# A Light Introduction to Code-based Cryptography

BRIDGES Problem Set 1

## 1 Background

Let $C(7,k,d)$ be the binary linear code with generator matrix

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

1. Find $k$.
2. Encode the message vector 1001.
3. How many distinct elements are in $C$?
4. For any generator matrix $G$ in standard form $G = [I_k|A]$, one can use the formula $H = [-A^T|I_{n-k}]$ to construct a parity check matrix for the code. Construct a parity check matrix for this code. Verify your answer.

## 2 Parity checks

Let $C(7,4)$ be a binary linear code described by parity check matrix

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

1. Let $x = (0,0,0,1,1,1,1) \in \mathbb{F}_2^7$. Is $x \in C$?
2. Find four codewords of $C$.
3. Let $b = (b_0, b_1, b_2, b_3, b_4, b_5, b_6) \in \mathbb{F}_2^7$. If $b \in C$, what three equations in terms of $\{b_i\}_{i=0^6}$ must be satisfied?
4. Find a generator matrix for $G$. Verify your answer.
5. Suppose $H \cdot b^T = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$. Find a codeword $b' \in C$ by altering $b$.

## 3 Error correction capability

Let $C$ be an $[n,k,d]$ linear code over $\mathbb{F}_q$. Prove that $C$ is able to correct at most $t = \lfloor \frac{d-1}{2} \rfloor$ errors.