CPSC 536N Randomized Algorithms (Term 2, 2012)
Assignment 1

Due: Thursday February 2nd, in class.

Question 1: In the first lecture we discussed the testing equality problem and described a randomized algorithm in which the number of bits exchanged between you and the server is $O(\log n)$ and the algorithm has constant probability of successfully testing equality of the vectors a and b.

Suppose now that you and the server somehow *share* an identical random string of length $\text{poly}(n)$. Give an algorithm that exchanges just k bits and succeeds in testing equality of a and b with probability at least $1 - 2^{-k}$.

Question 2: Consider a sequence of n unbiased coin flips. Consider the length of the longest contiguous sequence of heads.

- **(a):** Show that you are unlikely to see a sequence of length $c + \log_2 n$ for $c > 1$. Give a decreasing bound as a function of c.
- **(b):** Show that, for any $c \geq 1$, you will see a sequence of length $\log_2 n - O(\log_2 \log_2 n)$ with probability at least $1 - 1/n^c$. (The constant hidden by the O will depend on c.)

Question 3: Let $X_1, ..., X_n$ be independent, geometric random variables with parameter $p = 1/2$. (The number of fair coin flips needed to see the first head. So $\Pr[X_1 = 1] = 1/2$, $\Pr[X_1 = 2] = 1/4$, etc.)

- **(a):** For sufficiently small t, prove that $\mathrm{E}\left[e^{tX_i}\right] = \frac{e^t/2}{1-e^t/2}$.
- **(b):** Let $X = \sum_i X_i$. We will use the Chernoff-style method to prove a tail bound on X. Fix some $\delta = (0, 1)$. Prove that

$$\Pr[X > (1+\delta)2n] \leq \left(\frac{1+2\delta}{1+\delta}\right)^{-2(1+\delta)n} (1+2\delta)^n.$$

- **(c):** (Optional) Prove an exponential upper bound on the right-hand side in terms of δ and n.

Question 4: Let P be a non-negative matrix of size $n \times m$ such that $\sum_j P_{i,j} = 1$ for all $i = 1, ..., n$. Obtain the matrix Q from P by scaling each column to have sum equal to 1. In other words, $Q_{i,j} = P_{i,j} / \sum_k P_{k,j}$.

Prove that there exists a non-negative, integer vector $y \in \mathbb{Z}_+^m$ with $\sum_j y_j = n$ such that every coordinate of Qy is at most $O(\log n / \log \log n)$.