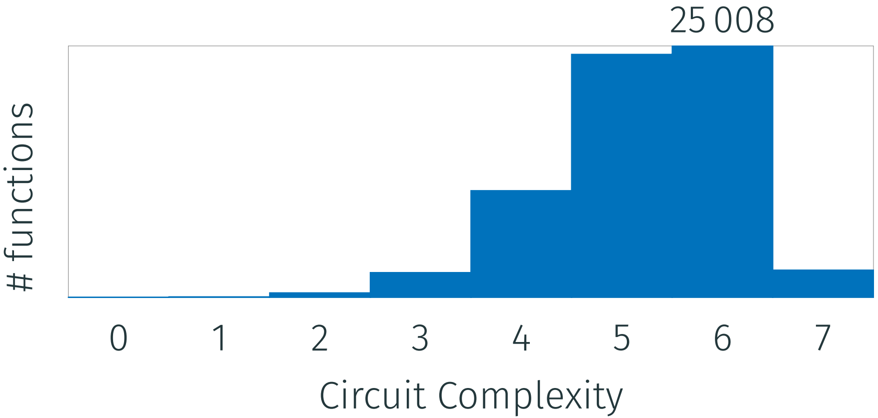
$P \neq NP$

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

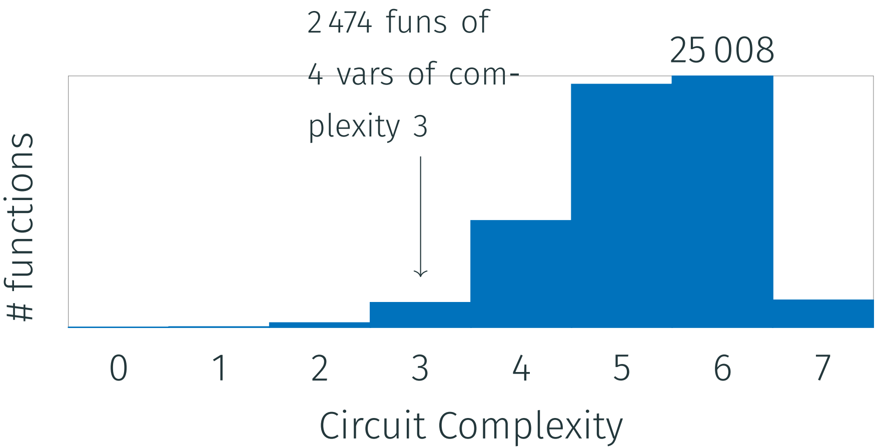


We can prove only $\approx 5n$ lower bounds

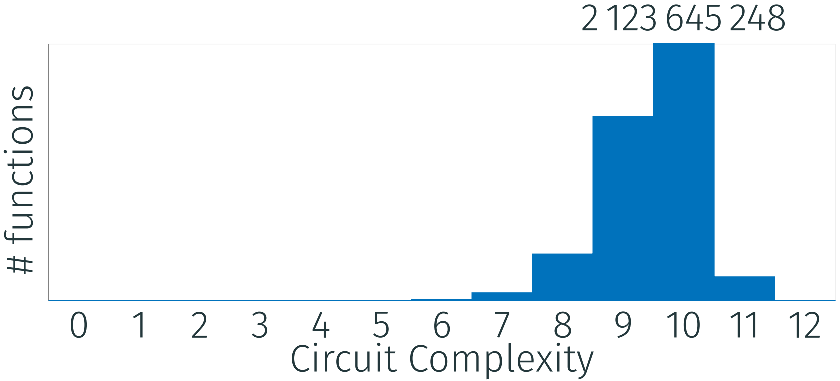
Circuit Complexity: $n = 4$



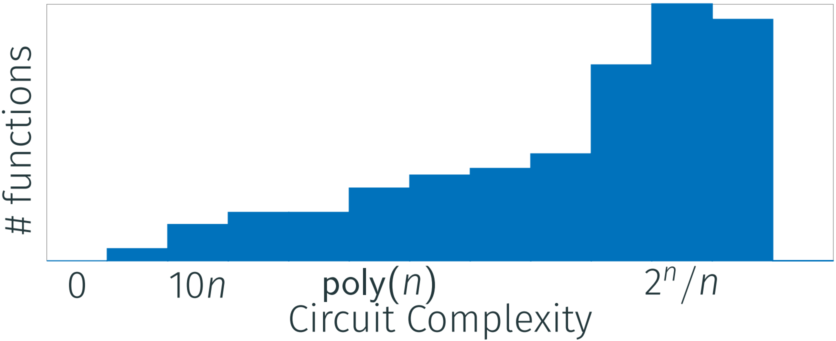
Circuit Complexity: $n = 4$



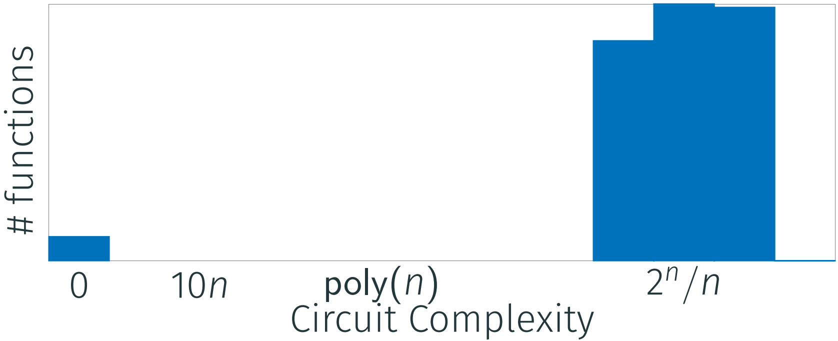
Circuit Complexity: $n = 5$



Circuit Complexity: General n



Circuit Complexity: General n



Hierarchy Theorem

Theorem

For any $T \leq 2^n/n$, there is a function $f\colon \{0,1\}^n \to \{0,1\}$ s.t.

$$\mathsf{Size}(f) = T \pm n\,.$$

Hierarchy Theorem

Theorem

For any $T \leq 2^n/n$, there is a function $f\colon \{0,1\}^n \to \{0,1\}$ s.t.

$$\mathrm{Size}(f) = T \pm n\,.$$

$$g_0(x) = 0\,, \forall x \in \{0,1\}^n$$

Hierarchy Theorem

Theorem

