Exercise Sheet 3

(Solutions)

Exercise 3.1.

1. If G_1 has rank below $k-1$, then it must be that for some nonzero $c_1 \in \mathbb{F}_q^{k-1}$, $c_1 G_1 = 0$. Now let $c := (0 \mid c_1)G$, which is nonzero (as G has rank k) and has all-zeros on its first $n-d$ coordinates. Suppose that one of the nonzero entries of c is $\alpha \in \mathbb{F}_q$, and observe that $(-\alpha \mid c_1)$ must have weight less than d. This contradicts the assumption that $\mathcal{C}$ has minimum distance d.

2. Let G_1' be the submatrix of G formed by removing its last d columns. This submatrix has rank equal to the rank of G_1, which is $k-1$. Thus the number of solutions for the linear equation $xG_1' = c_1$ is exactly q, and this is the number of the choices of c_2 that we are looking for.

   For the second part, let the unique nonzero choice of $x \in \mathbb{F}_q^{k-1}$ be such that $xG_1 = c_1$. If xG_2 has weight at most $d - \lceil d/q \rceil$ then we are done. Otherwise, the number of zeros in xG_2 is strictly less than $\lceil d/q \rceil$, and thus there is an $\alpha \mathbb{F}_q$ such that the number of α's in xG_2 is at least $\lceil d/q \rceil$ (as otherwise the length of xG_2 won't reach d). Then $(-\alpha \mid x)G$ must be the codeword of $\mathcal{C}$ with the desired properties.

3. Suppose for the sake of contradiction that there is a nonzero $x \in \mathbb{F}_q^{k-1}$ such that $c_1 := xG_1$ has weight less than $\lceil d/q \rceil$. Then use the result obtained in the previous part to complete c_1 to a codeword $(c_1 \mid c_2)$ of $\mathcal{C}$ such that c_2 has weight at most $d - \lceil d/q \rceil$. Thus the weight of $(c_1 \mid c_2)$ would be less than d, which is a contradiction.

Exercise 3.2.

1. Suppose that there is a code $\mathcal{C}$ of length smaller than $d + N_q(k-1, \lceil d/q \rceil)$. Then $\mathcal{C}$ has a generator matrix of the form given in the previous exercise, up to a permutation of the columns. By the last exercise, the matrix G_1 generates a code of dimension $k-1$, minumum distance at least $\lceil d/q \rceil$ but length less than $N_q(k-1, \lceil d/q \rceil)$, which is a contradiction.

2. The inequality is immediate from the previous part by induction on k. Observe that each term on the right hand side of this inequality is at least one, thus the right hand side is at least $d + (k-1) \cdot 1$, which implies the Singleton bound.

3. The minimum distance of the first-order Reed-Muller code is $q^{m-1}(q-1)$, as for every n-variate polynomial f of degree 1 and every $\alpha \in \mathbb{F}_q$, the number of solutions x for $f(x) = \alpha$ is q^{m-1} is q^{m-1}. Pluggin $d = q^m - q^{m-1}$ on the right hand side of the bound we get that

$$N_q(k, d) \geq \lceil q^m - q^{m-1} \rceil + \lceil q^{m-1} - q^{m-2} \rceil + \cdots + \lceil q^1 - q^0 \rceil + \lceil q^0 - q^{-1} \rceil = q^m.$$

   So the inequality is tight for the code because the length of the code is q^m.

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. Consider a codeword $c = (c_1, \ldots, c_n)$ that contradicts this assumption. Then $w = (c_1, \ldots, c_{i+t-1}, 0, 0, \ldots, 0)$ can be either the zero codeword with a burst of length t at left, or c with a burst of length t at right, and is thus not uniquely correctable, a contradiction.

2. The proof is similar to that of the Singleton bound. Since the number of codewords is $q^k > q^{k-1}$, there must be at least two codewords that agree on their first $k-1$ coordinates, and thus, there is a nonzero codeword that has all zeros on its first $k-1$ coordinates. Using the notation of the previous part we will have $j - i < n - k + 1$. Thus, $2t \leq n - k$ by the previous part.

3. The proof is similar to the classical sphere-packing bound except that the shape of the "balls" are now different. For the sphere-packing bound we had to count the number of points that are at distance t from a given point, or the "volume" of the Hamming ball of radius t around each codeword. Here instead we only need to count the number of points within such a ball that are different from the word at the center (denoted by w) by a burst of size at most t. Denote this quantity by V. We have to distinguish the following cases and add up the numbers:

   - The word w at the center,
   - Words that are different from w in only one position. The number of such words is $n(q-1)$,
   - Words that are different from w by a burst of size i, $2 \leq i \leq t$. The number of such words is $(n - i + 1)(q-1)^2 q^{i-2}$.

   Altogether, we will have

$$V = 1 + n(q-1) + (q-1)^2 \sum_{i=0}^{t-2} (n - i - 1) q^i,$$

   and similar to the sphere-packing bound, the "spheres" must be disjoint so that $q^k \leq q^n / V$. The bound follows.

Exercise 3.4.

1. $\binom{2t+1}{t}$.

2. For every $c \in \mathcal{C}$, denote by Y_c the set

$$Y_c := \{y \in \mathbb{F}_q^n \colon \mathrm{wgt}(y) = t + 1, \mathrm{dist}(y, c) = t\}.$$

   Note that for each $c \neq c' \in \mathcal{C}$, we must have $Y_c \cap Y_{c'} = \emptyset$ as otherwise c and c' might be confused. Thus the number of $y \in \mathbb{F}_q^n$ of weight $t+1$ that are at distance t from some codeword of $\mathcal{C}$ is exactly $M\binom{2t+1}{t}$, where $M := |\mathcal{C}|$. But on the other hand the number of such words cannot exceed $\binom{n}{t+1}(q-1)^{t+1}$, and the bound follows.