

1/10/2015

Mussert Lec 12

last: If there is any improved circ-sat, then keep it / pos.

How close are we to getting the type of circ? Special cases of SAT?

(SMT) improved SAT for circ size (series-parallel circs) → super-linear lower bound for EUP

(Those covers next week).

NP-completeness: emerged from SAT, then special cases of SAT, etc

- improved circs for ind. set, circuit, etc. Robson has best at this point

Circ SAT ~~is~~ 3SAT reduction:

$$\begin{aligned} x_1 &= s_1 & g_{n+1} &= OP_{n+1}(i_{n+1}, j_{n+1}) \\ & \vdots & & \\ x_n &= s_n & g_m & \end{aligned}$$

n inputs, m gates → inst. of 3SAT or k+m inputs.

$$\exists x_1, \dots, x_n, s_1, \dots, s_m \text{ s.t. } \underbrace{g_i = OP_i(g_{j_1}, g_{k_1})}_{\text{3 vars, so 3CNF}} \wedge g_m = 1$$

If can solve 3SAT in time  $(2^{\epsilon n})$  then circ-SAT  $\leftarrow$  time  $(2^{\epsilon m})$

So want  $\epsilon = o(1)$ .

Challenge: if we can find an alg for 3SAT that is time  $2^{o(n)}$ , then produce circ LB.

ETH: maybe such alg does not exist;  $\exists \epsilon$  s.t. no  $2^{\epsilon n}$ -time alg for 3SAT

- want  $(1+\epsilon)^n$  (for  $\forall \epsilon$ ) alg

- interesting if true, interestingly if false.

- can get such circ LB if ~~other~~ promise either no or many solutions.

Best known 3SAT (kSAT) alg

- alg based on switching lemma, prob. zero-error, in time  $2^{n^{1-\epsilon}}$  solve k-SAT (C is big, 8 or 10)

- other algs: same time, different techniques, maybe there is a barrier?

- should be able to make  $\epsilon$  arb-small to disprove ETH

As  $n$  increases, amount saved gets smaller.

SBTH (strong exp-time hypothesis)  $\forall \epsilon \exists k$  s.t. k-SAT  $\notin$  time  $2^{(1-\epsilon)n}$

"Conj": wh-site for SAT  $\rightarrow$  "superstrong ETH" + false.

SAT algs are used in practice: but these are heuristics w/ LBs. Have ETH-gre hardness for other, though not SBTH-hardness

[Paturi Padgug Zone] algo with  $n^{1/2}$  pp 2.

Compression method.

- 1) rand permute vars. 2) for each var, set it to rand value unless it is forced from previous choices: i.e. increase C,  $x_i = v_i$  in which rest of literals are false. (in that case set it to forced value.
- 3) check to see if sat sat assign.

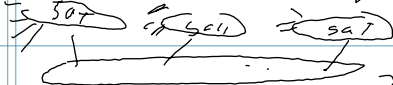
$(\exists v_1 \vee v_2) \wedge (\exists v_3 \vee v_4)$ . So  $v_1 = F, v_2 = T, v_3 = F, v_4 = F$ ;  $Z$  forced to  $T$ .  
 $\exists$  is set, non-trivial clause to set  $v_1, v_2$ .  
 - can thread up a bit of work.

What if  $\exists$  had just one assign?  $v_1, \dots, v_n = v$   
 (unit prob)  $2^{-n} (1-1/k)$ . Suppose flip  $v_i$ . Then made it unsex.  
 Suppose  $v_i = c, 1, \dots, n$ . Flip made  $v_i$  rest one  $c_j$ 's decrease  
 clause of the form  $(\exists v_i \vee \dots \vee \exists v_j \vee \exists v_k)$ , with  $\exists v_i$  only literal  
 satisfy  $c_j$ .

Prob [PPZ gives outputs  $x$ ] = Prob [all random decisions =  $x$ ]  
 $= 2^{\# \text{ rand. dec}}$  on the prob consistent w/  $x$ .  $= 2^{-n \# \text{ forced decisions}}$  on prob consistent w/  $x$ .

When does  $c_j$  force  $v_i$ ? pick  $v_i$  rest in  $c_j$  to branch on  $v_i$ .  
 $(c_j$ : critical clause for  $v_i)$ , Prob  $(x_i = 1) \geq 1/k$   
 (here, for simplicity do not do unit clause prob, and set  $v_i$  in only one clause)  
 So expected # of forced decisions is  $\frac{n}{k}$ . Overall prob,  $2^{-n \cdot n/k} = 2^{-n(1-1/k)}$

What if non-unique assign?

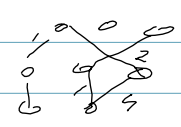
 neighbours are one forced var.  
 Let  $\deg^D(v_i) = \#$  of neighbours that  $v_i$  is forced

$n - D(v_i)$  vars w/ critical clauses, expected # of forced vars  $\geq \frac{n}{k}$

If  $D$  is large, also good for us: since vars set assigns, easy to find  $x$ .  
 If  $x \in \text{SAT}$ , assign, Prob [PPZ returns  $x$ ]  $\geq 2^{-n - (n-D(v_i))/k}$   $\geq 2^{-n(1-1/k) - D(v_i)/k}$

Prob [PPZ returns some sat assign]  $\geq \sum_{x \in \text{SAT}} 2^{-n(1-1/k) - D(x)/k} \geq 2^{-n(1-1/k)}$

Let  $E_i = \#$  of pairs that differ just in  $v_i$ .



Subtable w/  $v_i, \dots, v_n$  unsex, rest const 0,  $S = 2^i$ . Avg deg  $\leq 2$ , so  $S = i$  for  
 a set of size  $S$ . (Karger's lemma?)

Entropy  $H$ : measures randomness of dist.  $H(D) = \sum_x P(x) \log_2 P(x)$

$H(X|Y) =$  expected  $Y$  of entropy of  $X$  | true value of  $Y$ .

$H(X_1, \dots, X_n) = \sum_{i=1}^n H(X_i | X_1, \dots, X_{i-1})$ . Pick  $X \in S$ , let  $v_i$  be ith var of  $X$ .

$H(X) = \log_2 S = \sum_{i=1}^n H(X_i | X_1, \dots, X_{i-1}) \geq \sum_{i=1}^n H(X_i | X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n) = \text{Exp}(D(X))$

- if an edge at  $v_i$ , one bit of entropy, else no entropy.

$\sum 2^{-D(x)/k} \geq S 2^{-\log_2 S / k} = S - S^{-1/k}$ ; increases w/  $k$ . So unique case is worst.

$\times$  PPSZ: increased const to  $2^{-n(1-1/k)}$ .

Next class: Schoningh's algo - Then sparsification lemma.