Solutions 2

Exercise 2.1. Let $\mathcal{C}$ be the linear code generated by c. We are looking for the number of weight w words in $\mathcal{C}^\perp$, which is the coefficient of $x^w y^{n-w}$ in the weight enumerator of $\mathcal{C}^\perp$. The weight enumerator of $\mathcal{C}$ can be written as

$$W(x,y) = y^n + x^d y^{n-d},$$

and by MacWilliams identities, the weight enumerator of $\mathcal{C}^\perp$ is given by

$$W'(x,y) = \frac{1}{|\mathcal{C}|} W(y-x, y+x) = \frac{1}{2}((y+x)^n + (y-x)^d (y+x)^{n-d}).$$

The quantity we are looking for is the coefficient of $x^w y^{n-w}$ in the expansion of $\frac{1}{2}((1+x)^n + (1-x)^d(1+x)^{n-d})$, which is

$$\frac{1}{2}\left(\binom{n}{w} + \sum_{i=0}^{\min\{d,w\}} (-1)^i \binom{d}{i}\binom{n-d}{w-i}\right).$$

Exercise 2.2.

1. **Puncturing.** Note that C^i is the image of the projection

$$\begin{aligned} \pi : C &\rightarrow \mathbb{F}_q^{n-1} \\ x = (x_1, \dots, x_n) &\mapsto (x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \end{aligned}$$

   and is thus a subspace of $\mathbb{F}_q^{n-1}$. C^i is a linear code with the following parameters:

   - The length of C^i is $n-1$.
   - The dimension of C^i remains k, unless the original code C contains the codeword $e_i = (0 \cdots 10 \cdots 0)$ which has a 1 only at coordinate i.
   - If there is a codeword of C of weight d with a 1 at position i, the minimum distance of C^i is $d-1$. Otherwise, the minimum distance of C^i is d.

2. **Shortening.** Similarly to above, we see that C_i is the image of the projection of the subspace C' on $\mathbb{F}_q^{n-1}$ and is thus a subspace of $\mathbb{F}_q^{n-1}$. Its parameters are as follows:

   - The length of C_i is $n-1$.
   - If all codewords of C have a 0 at position i, the dimension of C^i (and of C') is k. Otherwise, the dimension is $k-1$.
   - Since C' is a subcode of C, its minimum distance is at least d. All codewords of C' have a zero at position i, so that the minimum distance of C_i is at least d.

3. On one hand, if a length-$(n-1)$ vector $(y_1 \cdots y_{i-1} y_{i+1} \cdots y_n)$ belongs to $(C^i)^\perp$, then by definition, for each $x = (x_1 \cdots x_{i-1} x_{i+1} \cdots x_n)$ in C^i, we have $\sum_{j \neq i} x_j y_j = 0$, which implies that the length-n vector $(y_1 \cdots y_{i-1} 0 y_{i+1} \cdots y_n)$ belongs to $C^\perp$, so that

$$(y_1 \cdots y_{i-1} y_{i+1} \cdots y_n) \in (C^\perp)_i.$$

On the other hand, if $(y_1 \cdots y_{i-1} y_{i+1} \cdots y_n) \in (C^\perp)_i$, then $(y_1 \cdots y_{i-1} y_{i+1} \cdots y_n)$ is the punctured version of a vector $(y_1 \cdots y_{i-1} 0 y_{i+1} \cdots y_n)$ in $C^\perp$, that is, a vector $(y_1 \cdots y_n)$ which satisfies $\sum x_j y_j = 0$ and $y_i = 0$. This implies that $\sum_{j \neq i} x_j y_j = 0$, i.e., that

$$(y_1 \cdots y_{i-1} y_{i+1} \cdots y_n) \in (C^i)^\perp.$$

Exercise 2.3.

1. Let $\mathcal{H}$ be the $[7,4,3]_2$-Hamming code and $\mathcal{H}'$ be the extended Hamming code. Clearly, $\mathcal{H}'$ has length 8. Further, it is easy to check that $\mathcal{H}'$ is a subspace of $\mathbb{F}_2^8$ and that it is isomorphic to $\mathcal{H}$. Thus the dimension of $\mathcal{H}'$ is 4. To see that the minimum distance of $\mathcal{H}'$ is 4, first note that the minimum distance of $\mathcal{H}'$ cannot be less than that of $\mathcal{H}$. Now there exists a codeword x of $\mathcal{H}$ of weight 3. Since the weight of x is odd, x has parity 1, so that the codeword $(x, \sum x_i)$ of $\mathcal{H}'$ is of weight 4. Moreover, if there was a codeword $(x, \sum x_i)$ of $\mathcal{H}'$ of weight 3, its 8th entry must be a 1 (otherwise by the argument above the weight of $(x, \sum x_i)$ would be 4) so that the corresponding $\mathcal{H}$-codeword x is of weight 2; but this is impossible.