For any $T \leq 2^n/n$, there is a function $f\colon \{0,1\}^n \to \{0,1\}$ s.t.

$$\text{Size}(f) = T \pm n\,.$$

$$g_0(x) = 0\,, \forall x \in \{0,1\}^n$$

$$\text{Size}(g_0) = 1$$

Hierarchy Theorem

Theorem

For any $T \leq 2^n/n$, there is a function $f\colon \{0,1\}^n \to \{0,1\}$ s.t.

$$\mathrm{Size}(f) = T \pm n\,.$$

$g_0(x) = 0\,, \forall x \in \{0,1\}^n$

$\mathrm{Size}(h) \geq 2^n/n$

$\mathrm{Size}(g_0) = 1$

Hierarchy Theorem

Theorem

For any $T \leq 2^n/n$, there is a function $f\colon \{0,1\}^n \to \{0,1\}$ s.t.

$$\mathrm{Size}(f) = T \pm n\,.$$

$$g_0(x) = 0\,, \forall x \in \{0,1\}^n$$

$$\mathrm{Size}(h) \geq 2^n/n$$

$$\mathrm{Size}(g_0) = 1$$

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

Hierarchy Theorem

Theorem

For any $T \leq 2^n/n$, there is a function $f\colon \{0,1\}^n \to \{0,1\}$ s.t.

