Let ρ distribution on $\{0,1,*\}^n$ set exactly $p\cdot n$ coordinates to $*$

set remaining $(1-p)\cdot n$ " to $\begin{cases} 0 & \text{w.pr. } 1/2 \text{ indep.} \\ 1 & \text{w.pr. } 1/2 \text{ indep.} \end{cases}$

Let C be a clause on n variables. Show that:

$$\Pr[C\restriction_\rho \text{ depends on } > t \text{ variables}] \le n^{-t/3}.$$

τ distr. set each var. independently to $\begin{cases} * & \text{with prob. } p. \\ 0 & \text{with prob. } (1-p)/2. \\ 1 & \text{with prob. } (1-p)/2. \end{cases}$

negative association $\Pr[x_i=0], \Pr[x_j=0]$ indep.

$\Pr[x_i=0 \mid x_j=0] < \Pr[x_i=0]$.

$\forall$ monotone f,g $\mathbb{E}[f(x_I)\cdot g(x_J)] \le \mathbb{E}[f(x_I)]\cdot\mathbb{E}[g(x_J)]$.

disjoint $I \subseteq [n]$

$J \subseteq [n]$

lemma: if $X_1 \dots X_n$ are indicators of a permutation then they are n.a.

S $\quad supp(X_i) = S$. $\quad X_1 \dots X_n$ is a permutation of S.

$S = \{pn\ *\} \cup \{0,1\}$

lemma: if $X_1 \dots X_n$ n.a. then $\Pr[\bigwedge X_i \ge x_i] \le \prod \Pr[X_i \ge x_i]$

$\Pr[\bigwedge X_i \le x_i] \le \prod \Pr[X_i \le x_i]$

lemma: if $X_1 \dots X_n$ n.a. then Chernoff-Hoeffding bound holds.

$\Pr[|\sum X_i - \mathbb{E}\sum X_i| > a] < e^{-c\cdot a^2/n}$ $\quad$ c constant.

=

Let C be a clause on n variables. Show that:

$$\Pr[C\restriction_{\cancel{\rho}\,\tau} \text{ depends on } > t \text{ variables}] \le n^{-t/3}.$$

split into cases: (i) C larger than $m = t\cdot\log n$ literals. (ii) $|C| \le m = t\cdot\log n$.

(i) $\Pr[\tau \text{ does not set any lit in } C \text{ to } 0] = \Pr[\bigwedge_{\ell_i \in C} \tau(\ell_i) \ne 0] =$ $\quad \le$ (with ρ).

$= \prod \Pr[\tau(\ell_i) \ne 0] = \prod \big(\underbrace{(1-p)/2 + p}_{1/2+\varepsilon}\big) \le \left(\tfrac12+\varepsilon\right)^m \le n^{-t/3}$.

$\tfrac12 + \varepsilon \le \sqrt{\tfrac12}$

(ii) $\Pr[C \text{ has } \ge t\ *] \le \sum_{\substack{V \subseteq Vars(C) \\ |V| = t}} \Pr[V \text{ are } *s] = \binom{m}{t}\cdot p^t \le \binom{t\log n}{t}\cdot p^t \le$

$\le \left(\frac{e\cdot \cancel{t}\log n}{\cancel{t}}\right)^t \cdot p^t = (e\cdot p\cdot\log n)^t \le \left(1/\sqrt[3]{n}\right)^t = n^{-t/3}$.

p: $1/\sqrt{n}$

F is a t-CNF for each $k \in \mathbb{N}$ $\exists s$ s.t.

$$\Pr[F\restriction_\rho \text{ depends on } \ge s \text{ variables}] \le n^{-k}.$$

induction on t.

pick G maximal set of clauses on disjoint variables.

$Y = vars(G)$.

(i) $|G| \ge k\cdot 2^t\cdot\log n \rightarrow$ show one $C \in G$ 0.

(ii) $|G| < k\cdot 2^t\cdot\log n$

compute $\Pr[Y \text{ has} \ge 4\cdot k\cdot s\ *s]$

$\Pr[F\restriction_\rho \text{ has} \ge 4ks\ *s] = \sum_j [F\restriction_\rho \text{ has } j\ *s \text{ in } Y]\cdot\Pr[F\restriction_\rho \text{ has} \ge 4ks - j\ *s \text{ outside } Y]$.

