6.080 / 6.089 Great Ideas in Theoretical Computer Science
Spring 2008

6.080/6.089 Problem Set 5

Assigned: April 29, 2008
Due: May 13, 2008

1. 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. 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.

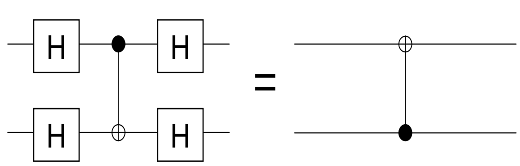
3. Recall that the *VC-dimension* of a concept class $\mathcal{C}$, or $\text{VCdim}(\mathcal{C})$, is the largest m for which there exist points $x_1, \ldots, x_m$ such that for all 2^m possible Boolean values of $c(x_1), \ldots, c(x_m)$, there exists a concept $c \in \mathcal{C}$ that realizes those values. If such $x_1, \ldots, x_m$ exist for arbitrarily large finite m, then $\text{VCdim}(\mathcal{C}) = \infty$.

   (a) Let $\mathcal{C}$ be the concept class consisting of all filled-in rectangles in the plane, whose sides are aligned with the x and y axes. Show that $\text{VCdim}(\mathcal{C}) = 4$.

   (b) Show that if $\mathcal{C}$ is finite, then $\text{VCdim}(\mathcal{C}) \leq \log_2 |\mathcal{C}|$.

   (c) Show that there is a class $\mathcal{C}$ with countably many concepts such that $\text{VCdim}(\mathcal{C}) = \infty$.

4. 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. Pictorially:



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).

5. 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.