Russell lec 9

If $f \in$ EXP-P/poly then CAPP $\in$ Time$(2^{n^{\epsilon}})$ $\forall \epsilon$

If CAPP $\in$ Time$(2^{n^{o_c(1)}})$, then NEXP $\not\subseteq$ P/poly.

↑ $o_c(1)$: computable little o of 1: $\epsilon(n)$, given n, can compute $\epsilon(n)$ effic.

Thm, KI: if PIT $\in$ Time$(2^{n^{o_c(1)}})$, then "NEXP $\not\subseteq$ Alg P/poly"

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

Cor: $\Sigma_2^{EXP} \not\subseteq$ P/poly.

NP: $= \exists y\ R(x,y)$, R: polytime, $|y| \le poly(|x|)$.

$\Sigma_k^P := \exists y_1 \forall y_2 \dots \exists y_k\ R(x, y_1 \dots y_k)$.

#P = count # of y s.t. $R(x,y)$, PH $\subseteq P^{\#P} \subseteq$ Exp.

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

Variant: Perm $= \sum \langle x_i, \sigma(i) \rangle$ $R(x,\sigma)$,

NEXP: $\exists y$, $|y| \le exp(|x|)$, $R \in P$

$\Sigma_k^{exp}: \exists y_1 \forall y_2 \dots \exists y_k$, $|| \le exp(|x|)$, $R(x, y_1 \dots y_k)$. $R \in P$

$\Sigma_k^{exp} = NEXP^{\Sigma_{k-1}^P}$

Σ_3^{EXP}: "first hardest fn there is". Shannon: $\exists f$, size$(f) \geq \Omega(2^n/n)$

proof. # of circs on $\le s$ gates: $(c \cdot s^2)^s$

# of Bool fns: 2^{2^n}: # truth tables = # of 2^n-length binary strings

$\exists f\ \forall C$, $|C| \le 2^n/n$, C does not compute f $\wedge$ $\forall g$, $g \le_{lex} f$ s.t. $\exists C'$, $|C'| < 2^n/n$ and C' computes f. Output $f(x)$. $\in \Sigma_3^{EXP}$.

Say a circ is locally uniform if given x (if given x, $i \in [1..s]$, can compute in polytime op_i, j_i, k_i.

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

Thm can do size $O(t \log t)$ [Fischer, Pippenger]

Meyer's thm: EXP $\subseteq$ P/poly $\Rightarrow$ $\Sigma_{EXP} \subseteq \Sigma_2^P$

$L \in$ EXP, C_n is locally unif. circ. For L, "given (x,i), compute gate i of $C_n(x)$ $\in$ EXP": GateL $\in$ P/poly. Let D compute GateL.

$x \in L \iff \exists D\ \forall i\ D(g,x,i) = op_i(D(x,j_i), D(x,k_i)) \wedge D(x,s)$

"Shortcut correctness argument"

Thm $\Sigma_2^{EXP} \not\subseteq$ P/poly.

Proof. Exp $\subseteq$ P/poly, or it's not. If it's not, done. Else EXP $= \Sigma_2^P = \Sigma_3^P$

Then $\Sigma_2^{EXP} = \Sigma_3^{EXP}$, which has hard prob.

Assume CAPP $\subseteq$ Time$(2^{n^{o_c(1)}})$. Exp $\in$ P/poly or not. If not, done. Else EXP $= \Sigma_2^P = P^{\#P}$

And Perm $\in$ P/poly.

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

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

Use CAPP alg to non-det. verify the witness.
So if $Exp \in P/poly$ and $CAPP \in Time(2^{n^{o(1)}})$, then $Exp \subseteq Ntime(2^{n^{...}})$
and $\Sigma_3^p = Exp_{+1}$. Since $o_c(1)$, can invert: $\exists T' = n^{\omega_c(1)}$
such that $\Sigma_3 \subseteq Ntime(2^n)$, but Kannan's constr. shows
$\Sigma_3^{T'} \subsetneq P/poly$ for any $T' = n^{\omega_c(1)}$. $\Rightarrow$ $NEXP \not\subset P/poly$.
Lemma 1 proof: Show $perm \in P/poly \Rightarrow$ perm $\in$ MA n coMA.
Given M, verify that perm(M) = k (given by Merlin). $\leftarrow$ witness check
Supposedly computes perm.
1) get circs $C_{n-1} \ldots C_1$, $C_i = C_n \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & M_{ij} \end{pmatrix}$
2) Pick a random prime q. Look at $C_i(x)$, M mod q.
$Perm(M) = \sum x_{1,i}\ Perm(M_{1,i})$
Compute $D_1 \ldots D_n$ or reject. If don't reject, $D_i = perm(M_{i \times i})_{mod\ q}$ w.h.p. $\forall M$
If C did compute perm, never reject.
Say we've computed D_i. Can use expansion by minors to compute perm of any $i+1 \times i+1$ matrix.
Check that $C_{i+1}(M_{i+1,i+1}) = perm(M_{i+1,i+1})$ for all but $\frac{1}{3}(n+1)$ 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+1} be the interpolation circ using C_{i+1} as almost everywhere correct alg