Lecture 10

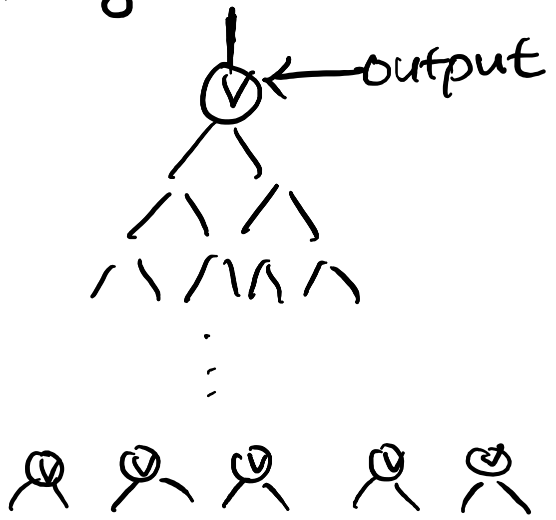
Recap : Boolean Circuit

· $\vee, \wedge, \neg$, in-degree ≤ 2 .

· XOR . XOR (addition mod2) .

$1+1=0$
$1+0=1$
$0+0=0$

ex Computing OR of n-bits.



All functions can be computed by circuit

boolean

exponentially many gates.

proof via induction.

$S(1) = O(1)$.

$S(k+1)$

base case ✓

induction input bits $\leq k$ can be computed via ckt. $\leq 2 \cdot S(k) + O(1)$

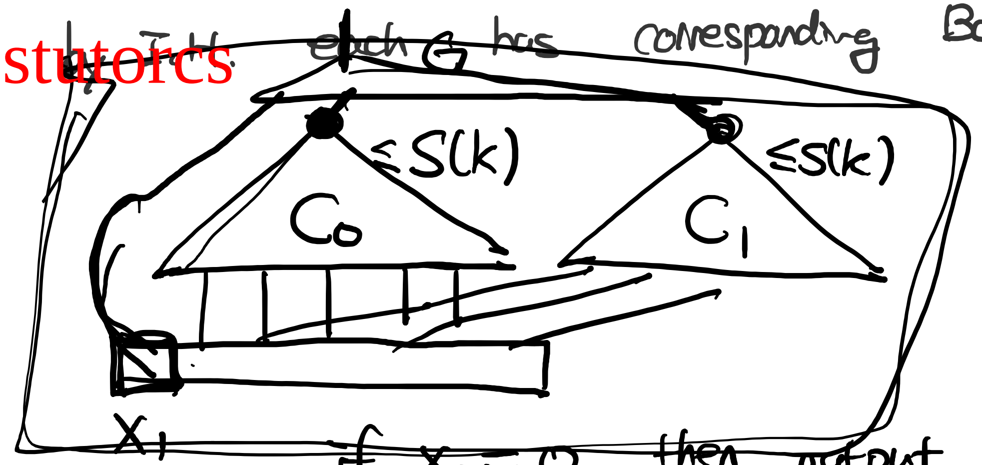
$S(n)$? $\Rightarrow S(n) \leq 2^{O(n)}$

$f : \{0,1\}^{k+1} \longrightarrow \{0,1\}$

each C has corresponding Boolean ckt.

$f|_{x_1=1} : \{0,1\}^k \to \{0,1\}$ $f \longrightarrow$ $0{:}1$ C_1

$f|_{x_1=0} : \{0,1\}^k \to \{0,1\}^{k+1}$ C_0



Compute f.