$$\text{Size}(f) = T \pm n\,.$$

$$g_0(x) = 0\,, \forall x \in \{0,1\}^n$$

$$\text{Size}(g_0) = 1$$

$$\text{Size}(h) \geq 2^n/n$$

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

$$y_1, \ldots, y_k \in \{0,1\}^n$$

$$h(y_i) = 1$$

Hybrid Method

$g_0(x) = 1$ never

Hybrid Method

$g_0(x) = 1$ never

$g_1(x) = 1$ if $x = y_1$

Hybrid Method

$g_0(x) = 1$ never

$g_1(x) = 1$ if $x = y_1$

$g_2(x) = 1$ if $x \in \{y_1, y_2\}$

Hybrid Method

$g_0(x) = 1$ never

$g_1(x) = 1$ if $x = y_1$

$g_2(x) = 1$ if $x \in \{y_1, y_2\}$

$g_3(x) = 1$ if $x \in \{y_1, y_2, y_3\}$

Hybrid Method

$g_0(x) = 1$ never

$g_1(x) = 1$ if $x = y_1$

$g_2(x) = 1$ if $x \in \{y_1, y_2\}$

$g_3(x) = 1$ if $x \in \{y_1, y_2, y_3\}$

$\dots$

$g_k(x) = 1$ if $x \in \{y_1, \dots, y_k\}$

Hybrid Method

$$g_0(x) = 1 \text{ never}$$

$$g_1(x) = 1 \text{ if } x = y_1$$

$$g_2(x) = 1 \text{ if } x \in \{y_1, y_2\}$$

$$g_3(x) = 1 \text{ if } x \in \{y_1, y_2, y_3\}$$

$$\cdots$$

$$h = g_k(x) = 1 \text{ if } x \in \{y_1, \ldots, y_k\}$$

Hybrid Method

$g_0(x) = 1$ never

$g_1(x) = 1$ if $x = y_1$

$g_2(x) = 1$ if $x \in \{y_1, y_2\}$

$g_3(x) = 1$ if $x \in \{y_1, y_2, y_3\}$

$\dots$

$h = g_k(x) = 1$ if $x \in \{y_1, \dots, y_k\}$

$$g_{i+1}(x) = g_i(x) \vee (x = y_{i+1})$$

