Problem set 9 - Extractors

out: 23/12/14
due: 5/1/15

For a distribution D on $\{0,1\}^n$:

- The entropy function is: $H(D) = \sum_x D(x) \log \frac{1}{D(x)}$.
- The R'enyi entropy of D is $H_2(D) = \log(\frac{1}{CP(D)})$, where $CP(D)$ is the collision probability of D - the probability that two independent samples from D are equal.
- The min-entropy function is: $H_\infty(D) = \log(\frac{1}{\max_x D(x)}) = \min_x \log(\frac{1}{D(x)})$.

We say D is *flat* if it is uniform over its support.

1. (Measuring entropy)
   - Prove that $H_\infty(D) \leq H_2(D) \leq H(D) \leq \log(|Supp(D)|)$ with equality iff D is flat.
   - Prove that $H_\infty(D) \geq \frac{H_2(D)}{2}$. On the other hand find an example where $H_\infty(D) \ll H(D)$.
   - It is a fact that $H(X,Y) \leq H(X) + H(Y)$. Find an example where $H_\infty(X,Y) > H_\infty(X) + H_\infty(Y)$.
2. (Flat sets vs. min-entropy)
   - Prove that if $H_\infty(D) = k$ then D is a convex combination of *flat* distributions each having k entropy.
   - Prove that $E : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^m$ is a (K,ε) extractor, iff E is an extractor for all distributions with min-entropy $\log(K)$.
3. (Non-explicit construction) Let $N \geq K(N)$, $M = M(N) > 0$ and $\varepsilon = \varepsilon(N) > 0$ be arbitrary functions. Prove that there exists an infinite family $\{G_N : [N] \times [D] \to [M]\}$ that is a (K,ε) extractor with degree $D = O(\frac{1}{\varepsilon^2} \cdot \log(\frac{N}{K}) + \frac{M}{K})$. What is the entropy loss of this extractor?
4. (Extractors as randomized hash functions) Prove that for every $n \geq k$ and $\varepsilon > 0$ there exists an explicit family of strong (k,ε) extractors $E : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ with seed length $d = O(n + m + \log(\frac{1}{\varepsilon}))$ and entropy loss $2\log(\frac{1}{\varepsilon})$.

   Hint: Use Ex 5, Q3.
5. A family $H = \{h : [N] \to [M]\}$ is ε-almost 2UFOHF if for every $a, b \in [N]$: $\Pr_{h \in H}[h(a) = h(b)] \leq \frac{1+\varepsilon}{M}$.
   - Prove that if H is a 2UFOHF than it is 0-almost 2UFOHF.
   - Prove that if H is ε^2-almost 2UFOHF, then $E : [N] \times [H] \to [M]$ defined by $E(x,h) = h(x)$ is a strong (k,ε) extractor for a k that gives entropy loss $2\log(\frac{1}{\varepsilon}) + O(1)$.
6. (Expanders as extractors) Suppose G is an $[N, D, \lambda]$ graph ($0 \leq \lambda \leq 1$). Define $E : [N] \times [D] \to [N]$ by $E(x,i) = x[i]$. Let $\varepsilon > 0$. Prove that E is a (K,ε) extractor for $K = (\frac{\lambda}{\varepsilon})^2 N$.

   Hint: Use Ex 7,Q3.