Homework 3

1. Let $\mathcal{R}_{n,k}$ be the set of all $k \times n$ matrices over $\mathbb{F}_q$, where $k = (1 - h(p) - \varepsilon)n$. We had seen in lecture that the linear code corresponding to a uniformly randomly chosen $G \in \mathcal{R}_{n,k}$ is a $[n, k, d = pn]_q$ code with $1 - \exp(-\Omega(n))$ probability. Note that we need $k \cdot n \cdot \log q = (1 - h(p) - \varepsilon)n^2 \log q$ bits of randomness to sample G. Our aim is to reduce the randomness required.

   A Toeplitz matrix $M \in \mathbb{F}_q^{k' \times n'}$ has the following property: The entry $M_{i,j} = M_{i-1,j-1}$, for all $i \in \{2, \ldots, k'\}$ and $j \in \{2, \ldots, n'\}$. That is, the matrix M is completely defined by its first column and first row. So, the total number of Toeplitz matrices of dimension $k' \times n'$ over $\mathbb{F}_q$ is $q^{n'+k'-1}$.

   (a) (20 points) Let $\mathcal{T}_{k \times n}$ be all Toeplitz matrices of dimension $k \times n$ over $\mathbb{F}_q$. Note that, sampling a random matrix from the set $\mathcal{T}_{k \times n}$ takes only $(n + k - 1) \log q = (2 - h(p) - \varepsilon)n \log q$ bits.

   Prove that the linear code corresponding to a randomly chosen $G \in \mathcal{T}_{k \times n}$ is an $[n, k, d = pn]$ code with $1 - \exp(-\Omega(n))$ probability.

   [Hint: A possible approach will be to consider the random generator matrix $G \in \mathcal{T}_{k \times n}$ and consider a linear combination of its rows. Show that this random variable is uniform.]

   (b) (20 points) Let $\mathcal{S}_{k \times (n-k)}$ be all matrices of the form $[I_{k \times k} | P_{k \times (n-k)}]$, where $P_{k \times (n-k)}$ is a Toeplitx matrix of dimension $k \times (n - k)$ over $\mathbb{F}_q$. Note that, sampling a random matrix from the set $\mathcal{S}_{k \times n}$ takes only $(n - 1) \log q$ bits.

   Prove that the linear code corresponding to a randomly chosen $G \in \mathcal{S}_{k \times n}$ is an $[n, k, d = pn]$ code with $1 - \exp(-\Omega(n))$ probability.

   [Hint: A possible approach will be to consider the corresponding parity check matrix $H = \left[-P^{\mathsf{T}}_{k \times (n-k)} | I_{(n-k) \times (n-k)} \right]$ and show that with high probability the sum of any $< d$ columns in H is not 0.]