6.045 Pset 6

Assigned: Monday, April 30, 2012
Due: Friday, May 11, 2012

To facilitate grading, remember to solve each problem on a separate sheet of paper, and to put your name on each problem separately! Also, please indicate which recitation you attend by writing "11" or "2" on the first page.

1. (carried over from pset5) 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.

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

3. 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, which requires only $O(1)$ arithmetic operations.

   (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.

4. Recall that, given a prime number p, a *linear congruential generator* starts with a random triple $a, b, x_0 \in \{0, \ldots, p-1\}$ as the seed, then sets $x_t := ax_{t-1} + b \pmod p$ for all $t \geq 1$, and outputs the sequence $x_1, x_2, x_3, \ldots$. Show that a linear congruential generator is *not* a cryptographic pseudorandom generator, by describing a polynomial-time algorithm that given p, distinguishes $x_1, x_2, x_3, \ldots$ from a random sequence of numbers in $\{0, \ldots, p-1\}$ with high probability.

5. A problem is said to have *worst-case / average-case equivalence* if, intuitively, any polynomial-time algorithm that works on many instances of the problem can be transformed into a polynomial-time algorithm that works on *every* instance. Or equivalently, if "every polynomial-time algorithm fails on some instance" implies "every polynomial-time algorithm fails on *most* instances." People often try to base cryptographic codes on problems with worst-case / average-case equivalence, since then the security of the code only relies a worst-case hardness assumption, rather than an average-case hardness assumption.

   Now, recall that the problem of breaking RSA boils down to the following: given a composite RSA modulus N, together with an integer y relatively prime to N, find the *cube root modulo* N of y: that is, an x such that $x^3 = y \pmod N$. Show that this problem has worst-case / average-case equivalence.

More formally, suppose you have a polynomial-time randomized algorithm M that, for each RSA modulus N, outputs outputs the cube root of y for a fraction c of all y's in Z_N, where $c > 0$ is some universal constant. (Here "outputs" means "with high probability over M's random coin tosses.") Give another polynomial-time randomized algorithm M' that outputs the cube root of y with high probability for *every* (N, y) pair. [*Hint:* Can you randomly transform the given y into another input, whose cube root can be used to obtain the cube root of y?]

6. Show that if you apply Hadamard gates to qubits A and B, followed by a CNOT gate from A to B, followed by Hadamard gates to A and B again, the end result is the same as if you had applied a CNOT gate from B to A. This illustrates a principle of quantum mechanics you may have heard about: that any physical interaction by which A influences B can also cause B to influence A (so for example, it is impossible to measure a particle's state without affecting it).

7. Consider the following game played by Alice and Bob. Alice receives a bit x and Bob receives a bit y, with both bits uniformly random and independent. The players win if Alice outputs a bit a and Bob outputs a bit b such that $a + b = xy \pmod 2$. (Alice and Bob are cooperating in this game, not competing.) The players can agree on a strategy in advance, but once they receive x and y no further communication between them is allowed.

   (a) Give a deterministic strategy by which Alice and Bob can win this game with 3/4 probability.

   (b) Show that no deterministic strategy lets them win with more than 3/4 probability.

   (c) *[Extra credit]* Show that no probabilistic strategy lets them win with more than 3/4 probability.

   Now suppose Alice and Bob share the entangled state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, with Alice holding one qubit and Bob holding the other qubit. Suppose they use the following strategy: if $x = 1$, then Alice applies the unitary matrix

$$\begin{pmatrix} \cos\frac{\pi}{8} & -\sin\frac{\pi}{8} \\ \sin\frac{\pi}{8} & \cos\frac{\pi}{8} \end{pmatrix}$$

   to her qubit, otherwise she doesn't. She then measures her qubit in the standard basis and outputs the result. If $y = 1$, then Bob applies the unitary matrix

$$\begin{pmatrix} \cos\frac{\pi}{8} & \sin\frac{\pi}{8} \\ -\sin\frac{\pi}{8} & \cos\frac{\pi}{8} \end{pmatrix}$$

   to his qubit, otherwise he doesn't. He then measures his qubit in the standard basis and outputs the result.

   d. Show that if $x = y = 0$, then Alice and Bob win the game with probability 1 using this strategy.

   e. Show that if $x = 1$ and $y = 0$ (or vice versa), then Alice and Bob win with probability $\cos^2\frac{\pi}{8} = \frac{1+\sqrt{1/2}}{2}$.

   f. Show that if $x = y = 1$, then Alice and Bob win with probability 1/2.

   g. Combining parts d-f, conclude that Alice and Bob win with greater overall probability than would be possible in a classical universe.

   You have just proved the *CHSH/Bell Inequality*—one of the most famous results of quantum mechanics—which showed the impossibility of Einstein's dream of removing "spooky action at a distance" from quantum mechanics. Alice and Bob's ability to win the above game more than 3/4 of the time using quantum entanglement was experimentally confirmed in the 1980's.