Solutions 3

Exercise 3.1.

1. We can take

$$G_6 = [\mathrm{I}_3|A] = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & \omega & \omega^2 \\ 0 & 0 & 1 & 1 & \omega^2 & \omega \end{pmatrix}.$$

   Note that A is a Vandermonde matrix. The length of $\mathcal{G}_6$ is 6 and dimension 3. The minimal length is at most 4, as shows the generator matrix. Let $y = xG = (x, b)$ be a codeword with $x, b \in \mathbb{F}_4^3$. If wgt$(x) = 1$, y has weight 4 ; if wgt$(x) = 2$, then wgt$(b) \geq 2$ as A has no singular 2×2 submatrix ; if wgt$x = 3$, $b = 0$ would mean $x = 0$ as A is invertible. So there is no codeword of weight ≤ 3 and the minimum distance is 4. We notice that this code is MDS.

2. For any two distinct rows $x, y$of G_6, we have $x \cdot y = 0 + 0 + 0 + 1 + \omega + \omega^2 = 0 \mod 2$ and $x \cdot x = 1 + 0 + 0 + 1 + \omega^3 + \omega^3 = 0 \mod 2$. So $\mathcal{G}_6$ is Hermitian self-dual.

3. Let $\mathcal{C}$ be such a code and C a generator matrix. Up to permutation, we assume that the 3 first columns are independent. Up to a change of basis, we may assume that $C = [\mathrm{I}_3|B]$. Up to multiplication of the 3 last columns by a scalar, we assume that the first row of B is $(1, 1, 1)$. Now we have

$$C = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & a & b & c \\ 0 & 0 & 1 & d & e & f \end{pmatrix}$$

   None of the letters $a, b \ldots f$ can be zero since the code has minimum weight 4. Suppose that λ is used twice among a, b, c, then $\lambda C_1 + C_2$ is a code word of weight ≤ 3 which is not possible (where C_i is the ith row of C). So $\{a, b, c\} = \{d, e, f\} = \{1, \omega, \omega^2\}$. Now again, if more than two of the following occurs $a = d$, $b = e$ or $c = f$, then, by taking $C_2 + C_3$ we have a codeword of weight 3. On the other hand, if not one of these happens, def is a permutation of abc and $C_2 + \omega C_3$ or $C_2 + \omega^2 C_3$ would have weight 3. So, up to equivalence

$$C = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & a & b & c \\ 0 & 0 & 1 & a & c & b \end{pmatrix}$$

   with a, b, c distinct. If a is not 1, one can divide rows 2 and 3 by a and multiply columns 2 and 3 by a. So $a = 1$. Up to permutation, we can choose $b = \omega$ and $c = \omega^2$, and we are luckily back to G_6.

Exercise 3.2.

1. It's enough to prove that $4|$wgt(x) and $4|$wgt(y) implies that $4|$wgt$(x+y)$. But wgt$(x + y) = \langle x + y, x + y \rangle = \langle x, x \rangle + \langle y, y \rangle + 2\langle x, y \rangle =$ wgt$(x) +$ wgt$(y) + 2\langle x, y \rangle$. As $\mathcal{C}$ is self dual, $\langle x, y \rangle \equiv 0 \mod 2$ so finally $4|$wgt$(x + y)$.

2. On the other hand,take x and y two codewords, then $\langle x, y\rangle = \frac{1}{2}\left(\langle x+y, x+y\rangle - \langle x, x\rangle + \langle y, y\rangle\right) \equiv 0 \mod 2$.

Exercise 3.3.

1. Let $(v_i)_i$ denote the row vectors of G_{24}. We check that v_1 and v_2 have even weight, $v_2 \cdot v_i = 0$. By permutation, this is enough to make sure that $v_i \cdot v_j = 0$ for any i, j. So $\mathcal{G}_{24}$ is self-dual.

2. Remember from the first exercise sheet that for systematic codes $[-A, \mathrm{I}]$ is a check matrix, but as the code is self-dual, it is also a generator matrix. Since characteristic is 2, $[A, \mathrm{I}]$ is indeed a generator matrix. If $(a, b) \in \mathcal{G}_{24}$, $(a, b) = b[A, \mathrm{I}]$, but $b[\mathrm{I}|A]$ is also a code word that is $(b, a) \in \mathcal{G}_{24}$. From previous exercise, the minimal weight of the codewords is 4 or 8. If there is a word (a, b) of weigth 4, we can assume that wgt$a \leq$ wgt$b$. The case wgt$a = 0$ or 1 are excluded by looking at A. Now if wgt$a =$ wgt$b = 2$, the codeword is the sum of two rows of G_{24} which never have weight 4. So the minimal distance is 8.

3. One can puncture the code $\mathcal{G}_{24}$ to obtain $[23, 12, 7]_2$-code.

Exercise 3.4.

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 3.5.

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 3.6. 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.