

1. Alice and Bob together agreed on a uniformly random n -bit string $x = x_1x_2 \dots x_n$. Unfortunately, Eve was able to pick $n/2$ bit locations $i_1, \dots, i_{n/2}$ and subsequently learn the value of $x_{i_1} \dots x_{i_{n/2}}$ (so $i_1, \dots, i_{n/2}$ do not depend on x). Alice and Bob do not know which bits Eve has learned. Moreover, Eve can hear any further conversations between Alice and Bob. Give a randomized protocol for Alice and Bob to agree on an $m = \Omega(n)$ bit string y , such that Eve has negligible information about y . In particular, for any set $S \subseteq \{0, 1\}^m$, $|S| = 2^{m-1}$, the probability that Eve can guess whether $y \in S$ is at most $1/2 + \epsilon$. (This probability is over the randomized choices in the randomized protocol, as well as the randomness in the choice of x .) How small can you make ϵ ?
2. (20 points) The goal of this problem is to construct K -expanding graphs: graphs where any two disjoint sets of K vertices share an edge. Assume $K \leq N/2$, where N is the number of vertices.
 - (a) (4 points) Show that the average degree of a K -expanding graph is at least $N/(2K)$.
 - (b) (6 points) Suppose that G is a D -regular graph whose transition matrix has optimal second largest eigenvalue in absolute value, $\lambda = \Theta(1/\sqrt{D})$. Show that the natural approach to show G is K -expanding requires $D = \Omega((N/K)^2)$.
 - (c) (10 points) Use a good disperser or extractor graph to construct a K -expanding graph with near-optimal average degree $N^{1+o(1)}/K$. If it's easier, you may construct a bipartite graph, each side of the bipartition having N vertices, such that any two sets of size K on opposite sides share an edge. (In fact, such a bipartite graph easily gives a K -expanding graph.) You may assume the disperser or extractor graph is bi-regular. Extra credit: remove this bi-regular assumption.
3. Vadhan, Problem 5.6.