Exercise Sheet 3

Exercise 3.1. Let $\mathcal{C}$ be a linear $[n, k > 1, d]$ code over $\mathbb{F}_q$ with a generator matrix of the form

$$G = \left(\begin{array}{cccc|cccc} 0 & 0 & \dots & 0 & 1 & 1 & \dots & 1 \\ \hline & & G_1 & & & & G_2 & \end{array} \right),$$

where the Hamming weight of the first row is d. Define $\mathcal{C}_1$ as the linear $[n_1 := n - d, k_1, d_1]$-code over $\mathbb{F}_q$ generated by G_1.

1. Show that G_1 has rank $k - 1$, and thus, $k_1 = k - 1$.
2. Let c_1 be a codeword of $\mathcal{C}_1$. Show that the number of words $c_2 \in \mathbb{F}_q^d$ such that $(c_1 \mid c_2) \in \mathcal{C}$ is exactly q, and that if c_1 is nonzero, there is such a choice for c_2 with Hamming weight at most $d - \lceil d/q \rceil$.
3. Show that $d_1 \geq \lceil d/q \rceil$.

Exercise 3.2. Denote by $N_q(k, d)$ the length of a shortest linear code of dimension k and distance d over $\mathbb{F}_q$.

1. Show that $N_q(k, d) \geq d + N_q(k - 1, \lceil d/q \rceil)$. (*Hint:* use the last exercise.)
2. Show that $N_q(k, d) \geq \sum_{i=0}^{k-1} \lceil d/q^i \rceil$. Derive the Singleton bound for linear codes using this result.
3. Show that the first-order Reed-Muller code over $\mathbb{F}_q$ achieves this bound. Recall that the first-order Reed-Muller code is defined as the linear $[q^m, m + 1]$-code over $\mathbb{F}_q$ with an $(m + 1) \times q^m$ generator matrix whose columns range over all the vectors in $\mathbb{F}_q^{m+1}$ with a first entry equaling 1.

Exercise 3.3. A *burst of length* ℓ is the event of having errors in a codeword such that the locations i and j of the first (leftmost) and last (rightmost) errors, respectively, satisfy $j - i = \ell - 1$. Let $\mathcal{C}$ be a linear $[n, k]$-code over $\mathbb{F}_q$ that is able to correct every burst of length t or less.

1. Show that in every nonzero codeword $c \in \mathcal{C}$, the locations i and j of the first and last nonzero entries in c must satisfy $j - i \geq 2t$.
2. Show that $n - k \geq 2t$.
3. (Sphere-packing:) Show that

$$q^{n-k} \geq 1 + n(q - 1) + (q - 1)^2 \sum_{i=0}^{t-2} (n - i - 1) q^i.$$

Exercise 3.4. An (n, M, d)-code of length n containing M codewords and minimum distance d is called an $(n, M, d; w)$ *constant-weight code* if each codeword has Hamming weight w. Let $\mathcal{C}$ be an $(n, M, d = 2t + 1; w = 2t + 1)$ constant-weight code over $\mathbb{F}_q$.

1. For every codeword $c \in \mathcal{C}$, how many words y of Hamming weight $t+1$ are there in $\mathbb{F}_q^n$ that are at Hamming distance t from c?

2. Show that

$$M \leq \frac{\binom{n}{t+1}(q-1)^{t+1}}{\binom{2t+1}{t}}.$$