TUTORIAL XI

1 Homework 4

1. Let $A_q(n, d)$ be the largest k such that a code over alphabet $\{1, \dots, q\}$ of block length n, dimension k and minimum distance d exists (recall that this corresponds to the notation $(n, k, d)_q$). Determine $A_2(3, d)$ for all integers $d \geq 1$.

2. Suppose C is a $(n, k, d)_2$-code with d odd. Construct using C a code C' that is a $(n+1, k, d+1)_2$-code.

3. By constructing the columns of a parity check matrix in a greedy fashion, show that there exists a binary linear code $[n, k, d]_2$ provided that

$$2^{n-k} > 1 + \binom{n-1}{1} + \cdots + \binom{n-1}{d-2} . \tag{1}$$

   This is a small improvement compared to the general Gilbert-Varshamov bound. In particular, it is tight for the $[7, 4, 3]_2$ Hamming code.

4. The Hadamard code has a nice property that it can be locally decoded. Let $C_{Had,r} : \{0, 1\}^r \to \{0, 1\}^{2^r}$ be the encoding function of the Hadamard code. Suppose you are interested only in the i-th bit x_i of the message $x \in \{0, 1\}^r$. The challenge is that you only have access to $y \in \{0, 1\}^{2^r}$ such that $\Delta(C_{Had,r}(x), y) \leq \frac{2^r}{10}$ and you would like to look only at a few bits of y. Show that by querying only 2 well-chosen positions (the choice will involve some randomization) of y, you can determine x_i correctly with probability $4/5$ (the probability here is over the choice of the queries, in particular x, y and i are fixed).

   Hint: You might want to query y at the position labelled by $u \in \{0, 1\}^r$ at random and the position $u + e_i$ where $e_i \in \{0, 1\}^r$ is the binary representation of i.

2 Parity check matrix

Let C be a $[n, k, d]_q$-linear code and $G \in \mathbb{F}_q^{k \times n}$ be a generator matrix. That is, $C = \{xG, x \in \mathbb{F}_q^k\}$. We call a parity check matrix of the code C a matrix $H \in \mathbb{F}_q^{(n-k) \times n}$ such that for all $c \in \mathbb{F}_q^n$ we have $cH^T = 0$ if and only if $c \in C$. The objective of this exercise is to show how to construct a parity check matrix from a generator matrix.

1. Show that H is a parity check matrix if and only if $GH^T = 0$ and rank$(H) = n - k$.

2. Show that, from G we can construct a generator matrix G' of the form $G' = [I_k|P]$ for some $P \in \mathbb{F}_q^{k \times (n-k)}$. (If n is not optimal, we may have to permute the coefficients of the vectors).

3. Construct a parity check matrix from G'.

4. Construct a parity check matrix of the code given by the generator matrix $G = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}$ in $\mathbb{F}_2$.

3 Singleton Bound

For every $(n, k, d)_q$-code, show that $k \leq n - d + 1$.

4 Weights of Codewords

Let C be an $[n, k, d]$-linear code over $\mathbb{F}_q$. Prove the following.

1. For $q = 2$, either all the codewords have even weight or exactly half have even weight and the rest have odd weight.
2. For any q, either all the codewords begin with 0 or exactly a fraction $1/q$ of the codewords begin with 0. In general, for a given position $1 \leq i \leq n$, either all codewords contain 0 at the i-th position or each $\alpha \in \mathbb{F}_q$ appears at the i-th position of exactly $1/q$ of the codewords in C.
3. The following inequality holds for the minimum distance d of C.

$$d \leq \frac{n(q-1)q^{k-1}}{q^k - 1}$$

5 Codes Achieving the Gilbert-Varshamov Bound

The purpose of this exercise is to use the probabilistic method to show that a random linear code lies on the Gilbert-Varshamov bound, with high probability.

1. Given a non-zero vector $\mathbf{m} \in \mathbb{F}_q^k$ and a uniformly random $k \times n$ matrix $\mathbf{G}$ over $\mathbb{F}_q$, show that the vector $\mathbf{mG}$ is uniformly distributed over $\mathbb{F}_q^n$.
2. Let $k = (1 - H_q(\delta) - \varepsilon)n$, with $\delta = d/n$. Show that there exists a $k \times n$ matrix $\mathbf{G}$ such that

$$\text{for every } \mathbf{m} \in \mathbb{F}_q^k \setminus \{\mathbf{0}\}, wt(\mathbf{mG}) \geq d$$

   where $wt(\mathbf{m})$ is the Hamming weight of the vector $\mathbf{m}$.
3. Show that $\mathbf{G}$ has full rank (i.e., it has dimension at least $k = (1 - H_q(\delta) - \varepsilon)n$)