Exercise Sheet 1

(Solutions)

Exercise 1.1. Observe that the Hamming distance of two vectors is the minimum number of bit flips required to transform one into the other. Using this, the first three conditions are trivial to verify, and the triangle inequality follows by noting that if x can be transformed into y using d_1 flips and y to z using d_2 flips, then z is no more than $d_1 + d_2$ flips aways from x.

Exercise 1.2.

1. Suppose that $x = (x_1, \ldots, x_{10})$ is a codeword and an error occurs at position i. Denote the new word by $x' = (x'_1, \ldots, x'_{10})$, which is identical to x except that at position i it contains x'_i, for some $x'_i \neq x_i \mod 11$. Then we need to show that x' is not a codeword. Indeed,
$$\sum_{i=1}^{10} ix'_i = \sum_{i=1}^{10} ix_i + i(x'_i - x_i) \neq 0 \mod 11.$$
2. Suppose that the codeword is transposed at positions i and $i+1$, and again denote the corrupted word by x'. Then
$$\sum_{i=1}^{10} ix'_i = \sum_{i=1}^{10} ix_i - ix_i - (i+1)x_{i+1} + (i+1)x_i + ix_{i+1} = x_i - x_{i+1} \mod 11,$$
which is zero iff $x_i = x_{i+1}$, in which case no error has occurred.
3. The distance is at least two by the fact that the code can detect a single error. Moreover, notice that the all-zero vector and $(1,0,0,0,0,0,0,0,0,0,1)$ are codewords. Thus the minimum distance is exactly two.
4. The code could still detect a single error by the same argument as before, but obviously not any transpositions because the new rule is symmetric with respect to all coordinate positions.

Exercise 1.3. Let the code be of length n and dimension k, and denote by C_o and C_e the set of codewords of odd and even lengths, respectively. If $C_o = \emptyset$, we are done. Otherwise, take any $x \in \mathcal{C}_o$. By linearity of the code, for each $y \in C_e$, $x + y$ is a codeword. Moreover, $x + y \in C_o$ as the bitwise XOR of an odd-weight and and even-weight vecotr has an odd weight. Therefore,
$$\{x + y \colon y \in C_e\} \subseteq C_o$$
and thus
$$|C_e| = |\{x + y \colon y \in C_e\}| \leq |C_o|.$$
Similarly we can show that $|C_o| \leq |C_e|$ and the claim follows.

Exercise 1.4. Let $G := (I_k | G_1)$ be a generator matrix of a linear k-dimensional code of length n over $\mathbb{F}_q$. Thus $(x, y) \in \mathbb{F}_q^k \times \mathbb{F}_q^{n-k}$ is a codeword iff $y = xG_1$, or in other words, $y^\top - G_1^\top x = 0$. Thus, $H := (G_1^\top | I_{n-k})$ is a parity check matrix for the code.

Exercise 1.5. No. A counterexample over $\mathbb{F}_2$ would be given by

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

It immediately follows by the previous exercise that H is a parity check matrix for the code generated by G. This is an example of a *self-dual* code, a code which coincides with its dual.

Exercise 1.6. Let G be a fixed generator matrix for C. Then a $k \times n$ matrix G' is a generator matrix for C iff $G' = AG$, for a $k \times k$ invertible matrix A. Thus the number of generator matrices of the code is the number of full-rank $k \times k$ matrices over $\mathbb{F}_2$. To count this number, construct A as follows: The first row can be picked as any nonzero vector, the second row can now be taken as any vector which is not in the 1-dimensional subspace generated by the first row (whose size is 2), and so on. Thus the number of choices for the ith row would be $2^k - 2^{i-1}$, which implies that the total number of full-rank $k \times k$ matrices over $\mathbb{F}_2$ is

$$\prod_{i=1}^{k}(2^k - 2^{i-1}) = 2^{\binom{k}{2}} \prod_{i=1}^{k}(2^i - 1).$$