1 Homework 6 (2016-2017)

1. Let $A_q(n, d)$ be the largest $k$ such that a code over alphabet $\{1, \ldots, q\}$ 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

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

2 Singleton Bound

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

3 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 $C$.

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

4 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 $m \in \mathbb{F}_q^k$ and a uniformly random $k \times n$ matrix $G$ over $\mathbb{F}_q$, show that the vector $mG$ 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 \( G \) such that

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

where \( \text{wt}(m) \) is the Hamming weight of the vector \( m \).

3. Show that \( G \) has full rank (i.e., it has dimension at least \( k = (1 - H_q(\delta) - \varepsilon)n \)).