

1/10/2015

Russell  
 Lec 11

Improved meta-algorithm and tied to lower bounds.

- deconstruction of CAPP and PIT
- "natural" and "beyond natural" properties

hard  
 $\Sigma_3$

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

$\Sigma_2$   
 $\Sigma_1$   
 $\Sigma_0$

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

If circuit SAT  $\in P$ ,  $\Sigma_3^P \subseteq P$ , so  $\Sigma_3^P = EXP$ , so EXP contains max hard prob.

(in [Kabanets-Cai])  
 3rd level:  $x \in L \Leftrightarrow \exists y_1, \forall y_2 \exists y_3 R(x, y_1, y_2, y_3)$  - possible possible

Given  $x, y_1, y_2, \exists y_3$  s.t.  $R(x, y_1, y_2, y_3) \in NP$

$\Sigma_2^P$   
 $\Sigma_1^P$   
 $\Sigma_0^P$   
 $P$

$x \in L \Leftrightarrow \exists y_1, \forall y_2 S(x, y_1, y_2) \in P$  since  $NP = coNP$ .

- having an alg better than a solver? e.g. quantum alg for SAT?  $\Sigma_2^P$   
 $L \in \Sigma_1^P \Leftrightarrow \exists y_1 \forall y_2 L(x, y_1, y_2) \in P \Rightarrow L \in \Sigma_1^P$

Collapses between classes translate upwards,  
 Separators between classes translate downwards  
 "pretty good alg" for circuit SAT? So circuit SAT  $\in TIME(2^{n^{o(1)}})$ .

then  $NP \neq P$  / poly

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

Meyer's thm:  $EXP \subseteq P/poly \Rightarrow EXP = \Sigma_2^P$   
 $x \in L \Leftrightarrow \exists y_1, \forall y_2 S(x, y_1, y_2) \in TIME(2^{n^{o(1)}})$

So  $L \in NTIME(2^{n^{o(1)}})$  and  $\Sigma_3^P \subseteq EXP \subseteq NTIME(2^{n^{o(1)}})$   
 $\exists T \in n^{o(1)}$  s.t.  $\Sigma_3^P \subseteq NEXP$ .  $\Sigma_3^P \not\subseteq P/poly \Rightarrow NEXP \not\subseteq P/poly$ .

(Meyer's thm) Circuit is locally computable, if given a name of a gate  $i$  can compute  $OPL(i), I(i), K(i)$  Two input gates and operation.

Fischer-Pippenger: for any time  $T(n)$  alg there is a size  $O(T(n)^{o(1)})$  locally computable circuit can simulate the alg.

Paul is adopting obvious  $k$ -tape to 2-tape simulation, (Norrman's, 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 exp deciding  $L$  on  $n$ -bit inputs

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

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

$x \in L \Leftrightarrow \exists C'' \forall i \text{ op}_i (C''(x, i(0)), C''(x, K(i))) = C''(x, i(0)) \wedge C''(x, K(i))$

[Minsky's]. naive alg for circuit SAT:  $|C| \cdot 2^n$ , If circuit SAT  $\in TIME(|C| \cdot 2^n/n^{o(1)})$ ,

then  $NEXP \not\subseteq P/poly$ ; moreover, enough to assume circ-sat  $\in NTIME(|C| \cdot 2^n/n^{o(1)})$

(circ-sat  $(C) = ?$  circuit SAT  $(TC)$ )

Assume  $NEXP \subseteq P/poly$  and Circ-TAUT  $\in TIME(2^n/n^{w(n)})$

- self contradiction w/ nondet time hierarchy thm.

Last class: easy witness lemma

$NEXP \subseteq P/poly \Leftrightarrow$  every possible instance of NEXP problem has succinctly describable witness (by possible circuit computing it) with bits of the witness

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

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

$x \in L \Leftrightarrow \exists C$  witness s.t.  $R(x, (C_x(C) \parallel C))$  - better witness, also

$x \in L \Leftrightarrow \exists g_1, g_2, \dots, g_{2^n/n}$  s.t. "even gate  $i$  is correct given its inputs and output = 1." (same as per  $C''$  gate  $i$ )  $g_i = op_i(g_{j(i)}, g_{k(i)})$   $T_{C''}(i)$

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

- exists by EWL (easy witness lemma) - has  $n + \log n + o(1)$  bits

$T_{C''}(i)$ :  $x \in L \Leftrightarrow \exists C''$   $T_{C''}$  is a tally log,  $g \in TIME(2^{n/n^{w(n)}})$

$\approx NTIME(poly(n) \cdot poly(n) \cdot 2^n/n^{w(n)})$ .

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

$NTIME(2^n/n^{w(n)}) \not\subseteq TIME(o(2^n/n^{w(n)}))$ .  $\square$

Now, ACC  $\not\subseteq NEXP$ .

Williams: ACC - SAT  $\in TIME(2^{n-n^2})$  ( $\forall d \exists \epsilon$ ).

Cor Lemma if  $P$  a class of circs  $C$ , C-TAUT  $\in TIME(2^n/n^{w(n)})$

and  $P \subseteq C$ . Then circ-TAUT  $\in TIME(2^n/n^{w(n)})$

Cor if C-TAUT  $\in TIME(2^n/n^{w(n)})$ , then  $NEXP \not\subseteq C$ .

Cor  $NEXP \not\subseteq ACC$ .

Proof if  $P \in C$ , then  $P/poly \in C$ . Let  $D$  be an instance of circ-TAUT. Let

$g_1, \dots, g_m$  be the gates. Given  $g_i$  defines a subcircuit of  $D$ . For each  $g_i$ ,  $\exists C_i \in C$

$\forall x, g_i(x) = C_i(x)$  - non-det alg to verify that  $i$  guess each  $C_i$ , etc. -

Verify that  $\forall x, C_i(x) = op_i(C_{j(i)}(x), C_{k(i)}(x))$  (this expression

is in C-TAUT). Do this once for each gate  $i$ , poly in input size. Finally, check

"output(x)" is a text.

- any improved alg for circ SAT gives lower bounds -