1/10/2015

Russell Lec 12

last: If there is any improved circ-SAT algs, then NEXP ⊄ P/poly.
How close are we to settling this type of algs? Special cases of SAT?
[IMV] improved SAT for ckt size (series-parallel case) → some lower
lower bound for ENP
(Those comes next week).
NP-completeness: emerged from SAT, then special cases of 3SAT, etc
- improved algs for ind. set, cliques, etc. Robson has best alg for max

Circ SAT ≤_p 3SAT reduction:

$x_1 = s_1$ $\quad g_{n+i} = OP_{n+i}(i_{n+i}, j_{n+i})$
$\vdots$ $\quad \vdots$
$x_n = s_n$ $\quad g_m$.

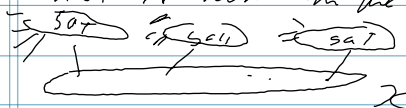
n inputs, m gates → inst. of 3SAT on n+m inputs.

∃ $x_1 \ldots x_n, s_1 \ldots g_m$ s.t. $g_i = OP_i(g_{j_i}, g_{k_i}) \wedge g_m = 1$
(3 vars, so 3CNF)

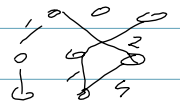
If can solve 3SAT in time $(2^{\varepsilon m})$ then circ-SAT ∈ time $(2^{\varepsilon m})$
so want $\varepsilon = o(1)$.
Challenge: if we can find an alg for 3SAT that is time $2^{o(n)}$, then
prove a circ lb.
ETH: maybe such alg does not exist; ∃ ε s.t. no $2^{\varepsilon n}$-time alg for 3SAT
- want $(1+\varepsilon)^n$ (for $\forall \varepsilon$) algs
- interesting if true, interesting if false.
- can get such circ lb if ~~Either~~ promise either no or many solutions.
Best known 3SAT (USAT) algs
- alg based on switching lemma, prob. zero-error, in time $2^{n(1-1/ck)}$ $\forall c$
solve k-sat (c is big, 8 or 10)
- other algs: same time, different techniques, may be true, more general?
- should be close to move ε and k-sat to ETH
As k increases, amount saved gets smaller.
SETH (strong exp. time hypothesis): $\forall \varepsilon$ ∃k s.t. k-sat ∉ time $(2^{(1-\varepsilon)n})$
"Conj": nk-size ckt ⇒ "superstrong ETH" ↛ false.
SAT algs are used in practice: but those are heuristics w/ lbs. Hence ETH-type
hardness for them, though not SETH-hardness
[Paturi Pudlak Zane] algorithm: PPZ.
Compression method.
1) some permute vars. 2) for each var, set it to some value unless it is forced
from previous choices: i.e. I clause 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 set assign.

$(x_1 \vee \bar{x}_2) \wedge (z \vee w \vee u)$. Say $u = F$, $w = T$, $x = F$, $z = F$: 2 forced to sat assign.
If rest is sat, non-unique chance to get sat assign.
– can proceed w/ a bit of work.
What if rest had just one assign? $x_1 \dots x_n = x$
(min prob $> 2^{-n(1-1/k)}$). Suppose trip x_i. Then made it unsat.
Suppose $\psi = c_1 \wedge \dots \wedge c_m$. Trip made each rest one c_j is 2-clause
clause of the form $c_j = (x_i \vee \dots \bar{x}_j \vee \bar{x}_u)$, with $\bar{x}_i$ own literal
satisf. c_j.
Prob [PPZ ans outputs x] = Prob [all random decisions = x]
$= 2^{\#\text{rand. dec}}$ on the rest consistent w/ x. $= 2^{-n + \#\text{forced decisions}}$ on pairs consist. w/ x
When does c_j force x_i? pick x_i rest in c_j: to branch on
(c_j : critical clause for x_i). Prob (x_i is rest) $\geq 1/k$
(here, for simplicity do not do unit clause prop. and say x_i is on one cla
So expected # of forced decisions is $\geq \frac{n}{k}$. Overall prob $\geq 2^{-n}\sqrt{n/k} = 2^{-n(1-1/k}$

What if non-unique assign?



neighbours are one flipped var.
Let $\deg^D(x)$ = # of neighbours that $\dots$
$n - D(x)$ vars w/ critical clauses, expected # forced vars $\geq \frac{n-D}{k}$
If D is large, also good for us: since vars set assigns, exp to find $\dots$ $2^{-n(1-1/k)} \cdot 2^{D(x)}$
$\forall x \in SAT_{\text{assign}}$, prob [PPZ returns x] $\geq 2^{-n + (n-D(x))/k} \geq 2^{-D(x)/k}$
Prob [PPZ returns some sat assign] $\geq \sum_{x \in SAT} 2^{-n(1-1/k)} \sum_{x} 2^{-D(x)/k}$



Let $\bar{z}_i$ = # of pairs that differ just in x_i.
Subcube w/ $x_1 \dots x_i$ unset, rest const $= 0$, $S = 2^i$. Any deg $\leq \log S = i$, for
a set of size S. (Hamming's lemma?).
Entropy H: measures randomness of dist. $H(D) = \sum_{x : p(x) > 0} p(x) \log p(x)$
$H(X|Y)$ = expected Y of entropy of X | that value of Y.
$H(\langle X_1 \dots X_n \rangle) = \sum_{i=1}^{n} H(X_i | X_1 \dots X_{i-1})$. Pick $X \in S$, let x_i be ith bit of X.
$H(X) = \log S = \sum_{i=1}^{n} H(X_i | X_1 \dots X_{i-1}) \geq \sum H(X_i | X_1 \dots X_{i-1} X_{i+1} \dots X_n) = \text{exp}(D(x))$
– if can fix all x_i, one bit of entropy, else no entropy.
$\sum 2^{D(x)/k} \geq S\, 2^{-\log S/k} = S - S^{-1/k}$; increases w/ k. So unique case is worst.
PPSZ: increased const to $2^{-n(1-1/k)}$.
Next class: Schoning alg. Then sparsification lemma.