1. For each constant k there exists a language in PH that requires circuits of size $\Omega(n^k)$.

$\forall n\ \exists f_n : \{0,1\}^{2k\log n} : \{0,1\}$ that requires circuits of size $n^{2k}/2k\log n$.

language in PH: given x, find $f_{|x|}$. if $f_{|x|}(x) = 1 \quad x \in L$
$\qquad 0 \quad x \notin L$.

↳ first function sh....

$$\exists f_{|x|}\ \forall g < f_{|x|}\ \exists C\ |C| < n^{2k}/2k\log n,\ \forall D,\ |D| < n^{2k}/2k\log n,\ \forall y,\ \exists z$$

$\underbrace{C \text{ circuit for } g}_{C(y)=g(y)}$, $\underbrace{D \text{ not a circuit for } f_{|x|}}_{D(z) \neq f_{|x|}(z)}$, $f_{|x|}(x) = 1$.

(first $2k\log n$ bits).

$$L = \bigcup_{n \in \mathbb{N}} \{x : |x| = n \quad f_n(x) = 1\}.$$

⋕

2. show that $\exists L \in \Sigma^2 P$ not computable by circuits of size $O(n^k)$.

Karp-Lipton: either $NP \subseteq P/poly \Rightarrow$ PH collapses to Σ_2.
so language from before is in Σ_2.

o/w $NP \not\subseteq P/poly \Rightarrow NP = \Sigma^1 \subseteq SIZE(n^k)$ for any K.

3. if $P = NP$ then exists language in EXP that requires circuits of size $\Omega(2^n/n)$.
not computable by ckt. of size $O(2^n/n)$.

f_n has n vars.

$$\exists f_{|x|}\ \forall g < f_{|x|}\ \exists C\ |C| < 2^n/10n,\ \forall D,\ |D| < 2^n/10n\ \forall y,\ \exists z$$

$\underbrace{C \text{ circuit for } g}_{C(y)=g(y)}$, $\underbrace{D \text{ not a circuit for } f_{|x|}}_{D(z) \neq f_{|x|}(z)}$, $f_{|x|}(x) = 1$.

$EXP^{EXP} = EXP$? $\qquad P^P = P$. $\qquad EXP^P = EXP$.

input x of size n:
call oracle with input of size 2^n.
oracle can run in time $2^{(2^n)}$.

same language, f_n on n variables $L \in EXP^{PH}$. $\qquad$ if $P = NP \Rightarrow PH = P$.

$EXP^{PH} = EXP^P = EXP$.

4. $Maj : \{0,1\}^n \to \{0,1\}$
$x \mapsto 1$ iff $hw(x) \geq n/2 \qquad hw(x) = \sum_{i=1}^n x_i$.

Show that Maj not in AC^0. (constant depth, unbounded degree, poly size).

We'll show how to solve Parity.

$$Parity(x) = \bigvee_{i=1,3,5,\dots} hw(x) = i$$

← poly.

$$[hw(x)=i] = [hw(x) \leq i] \wedge [hw(x) \geq i]$$

$\qquad \| \qquad\qquad\qquad\qquad$ add enough 1s / 0s.

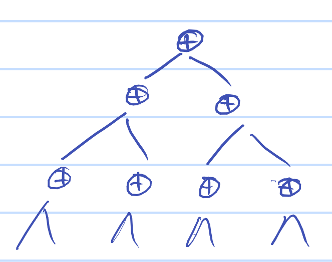
$[hw(\bar{x}) \geq n-i]$

$i < n/2$, $2i < n$ $\qquad \ell : \frac{\ell + n}{2} = i + \ell$

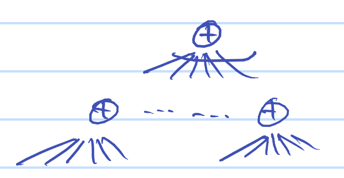
add 1s: $x \to x\overbrace{1}^{\ell}$

if $Maj \in AC^0 \Rightarrow$ have shown $Parity \in AC^0$!! $\qquad$ ⋕

5. Show that for $d \geq 3$ Parity can be computed by circuits of size $2^{O(n^{1/d})}$, depth $d+1$, unbounded degree.



complete tree of size n / depth $\log n$.



depth d

degree $n^{1/d}$.

replace ⊕ of degree $n^{1/d}$ by $\wedge, \vee$ gates:

e.g. in CNF $\quad \wedge$ over $\vee\vee\vee\vee\vee$ $\quad 2^{\#vars} = 2^{n^{1/d}}$.

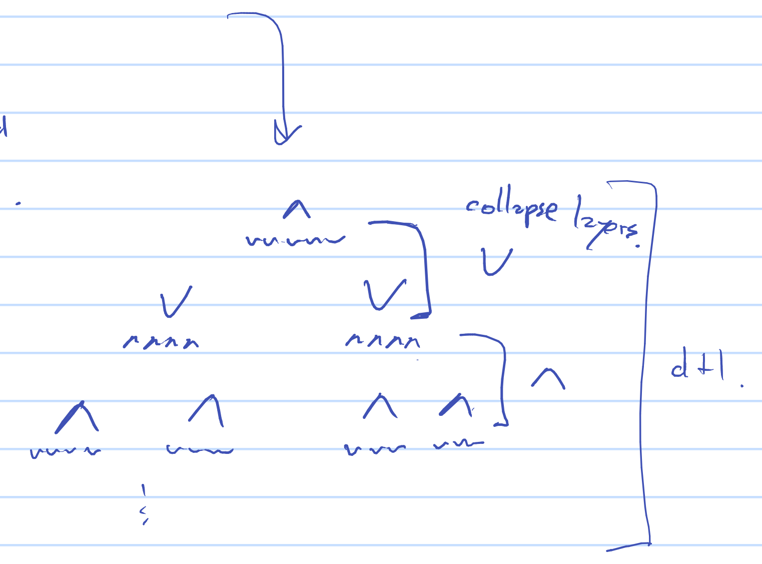
↓

2 layers.

DNF $\quad \vee$ over $\wedge\wedge\wedge\wedge$.

↓

2 layers



$poly(n) \cdot 2^{n^{1/d}}$ size, $d+1$ layers. ⋕

6. $p = n^{-1/2}$, ρ random restr. $\quad$ set pn vars to $*$
remaining 0/1 unif. random.

set var to $*$ with prob p.
set var to 0 — $(1-p)/2$
— 1 — $(1-p)/2$.

easier to work with.

clause

(i) $\Pr[C|_\rho$ depends on $> t$ vars$] < n^{-t/3}$. $\qquad$ C small $\sim < t\log n$; C large. $\geq t\log n$

(ii) $\Pr[F|_\rho$ depends on $> s$ vars$] < n^{-k}$.

t-CNF.

induction on t (width of CNF).

+ small case / large case.