1/10/2015

Russell
Lec 21

Improved meta-algorithm and tied to lower bounds.

- derandomization of CAPP and PIT
- "natural" and "being natural" properties

hard fn − Σ_3^{EXP}

Circuit SAT: given Bool ckt C, is there x s.t. $C(x)=1$?

Σ_2^{EXP} = EXP

If circuit SAT $\in P$, then EXP has hard fns (size$(f) \geq 2^n/n$).

If CircSAT $\in P$, $\Sigma_3^P = P$, so $\Sigma_3^{EXP} = EXP$, so EXP contains max hard prob.

(in [Kabanets-Cai])

3rd level: $x \in L \Leftrightarrow \exists s_1 \forall s_2 \exists s_3\ R(x, s_1, s_2, s_3)$ (poly time, poly size) $- \Sigma_3^P$

Σ_3^P = $\Sigma_2^{P^{NP}}$ = NP^P = P − circSAT

Given x, s_1, s_2: $\exists s_3$ s.t. $R(x, s_1, s_2, s_3)$ is $\in NP$ — $S(x, s_1, s_2)$

$x \in L \Leftrightarrow \exists s_1 \forall s_2\ S(x, s_1, s_2) \in P$ since $NP = coNP = P$. $- \Sigma_2^P$

$x \in L \Leftrightarrow \exists s_1\ T(x, s_1)$ … $T(x, s_1) \in NP = P$.

– having an alg better than a decider e.g. quantum alg for Sat $\Rightarrow \Sigma_2^{EXP}$

$L \in \Sigma_i^{EXP}$, $1^{x} \in \hat{L} \leftrightarrow x \in L$, $\hat{L} \in \Sigma_i^P = P \Rightarrow L \in E$.

Collapses between classes translate upwards,

Separators between classes translate downwards

"Pretty good alg" for CircSAT? Say CircSAT $\in TIME(2^{n^{o(1)}})$.

then NEXP $\not\subseteq$ P/poly

Either EXP $\subseteq$ P/poly, or not. If EXP $\not\subseteq$ P/poly, done.

Meyer's thm: EXP $\subseteq$ P/poly $\Rightarrow$ EXP $= \Sigma_2^P$

$x \in L \Leftrightarrow \exists s_1 \forall s_2\ S(x, s_1, s_2) \in Time(2^{n^{o(1)}})$

So $L \in NTIME(2^{n^{o(1)}})$. And $\Sigma_3^P \subseteq EXP \subseteq NTIME(2^{n^{o(1)}})$

$\exists T \in n^{\omega(1)}$ s.t. $\Sigma_3^{T(n)} \subseteq NEXP$. $\Sigma_3^{T(n)} \not\subseteq$ P/poly $\Rightarrow$ NEXP $\not\subseteq$ P/poly.

(Meyer's thm) Circuit is locally computable, if given a name of a gate i we can compute $op(i), j(i), k(i)$

two input gates and operation.

Fischer-Pippenger: for any time $T(n)$ alg there is a size $O(T(n)\log T(n))$ locally computable circuit can simulate the alg.

Pf: adapting oblivious k-tape to 2-tape simulation. (Hartmanis, Stearns + Lewis?)

Meyer's thm: if EXP $\subseteq$ P/poly, then EXP $\subseteq \Sigma_2^P$.

Proof: Let $L \in EXP$, C_n locally computable ckt deciding L on n-bit inputs

let L': given gate i of C_n, what is the value of gate i on input x?

$L' \in EXP \Rightarrow L' \in$ P/poly, so $\exists$ ckt C' deciding L', $C'(x, i)$.

$x \in L \Leftrightarrow \exists C'' \forall i\ op_i(C''(x, j(i)), C''(x, k(i))) = C''(x, i) \wedge C''(x, out) = True$

[Williams]. Naive alg for CircSAT: $|C|2^n$. If circ-SAT $\in Time(|C| \cdot 2^n / n^{\omega(1)})$,

then NEXP $\not\subseteq$ P/poly. Moreover, enough to assume circ-Taut $\in NTIME(|C|2^n/n^{\omega(1)})$

(circ-taut$(C) = \neg$CircSAT$(\neg C)$)

Assume $NEXP \subseteq P/poly$ and circ-TAUT $\in NTIME(|C| 2^n / n^{\omega(1)})$
- self contradiction w/ nondet time hierarchy thm.

Last class: easy witness lemma

$NEXP \subseteq P/poly \iff$ every positive instance of Nexp problem has succinct describable witness (by possibly exp computing bits of the witness)

$L \in NTIME(2^n)$. $x \in L \iff \exists y, |y| = 2^n$ s.t. $R(x, y)$, R poly in $|x|, |y|$

Let C_R be poly computable circ that computes R, and $size(C_R) = O(2^n)$

$x \in L \iff \exists$ (witness s.t. $R(x, (C_R(\emptyset) \ldots C_R(2^n-1)))$ — better poly size

$x \in L \iff \exists g_0, g_1, \ldots g_{2^n-1}$ s.t. "each gate in g_i is correct given its inputs and output = 1." (same as for C'' before) $\forall i$ $g_i = op_i(g_{j(i)}, g_{k(i)})$ & $T_{C''}(i)$ (uses x)

This relation has succinct witness if $x \in L$, C'' is a succinct witness.

- exists by $\Sigma_2 L$ (easy witness lemma) - has $n + \log n + O(1)$ inputs

$T_{C''}(i)$: $x \in L \iff \exists C''$ $T_{C''}$ is a tautology $\Rightarrow L \in NTIME(2^{n+\log n + O(1)} / n^{\omega(1)})$

$= NTIME(poly(n) \cdot poly(n) \cdot 2^n / n^{\omega(1)})$.

$\Rightarrow L \in NTIME(2^n / n^{\omega(1)})$, contradiction w/ nondet time hierarchy thm:

$NTIME(2^n / n^{\omega(1)}) \not\subseteq NTIME(o(2^n / n^{\omega(1)}))$. ☐

Now, $ACL_6 \subseteq NEXP$.

Williams: ACC_6-SAT $\in NTIME(2^{n - n^\varepsilon})$ $(\forall d\ \exists \varepsilon)$.

Cor Lemma: If for a class of circs $\mathcal{C}$, $\mathcal{C}$-TAUT $\in NTIME(2^n / n^{\omega(1)})$ and $NP \subseteq \mathcal{C}$. Then circ-TAUT $\in NTIME(2^n / n^{\omega(1)})$

Cor: If $\mathcal{C}$-TAUT $\in NTIME(2^n / n^{\omega(1)})$, then $NEXP \not\subseteq \mathcal{C}$.

Cor $NEXP \not\subseteq ACC_6$.

Proof: if $P \in \mathcal{C}$, then $P/poly \in \mathcal{C}$. Let D be an instance of circ-TAUT. Let $g_1 \ldots g_m$ be the gates. Each g_i defines a subcircuit of D. For each g_i, $\exists C_i \in \mathcal{C}$ $\forall x$, $g_i(x) = C_i(x)$. Non-det alg to verify that: guess each C_i, $i = 1 \ldots m$. Verify that $\forall x$, $C_i(x) = op_i(C_{j(i)}(x), C_{k(i)}(x))$ & (this expression is in $\mathcal{C}$-TAUT), do this once for each gate in poly in input size. Finally, check "$C_{output}(x)$" is a yes.

- any improved alg for circ SAT gives some new bounds -

computer