1 Types of Linear Code

There are many types of linear block codes, such as

- Cyclic codes (e.g., Hamming codes)
- Repetition codes
- Parity codes
- Polynomial codes (e.g., BCH codes)
- Reed-Solomon codes
- Algebraic geometric codes
- Reed-Muller codes
- Perfect codes

1.1 Cyclic Codes

Let $\mathcal{C}$ be a linear code over a finite field $GF(q)$ of block length n.$\mathcal{C}$ is called a cyclic code if, for every codeword $c = (c_1, \ldots, c_n)$ from C, the word $(c_n, c_1, \ldots, c_{n-1})$ in $GF(q)^n$ obtained by a cyclic right shift of components is again a codeword. Because one cyclic right shift is equal to $n-1$ cyclic left shifts, a cyclic code may also be defined via cyclic left shifts. Therefore the linear code $\mathcal{C}$ is cyclic precisely when it is invariant under all cyclic shifts.

Cyclic Codes have some additional structural constraint on the codes. They are based on Galois fields and because of their structural properties they are very useful for error controls. Their structure is strongly related to Galois fields because of which the encoding and decoding algorithms for cyclic codes are computationally efficient.

1.1.1 Example

For example, if $A = F_2$ and $n = 3$, the set of codewords contained in cyclic code generated by (1,1,0) is precisely

$$((0,0,0),(1,1,0),(0,1,1),(1,0,1))$$

It corresponds to the ideal in $F_2[x]/\left(x^3-1\right)$ generated by $(1+x)$. The polynomial $(1+x)$ is irreducible in the polynomial ring, and hence the code is an irreducible code. The idempotent of this code is the polynomial $x+x^2$, corresponding to the codeword (0,1,1).

1.1.2 Generator Matrices

A generator matrix can easily be given by using the coefficients of the generator polynomial $g = \sum_{i=0}^{n-k} g_i x^i$:

$$G = \begin{pmatrix} g \\ xg \\ \vdots \\ x^k g \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots \\ \vdots & & \ddots & \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{pmatrix}$$

Proof. First, note that g_0 is nonzero: Otherwise, $(0, g_1, \ldots, g_{r-1}) \in C$ which implies that $(g_1, \ldots, \ g_{r-1}, 0) \in C$ which implies that $g_1 + g_2 x + \cdots + g_{r-1}x^{r-1} \in C$, which contradicts the minimality of the degree r of the generating polynomial. Now, we see that the $n-r$ rows of the matrix G are linearly independent because of the echelon of nonzero g_0 s with 0 s below. These $n-r$ rows represent the code polynomials $g(x), xg(x), x^2g(x), \ldots, x^{n-r-1}g(x)$. In order to show that G is a generator matrix for C we must show that every code polynomial in C can be expressed as a linear combination of $g(x), xg(x), x^2g(x), \ldots, x^{n-r-1}g(x)$. Part 2 of Theorem 3.3 .3 shows that if $c(x)$ is a code polynomial in C, then $c(x) = m(x)g(x)$ for some polynomial $m(x)$ of degree less than $n - r$ in $GF(q)[x]$. Hence,

$$c(x) = m(x)g(x) = \left(m_0 + m_1 x + \cdots + m_{n-r-1}x^{n-r-1}\right) g(x)$$

$$= m_0 g(x) + m_1 x g(x) + \cdots + m_{n-r-1}x^{n-r-1} g(x)$$

which shows that any code polynomial $c(x)$ in C can be written as a linear combination of the code polynomials represented by the $n - r$ independent rows of G. We conclude that G is a generator matrix for C and the dimension of C is $n - r$.

1.1.3 Parity Check matrix

Suppose C is an $[n, k]$ cyclic code with parity check polynomial $h(x) = h_0 + h_1 x + \cdots + h_k x^k$. Then, a parity check matrix for C is the following $(n - k) \times n$ matrix:

$$H = \begin{bmatrix} h_k & h_{k-1} & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & 0 & h_k & h_{k-1} & \cdots & h_0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \cdots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_0 \end{bmatrix}$$

1.2 Repetition Codes

In coding theory, the repetition code is one of the most basic error-correcting codes. In order to transmit a message over a noisy channel that may corrupt the transmission in a few places, the idea of the repetition code is to just repeat the message several times. The hope is that the channel corrupts only a minority of these repetitions. This way the receiver will notice that a transmission error occurred since the received data stream is not the repetition of a single message, and moreover, the receiver can recover the original message by looking at the received message in the data stream that occurs most often.

