Assignment 1
CS289: Pseudorandomness, Winter 2016
Due: February 10

Guidelines for submitting the solutions:

- It is strongly recommended to use LaTeX or other word processing software for submitting the homework. This is not mandatory but will be helpful both for you and for us. If submitting electronically, email the solutions to me before midnight the day they are due. You also **have to scan your document to a PDF** and cannot submit image files (they are very hard to read when you print them out).
- All problem numbers below refer to the text Pseudorandomness by Salil Vadhan.

1. Give an example of a random variable X over $\{0,1\}^n$ that is $(n-1)$-wise independent but not uniformly distributed. [5 points]

2. Call a subset $S \subseteq \{0,1\}^n$ k-shattering if for any subset $I \subseteq [n]$ with $|I| \leq k$, $\{x_I : x \in S\} = \{0,1\}^k$. That is, the projection of S onto any k coordinates has all elements of $\{0,1\}^k$. Show how to get an explicit k-shattering set with as good a size as you can using primitives discussed in class. [10 points]

3. Let $1 \leq k \leq n$ and $0 \leq \varepsilon \leq 1$. Give an efficient algorithm to generate a random variable X over $\{0,1\}^n$ that is k-wise ε-biased using only $O(\log k + \log\log n + \log(1/\varepsilon))$ random bits. Here, k-wise ε-biased means that for every $I \subseteq [n]$ with $|I| \leq k$, $|\mathsf{Pr}[\oplus_{i \in I} X_i = 0] - 1/2| \leq \varepsilon$. [15 points]
   (Hint: Try to combine a "linear" k-wise independent generator, i.e., $Y = yH$ for $y \in_u \{0,1\}^{n-D}$ and $H \in \{0,1\}^{n-D \times n}$ the parity-check matrix of a suitable code, with an ε-biased generator.)

4. Let X over $\{0,1\}^n$ be an ε-biased space and let $S = \mathit{Support}(X)$. A non-trivial lower bound is $|S| \geq \Omega(n/\varepsilon^2 \log(1/\varepsilon))$. In this exercise you will show a simpler lower bound:
   (a) Prove that $|S| \geq n$. (Hint: Work over $\mathbb{F}_2^n$). [10 points]
   (b) Show that $|S| \geq \max(n, (1/\varepsilon^2) - 1)$. [15 points]
   (Hint: Compute the second moment of a signed sum as we did in the lower bound proof for k-wise independent spaces in class.)

5. Let p be a prime. Call a random-variable X over $\mathbb{F}_p^n$ ε-biased if for any non-zero $a \in \mathbb{F}_p^n$ and $b \in \mathbb{F}_p$, $|\mathsf{Pr}[\langle a, X\rangle = b] - 1/p| \leq \varepsilon$. Extend the powering construction used in class to this setup. [15 points]