Solutions 3

Exercise 3.1. Let $\mathcal{C}$ be the linear code generated by x. 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 3.2.

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

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

   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 3.3.

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 3.4. 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 3.5. 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).