$\sum_{j=1}^{4k} \Pr[F\restriction_\rho\ 4ks - 4k \text{ outside } Y]$ $\rightarrow$ $F|_Y$ fixed is a $t-1$-CNF.

can use induction

$+ \sum_{j \ge 4k}$ small

claim: each clause in F has a variable in Y. (o/w add to G)

= $\exists p \in \mathbb{R}$, L undecidable language.

Show that if TM has access to p-biased coin, can decide L.

$p = 0.p_1p_2p_3\dots$ $\qquad p_{3i} = \begin{cases} 1 & \text{if } bin(i) \in L \\ 0 & \text{o/w.} \end{cases}$

$p_{3i+1} = 0$.

$p_{3i+2} = 1$.

can decide $x \in L$ if we can compute p with error $\le \underbrace{2^{-(3i+3)}}_{t}$.

throw a coin M times, $X_1 \dots X_m$, compute $X = \frac{\sum X_i}{M}$. $\quad \mathbb{E}X = p$.

$\Pr[|X - p| > t] \le \frac{Var(X)}{t^2} < \frac13$ $\qquad Var(X) = \frac{p(1-p)}{M}$

for M large enough

$P \stackrel{?}{=} BPP$

$ZPP = RP \cap coRP$. $\qquad RP: \begin{cases} x \in L & \text{ok w/pr} > 2/3 \\ x \notin L & \text{ok w/pr } 1. \end{cases}$

1. $ZPP \subseteq RP \cap coRP$.

enough $ZPP \subseteq RP$ b/c ZPP closed under complements.

$L \in ZPP$. M solving L. $\qquad M'$: simulates M for $3\cdot n^c$ steps.

exp. time n^c. $\qquad$ if finished: answer accordingly.

o/w: answer 0.

$\Pr[M'(x) \ne L(x)] = \begin{cases} x \notin L & 0. \\ x \in L & \le \Pr[M' \text{ did not finish}] = \Pr[T(M') > 3n^c] \le \frac13. \end{cases}$

$\mathbb{E}T = n^c$ $\qquad$ Markov

2. $ZPP \supseteq RP \cap coRP$.

M_1, M_2. $\qquad M_1(x) = 1 \Rightarrow x \in L$.

$M_2(x) = 0 \Rightarrow x \notin L$.

Repeat M times:

compute $M_1(x), M_2(x)$.

if $M_1(x) = 1$ answer 1

if $M_2(x) = 0$ answer 0

continue.

$\Pr[\text{repeat} \ge n \text{ times}] \le (1/3)^n$.

$\mathbb{E}\,\text{time} = poly(|x|)\cdot\sum_i i(1/3)^i = poly(|x|)$.

Show that $NP \subseteq PP$.

solve SAT: given formula φ: generate random assignment $\alpha_1 \dots \alpha_n$.

evaluate $\varphi(\alpha_1 \dots \alpha_n)$. if 1: answer SAT

if 0: answer 0 w/prob $1/2 + \varepsilon$.

φ UNSAT $\Rightarrow pr(0) = 1/2 + \varepsilon$.

φ SAT $\Rightarrow pr(1) \ge (1/2)^n + (1 - (1/2)^n)\cdot(1/2 - \varepsilon)$

choose ε st $> 1/2$.

Algorithm for 2-SAT:

$\alpha = 0^n$

repeat $10\cdot n^2$ times:

$C = \ell_i \vee \ell_j$ not sat. by α

$k \in \{i,j\}$ uniformly.

flip α_k.

if α satisfies φ accept

reject.

assume β correct assignment.

v = # agreements b/w α and β.

goal: $v = n$.

at each step:

w/pr $\ge 1/2$ $\quad v \to v+1$

$\le 1/2$ $\quad v \to v-1$.

look at process where start $v=0$, do $\begin{cases} +1 & 1/2 \\ -1 & 1/2. \end{cases}$ for n^2 times, look if $v \ge n$.

claim: $\Pr[v \ge n] \le \Pr[\text{alg stops in } n^2 \text{ steps}]$.

$\Pr[v \ge n] = \frac12 \Pr[|v| \ge n] = 1/2 - \varepsilon$.

by repeating 10 times: $(\frac12 - \varepsilon)^{10} < 1/3$ ok.