6.045 Pset 6: Randomness and Cryptography

Assigned: Thursday, April 21, 2011
Due: Monday, May 2, 2011

To facilitate grading, remember to solve each problem on a separate sheet of paper! Also remember to write your name on each sheet.

1. Prove the law of linearity of expectation: $\mathrm{E}[X+Y] = \mathrm{E}[X] + \mathrm{E}[Y]$ for random variables X and Y. (You can assume, for simplicity, that X and Y are nonnegative-integer valued.)

2. Prove Markov's inequality: for all random variables $X \geq 0$ and all k,

$$\Pr[X > k\,\mathrm{E}[X]] < \frac{1}{k}.$$

3. Recall that ZPP (Zero-Error Probabilistic Polynomial-Time) is the class of languages L for which there exists a randomized algorithm that (i) for every input $x \in \{0,1\}^n$, halts after an *expected* number of steps polynomial in n, and (ii) when it does halt, always decides correctly whether $x \in L$. Show that $\mathsf{ZPP} = \mathsf{RP} \cap \mathsf{coRP}$. [*Hint:* You may want to use Markov's inequality.]

4. In this problem, you'll study the consequences if NP-complete problems were solvable by probabilistic (BPP) algorithms.

   (a) Show that if $\mathsf{NP} \subseteq \mathsf{BPP}$, then given a satisfiable SAT instance $\varphi(x_1, \ldots, x_n)$, you can actually *find* a satisfying assignment for φ in probabilistic polynomial time with high probability. [*Hint:* This is similar to the problem on a previous pset that asked you to prove the equivalence of search and decision—except that both the assumption and the conclusion now involve *probabilistic* algorithms. Generalizing your earlier solution to the probabilistic case may require amplification and the union bound.]

   (b) Using part a, show that if $\mathsf{NP} \subseteq \mathsf{BPP}$, then $\mathsf{NP} = \mathsf{RP}$.

5. In class, we discussed the following communication protocol, call it $\mathcal{C}$, for deciding whether two integers $x \in \{0, \ldots, 2^n - 1\}$ and $y \in \{0, \ldots, 2^n - 1\}$, held by Alice and Bob respectively, are equal. First, Alice chooses a random prime number p between 1 and n^{10}. Next, Alice sends p and $x \bmod p$ to Bob. Finally, Bob checks whether $x \bmod p = y \bmod p$, reports that $x \neq y$ if not, and guesses that $x = y$ if so.

   (a) Approximately how many bits does Alice need to send Bob in this protocol? What sort of improvement is that (polynomial, exponential, etc.) over the "naïve protocol" of sending x in its entirety?

   (b) Show that the number $|x - y|$ has at most $n + 1$ distinct prime factors.

   (c) Let $\pi(n)$ be the number of prime numbers less than n. The *Prime Number Theorem*, one of the greatest results of number theory, says that $\pi(n)$ asymptotically approaches $n/\ln n$:

$$\lim_{n \to \infty} \frac{\pi(n)}{n/\ln n} = 1.$$

   Using the Prime Number Theorem together with part a, show that if $x \neq y$, then $\Pr_p[x = y \pmod p] = o(1)$. Conclude that the protocol $\mathcal{C}$ succeeds with high probability.

(d) *[Extra credit]* Show that $\mathcal{C}$ is optimal, in the sense that no other protocol for equality-testing uses asymptotically fewer bits. [*Hint:* Can you simulate the randomized protocol $\mathcal{C}$ by a deterministic protocol that uses exponentially more bits? If so, what can you conclude from that?]

6. Show that there is no one-way function where every bit of the output depends on only two bits of the input. [*Hint:* Use the fact that $2SAT$ is in P.]

7. Let a *puzzle generator* be a polynomial-time algorithm that maps a random string r to a pair (φ_r, x_r), where φ_r is a 3SAT instance and x_r is a satisfying assignment for φ_r, such that for all polynomial-time algorithms A,

$$\Pr_r [A \text{ finds a satisfying assignment for } \varphi_r]$$

is negligible (less than $\frac{1}{\text{poly}(n)}$). Show that puzzle generators exist if and only if one-way functions exist.

8. The following questions concern the RSA cryptosystem.

   (a) Recall that, having chosen primes p and q such that $p-1$ and $q-1$ are not divisible by 3, a key step in RSA is to find an integer k such that $3k \equiv 1 \bmod (p-1)(q-1)$. Give a simple procedure to find such a k given p and q.

   (b) Given a product of two primes, $N = pq$, show that if an eavesdropper can efficiently determine $(p-1)(q-1)$ (the order of the multiplicative group mod N), then she can also efficiently determine p and q themselves.

6.045J / 18.400J Automata, Computability, and Complexity

Spring 2011