Hybrid Method

$$g_0(x) = 1 \text{ never}$$

$$g_1(x) = 1 \text{ if } x = y_1$$

$$g_2(x) = 1 \text{ if } x \in \{y_1, y_2\}$$

$$g_3(x) = 1 \text{ if } x \in \{y_1, y_2, y_3\}$$

$$\dots$$

$$h = g_k(x) = 1 \text{ if } x \in \{y_1, \dots, y_k\}$$

$$g_{i+1}(x) = g_i(x) \vee (x = y_{i+1})$$

$$g_{i+1}(x) = g_i(x) \vee (x = 1011)$$

Hybrid Method

$$g_0(x) = 1 \text{ never}$$

$$g_1(x) = 1 \text{ if } x = y_1$$

$$g_2(x) = 1 \text{ if } x \in \{y_1, y_2\}$$

$$g_3(x) = 1 \text{ if } x \in \{y_1, y_2, y_3\}$$

$$\dots$$

$$h = g_k(x) = 1 \text{ if } x \in \{y_1, \dots, y_k\}$$

$$g_{i+1}(x) = g_i(x) \vee (x = y_{i+1})$$

$$g_{i+1}(x) = g_i(x) \vee (x = 1011)$$

$$g_{i+1}(x) = g_i(x) \vee (x_1 \wedge \bar{x}_2 \wedge x_3 \wedge x_4)$$

Hybrid Method

$$g_0(x) = 1 \text{ never}$$

$$g_1(x) = 1 \text{ if } x = y_1$$

$$g_2(x) = 1 \text{ if } x \in \{y_1, y_2\}$$

$$g_3(x) = 1 \text{ if } x \in \{y_1, y_2, y_3\}$$

$$\ldots$$

$$h = g_k(x) = 1 \text{ if } x \in \{y_1, \ldots, y_k\}$$

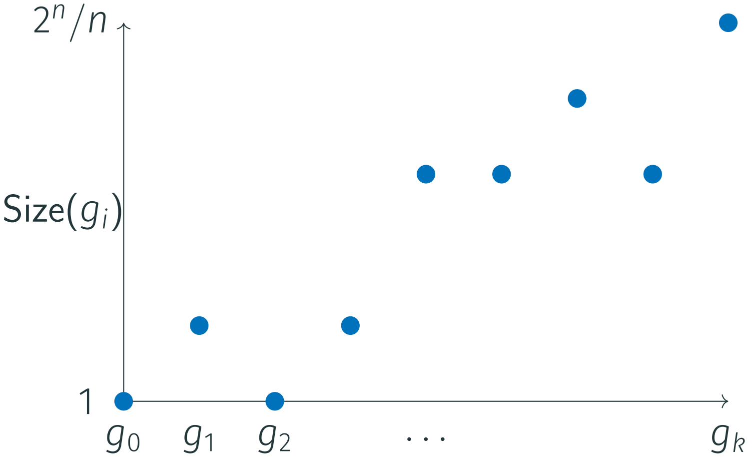
$$g_{i+1}(x) = g_i(x) \vee (x = y_{i+1})$$

$$g_{i+1}(x) = g_i(x) \vee (x = 1011)$$

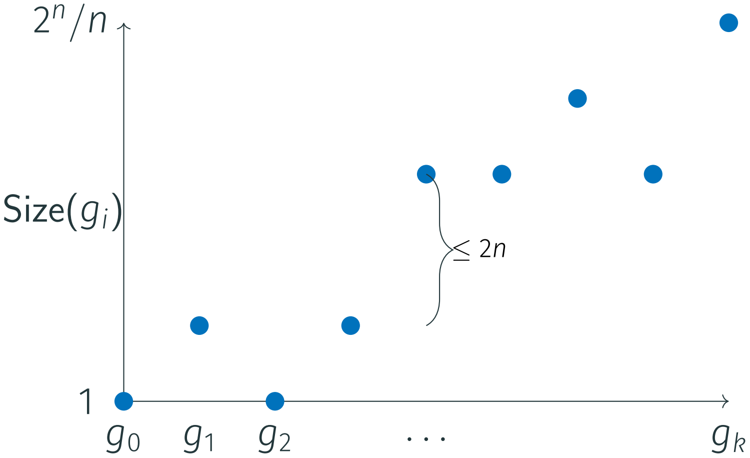
$$g_{i+1}(x) = g_i(x) \vee (x_1 \wedge \bar{x}_2 \wedge x_3 \wedge x_4)$$

