Solutions 1

Exercise 1.1. 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 1.2. 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.

Another counterexample over $\mathbb{F}_2$ is the following: let

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

The code is thus the repetition code of length 4. A possible check matrix for it is

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

(This is the generator matrix of the dual code, the parity code). It is easy to check that the corresponding matrix

$$\begin{pmatrix} G \\ H \end{pmatrix}$$

is not invertible, as its rows are not linearly independent.

Exercise 1.3. C is a k-dimensional subspace of $\mathbb{F}_2^n$. Choosing a generator matrix G for C amounts to choosing a basis of the subspace. Let us construct such a basis, picking the vectors one by one. For the first vector v_1, we have $2^k - 1$ choices, as v_1 can be chosen to be any nonzero vector in the subspace C. The second vector v_2 can be any vector in C not contained in the span of v_1. There are $2^k - 2$ choices. In general, the ith vector v_i can be any vector in $C \setminus \text{span}(v_1, \ldots, v_{i-1})$; there are thus $2^k - 2^{i-1}$ choices for v_i. The number of distinct generator matrices for C is thus

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

Exercise 1.4. Let C be a code of dimension k over $\mathbb{F}_2^n$. Define the linear form

$$\begin{aligned} \phi : C &\to \mathbb{F}_2 \\ x &\mapsto \Sigma_i x_i \end{aligned}$$

The set C_e of even-weight codewords is the kernel of ϕ and is thus a subspace of C. Either C_e is equal to the whole space C, or ϕ is surjective. In the latter case,

$$|C_e| = |\text{Ker}\phi| = |C|/|\mathbb{F}_2| = |C|/2,$$

and C_e is thus a subspace of dimension $k-1$.

Exercise 1.5.

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,
$$\sum_{i=1}^{10} i x'_i = \sum_{i=1}^{10} i x_i + i(x'_i - x_i) \neq 0 \mod 11.$$

2. Suppose that the codeword is transposed at positions i and $i+1$, and again denote the corrupted word by x'. Then
$$\sum_{i=1}^{10} i x'_i = \sum_{i=1}^{10} i x_i - i x_i - (i+1)x_{i+1} + (i+1)x_i + i x_{i+1} = x_i - x_{i+1} \mod 11,$$
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.