saw switching lemma: let f t-CNF,

let ρ random restriction where $\rightarrow$ pick pn variables, set to $*$

$\rightarrow$ set all remaining variables to 0/1 uniformly.

then $\Pr_{\rho}[f|_{\rho} \text{ not an } s\text{-DNF}] \leq (24 \cdot p \cdot t)^s$.

CNF $\rightarrow$ DNF. also true if DNF $\rightarrow$ CNF (take $\bar{f}$)

thm: parity $\notin AC^0$.

proof: assume circuit size $\leq S$, depth d.

$s, t = K = \log S$. $p = \frac{1}{100K}$. $n \rightarrow \frac{n}{100K} \rightarrow \ldots$

$n_i = n/(100K)^i$ variables left.

add extra layer of $\wedge$ gates, all of degree $\leq t$. circuit depth $d+1$.

last two layers: t-DNF. apply switching lemma:

$\Pr_{\rho}[g|_{\rho} \text{ not an } s\text{-CNF}] \leq (24 \cdot \frac{1}{100K} \cdot K)^K \leq 4^{-K} = 4^{-\log S} \ll \frac{1}{S}$.

have $< S$ gates: can do union bound:

$\Pr_{\rho}[\text{some gate } g|_{\rho} \text{ not an } s\text{-CNF}] \leq \sum_{g \text{ gate}} \Pr_{\rho}[g|_{\rho} \text{ not } s\text{-CNF}] < S \cdot \frac{1}{S} = 1$

$\Rightarrow \exists \rho$ st all gates satisfy $g|_{\rho}$ is an s-CNF.

depth reduced by 1.

apply lemma again (but CNF $\rightarrow$ DNF version).

after $d+1$ applications: ~~function~~ parity on $n_{d+1} = \frac{n}{(100K)^{d+1}}$ variables.

computed by s-CNF.

$\downarrow$

$S = n_i$

if $\frac{n}{(100K)^{d+1}} > K \rightarrow$ have !!

$100 \log S < n^{1/d+1} \Rightarrow$!! $\quad S < 2^{\frac{n^{1/d+1}}{100}} \Rightarrow$!!

Randomized Computation.

def probabilistic TM: like nondet TM: 2 transition functions

at each step: throw coin, pick one r.f. with prob $1/2$.

can measure $\Pr[M(x)=1]$.

def BPTIME: $L \in \text{BPTIME}(t)$ if $\exists$ PTM running in time $t(|x|)$, st

if $x \in L \Rightarrow \Pr[M(x)=1] \geq 2/3$

$x \notin L \Rightarrow \Pr[M(x)=0] \geq 2/3$. $\leftarrow \frac{2}{3} - \frac{1}{2}$ advantage.

all def: y is coin tosses. $\Pr[M(x,y)=1]$.

does randomness help?

for example:

- primality testing $\longrightarrow$ easy BPP algorithm. but nowadays: primes $\in$ P.
- polynomial identity testing $\rightarrow$ given P, is $P \equiv 0$? easy BPP algorithm but no algorithm in P!
- perfect matching
- sorting

BPP algorithms, P algorithms too.

$O(n^6)$?

perfect matching in a bipartite graph.

$G(V,E) = V_1 \cup V_2$ $\exists n \cdot V_1 \rightarrow V_2$ perm using edges in E.

symbolic adj. matrix X: X_{ij} if $(i,j) \in E$; 0 o/w.

perf. match iff $\bigvee_{\sigma \in S^n} \bigwedge_{i=1} A_{i,\sigma(i)} = 1$

$\equiv \bigvee_{\sigma} \bigwedge_{i} X_{i,\sigma(i)} \neq 0 \equiv \bigvee_{\sigma} \prod X_{i,\sigma(i)} \neq 0 \equiv$

$\equiv \sum_{\sigma} \prod x_{i,\sigma i} \neq 0 \equiv \det(X) \neq 0$

$\det = x_{11}x_{22} - 0 \cdot 0$

$\neq 0 \quad = 0$

$\Rightarrow \equiv \sum_{\sigma} \text{sign}(\sigma) \cdot \prod x_{i,\sigma i} \neq 0$

$\sum_{\sigma} \prod x_{i,\sigma i} = 0$ iff all $\prod x_{i,\sigma i} = 0$

test if poly $\det(x) = 0$? no, $\det(x)$ might be too large.

lemma (de Millo-Lipton-Schwartz-Zippel): ??

if $p \not\equiv 0$ of total degree $\leq d$, pick S finite set of integers

$\Pr_{a_1 \ldots a_n \in U(S^n)}[p(a_1 \ldots a_n) = 0] \leq \frac{d}{|S|}$

$x_1^2 x_3^4 x_4$ total degree $2+4+1$

algorithm for PM:

pick $a_1 \ldots a_{n^2} \in [-2n, 2n]$. compute $\det(X|_{x_{ij} \rightarrow a_{ij}}) \neq 0$.