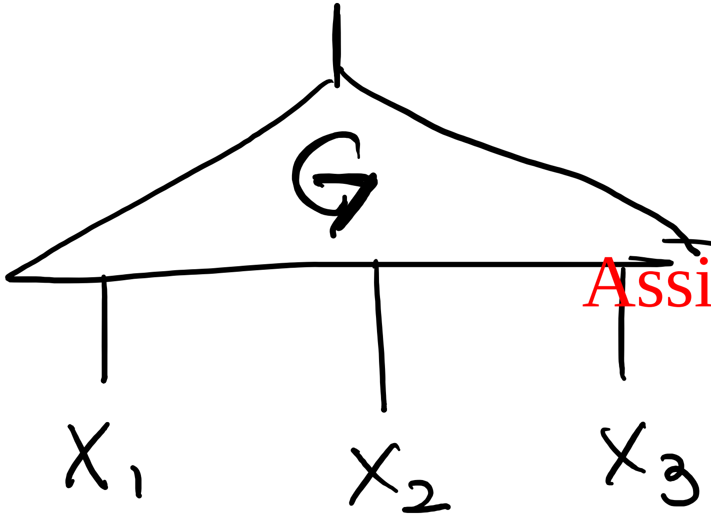
if $x_1 = 0$, then output C_0

$x_1 = 1$, " C_1

$\Rightarrow$ all $f : \{0,1\}^{k+1} \longrightarrow \{0,1\}$

has corresponding Boolean ckt.

Exercise) control bit



if $x_1 = 0$, output x_2

$x_1 = 1$, output x_3

this is doable with $O(1)$-gates.

So for circuit this is ill-posed problem

For every $L \subseteq \{0,1\}^*$, $\exists \{C_n\}_{n\in\mathbb{N}}$ which decides L.

$$\chi_L(x) = 1 \text{ if } x \in L$$
$$= 0 \text{ o/w.}$$

Why circuit is interesting to study then?

Two unrealistic strength that we gave

- ~~Exponential # of gates~~

  poly # of gates

  whether or not ~~b~~ has ~~each~~ family of ckts.

- ~~Non-uniform~~ computation

  Uniform then it becomes equiv. to T.M.

Instead, suppose we reduce # of gates

- $O(2^n)$ -gates to compute any f

  bad and unrealistic.

poly(n) -gates to compute any f ?

Shannon's counting argument

with C # of gates. you can compute $2^{\tilde{O}(C)}$ many function

$C \to poly(n)$

Total # of functions with n boolean input. 2^{2^n}

$2^{O(poly(n))} \lll 2^{2^n}$

~~all~~ possible inputs | 000 | 001 | ...

