Exercise Sheet 2

(Solutions)

Exercise 2.1. 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, weight enumerator of $\mathcal{C}^\perp$ is given by

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

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

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

Exercise 2.2. For the "if" part, suppose that there is a $(n+1, k, d+1)_2$-code. Take two codewords x, y of distance $d+1$ that differ at some ith position. 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 and y correpond to a pair of codewords in the new code that differ at exactly d positions.

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

Exercise 2.3. 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 2^{n-1}.

Exercise 2.4. The extended Hamming code has minimum distance 4 by the argument given in the solution of Exercise 2 (the "only if" part). A parity check matrix for this code is

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

which, in "systematic form" is

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

Thus a generator matrix for the extended Hamming code would be

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

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 2.5.

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.