---

choices with def. of BPP:

- branching with Pr. $1/2$. why not any p?
- worst-case time. why not expected?
- error $< 1/3$ (correct $> 2/3$) why not more/less?

error does not matter (if in reasonable range).

thm (error reduction): L long. M poly-time TM st $\forall x$ $\Pr[M(x)=L(x)] \geq \frac{1}{2} + \frac{1}{|x|^c}$.

then $\forall d$ $\exists M'$ poly-time st $\forall x$ $\Pr[M'(x)=L(x)] \geq 1 - 2^{-|x|^d}$.

proof: run M for $8 \cdot |x|^{c+d}$ times, answer according to majority.

lemma: Chernoff-Hoeffdy bound. r.v. $Y_1 - Y_n$ in $[0,1]$, indep. $X = \sum X_i$, $\mu = \mathbb{E}X$.

then $\Pr[|X - \mu| > a] \leq e^{-a^2/2n}$.

$8|x|^{2c+d}$ r.vars. X_i. $X = \sum$. if $x \in L$ then $\mathbb{E}X \geq (\frac{1}{2} + \frac{1}{|x|^c}) \cdot M$.

M

$\Pr[\text{bad}] = \Pr[X < \frac{1}{2} \cdot M] \leq \Pr[|X - \mu| > \frac{1}{|x|^c} M] \leq e^{-\left(\frac{1}{|x|^c} M\right)^2 / 2M}$.

but: used that advantage is at least $\frac{1}{|x|^c}$ for some c.

if no limits on advantage:

e.g. $\Pr[M(x)=L(x)] \geq \frac{1}{2} + \varepsilon(x)$ ε any function st $\varepsilon(x) \neq 0$ $\forall x$.

then have class PP. $\rightarrow$ conj. PP $\neq$ P.

one-sided/zero-sided error:

$x \in L \Rightarrow \Pr[M(x)=1] \geq 2/3$
$x \notin L \Rightarrow \Pr[M(x)=1] = 0.$ } RP (one-sided).

$x \in L \Rightarrow \Pr[\quad 1] = 1$
$x \notin L \Rightarrow \Pr[\quad 1] = 0$ } ZPP (zero-sided error).

$\text{ZPP} = \{L : \exists M, \text{worst-case/expected poly-time, st. } \}$.

$\rightarrow$ expected vs worst case: does not matter.

if M in worst case $T \Rightarrow$ also $\leq T$ in expected time.

if M in expected time $T \Rightarrow$

1. reduce error to $1/4 \rightarrow$ time $c \cdot T$.
2. run for $8 \cdot c \cdot T$ steps. if finished ok.
   o/w answer arbitrarily.

by Markov: $\Pr[\text{not finished}] < 1/4$.

$\rightarrow$ coin probability does not matter (if reasonable number).

lemma: can simulate a coin w/prob p with a coin w/prob $1/2$ if p computable in poly time.

$p = 0.b_1 b_2 \ldots$ b_i can be computed in time i^c for some c.

throw coin. ($1/2$). if $> b_i$: answer 0
if $< b_i$: answer 1
o/w : next i.

$\mathbb{E}\text{steps} = \sum 2^{-i} = 1$.

$\mathbb{E}\text{time} = \sum i^c \cdot 2^{-i} = \text{Constant}$.

$p = 0.0100\ldots$

$\Pr[\text{coin} = 1]$

with Pr $1/2$: 0
with Pr $1/2$ $\rightarrow$ next.
Pr $1/2 \cdot 1/2$: 1
Pr $1/2 \cdot 1/2 \Rightarrow$ next.
Pr $1/4$: 0
$1/16$: 0
$1/32$: 0
$\vdots$

$\Pr[\quad 1] = 1/4$.