Coding and cryptography
Assignment 1

Due **11:00am Tuesday 28th February 2023**

- This assignment is *optional*. It will allow you to get feedback on the standards used in this course.
- You may hand in this assignment in pairs. If you do this then hand in the same copy (with both names on it) for both people in canvas.
- The use of computer programs, etc., is not allowed.
- If you have any questions, email Ronen at `r.z.brilleslijper@vu.nl` .

1. We fix $n \geq 1$ and d with $1 \leq d \leq n$. For w in K^n, we let

$$B_w(r) = \{w' \in K^n \mid d(w, w') \leq r\}.$$

Let C be a code of length n and distance $d(C)$ *at least* d.

   (a) For a codeword v in C show that $B_v(d-1) \cap C = \{v\}$.

   (b) If $|C| \cdot |B_0(d-1)| < 2^n$ then show that there is a word w in $K^n \setminus C$ such that $C \cup \{w\}$ is a code of distance at least d. (Hint: Compare the sizes of K^n and the union of the $B_v(d-1)$ for v in C.)

   (c) Show that there exists a code C of length n and distance at least d such that $|C| \cdot |B_0(d-1)| \geq 2^n$. In other words,

$$\max_{\substack{\text{length}(C)=n \\ d(C) \geq d}} |C| \geq \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{d-1}}.$$

2. Giving reasons, determine whether each of the following linear codes exists. If it does, construct an example by giving a suitable parity check matrix (and explaining carefully that it has the right properties).

   (a) A $(12, 6, 5)$-code.

   (b) A $(63, 57, 3)$-code.

3. Let

$$X = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix},$$

and let C be the code whose parity check matrix is $H = \begin{bmatrix} X \\ I_8 \end{bmatrix}$, i.e., $C = \{v \in K^{12} \mid vH = 0\}$.

   (a) Let r_1, r_2 and r_3 be any three distinct rows of X. Show that $wt(r_1) = 6, wt(r_1 + r_2) = 4$ and $wt(r_1 + r_2 + r_3) = 2$.

   (b) Show that any four rows of H are linearly independent, and that $d(C) = 5$.

   (c) Verify the Singleton bound for C. Is C an MDS-code?

   (d) Use syndromes to decode (with justification) the following words to their unique nearest neighbour in C under IMLD, where we only correct error patterns of weight at most 2 and do not decode otherwise: 110000000011, 101010101010 and 111111111111.