CPSC 536N Randomized Algorithms (Term 2, 2012)
Assignment 3

Due: Tuesday, April 3rd, in class.

Grading: You are required to do both questions 1 and 2. You are only required to do two of questions 3, 4 and 5.

Question 1: Let $G = (L, R, E)$ be a bipartite graph. We say that G is a (n, m, d, d')-expander if

- $|L| = n$ and $|R| = m$,
- every vertex in L has degree at most d,
- every vertex in R has degree at most d',
- $|\Gamma(S)| \geq |S|$ for every $S \subseteq L$ with $|S| \leq \frac{n}{2}$.

In this problem, we will prove that $(n, 3n/4, d, d')$-expanders exist for some constants d and d'.

(a): Let $m = 5n/8$ and $d = 20$. Generate a random graph G by having each vertex in U choose d neighbors in V at random. (We allow multiple edges.) Prove that, with constant probability, for sufficiently large n, this graph is a (n, m, d, ∞)-expander. (In other words, we don't care about the degree of the vertices in V.)

(b): Given such a G, construct a $(n, 3n/4, 20, 160)$ expander.

(c): Prove that, for any n, there are superconcentrators with n inputs, n outputs, $O(n)$ edges, and for which *every vertex has degree* $O(1)$.

Question 2: Suppose we have an algorithm $\mathsf{Test}(x, r)$ for deciding whether x belongs to a language L. Here r is an additional bitstring of length $f(x)$ which contains "advice". (This notion of advice should be familiar to you from the study of NP-completeness: if L is an NP-complete language then there always exists an efficient algorithm $\mathsf{Test}(x, r)$ which can decide if $x \in L$, if it is given the right advice.)

Let us suppose that our algorithm Test satisfies the following property.

- If $x \in L$ then $\mathsf{Test}(x, r) = 1$ for at least half of the possible bitstrings r of length $f(x)$. A string r such that $\mathsf{Test}(x, r) = 1$ is called a *witness* for x.
- If $x \notin L$ then $\mathsf{Test}(x, r) = 0$ always.

For this problem we are interested in testing whether $x \in L$ without using too much randomness. Suppose we choose two random bitstrings r_1 and r_2 of length $f(x)$ independently and uniformly. Consider running the algorithm Test twice: first we call $\mathsf{Test}(x, r_1)$, then $\mathsf{Test}(x, r_2)$. Then, assuming $x \in L$, the probability that either r_1 or r_2 is a witness is at least $3/4$.

Argue that, given just these two random bitstrings r_1 and r_2, we can actually find a witness with probability at least $1 - 1/t$ by evaluating $\mathsf{Test}(x, r_1 + z \cdot r_2)$ for all values $z \in \mathbb{F}_{2^{f(x)}}$. (Here the arithmetic $r_1 + z \cdot r_2$ is in the field $\mathbb{F}_{2^{f(x)}}$.)

Question 3: In Assignment 1, we considered the following problem.

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, $Q_{i,j} = P_{i,j} / \sum_k P_{k,j}$. Give a randomized algorithm that, with probability at least a constant, constructs 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 $O(\log n / \log \log n)$.

Give a deterministic, polynomial time algorithm for the same problem.

Question 4: Let $D = (N, A)$ be a digraph with $n = |N|$ and $m = |A|$. Let Δ be the maximum degree of any node, **excluding** s and t. Formally, for $v \in N$, let $d^+(v)$ be the number of arcs whose head is v and let $d^-(v)$ be the number of arcs whose tail is v. Then $\Delta = \max\{\, d^+(v) + d^-(v) \,:\, v \in N \setminus \{s,t\} \,\}$.

Suppose we have an algorithm that, given nodes $s, t \in N$, computes the maximum number of arc-disjoint s-t dipaths, with running time $O(m \cdot f(\Delta))$ where f is some function (e.g., $f(x) = x^2$). Such an algorithm seems not very useful, since we could have $\Delta = \Theta(n)$ and $O(mn^2)$ is not a particularly great running time.

But actually, such an algorithm would be very useful. Use it to give a randomized algorithm that computes the maximum number of arc-disjoint s-t dipaths in time $O(m)$. The success probability of the algorithm should be at least 1/2.

Question 5:

(a): Let X be a finite set of elements. Let $A_1, \ldots, A_\ell$ be random subsets of X where each A_i is chosen by including each element of X independently with probability $p < 1/\ell$. Let $Y = \sum_{j=1}^{\ell} |A_j| - \left| \cup_{j=1}^{\ell} A_j \right|$. Prove that:

$$\mathrm{E}[\,Y\,] \;\leq\; n(p\ell)^2/2$$

(b): Prove that:

$$\Pr[\,Y \geq t\,] \;\leq\; (1 + (p\ell)^2)^n \cdot 2^{-t} \qquad \text{(for all } t \geq 0\text{)}.$$

(c): Let U and V be disjoint sets of vertices with $|V| = n$ and $|U| = n^2$. Let $G = (U \cup V, E)$ be a random bipartite graph generated by including every possible edge with probability $p = n^{-2/3}$. For every $u \in U$, let d_u be the degree of vertex u. For every $S \subseteq U$, let

$$\Gamma(S) \;=\; \{\, v \in V \,:\, \exists u \in S \text{ such that } \{u, v\} \in E \,\}.$$

So $\Gamma(S)$ is the set of neighbours of S. Obviously $|\Gamma(S)| \;\leq\; \sum_{u \in S} d_u$.
Let $\alpha = 4\log(n)$. Prove that, with high probability, every $S \subseteq U$ with $|S| \leq n^{1/3}$ satisfies

$$|\Gamma(S)| \;\geq\; \sum_{u \in S} (d_u - \alpha).$$