

22/8/2015 Russell's class, lecture 1.

Sideos:

1) A's design \leftrightarrow L6

2) multi-dimensional circuits of class \rightarrow more info on definition of types of instances

3) reductions at finer grain, e.g. "if ed. distance \in Time(n^2), then SAT \in Time($2^{n(1-\delta)}$)"

Exact complexity of NP-complete; meta-algorithmic programs (i.e., input and/or outputs are representations of algorithms) e.g. halting problem, circuit-SAT, program verification, circuit value, circuit minimization, compiler design...

Random circuits: introduced in Rivest & Schnorr; $\forall n \exists \delta$ on n -bit inputs s.t. $size(x) = \Omega(2^{n/\delta})$

For any function we know how to construct, best lower bound is $\Omega(n)$ (Merkle & Blum).

Restricted circuits: CNF and DNF: 2^n upper bound

Exercise: prove that parity $R(2n, 2n) = \binom{2n}{n} \bmod 2$ the # of terms in DNF / circuits is $\Omega(2^n)$

SAT: satisfiability of CNF. k -SAT: k clauses $\leq k$ literals

Depth unbounded fan-in circuit. δ gates with $1, \forall$ regers, \exists, x and y .

poly size. AC^0 equiv to polynomial const-time w/ shared memory

$size(x) \geq \Omega(2^{n^{1/(k+1)}})$, for $\delta = \text{parity}$.

Ajtai, Furst, Saegrovsky, Yao, Cai, Hastad.

k -HSAT: given k -CNF ϕ , count # of satisfying assignments

Best alg: for k -SAT: $2^{n(1-1/k)}$, Schonitz, PPSZ, IMP.

- different techniques, same expression

for k -HSAT: IMP.

Random restrictions method: $f: \mathbb{F}_2^n \rightarrow \{0, 1, \delta\}$. δ/p

Hastad switching lemma: let ϕ be a k -CNF

(decision tree: k nodes and unary internal vertices are vars, leaf \rightarrow output \rightarrow 1, leaves: possible output values 0,1)

E.g. $x \rightarrow y$ and $y \rightarrow z$. Decision tree $\begin{matrix} 0, y \\ \swarrow \downarrow \searrow \\ \mu \\ \swarrow \downarrow \searrow \\ 1, 0, 1 \end{matrix}$. $DTD(x) =$
 min. decision tree depth of x . $DTD = D \Rightarrow D - CNF$ and $D - S DNF$
 Canonical decision tree for a CNF: query ~~is~~ vars ~~are~~ in DNF +
 clause; then subtract and simplify; query next unset clause
 If any clause empty clause, set to false. If no clause, output 1.
Master containing lemma

Let \mathcal{C} be a k -CNF. Let p be a random restriction. Recall
 p n vars unset. Then $\text{Prob}[\text{depth}(CDT(\mathcal{C}|_p)) \geq D] \leq$
 $(4e \frac{p}{1-p} k)^D$

If $p > 1/k$, then each clause has decent chance of not disappearing.
 Proving lower bound for parity:

After one restriction, each V_i on lowest degree becomes (ns) size of $p \geq 1/(ns)$. After i th restriction, how $\frac{n}{(ns)^i} \geq 1$. So for parity,
 $(ns)^d \geq n$, so $s \geq \exp(\frac{d}{n})$.

~~u~~ algorithm: let $p = 1/8ed$. Divide input into $6ns$
 $0 \leq (1-p)n$, (pn) is random. Over all such partitions, n is
 blocks of restricted.