   In general, adding a parity check to a code with check matrix H results in a code with check matrix

$$\begin{pmatrix} & & & 0 \\ & H & & \vdots \\ & & & 0 \\ 1 & 1 & \cdots & 1 \end{pmatrix}$$

   A check matrix for $\mathcal{H}'$ is thus

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

   We can also replace the last check by a linear combination of all checks, thus getting a check matrix

$$H' := \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

   This check matrix contains the identity matrix of dimension 4 as a submatrix (we say that H' is in "systematic form"). It is now easy to get a generator matrix for $\mathcal{H}'$ using the technique of Exercise 1 of Exercise Sheet 2. Thus a generator matrix for $\mathcal{H}'$ would be

$$G' := \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

2. It is easy to verify (by Gaussian elimination) that G' can be transformed into H' using elementary row operations. Thus the extended Hamming code is self-dual.

Exercise 2.4. Consider an $[n = 2^r - 1, k = 2^r - r - 1, 3]_2$-Hamming code. Since it has minimum distance 3, the spheres of radius 1 centered around the codewords are disjoint. Each sphere of radius 1 contains $n + 1 = 2^r$ vectors of $\mathbb{F}_2^n$. There are $2^k = 2^{2^r - r - 1}$ such spheres, so that the spheres cover $2^r 2^{2^r - r - 1} = 2^{2^r - 1} = 2^n$ vectors. The spheres of radius 1 centered around the codewords thus cover the whole space $\mathbb{F}_2^n$.

Exercise 2.5. Given integers $N \leq n$, $K \geq k$, and $D \geq d$, we show that if there exists a $[N, K, D]_q$-code, then we can construct a $[n, k, d]_q$-code. Appending $n - N$ 0s to the end of every codeword gives us an $[n, K, D]_q$-code. We can form a new code of any desired dimension less than or equal to K by taking a subcode. In particular, we can take a subcode of dimension k. This is an $[n, k, D']_q$-code with $D' \geq D \geq d$. As long as the distance of the code is strictly greater than d, we do the following: pick a coordinate i where a minimum-weight codeword has a 1 and set the ith coordinate of every codeword to 0. This reduces the minimum distance by 1. To see that this operation does not affect the dimension, note that the only way to reduce the dimension with this operation is if there existed a codeword whose only nonzero entry is at position i. But this is impossible since our code has distance strictly greater than d (hence strictly greater than 1).

Exercise 2.6. For the "if" part, suppose that there is a $(n+1, k, d+1)_2$-code. Take a codeword x of weight $d + 1$ with a one at some position, say the i-th. Then remove the ith coordinate from all the codewords, to obtain a new code of length n, which obviously has distance at least d. Indeed the distance of the new code is exactly d as x correponds to a codeword in the new code of weight exactly d.

For the "only if" part, let $\mathcal{C}$ be a (n, k, d)-code. Extend the code by adding one coordinate, where each codeword $(x_1, \dots, x_n) \in \mathbb{F}_2^n$ is replaced by $(x_1, \dots, x_n, x_1 + \cdots + x_n) \in \mathbb{F}_2^{n+1}$. The new code has the same number of codewords, and its distance is either d or $d + 1$. Take a codewords x in the original code whose Hamming weight is d. As d is odd, the extension of x has a one in the last position ; thus, the minimum distance of the extended code is indeed $d + 1$.

Exercise 2.7. By the previous exercise, there is a one-to-one correspondence between $(n, k, 2)_2$ codes and $(n - 1, k, 1)_2$ codes. Thus, $A_2(n, 2) = A_2(n - 1, 1)$, where the latter quantity is obviously $n - 1$.

Exercise 2.8.

1. Let $G \in \mathbb{F}_2^{k \times n}$ be a generator matrix for $\mathcal{C}$. For $J \subseteq [n]$, denote by G_J the submatrix of G obtained by removing the columns picked by J. Similarly, for a vector $x \in \mathbb{F}_2^n$, denote

by x_J the vector obtained from x by removing the coordinates chosen by J.

