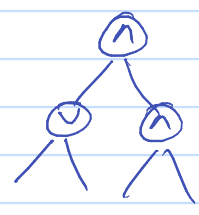
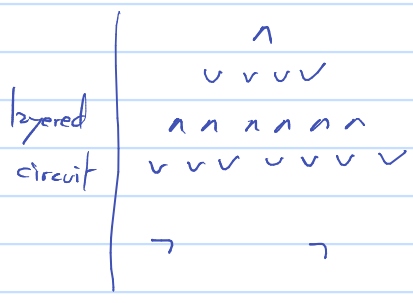
Restricted classes of circuits.

→ monotone circuits : no negations (only $\vee$, $\wedge$ gates). can compute exactly set of all monotone functions.
exponential lower bounds are known.

→ depth-bounded circuits : few layers

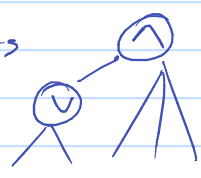




AC^i, NC^i

AC^i : circuits of $O(\log^i(n))$ layers and unbounded degree. poly-size

NC^i : circuits of $O(\log^i(n))$ layers indegree 2. poly-size.



$NC^0 \subsetneq AC^0 \subsetneq NC^1 \subseteq AC^1 \subseteq NC^2 \cdots \subseteq P/poly.$

NC^0: constant depth, indegree 2, constant size

AC^0: any function (contains DNFs, CNFs) ← (maybe exp. size).

thm Parity : $\{0,1\}^n \to \{0,1\}$, $x \mapsto \sum x_i \bmod 2$ is not in AC^0.

---

switching lemma.

p-random restriction : pick a set of size $p \cdot n$, leave unassigned (→ unif. random); set remaining $n - pn$ variables to 0 or 1 unif. random, independently.

f on n variables

set $n/2$ variables to 1 or 0 units

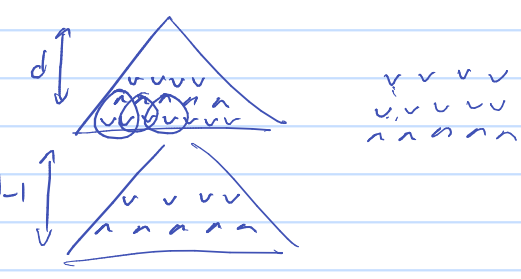
f' on $n/2$ variables.

f = or function

$n/4$ vars to 1 → f' 1 whp.

lemma: f expressed as t-CNF, let ρ p-random restriction. then

$$\Pr[f|_\rho \text{ not an } s\text{-DNF}] \le (24pt)^s$$



proof. R^ℓ = {restrictions of n vars, set ℓ *}.

$$|R^\ell| = \binom{n}{\ell} \cdot 2^{n-\ell}.$$

$Bad(\ell, s) = \{\text{restrictions } \rho \in R^\ell : C'(f|_\rho) > s\}$

(iff)

claim $C'(f) \le s$ then has a s-DNF $\alpha_1 \cdots \alpha_k$, $|\alpha_i| \le s$.

$$\bigvee_{i=1}^{k} \bigwedge_{j=1}^{s} x_{a_j} = \alpha_j$$

never accepts 0: by def cert.

accept all 1s: by def set cert. $\exists \alpha_i$

OR. $\{x_1 = 1\}$, $\{x_2 = 1\}$, ⋮, $\{x_n = 1\}$. $C'(OR) = 1$.

AND. $\{x_1 = 1, x_2 = 1 \cdots\}$ $C'(AND) = n$.

certificate complexity.

a 1-certificate for f if $\forall x \supseteq \alpha$ $f(x) = 1$.

A set of certificates covers f if $\forall x \in f^{-1}(1)$ $\exists \alpha \in A$ $x \supseteq \alpha$

$width(A) = \max_{\alpha \in A} |\alpha|$

1-cert. complex. of f is min. width of a set of certificates.

(†) $|Bad(\ell, s)| \le |R^{\ell-s}| \cdot (6t)^s$.

$$\frac{\binom{n}{\ell-s} \cdot 2^{n-\ell+s} \cdot (6t)^s}{|R^\ell| \le \binom{n}{\ell} \cdot 2^{n-\ell}} \qquad \binom{n}{\ell} \cdot 2^{n-\ell}$$

lemma follows by calculation (not immediate.)

$$\le \left(24 \left(\frac{\ell}{n}\right) t\right)^s$$

$\uparrow p$

$code(\rho) \mapsto (\rho', \text{extra})$ injective. f is a t-CNF

$\rho \mapsto \rho \cup \pi$ $|\pi| = s$. s n-bit-numbers : too big.

pick $\rho \in Bad(\ell, s)$. $\exists$ cert π' of size $\ge s+1$ for $f|_\rho$.

we will build $\pi \subsetneq \pi'$ in steps, initially $\pi = \emptyset$.

F CNF representing f. $F|_{\rho \cup \pi}$ π not a 1-cert. $\pi \subseteq s < s+1$

→ not identically 1. → $\exists$ clause C not set to 1 by $\rho \cup \pi$. pick the first such clause.

C_1 = first clause in $F|_{\rho\cup\pi}$ not $\equiv 1$.

$\pi_1 = \pi' \setminus \pi \cap vars(C_1)$ | same vars, π_1 agrees with π'

$\bar{\pi}_1 = vars(\pi' \setminus \pi) \cap \bar{C}_1$ | $\bar{\pi}_1$ agrees with $\bar{C}_1$.

all literals of $\bar{C}_1$ set by $\bar{\pi}_1$ are 0.

$C_1|_{\rho \cup \pi \cup \bar{\pi}_1} = 0$.

a_1 = string of length t, $a_1[j] = 1$ iff j-th var of C_1 in π_1.

add π_1 to π, find $C_2, \pi_2, a_2, \cdots C_m, \pi_m, a_m$. stop when $|\pi - \pi_m| = s$

$m \le s$.

finally add to code b : polarities of π : string of length s.

given C_1, a_1 : can rebuild $\bar{\pi}_1$ (not π_1). so need b to go from $\bar{\pi}_i$ to π_i

$code(\rho) \mapsto (\rho \cup \bar{\pi}_1 \cup \bar{\pi}_2 \cdots \cup \bar{\pi}_m, a_1 a_2 \cdots a_m b)$.

claim 1: injective.

given $\rho \bar{\pi}_1 \cdots \bar{\pi}_m = \tau$, $a_1 \cdots a_m b$.

find first clause in F not set to 1 by τ.

we will find C_1. using a_1 can identify $\bar{\pi}_1$ $\rho \pi_1$

using b can flip $\bar{\pi}_1$ to π_1 $\rho \bar{\pi}_1$

$\tau_1 = \rho \boxed{\pi_1} \bar{\pi}_2 \cdots \bar{\pi}_m$

find first clause not set to 1 by τ_1. find C_2. $a_2 \to \bar{\pi}_2$. $b \to \pi_2$.

$\tau_m = \rho \boxed{\pi_1}\boxed{\pi_2} \cdots \boxed{\pi_m}$: have identified ρ. → code is invertible.

claim 2: code small enough.

$(z_1 \cdots z_m, h)$ small. $z_1 \cdots z_m$: $\le s$ strings of length t exactly s ones. in total.

$$\binom{s \cdot t}{s} \le \left(\frac{e \cdot st}{s}\right)^s = (et)^s$$

b length t 2^s

$< (6t)^s$. ※

thm $Parity \notin AC^0$. complete proof next day.

→ $Maj \notin AC^0$.