

Ans 8/12  
lec 9

If  $\exists \epsilon > 0$  s.t.  $P/PPOS$  then  $CAPP \in TIME(2^{n^\epsilon}) \forall \epsilon$   
 If  $CAPP \in TIME(2^{n^{o(1)}})$ , then  $NP \neq P/PPOS$ .

$\uparrow$   $O_c(1)$ : complexity of circuit of size  $n$ :  $C(n)$ , given  $n_i$  can compute  $C(n)$  circuit.  
 In  $U$ ,  $U_i$ : if  $P \not\subseteq P/PPOS \in TIME(2^{n^{o(1)}})$ , then "MEXP  $\neq$  Alg P/PPOS"

Kannan: there is a fn.  $f \in \Sigma_3^{EXP}$  so that  $size(f) \geq \Omega(2^n/n)$   
 corr  $\Sigma_2^{EXP}$  & P/PPOS.

$NP_i = \exists \delta R(x, \delta)$ ,  $R$ : pos time,  $|\delta| \leq pos(|x|)$ .

$\Sigma_k^P = \exists \delta_1 \forall \delta_2 \dots \exists \delta_k R(x, \delta_1, \dots, \delta_k)$ .

$\#P =$  count # of  $\delta$  s.t.  $R(x, \delta)$ ,  $\#P \subseteq P^{\#P} \subseteq EXP$ .

(Toda:  $BPP^{\#P} \supseteq \#P$ ; essentially Razborov-Smolensky). Then  $BPP^{\#P} \subseteq P^{\#P}$ .

Veronx: Perm =  $\exists \langle x_i, \delta(i) \rangle R(x, \delta)$ ,

$\#EXP: \exists \delta, |\delta| \leq exp(|x|)$ ,  $R \in P$

$\Sigma_k^{EXP}: \exists \delta_1 \forall \delta_2 \dots \exists \delta_k, |\delta_i| \leq exp(|x|)$ ,  $R(x, \delta_1, \dots, \delta_k)$ ,  $R \in P$ .

$\Sigma_k^{EXP} = MXP^{\Sigma_{k-1}^{EXP}}$

$\Sigma_3^{EXP}$ : "hardest fn there is" - Smaron:  $\exists f, size(f) \geq \Omega(2^n/n)$

Proof: if  $of$  gives on  $ES$   $scas$ :  $(c \cdot s^2)^3$

if  $of$  bool ans:  $2^{2^n}$ : # truth values = # of  $2^n$ -length binary strings

$\exists f \forall c, |c| \leq 2^n/n$ ,  $c$  does not compute  $f$   $\forall \delta, \delta \leq exp \tau$  s.t.

$\exists c', |c'| \leq 2^n/n$  and  $c'$  computes  $f$ . Output  $\delta(c)$ ,  $\in \Sigma_3^{EXP}$ .

Say a circ is locally uniform if given  $\delta$  (if given  $\delta$ , if  $\{1..s\}$ , can compute in pos time  $O_i, j_i, k_i$ ).

Claim: if TM  $M$  runs in time  $T$ , then there is a locally uniform circ of size  $O(T^2)$ , so that  $\forall x, C_n(x) = M(x)$  ( $n$  pos in  $i$ ,  $n$ )

In can do size  $O(\# pos \#)$  [Fischer, Piprenser]

Meyer's UL:  $\exists P \notin P/PPOS \rightarrow \Sigma_2^P \subseteq \Sigma_2^P$

$L \in B^P$ ,  $C_n \rightarrow$  locally unif. circ. For  $L_i$  "given  $(x, i)$ , compute  $\delta(x, i)$  or  $C_n(x) \in EXP$ ". Given  $L \in P/PPOS$  let  $D$  compute  $C_n(x)$ .

$\forall x \in L \rightarrow \exists \delta \forall i D(x, i) \neq OP: (D(x, i), D(x, k_i))$ .  $\wedge D(x, s)$

"Shear collapse argument"

In  $\Sigma_2^{EXP} \not\subseteq P/PPOS$ .

Proof:  $C_n \in P/PPOS$ , or it's. If it is not done, use  $EXP = \Sigma_2^P = \Sigma_3^P$   
 Then  $\Sigma_2^{EXP} = \Sigma_3^{EXP}$ , which has hard prob.

Assume  $CAPP \in TIME(2^{n^{o(1)}})$ .  $\exists P \in P/PPOS$  or not. If not done, use  $\Sigma_2^P \subseteq P^{\#P}$   
 And Perm  $\in P/PPOS$ .

Lemma 1: if Perm  $\in P/PPOS$ , then Perm  $\in MA$ .

Lemma 2: If  $CAPP \in TIME(2^{n^{o(1)}})$ , then  $MA \subseteq NTIME(2^{n^{o(1)}})$

Use CAPP as a no-det. ver. of the witness.

So if  $\exists x_p \in P/Pog$  and CAPP time  $(2^{o(1)})$ , then  $\exists x_p \in VTIME(2^n)$  and  $\Sigma_3^P = \{x_p\}$ . Since  $o(1)$ , can in fact:  $\exists T' = n^{o(1)}$  such that  $\Sigma_3 \subseteq VTIME(2^n)$ . But Kozen's const. ~~can~~  $\Sigma_3 \not\subseteq P/Pog$  for any  $T' = n^{o(1)}$ .  $\Rightarrow VEXP \neq P/Pog$ .

Lemma 1 proof: Show  $perm \in P/Pog \Rightarrow perm \in MA \cap coMA$ .

Given  $n$ , verify that  $perm(n) = 1$  (given by oracle).  $\Leftarrow$  witness check. Suppose  $perm$  complex.

1) set circs  $C_{n-1} \dots C_1$ , ~~and~~  $C_i = C_n \begin{pmatrix} 1 & \dots & 0 \\ 0 & \dots & n_{ii} \end{pmatrix}$

2) pick a random prime  $q$ , know  $q \nmid perm(n)$ .  $C_i(x)$ ,  $n \bmod q$ .  $perm(n) \equiv \sum n_{ii} \cdot perm(n_{ii}) \pmod q$

Computes  $D_1 \dots D_n$  or reject. If don't reject,  $D_i = perm(n_{ii}) \pmod q$ . If  $C$  did compute  $perm$ , never reject.

So we've computed  $D_i$ . Can use expansion by minors to compute  $perm$  of any  $(i+1) \times (i+1)$  matrix.

Check that  $C_i(M_{i+1}, i+1) = perm(M_{i+1}, i+1)$  for all  $C_i$   $\frac{1}{3}(n+1)$  fraction of matrices. If not, reject.

$perm$  is multilinear, so using interpolation can turn any approx correct alg into everywhere correct alg. Let  $D_i$  be the interpolation circ using  $C_i$  as almost everywhere correct circ.