Suppose that for every $J \subseteq [n]$ of size i, G_J has rank k. Then the minimum distance of $\mathcal{C}$ has to be at least $i+1$. Suppose not, and take $x \in \mathbb{F}_2^k$ such that $x \neq 0$ and xG has weight at most i. Let J of size i contain the support (the set of nonzero coordinate positions) of xG. Then $xG_J = (xG)_J = 0$, which contradicts the assumption that G_J has maximal rank k.

Moreover, suppose that the minimum distance of $\mathcal{C}$ is d. Take some nonzero codeword xG of Hamming weight d and let $J \subseteq [n]$ be its support. Then G_J has a nontrivial left kernel, as $xG_J = 0$; thus, G_J must have rank less than k.

We conclude that the minimum distance of $\mathcal{C}$ s exaclty the largest integer d such that every $k \times (n-d+1)$ submatrix of its generator matrix has rank k.

2. By the previous part, every $k \times k$ submatrix of any generator matrix of an MDS code must have full rank, and conversely, if every $k \times k$ submatrix of a generator matrix of a code has full rank, then the code is MDS.

   Moreover, as the minimum distance of an $[n,k]$ MDS code is $n-k+1$, every $(n-k) \times (n-k)$ submatrix of a parity check matrix of such a code must have full rank (as otherwise a nontrivial linear dependence on some $n-k$ columns of the code and thus a codeword of weight at most $n-k$ must exist, contradicting the MDS assumption) and vice versa. The claim follows by noting the fact that any generator matrix of the code is a parity check matrix for the dual.

Exercise 2.9. Since the code $\mathcal{C}$ is perfect, the balls around codewords of radius t form a tiling of the space $\mathbb{F}_q^n$. So any word $x \in \mathbb{F}_q^n$ of weight $t+1$ must lie in such a ball, which must be centered in a codeword of weight between 1 and $2t+1$. Now since 0 in a codeword, there cannot be another codeword of weight less than $2t+1$. So any word $x \in \mathbb{F}_q^n$ of weight $t+1$ is contained in the ball around a codeword of weight $2t+1$.

Given a codeword c of weight $2t+1$, a word x of weight $k+1$ can be at distance $\leq t$ only if x is obtained from c by changing non-zero symbols to a zero. Thus there are $\binom{2t+1}{t}$ such words. On the other hand, there are $\binom{n}{t+1}(q-1)^{t+1}$ words of weight $t+1$. So we have indeed

$$W_{2t+1} = \frac{\binom{n}{t+1} \cdot (q-1)^{t+1}}{\binom{2t+1}{t}}.$$

Exercise 2.10. Every coin can be in three states : of the right weight, too heavy or too light. The balance also gives us three informations : balanced, moving to the right or moving to the left. So it seems natural to work in the finite field $\mathbb{F}_3 = \{0, +1, -1\}$. If $x_i = 0$ when the i-th coin has the right weight, $+1$ if it is too heavy and -1 when too light, a weighting with less than one counterfeited coin amounts to check an equation like

$$s = x_{i_1} + x_{i_2} + \cdots + x_{i_k} - x_{j_1} - x_{j_2} + \cdots - x_{j_k} \equiv 0 \mod 3$$

To sum up, we are looking for a code that can correct one error (because only one x_i can be non zero) given by three check equations over $\mathbb{F}_3$ where each equation has as many +1 as -1 coefficients.

Codes that can correct one error have minimum distance three. They are the Hamming codes. The columns of the check matrix of a Hamming code are a representatives of vectors that direct all the lines of $(F_3)^r$. Since we have 3 weightings, we take $r = 3$. This gives for example

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & 0 & 1 & -1 & 0 & 1 & -1 & 0 & 1 & -1 & 0 & 1 & -1 \end{pmatrix}$$

where we wrote the columns systematically.

We have one column in excess so we remove the last one. The we try satisfy the constrains on the number of ocurences of 1 and -1 by multiplying some columns by -1. We do that on column 9,10,11, 12, and 3,4 to end up with

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 0 & 1 & -1 & -1 & 0 & 0 & 0 & -1 & 1 & -1 & 1 & 1 \\ 1 & 0 & -1 & 1 & 0 & 1 & -1 & 0 & -1 & 1 & 0 & -1 \end{pmatrix}$$