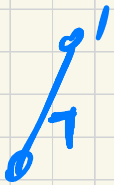
HONORS ALGORITHMS

2025-02-24

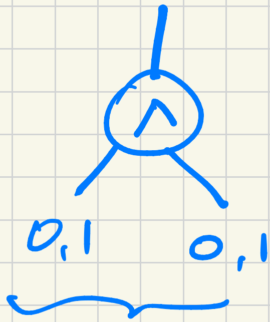
p 1

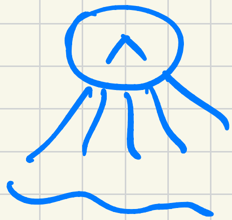
$\neg$, $\wedge$, $\vee$

Boolean gate



0 negation



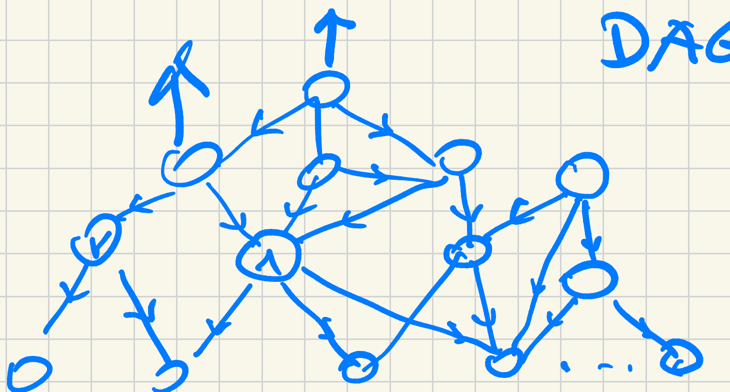


fan-in 2 fan-in k

Boolean circuit

DAG

output



wires

input gates →

x_1 x_2 x_j x_n

fan-in = 0

Boolean function

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

Boolean circuit with 1 output gate computes a Boolean function

Thm ∀ B. fcts can be computed by a Boolean ckt ← circuit

∨ OR: disjunction

∧ AND: conjunction

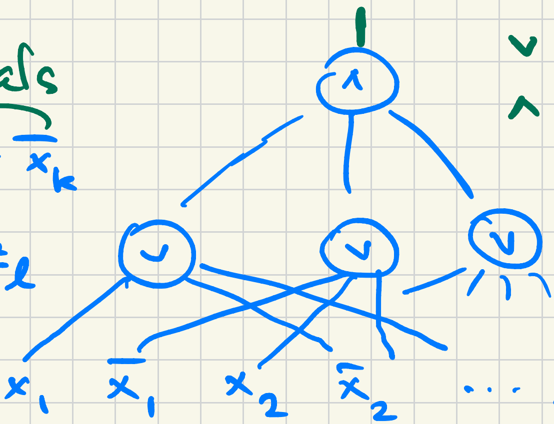
$\underbrace{\text{literals}}$

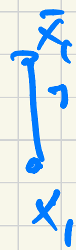
$z_i :\ x_k$ or $\bar{x}_k$

$C_j = z_{i_1} \vee \dots \vee z_{\ell}$

$\downarrow$

Clause (disjunctive)





CONJUNCTIVE NORMAL FORM CNF

$$f(x) = \bigwedge_j C_j .$$

$\boxed{\text{DD}}$

$\forall$ Boolean fcn rep by

DNF disjunctive normal form:

$\bigvee$ conjunctions of literals

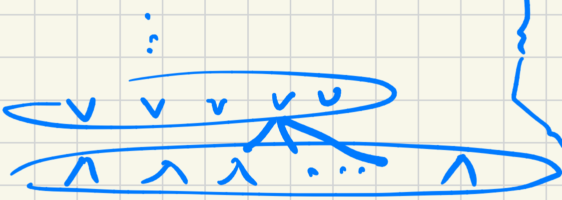
$\neg f$: CNF is in DNF

EX. PARITY $= \sum x_i \bmod 2$

requires 2^{n-1} clauses in CNF

---

layered circuits



literals

negations can be pushed to bottom

EX how much bigger ckt

depth of ckt : max dist to literal

layered ckts of bdd depth

depth 2 CNF DNF

HW → depth 3 PARITY CAN BE COMPUTED

with $\underline{O}(n \cdot 2^{\sqrt{n}})$

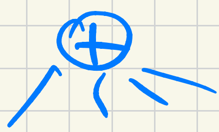
gates

depth 4 $O(n^{?} \cdot 2^{n^{1/3}})$

⋮

depth k $(\cdot \cdot\cdot 2^{n^{\frac{1}{k-1}}})$

PARITY GATE



$$\oplus_3 : \begin{cases} 1 & \text{if } \sum x_i \equiv 0 \pmod 3 \\ 0 & \text{o/w} \end{cases}$$

