§ 4.1* An Introduction of Channel Coding

- Encoding of a k-dimensional message vector over finite field of size q, i.e., $\mathbb{F}_q$.

$$\bar{u} = (u_1, u_2, \cdots, u_k) \in \mathbb{F}_q^k$$

$$\xrightarrow{\text{Enc.}}$$

$$\bar{c} = (c_1, c_2, \cdots, c_k, c_{k+1}, \cdots, c_n) \in \mathbb{F}_q^n$$

- This can be seen as adding $n - k$ parity-check symbols into $\bar{u}$, which are known as the redundancy.
- Sometimes, the parity-check symbols can be denoted as $p_1, p_2, \cdots, p_{n-k}$.

§ 4.1* An Introduction of Channel Coding

- **Hamming Sphere**
- Given a length n code defined over $\mathbb{F}_q$.
- Any codeword $\bar{c}$ can define a Hamming sphere of radius t. The sphere contains

$$V_q(n,t) = \sum_{j=0}^{t} \binom{n}{j} (q-1)^j$$

length-n vectors.

- **Hamming Bound**
- With a codebook $\mathcal{C}$, the number of message and symbols are $\log_q |\mathcal{C}|$.
- Redundancy

$$R = n - \log_q |\mathcal{C}|$$

For linear codes, $|\mathcal{C}| = q^k$, and

$$R = n - k$$

§ 4.1* An Introduction of Channel Coding

- In an n-dimensioned vector space, there are q^n vectors. A t-error-correcting code does not allow the Hamming sphere of the codewords overlap. Hence,

$$|\mathcal{C}|\, V_q(n,t) \leq q^n$$

and

$$\frac{q^n}{|\mathcal{C}|} \geq V_q(n,t)$$

Hence,

$$\log_q \frac{q^n}{|\mathcal{C}|} \geq \log_q V_q(n,t)$$

$$n - \log_q |\mathcal{C}| \geq \log_q V_q(n,t)$$

$$R \geq \log_q V_q(n,t)$$

§ 4.1* An Introduction of Channel Coding

- If $q^R = V_q(n, t)$, the code is a **perfect code**.

- **Properties of a perfect code**:
  (1). The number of redundancy patterns = The number of vectors in the Hamming sphere of radius t;
  (2). Bounded distance decoding is optimal, i.e., maximum likelihood (ML) decoding.

- Perfect codes include: Hamming codes, Repetition codes, Golay codes.