Exercise Sheet 1

Exercise 1.1. Show that for a fixed length n, the Hamming distance is a metric on the space of the words of that length. Recall that a metric function satisfies the following conditions:

1. $d(x, y) \geq 0$ (non-negativity).
2. $d(x, y) = 0$ if and only if $x = y$ (identity of indiscernibles).
3. $d(x, y) = d(y, x)$ (symmetry).
4. $d(x, z) \leq d(x, y) + d(y, z)$ (triangle inequality).

Exercise 1.2. The *International Standard Book Number* (ISBN) is a numeric book identifier used for the ease of handling books particularly by booksellers and libraries. According to the 2001 standard, a unique 10-digit identifier is assigned to each book (based on the language of the publishing country, publisher, and the title) and a check digit is then affixed to the identifier. The aim of the checksum is to facilitate detection of two common typing errors made in book handling: Typing a wrong digit and interchanging two subsequent digits. Taking the check digit into account, a valid ISBN can be regarded as a vector

$$x = (x_1, \ldots, x_{10})$$

where $x_2, \ldots, x_{10} \in \{0, \ldots, 9\}$ and $x_1 \in \{0, \ldots, 10\}$ is the checksum, computed according to the rule

$$\sum_{i=1}^{10} i x_i = 0 \mod 11.$$

1. Show that the ISBN code can detect a single error.
2. Show that it can detect transposition of any digit with an adjacent digit.
3. What is the minimum distance of this code?
4. If we used the simpler rule
$$\sum_{i=1}^{10} x_i = 0 \mod 11$$
instead of the one above, could the code still detect errors? What about transpositions?

Exercise 1.3. Show that in a binary linear code, either all the codewords have even Hamming weights or else the number of odd-weight and even-weight codewords are equal.

Exercise 1.4. Show that if $(I_k|G_1)$ is a generator matrix for a linear code C, then $(-G_1^\top|I_r)$ is a check matrix for C, where $r = n - k$.

Exercise 1.5. Suppose that G and H are generator and partity-check matrices for a linear code $C \subseteq \mathbb{F}_2^n$. Is the matrix

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

necessarily invertible? Prove or exhibit a counterexample.

Exercise 1.6. Show that any k-dimensional linear code $C \subseteq \mathbb{F}_2^n$ has

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

distinct generator matrices.

Exercise 1.7. Let $x \in \mathbb{F}_2^n$ be of weight d. What is the number of binary vectors of weight w that are orthogonal to x? (*Hint:* Use MacWilliams identities.)