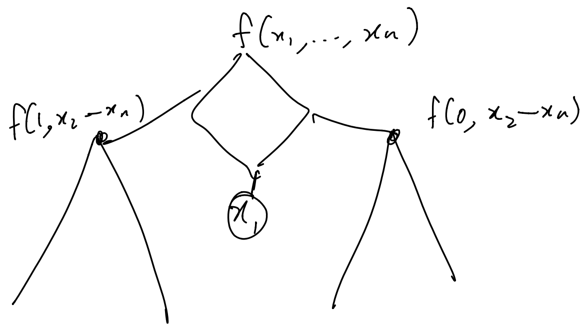
Boolean Circuits

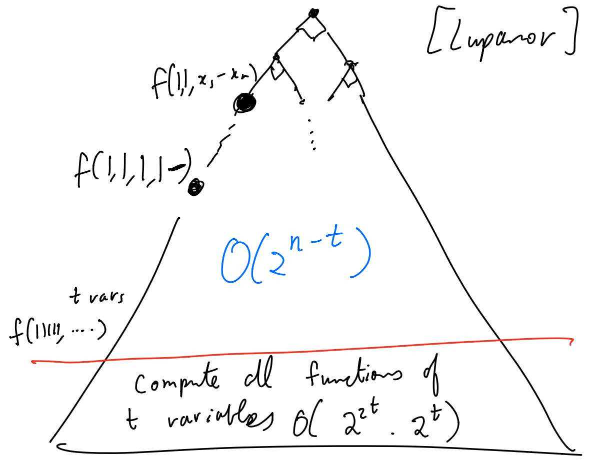
$f: \{0,1\}^n \to \{0,1\}$

Thm: Can be computed in size $O(2^n)$.

$f(x_1, \dots, x_n)$

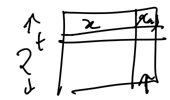


[Lupanov]



\# functions that depend on t inputs

$g: \{0,1\}^t \to \{0,1\} = 2^{2^t}$



$$\text{Size} \le O\left(2^{2^t} \cdot 2^t + 2^{n-t}\right)$$

set $t = \log n - 1$ $\quad = 2^{n/2} \cdot 2^{\log n - 1} + 2^{n - \log n + 1}$

$$= \frac{2^{n/2 + \log n}}{2} + 2 \cdot 2^n/n \le O(2^n/n).$$

Thm: $\forall f: \{0,1\}^n \to \{0,1\}$, there is a circuit of size $O(2^n/n)$ computing f.

Thm: $\exists f: \{0,1\}^n \to \{0,1\}$, s.t. need $\ge 2^n/3n$ gates to compute f.

Counting Argument

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

$\#$ functions $f = 2^{2^n}$

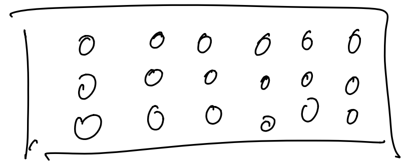
$\#$ functions f computable by circuits of size s $< 2^{3s\log s}$

$(s > n)$

$(n > 4)$

set $s = \frac{2^n}{3n}$ $\quad < 2^{3\frac{2^n}{3n}\cdot n} = 2^{2^n}$

$s = 2^n/4n$ $\quad \leq 2^{\frac{3}{4}2^n}$



$\#$ choices for each location

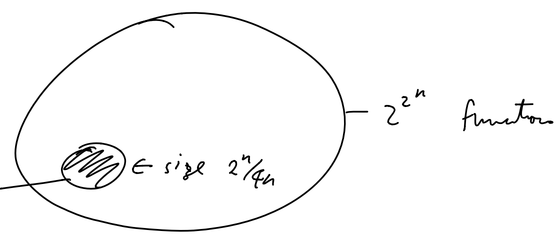
$(n + 3s^2)$

$\#$ circuits $\leq (n+3s^2)^s$

$\leq (4s^2)^s$

$= 2^{s\log(4s^2)}$

$\leq 2^{3s\log s}$



$2^{\frac{3}{4}2^n - 2^n}$

$= 2^{-2^n/4}$

Counting for T.M

$\#$ Turing machines $\overset{?}{<<}$ $\#$ functions $f : \{0,1\}^* \to \{0,1\}$

$\mathbb{N} = \{1,2,3,4,\ldots\}$ } countably infinite

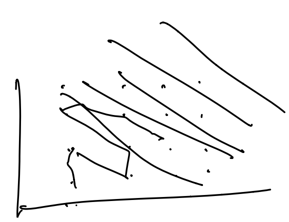
$\mathbb{Z} = \{\ldots,-2,-1,0,1,2,\ldots\}$ }

$\{0,1\}^*$ }

Def: S is countable if $\exists\ \phi : \mathbb{N} \to S$ that is surjective.

$\phi(1), \phi(2), \ldots$

$\mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\}$



$\mathbb{Q} =$

Thm: $2^{\mathbb{N}} = \{ S : S \subseteq \mathbb{N} \}$ is not countable

$$\begin{array}{c|cccccc}
 & 1 & 2 & 3 & 4 & 5 & 6 \; \ldots \\
\hline
S_1 & 0 & 1 & 1 & 0 & 0 & 0 \\
S_2 & 0 & 1 & 1 & 1 & 1 & 0 \\
S_3 & 0 & 1 & 0 & 1 & 0 & 1 \\
S_4 & 1 & 1 & 1 & 1 & 1 & 1 \\
\vdots & & & & & & \\
T = S_j & & & & & & \boxed{}
\end{array}$$

$(i,j)^{th}$ entry is
$0 \iff j \notin S_i$
$1 \iff j \in S_i$

$\exists\, T \subseteq \mathbb{N}$ which does not occur in the list

$T = \{ i : (i,i)^{th} \text{ entry is } 0 \}$.

Consider $\alpha \in \{0,1\}^*$ M_α = T.M using code α.

$$f : \{0,1\}^* \to \{0,1\}$$

$$f(\alpha) = \begin{cases} 1 & \text{if } M_\alpha(\alpha) = 0 \\ 0 & \text{otherwise (includes } M_\alpha(\alpha) \text{ does not halt)} \end{cases}$$

Claim: f cannot be computed.

$M_\gamma(\gamma) = 0 \quad \times \quad f(\gamma) = 1$
$\quad\quad\;\; = 1 \quad \times \quad f(\gamma) = 0$
or does not halt

$\mathrm{HALT}(\alpha, x) = 1$ if $M_\alpha(x)$ halts
$\quad\quad\quad\quad\;\; = 0$ o.w.

Thm: HALT cannot be computed by a T.M.

Pf: If H computes HALT.

$\underline{M(\alpha)}$
Check that $M_\alpha(\alpha)$ Halts using H.
If $M_\alpha(\alpha) = 0$ output 1 o/w output 0.

Gödel's Incompleteness Theorem

Thm: Every consistent finite set of axioms is incomplete $\rightarrow$ $\exists$ true statement that cannot be proved

$x \in \{0,1\}^*$

$K(x)$ = length of shortest program that outputs x.

$S_{x,N}$ $\quad\quad K(x) > N$

Fact: For every N, $\exists\ x$ s.t $S_{x,N}$ is true.

Pf: M_N

- Enumerate over all pairs (x, α). If α describes a proof of $S_{x,N}$ using the axioms, output x.

$O(\log N)$

$\rightarrow$ M_N always outputs x s.t $S_{x,N}$ holds.