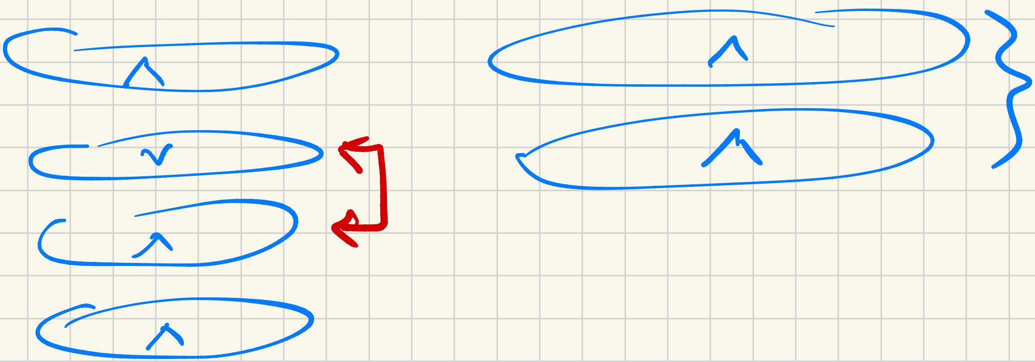
$$\text{MAJORITY}(x_1 \cdots x_n) = \begin{cases} 1 & \text{if } \sum x_i \geq \frac{n}{2} \\ 0 & \text{o/w} \end{cases}$$

YAO – HÅSTAD : 1988

in depth k

parity requires $\Omega\left(2^{c \cdot n^{\frac{1}{k-1}}}\right)$

HÅSTAD's switching lemma



CLAUDE SHANNON info thy

A.a. Boolean fctns require (exp. size circuits) $\leftarrow$ EX $\boxed{k > c\frac{2^n}{n}}$

$\uparrow$

wires

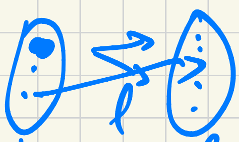
exp # gates

Boolean fctns in n variables $\qquad 2^{2^n}$

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

$|A| = k \qquad |B| = \ell$

$f : A \to B \qquad\qquad |B|^{|A|} = |B^A|$



$k \qquad \ell$

notation:

$B^A = \{f : A \to B\}$

$\ell \cdot \ell \cdot \ldots = \ell^k$

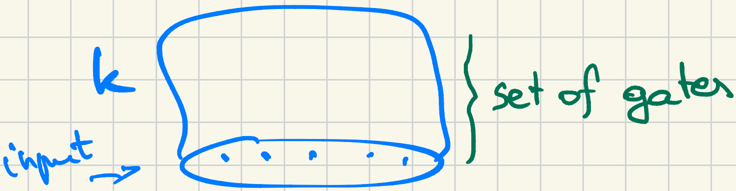
PROOF BY PROBABILISTIC METHOD

proof of existence without constructing an explicit example

raises question of derandomization

Suppose all the 2^{2^n} B. fctns can be computed w ckts with k gates

ckts : 2^{k^2-k} irreflexive DIGRAPHS



$$\therefore 2^{k^2} > 2^{k^2-k} > 2^{2^n}$$

$$k^2 > 2^n$$

$$\boxed{k > 2^{n/2}}$$

need $2^{k^2-k} > \frac{1}{100} 2^{2^n}$ $\qquad \frac{2^{k^2}}{2^k} > \frac{2^{2^n}}{100}$

to have at least 1% chance for a random B. fctn to be computable w k gates

$\Rightarrow \underline{k > 2^{\frac{n}{2}}}$