

17/9/2015 Russell's course, lec 7

Lower bounds: necessary why functions are hard to compute.

Upper bounds: circuit design. So for, techniques for LB = techniques for UB.

Next few lectures: $UB \rightarrow UB \rightarrow LB$, and later technique is used a second, back is ~~is~~.

Derandomization. Primarily testing: given circuit C , is it a prime?

PIT: given some complex desc of a poly, as a sum of t char polys, is $poly \equiv 0$?

eg 1, $(x+y+z+w)^4 - (x+y-z-w)^4 - (x-z+y-w)^4 - (x-y-z+w)^4 \equiv 0$?

Algebraic circuits over integers.

DLST: pass in random values. If have random values then desc, then can determine

Issue: numbers get too big - (e.g. $x^n + y^n = z^n$, for $n=4, x, y, z$ non zero check?)

have mod random primes. Non-zero mod random prime is non zero. WRP as

PIT \in WRP, BPP: two-sided error, const.

Rabin, Solovay, Strassen: randomized polynomial testing in \mathbb{F}_p .

2001: Agrawal, Kayal, Saxena: Primality $\in P$

PIT: not known to be in P .

Generic probabilistic alg: $A(x, \text{pick } r \text{ random}) = \text{no}$

Let test $T_x(r) \equiv A(x, r)$

$|r| \leq \text{time for } A \text{ on } |x|$. For each x , $T_x(P)$ is a circuit with input.

Want to find: $\text{prob } T_x(r) = 1$ to within small additive error. (analog to solving

CAPP: given $C(r, r_m)$ estimate $\text{prob } (C(r) = 1) \pm 1/4$ (see BPP correct? 2/3)

Randomized alg: pick values, estimate fraction which is accepted.

Generator $G: \{0,1\}^l \rightarrow \{0,1\}^m$, $l \leq m$ and G is not too horrible to compute

Break w/ G -derandomization: for each $s \in S, \dots, S_l$, define $T_s = G(s)$.

Compute $C(T_s)$, estimate fraction on which C accepts. Time: $2^l (\text{Time}_C(l) + \text{gen cost})$

Yao: crypto PRG: $\text{Time}_G(l) = \text{poly}(l)$, here $\{N, K\}$: $\text{Time}_G(l) \approx 2^{O(l)}$

Goal: minimize l .

A circ. C solves G -RDP: C vs. randomness distinguishing problem, if

$\text{prob } [C(G(s)) = 1] - \text{prob } [C(r) = 1] \geq \epsilon$

Lower bound for G -RDP: for every small G , C fails to solve G -RDP.

Upper bound (on correctness for our alg): for small C , $C(G(s))$ is good approx to $C(r)$

(here, small ϵ fixed in size). i.e., C & r fail to solve G -RDP.

Constructing a PRG: Let $F(y_1 \dots y_n)$ be (S, E) -hard it's circ C of size S , $\text{prob } \{F(y) \in C\}$

Special case: $\epsilon = 0$; then worst case. $\epsilon = \text{const}$, almost everywhere: $\epsilon = 1/2^d$, where $d \ll 1/l$ $\epsilon = 1/2^d$

NW: construction of a PRG $G: \{0,1\}^n \rightarrow \{0,1\}^m$, $S = \text{poly}(m)$, $\epsilon = \frac{1}{2} - \frac{1}{S}$

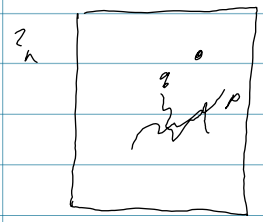
For AC^0 , $S = 2^{n^k}$ parity is hard.

Let $G_{+1}: \{0,1\}^n \rightarrow \{0,1\}^{n+1}$. $G_{+1}(x) = x, F(x)$

$C \subseteq \mathbb{Z} \rightarrow \mathbb{Z}_1, \dots, \mathbb{Z}_m$, and each $\mathbb{Z}_i, |\mathbb{Z}_i| = k$. Then output $F(\mathbb{Z}_1), \dots, F(\mathbb{Z}_m)$.
 Design (in HW terms). Let $\ell = O(n^2)$. $\mathbb{Z}_1, \dots, \mathbb{Z}_\ell$ restriction on \mathbb{Z} to some bit positions. $A_i \subseteq \{0, \dots, \ell\}$, $\mathbb{Z}_i = \mathbb{Z}|_{A_i}$.

would be good if $A_i \cap A_j = \emptyset$, but next best $|A_i \cap A_j| \leq k$ for small k .
 If so, 2^k advantage in computing \mathbb{Z}_i . Could produce $F(\mathbb{Z}_i)$ given $\{F(\mathbb{Z}_j) | i=j\}$.
 $\mathbb{Z}_i = \mathbb{Z}|_{A_i}$, $\mathbb{Z}|_{\mathbb{Z} \setminus A_i}$. For \mathbb{Z}_i , prediction of $F(\mathbb{Z}_i)$ given $\{F(\mathbb{Z}_j) | i=j\}$ with
 \mathbb{Z}_i \mathbb{Z}_j

fixed w_i still just as ... So every bit of \mathbb{Z}_j with $A_i \cap A_j = \emptyset$ fixed to a bit in w_i . So $\mathbb{Z}_j|_{w_i}$ is k -bit input. 2^k possible values. For small k , can do a truth table. For each $F(\mathbb{Z}_j)$, of size $\leq 2^k$.
 Get circ of size $S_2 = S_1 + O(2^k \cdot m)$



Suppose n is a prime (round up), $\ell = n \times n$
 n^2 : because of Girard's paradox.
 Polynomials of low deg have few roots in common, look at univariate polynomials of deg k mod n .
 $A_p = \{i, p(i) | i=0, \dots, n-1\}$, $a_0 + a_1 x + \dots + a_k x^k$
 $m = n^k$, $k = \log n / \log m < \log m$.

$$|A_p \cap A_q| \leq k, = \left| \{i | p(i) = q(i)\} \right| \quad \text{So } O(2^k \cdot m) = O(m^2), S_2 = S_1 + O(m^2)$$

As S_1 is $O(m)$, need F to be $O(m^2)$ -hard
 Application: if C is size m in C^0 circ, depth d , it can estimate parity on
 with prob $\leq \exp(-n / \log^d m)$. Pick $n = \log^{2d} m$, let P be parity on
 $\log^{2d} m$ bit inputs, 6 nodes size m depth d circs.
 CAPP(C^0) in time $2^{\log^{2d} m}$: quasipoly in circ size.