$$\text{Size}(g_{i+1}) \leq \text{Size}(g_i) + 2n$$

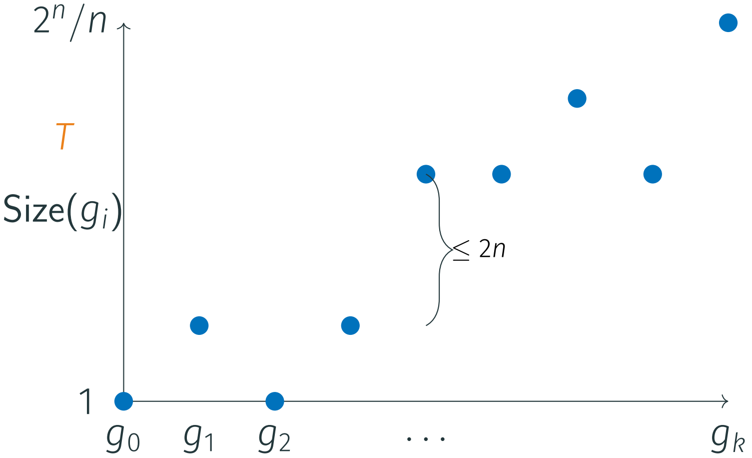
Hierarchy Theorem



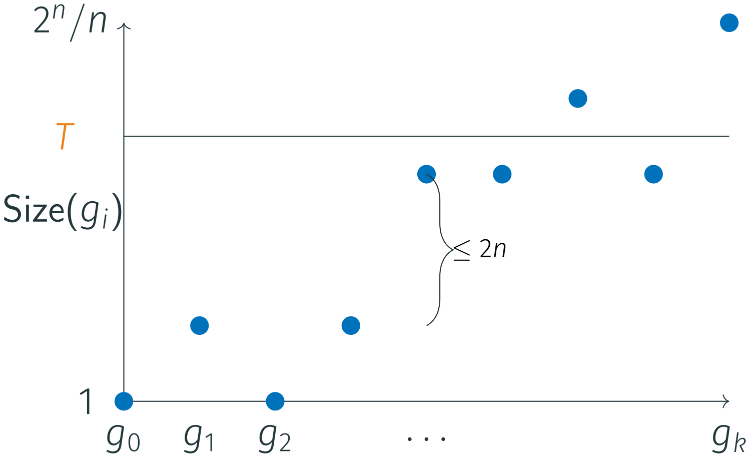
Hierarchy Theorem



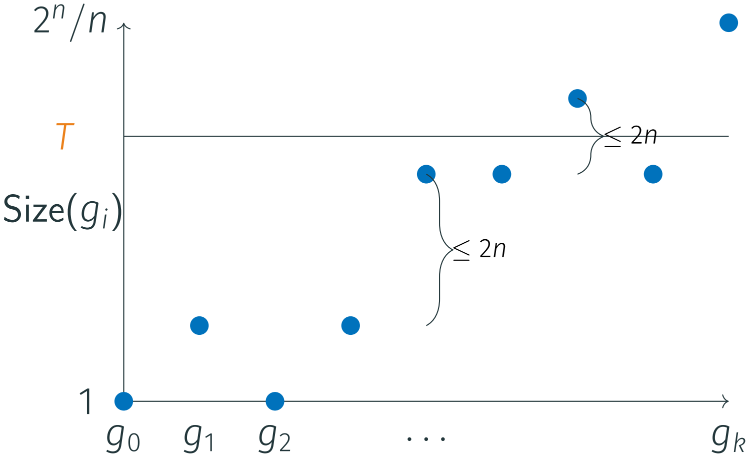
Hierarchy Theorem



Hierarchy Theorem



Hierarchy Theorem



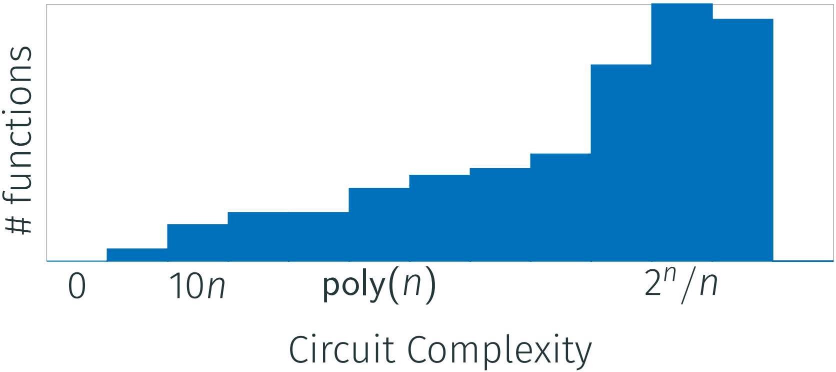
Hierarchy Theorem

Theorem

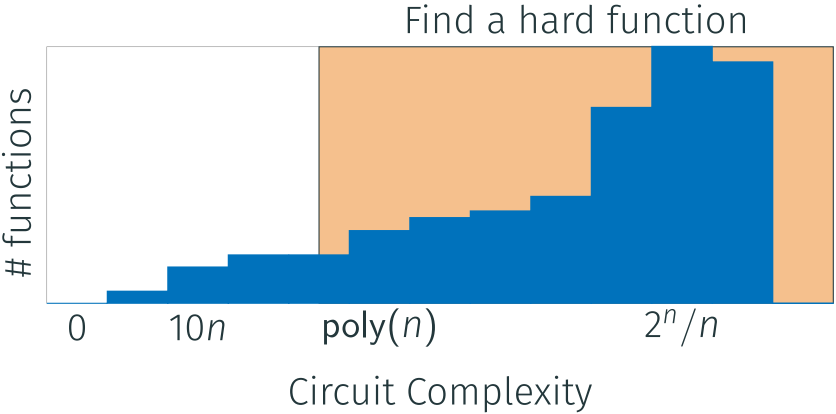
For any $T \leq 2^n/n$, there is a function $f\colon \{0,1\}^n \to \{0,1\}$ s.t.

