Problem set 10 - PRG for BP

out: 30/12/14
due: 12/1/15

Notation for the exercise: A $[W, T, \Sigma]$ branching program is a branching program with width W, length L and input alphabet Σ. Every layer is labeled with some $i \in [T]$. The BP is *read-once* if all the indices are distinct (which means that the BP reads all input variables in some order, but each input variable is read only once). The BP has two special vertices: one marked as the initial vertex and the other as an accepting vertex. The BP accepts an input $(a_1, \ldots, a_T) \in \Sigma^T$ iff starting at the initial vertex and walking according to $a_1, \ldots, a_T$ (meaning that at a layer labeled by i we move as instructed by $a_i \in \Sigma$) leads to the accepting vertex. A BP accepts a function $f : \{0,1\}^T \to \{0,1\}$ iff it accepts x iff $f(x) = 1$.

1. Prove that every function $f : \{0,1\}^n \to \{0,1\}$ is accepted by some $[2^n, n, \{0,1\}]$ read-once branching program.
2. Define $ExactHalf(x_1, \ldots, x_n) = \begin{cases} 1 & \sum x_i = n/2 \\ 0 & \text{otherwise} \end{cases}$

   Prove that there exists a $[W = O(\log n), O(n \log n), \{0,1\}]$ branching program that accepts ExactHalf. Notice that the branching program does not have to be read-once.
3. Define the $ExactHalfClique_n$ function as follows. n is a fixed even integer. The input to the problem is a sequence $e_{i,j}$ for $1 \leq i < j \leq n$ with $e_{i,j} \in \{0,1\}$. The input defines an undirected graph $G = (V = [n], E)$ with $(i,j) \in E$ iff $e_{i,j} = 1$. The function is 1 on the input iff the graph G has a clique of size $n/2$ and *no other edge*.

   Prove that every $[W, \binom{n}{2}, \{0,1\}]$ read-once branching program that accepts $ExactHalfClique_n$ must have width $W = \Omega(\frac{\binom{n}{n/2}}{n})$.
4. Show that there exists $G : \{0,1\}^\ell \to \{0,1\}^T$ that is an ε-PRG against $[W, T, \Sigma]$ Branching programs with $\ell = O(\log \frac{|W| \cdot T \cdot |\Sigma|}{\varepsilon})$.
5. Assume there exists a PRG as above that runs in space linear in its input length. Prove that:
   - $\mathsf{BPL} = L$,
   - There exists an L-explicit UTS for undirected, arbitrarily labeled, graphs.
6. (The Nisan-Zuckerman PRG) In this question we assume the existence of (s, ε) extractor $E : \{0,1\}^{10s} \times \{0,1\}^t \to \{0,1\}^s$ for $\varepsilon \geq 2^{-s}$ with seed length $t = O(\log s + \log(\frac{1}{\varepsilon}))$. We furthermore assume E is explicit and runs in space linear in its input length. We remark that such explicit extractors are indeed known.
   - Prove that $G : \{0,1\}^{10s+\ell t} \to \{0,1\}^{10s+\ell s}$ defined by

     $$G(x; y_1, \ldots, y_\ell) \quad = \quad x \circ E(x, y_1) \circ E(x, y_2) \ldots \circ E(x, y_\ell)$$

     is an $O(\ell\varepsilon)$–PRG against $[W = 2^s, 10s + \ell s, \{0,1\}]$ branching programs.
   - Conclude that any language solvable by a BPL machine using at most $\frac{\log^2 n}{\log \log n}$ random bits, already belongs to L.