15-251: Great Theoretical Ideas In Computer Science

Recitation 11 : Randomized Algorithms and Modular Arithmetic

Announcements

- NO QUIZZES for the rest of the semester.

`fastPow` Redux!

Design an efficient algorithm to compute $A^E \mod N$ (modular exponentiation) where A, E, and N each have at most n bits, and analyze its time complexity.

Atlantic City to Monte Carlo.

Suppose you are given a randomized algorithm that solves $f : \Sigma^* \to \Sigma^*$ in expected time $T(n)$ and with ε probability of error (i.e., the algorithm gambles both with correctness and running time). Show that for any constant $\varepsilon' > 0$, there is a Monte Carlo algorithm computing f with running time $O(T(n))$ and error probability $\varepsilon + \varepsilon'$.

Max number of Min cuts

Show that a graph can have at most $n(n-1)/2$ distinct minimum cuts.

(EXTRA) PITiful polynomials

Consider the PIT problem: given as input a polynomial, written using any of

$$\Sigma = \{(,), +, -\} \cup \{x_i : i \in \mathbb{N}\} \cup \mathbb{Q},$$

calculate whether the polynomial is equal to 0.

Example input:

- $(x_1x_1x_1 + x_3)(x_5 + x_1)$ (which is not 0).
- $(x_1 + x_2)(x_1 - x_2) - x_1x_1 - x_2x_2$ (which is 0).

(a) Before we solve this problem, we need a lemma which you might find helpful.

Lemma 1 (Schwartz-Zippel) *If P is a non-zero polynomial on variables $x_1, \ldots, x_n$, and is of degree at most d, then if we draw each x_i uniformly from any set $S \subseteq \mathbb{R}$,*

$$\Pr[P(x_1, x_2, \ldots, x_n) = 0] \leq \frac{d}{|S|}.$$

Remark: You can think of this lemma as a kind of multivariable fundamental theorem of algebra.

Hint: You can prove this by induction on n. You probably know the base case, and don't forget FToA in the inductive step.

(b) Come up with an efficient randomized algorithm to solve this problem with error probability ε.

(Hint: Schwartz-Zippel Lemma)

(c) Something to ponder: some people believe that randomization gives you no more power than determinism. If we believe them, then try to come up with a deterministic algorithm to solve this problem.