$$\mathrm{Size}(f) = T \pm n\,.$$

Goal



Goal



Find a hard function
functions
0
10n
poly(n)
$2^n/n$
Circuit Complexity

Circuit Complexity

- Goal: Find a hard function

Circuit Complexity

- Goal: Find a hard function
- Lower bounds: what functions are hard

Circuit Complexity

- Goal: Find a hard function
- Lower bounds: what functions are hard
- Upper bounds: what functions are easy

Circuit Upper Bound. Proof

Upper Bound [Lup1958]

Any function can be computed by a circuit of size

$$\leq 10 \cdot 2^n$$

Circuit Upper Bound. Proof

Upper Bound [Lup1958]

Any function can be computed by a circuit of size

$$\leq 10 \cdot 2^n$$

$$f(x_1, \dots, x_n) = \begin{cases} f(1, x_2, \dots, x_n), & \text{if } x_1 = 1 \\ f(0, x_2, \dots, x_n), & \text{if } x_1 = 0 \end{cases}$$

Circuit Upper Bound. Proof

Upper Bound [Lup1958]

Any function can be computed by a circuit of size

$$\leq 10 \cdot 2^n$$

$$f(x_1, \ldots, x_n) = \begin{cases} f(1, x_2, \ldots, x_n), & \text{if } x_1 = 1 \\ f(0, x_2, \ldots, x_n), & \text{if } x_1 = 0 \end{cases}$$

$$= (x_1 \wedge f(1, x_2, \ldots, x_n)) \vee (\bar{x}_1 \wedge f(0, x_2, \ldots, x_n))$$

Circuit Upper Bound. Proof

Upper Bound [Lup1958]

Any function can be computed by a circuit of size

$$\leq 10 \cdot 2^n$$

$$f(x_1, \ldots, x_n) = \begin{cases} f(1, x_2, \ldots, x_n), & \text{if } x_1 = 1 \\ f(0, x_2, \ldots, x_n), & \text{if } x_1 = 0 \end{cases}$$

$$= (x_1 \wedge f(1, x_2, \ldots, x_n)) \vee (\bar{x}_1 \wedge f(0, x_2, \ldots, x_n))$$

$$= (x_1 \wedge g_1(x_2, \ldots, x_n)) \vee (\bar{x}_1 \wedge g_0(x_2, \ldots, x_n))$$

Circuit Upper Bound. Proof

Upper Bound [Lup1958]

Any function can be computed by a circuit of size

$$\leq 10 \cdot 2^n$$

$$f(x_1, \ldots, x_n) = \begin{cases} f(1, x_2, \ldots, x_n), & \text{if } x_1 = 1 \\ f(0, x_2, \ldots, x_n), & \text{if } x_1 = 0 \end{cases}$$

$$= (x_1 \wedge f(1, x_2, \ldots, x_n)) \vee (\bar{x}_1 \wedge f(0, x_2, \ldots, x_n))$$

$$= (x_1 \wedge g_1(x_2, \ldots, x_n)) \vee (\bar{x}_1 \wedge g_0(x_2, \ldots, x_n))$$

$$\mathsf{Size}(n) \leq 4 + 2\,\mathsf{Size}(n-1) = O(2^n)$$

Circuit Lower Bound. Proof

Lower Bound [Sha1949]

Almost all functions of n variables have circuit size

$$\geq 2^n/(10n)$$