

szw switching lemma: let  $f$   $t$ -DNF,  
 let  $p$  random restriction where  $\rightarrow$  pick  $pn$  variables, set to  $x$   
 $\rightarrow$  set all remaining variables to  $0/1$  uniformly.

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

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

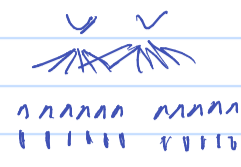
thm: parity  $\notin AC^0$ .

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



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

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



add extra layer of  $n$  gates, all of degree 1. circuit depth  $d+1$ .

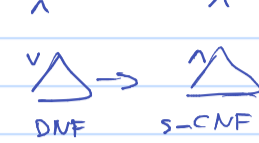
last two layers:  $t$ -DNF. apply switching lemma:

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

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

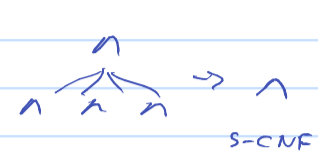
$\Pr[\text{some gate } g|_p \text{ not an } s\text{-DNF}] \leq \sum_{g \text{ gate}} \Pr[g|_p \text{ not } s\text{-DNF}] < S \cdot \frac{1}{S} = 1$

$\Rightarrow \exists p$  st all gates satisfy  $g|_p$  is an  $s$ -DNF.



depth reduced by  $t$ .

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



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

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

$s = n_i$

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

Randomized Computation.

def probabilistic TM: like nondet. TM: 2 transition functions

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

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

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

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

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

does randomness help?

for example:

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

$O(n^6)$ ?

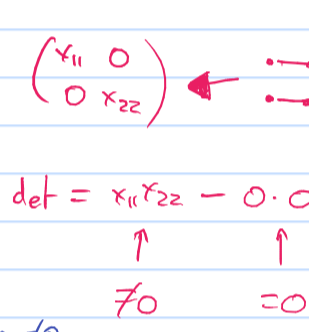
perfect matching in a bipartite graph.

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

symbolic adj. matrix  $X: \begin{cases} x_{ij} & \text{if } (i,j) \in E \\ 0 & \text{o/w.} \end{cases}$

$\sum_i \prod_j x_{i,j} = 0$   
 iff all  $\prod_j x_{i,j} = 0$

perf. match iff  $\bigvee_{\sigma \in S^n} \prod_{i=1}^n A_{i, \sigma(i)} = 1$   $\equiv \bigvee_{\sigma} \prod_i X_{i, \sigma(i)} \neq 0 \equiv \sum_{\sigma} \prod_i x_{i, \sigma(i)} \neq 0 \equiv \det(X) \neq 0$



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

lemma (deMillo-Lipton-Schwartz-Zippel)  $++?$

if  $p \neq 0$  of total degree  $\leq d$ , pick  $S$  finite set of integers

$x_1^2 x_3^4 x_4$   
 total degree  $2+4+1 = 7$ .

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

algorithm for PTM:

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

choices with det. of BPP:

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

error does not matter (if in reasonable range).

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

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

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

lemma: Chernoff-Hoeffding bound. r.v.  $X_1, \dots, X_n$  in  $[0, 1]$ , indep.  $X = \sum X_i$ ;  $\mu = EX$ .

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

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

$\Pr[\text{bad}] = \Pr[X < \frac{1}{2} \cdot M] \leq \Pr[|X - \mu| > \frac{1}{4} \cdot M] \leq e^{-\frac{(\frac{1}{4} \cdot M)^2}{2M}}$

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

if no limits on advantage:

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

then have class PP. w/ conj.  $PP \neq P$ .

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

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

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

$\rightarrow$  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  $T \Rightarrow$

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

by Markov:  $\Pr[\text{not finished}] < 1/8$ . //

$\rightarrow$  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.

$p = 0, b_1, b_2, \dots$   $b_i$  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  $i$ .

$\sum_{i=1}^{\infty} 2^{-i} = 1$ .

$\sum_{i=1}^{\infty} i^c \cdot 2^{-i} = \text{Constant}$ .  $p = 0, 0100, \dots$

$\Pr[\text{sim} = 1] \quad \left. \begin{array}{l} \text{with } \Pr 1/2 : 0 \\ \text{with } \Pr 1/2 \rightarrow \text{next.} \\ \Pr 1/2 \cdot 1/2 : 1 \\ \Pr 1/2 \cdot 1/2 \rightarrow \text{next.} \\ \Pr 1/8 : 0 \\ 1/16 : 0 \\ 1/32 : 0 \\ \vdots \end{array} \right\} \Pr[1] = 1/4$