COS 522 Homework 3: Due Nov. 11 in class

Below, U_n denotes the uniform distribution on n-bit strings.

1. **k-wise independent sample space:**

   (a) Let $v_1, \ldots, v_n \in \{-1, 1\}^m$ be orthogonal vectors with an equal number of 1's and -1's. Let $x_1, \ldots, x_n$ be random variables generated in the following way: Choose $j \in [m]$ uniformly at random. Take x_i to be the jth coordinate of v_i. Show that $x_1, \ldots, x_n$ are pairwise independent.

   (b) Let $x_1, \ldots, x_n \in \{-1, 1\}$ be pairwise independent random variables with expectation 0. Let Ω be the sample space from which the x_i are chosen. Show that $|\Omega| \geq n$. *Hint:* Define $v_1, \ldots, v_n \in \{-1, 1\}^m$ similarly to the above, and show that they are linearly independent.

   (c) Let S be an arbitrary set, and $x_1, \ldots, x_n$ be random variables attaining values in S. We say that the $x_1, \ldots, x_n$ are *k-wise independent*, if for every subset $I = \{i_1, \ldots, i_k\} \subseteq [n]$, and every $t_1, \ldots, t_k \in S$, $Pr[\forall j = 1, \ldots, k \;\; x_{i_j} = t_j] = \prod_{j=1}^{k} Pr[x_{i_j} = t_j]$.
   Let F be a finite field of characteristic 2 and size n. Let $x_1, \ldots, x_n$ be random variables generated in the following way: Choose uniformly at random a polynomial $p(t)$ of degree k over F (how can this be done?). Define x_i to be the value of p on the i'th element of F.
   Show that $x_1, \ldots, x_n$ are k-wise independent. Note that $x_1, \ldots, x_n$ are in F. How can you generate k-wise independent *Boolean* variables?

2. Suppose $g : \{0, 1\}^n \to \{0, 1\}^{n+1}$ is any pseudorandom generator. Then use g to describe a pseudorandom generator that stretches n bits to n^k for any constant $k > 1$.

3. Prove Question 6 in Chapter 9.

4. Prove Lemma 17.9.

5. Suppose π is an arbitrary distribution over $\{0, 1\}^n$. For a nonempty subset $S \subseteq \{1, \ldots, n\}$ let $bias(\pi, S)$ be $|\Pr_\pi[x \in \mathrm{ODD}(S)] - \Pr_\pi[x \in \mathrm{EVEN}(S)]|$, where $\mathrm{ODD}(S)$ is the set of $x \in \{0, 1\}^n$ such that $\oplus_{i \in S} x_i = 1$ and $\mathrm{EVEN}(S)$ is the complement of $\mathrm{ODD}(S)$. The *max-bias* of π is the maximum of $\mathrm{bias}(\pi, S)$ among all subsets S.

   Show that $||\pi - U_n||$ is at most 2^{n-1} times the max-bias of π. (Hint: View a distribution as a vector in a 2^n-dimensional space. The inquality here concerns going from the standard basis in this space to another orthonormal basis another.)

   For extra credit, show the same is true with 2^{n-1} replaced by $2^{n/2-1}$.

6. Suppose somebody holds an unknown n-bit vector a. Whenever you present a random subset of indices $S \subseteq \{1, \ldots, n\}$, then with probability at least $1/2 + \epsilon$, she tells you the parity of the all the bits in a indexed by S. Describe a guessing strategy that allows you to guess a (an n bit string!) with probability at least $(\frac{\epsilon}{n})^c$ for some constant $c > 0$.