f $f(x)$ 2^n

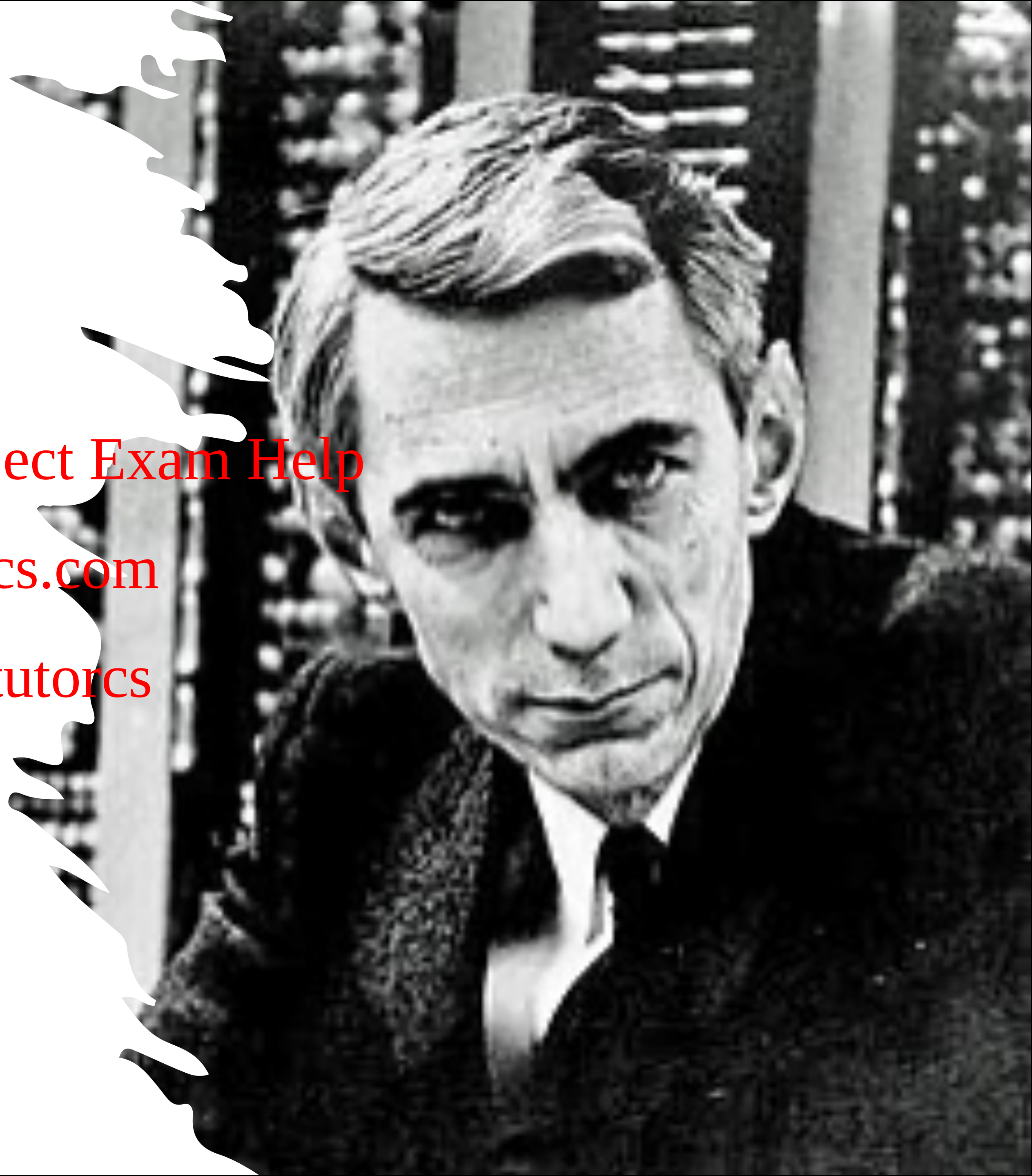
$\to x_f$

x 2^{2^n}

f with n inputs $\to$ non-empty.

Side Note : Claude Shannon

- Father of Information Theory
- How to transmit message efficiently from A to B? – related to physics
- Need to obtain information before computing on top of it

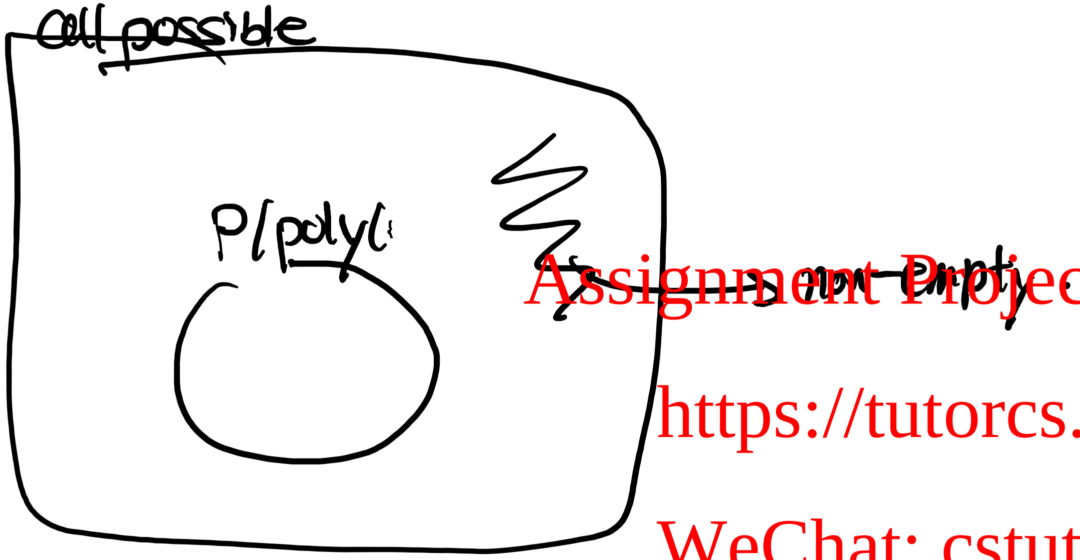


Total # of possible Boolean Functions

of possible circuits with K gates

If fewer gates then … ?

