CMSC 858C, Spring 2017, University of Maryland, HW 3
Due as a PDF file by email to Khoa Trinh by 9AM on March 13th

Instructions. Please work on this with your group and submit a neatly typed (or handwritten) file to Khoa: one submission per group. Use of other resources including books and the Web is not allowed. In case you can make partial progress on a problem, please write your approach clearly instead of giving no answer.

1. Prove that the simple construction of n pairwise independent, unbiased random bits using just $1+\lceil \log_2 n \rceil$ random bits that we saw in class, actually yields 3-wise independence.

2. Adapt the median-finding algorithm we discussed in class so that it uses $1.5n + o(n)$ comparisons in expectation. As with all our problems, prove your claim.

3. Use the probabilistic method to show the following. For any two vectors of the same length, their *Hamming distance* is the number of coordinates in which they differ. Prove that for any constant $c_0 \in (0, 1/2)$, there exists a constant $c_1 > 0$ such that the following holds for all n large enough: there exists a set $S \subseteq \{0,1\}^n$ with $|S| \geq 2^{c_1 n}$ such that for any pair of distinct elements of S, their Hamming distance is at least $c_0 n$.

4. We are going to show that there exists n_0 large enough such that for all $n \geq n_0$, there exist n-vertex graphs with minimum degree δ, and with *no* dominating set D [1] of size $\ell = \lceil (1-\epsilon) \cdot (n/\delta) \cdot \ln(\delta) \rceil$. For the rest of this problem, "$o(1)$" will refer to some function of n that goes to zero as n increases – *different invocations of this notation may mean different such functions.*

To do this, take a random graph G from the random model $G(n,p)$; your task is to take $p = p(n)$ appropriately, and not vanishing too fast as a function of n, so that: (i) via a 4th-moment calculation and a union bound, you can show that the minimum degree is at least $(1-o(1))np$ with probability at least $1-o(1)$; and (ii) via a union bound, you can show that the probability that there exists a subset of the vertices of size ℓ that is dominating, is $o(1)$.

(a) Prove (i) and (ii), and convince yourself that these two suffice to show what we wanted to. (The bound $1-x \geq e^{-x-2x^2}$ for $0 \leq x \leq 1/2$, will be helpful.)

(b) At how fast a rate can you let $p(n) \to 0$?

5. Recall that repetitions are allowed in a multiset. Let $\bigoplus$ denote the usual XOR function: i.e., for any multiset $\{b_i : i \in B\}$ of bits, then $\bigoplus_{i \in B} b_i$ equals 1 if $\{b_i : i \in B\}$ has an odd number of bits that are 1, and equals 0 otherwise.

Suppose an integer n and some $\epsilon \in [0, 1/2]$ are given. Prove that there exists a multiset S of n-bit strings with the following two properties: (i) S has cardinality at most $O(n/\epsilon^2)$; (ii) Suppose a vector $X = (X_1, X_2, \ldots, X_n)$ is sampled uniformly at random from S. (Recall that S is a multiset. So, if a string s occurs k times in S, then $\Pr[X = s] = k/|S|$.) Then, for all nonempty $A \subseteq \{1, 2, \ldots, n\}$,

$$1/2 - \epsilon \leq \Pr\left[\left(\bigoplus_{i \in A} X_i\right) = 1\right] \leq 1/2 + \epsilon.$$

(**Hint:** Use the probabilistic method. Use care with the quantification in the question.)

[1] D is a dominating set iff every vertex not in D has at least one neighbor in D.