Because of the bad error correcting performance and the low ratio between information symbols and actually transmitted symbols, other error correction codes are preferred in most cases. The chief attraction of the repetition code is the ease of implementation.

1.2.1 Code Parameter

In the case of a binary repetition code, there exist two code words - all ones and all zeros - which have a length of n. Therefore, the minimum Hamming distance of the code equals its length n. This gives the repetition code an error correcting capacity of $\frac{n-1}{2}$ (i.e. it will correct up to $\frac{n-1}{2}$ errors in any code word).

If the length of a binary repetition code is odd, then it's a perfect code. [1] The binary repetition code of length n is equivalent to the $(n, 1)-$Hamming code.

1.2.2 Example

Consider a binary repetition code of length 3 . The user wants to transmit the information bits 101 . Then the encoding maps each bit either to the all ones or all zeros code word, so we get the 111000 lil, which will be transmitted.

Let's say three errors corrupt the transmitted bits and the received sequence is 111010100. Decoding is usually done by a simple majority decision for each code word. That lead us to 100 as the decoded information bits, because in the first and second code word occurred less than two errors, so the majority of the bits are correct. But in the third code word two bits are corrupted, which results in an erroneous information bit, since two errors lie above the error correcting capacity.

1.3 Parity Code

1.3.1 Parity

In mathematics, parity refers to the evenness or oddness of an integer, which for a binary number is determined only by the least significant bit. In telecommunications and computing, parity refers to the evenness or oddness of the number of bits with value one within a given set of bits, and is thus determined by the value of all the bits. It can be calculated via a XOR sum of the bits, yielding 0 for even parity and 1 for odd parity. This property of being dependent upon all the bits and changing value if any one bit changes allows for its use in error detection schemes.

1.3.2 Error Detection

If an odd number of bits (including the parity bit) are transmitted incorrectly, the parity bit will be incorrect, thus indicating that a parity error occurred in the transmission. The parity bit is only suitable for detecting errors; it cannot correct any errors, as there is no way to determine which particular bit is corrupted. The data must be discarded entirely, and re-transmitted from scratch. On a noisy transmission medium, successful transmission can therefore take a long time, or even never occur. However, parity has the advantage that it uses only a single bit and requires only a number of XOR gates to generate.

2 Dual Code

The following definitions are from linear algebra.

- The inner product $\mathbf{u}\cdot\mathbf{v}$ of vectors $\mathbf{u} = (u_0, \ldots, u_{n-1})$ and $\mathbf{v} = (v_0, \ldots, v_{n-1})$ in $V(n, q)$ is the scalar defined by $\mathbf{u} \cdot \mathbf{v} = u_0v_0 + u_1v_1 + \cdots + u_{n-1}v_{n-1}$
- Two vectors $\mathbf{u}$ and $\mathbf{v}$ are orthogonal if $\mathbf{u} \cdot \mathbf{v} = 0$
- Given a subspace S of some vector space $V(n, q)$, the space of all vectors orthogonal to S is called the orthogonal complement of S, and is denoted $S^\perp$.
- The nullspace of a matrix is the orthogonal complement of the rowspace of that matrix.

Given a linear $[n, k]$ code C, the dual code of C, denoted $C^\perp$, is the set of vectors of $V(n, q)$ which are orthogonal to every codeword in C, i.e.

$$C^\perp = \{\mathbf{v} \in V(n, q) \mid \mathbf{v} \cdot \mathbf{u} = 0, \forall \mathbf{u} \in C\}$$

If C is an $[n, k]$ linear code, then $C^\perp$ is an $[n, n-k]$ linear code. Furthermore, if C has generator matrix G then $C^\perp$ has an $(n - k) \times n$ generator matrix

H that satisfies $GH^T = 0$. The generator matrix H for $C^\perp$ is also called a parity check matrix for C, as explained below

Let C be a linear code, and let H be a generator matrix for $C^\perp$, the dual code of C. Then a vector $\mathbf{c}$ is a codeword in C if and only if $\mathbf{c}H^T = \mathbf{0}$, or equivalently, if and only if $H\mathbf{c}^T = \mathbf{0}$ Therefore

- H is the generator matrix of $C^\perp$, i.e. $C^\perp$ is the rowspace of H.
- C is in the nullspace of H
- The rows of G are orthogonal with the rows of H.