Regime of interest : poly(n) gates : **P/poly**



Non-uniformity ?

Uniform model of comp.

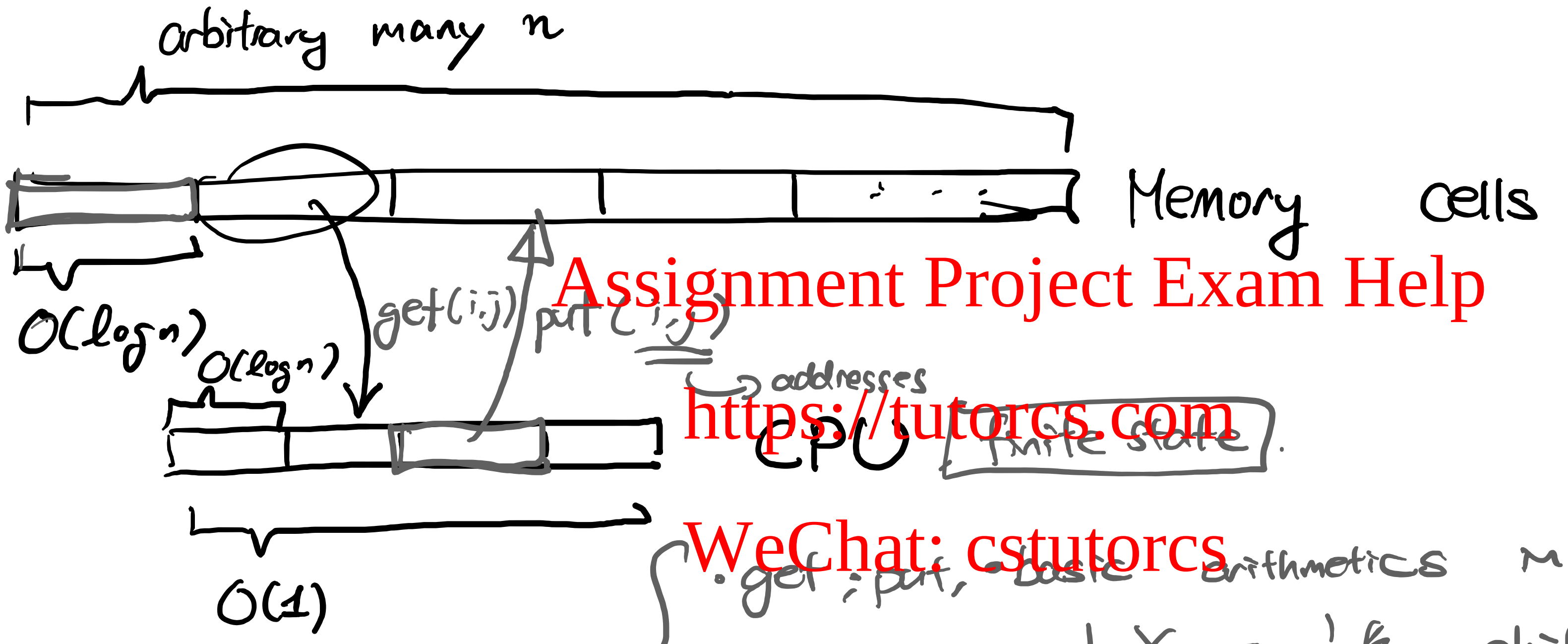
Uniform Ckts : Uniform Ckt $\Leftrightarrow$ T.M.

Output circuit using TM.

Given $\underbrace{1 \dots 1}_{n}$ $\exists$ T.M must output $\langle C_n \rangle$

ex) OR, AND.

wordRAM Model



- get ; put, basic arithmetics in CPU, (within CPU).
  $+ \times, -, \div \&,$ shift operations.
- copy CPU.
  → unit operations.
-

T.M. $\Longleftrightarrow$ wordRAM.