1 Classical linear codes 15.07.22

1.1 Repetition code

Repetition code. Encoding

$$0 \to 000, 1 \to 111 \tag{1}$$

Decoding: majority vote, e.g. $010 \to 0, 011 \to 1$. Succeeds when 0 or 1 bit is flipped, fails when 2 or 3 bits are flipped. Error probability is reduced from p to $3p^2$ (for $p \ll 1$).

1.2 Linear codes

Repetition code is an example of a linear code. A linear code (n, k, d) is defined by a generator matrix G of size $k \times n$ and a parity check matrix H of size $(n-k) \times n$. Code subspace is bG, for all k-bitstrings b. Alternatively, code supspace consists of all n-bitstings b' satisfying $H(b')^T = 0$. For the repetition code

$$G = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \qquad H^T G = 0 \tag{2}$$

1.3 Code distance

Code distance is the minimum Hamming distance between any two code words. For a linear code, code distance is the minimum (non-zero) weight of n-bitstrings in the code space. For the repetition code $d = 3$. A code that can correct t errors has distance $d = 2t + 1$.

1.4 Dual code

For a linear code with generator matrix G and parity check matrix H the dual code is another linear code with G and H swapped $G^\perp = H, H^\perp = G$. For the dual repetition code

$$G = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \qquad H = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}, \quad H^T G = 0 \tag{3}$$

Dual repetition code encodes 2 bits into 3 bits

$$00 \to 000 \tag{4}$$
$$01 \to 011 \tag{5}$$
$$10 \to 110 \tag{6}$$
$$11 \to 101 \tag{7}$$

Distance of the code is 2. It can detect one error, but correct none.

1.5 Hamming bound

"Good enough" codes exist. Encoding k-bitstrings and being able to correct t errors (distance at least $d \geq 2t + 1$) requires the embedding space to have dimension at least n

$$2^n \geq 2^k \sum_{i=0}^{t} C_n^i \tag{8}$$

1.6 Gilbert–Varshamov bound

Codes need not be "too bad". Given n physical bits a code with distance d exists encoding k logical bits with

$$2^k \geq \frac{2^n}{\sum_{i=0}^{d-1} C_n^i} \tag{9}$$