Linear codes (线性码)

线性码的定义

- 令A=F, F为一个域，则$A^n = F^n$是F上的一个n维向量空间。
- 定义　设 F_q为一个q个元素的有限域，令 $C \subseteq F_q^n$ 为一个码。称码C是线性的，如果

(1) C非空；

(2) 对任意的 $x, y \in C, x + y \in C;$

(3) 对每一个 $a \in F_q$, 任意的 $x \in C$,都有 $ax \in C.$

换句话说，一个码C是线性的当且仅当它是非空的且在加法和数乘下封闭。

- Definition. A linear code C of length n over F_q is a subspace of F_n^q .
- Examples. The following are linear codes:

(1) $C = \{(\lambda, \lambda, \ldots, \lambda) : \lambda \in F_q\}$. This code is called a repetition code.

(2) $(q = 2) C = \{000, 001, 010, 011\}$.

(3) $(q = 3) C = \{0000, 1100, 2200, 0001, 0002, 1101, 1102, 2201, 2202\}$.

(4) $(q = 2) C = \{000, 001, 010, 011, 100, 101, 110, 111\}$.

Definition. Let C be a linear code in $\mathbb{F}_q^n$.
(i) The dual code of C is $C^{\perp}$, the orthogonal complement of the subspace C of $\mathbb{F}_q^n$.
(ii) The dimension of the linear code C is the dimension of C as a vector space over $\mathbb{F}_q$, i.e., $\dim(C)$.

- The orthogonal complement of C is

$$C^{\perp} = \{u \in F_q^n \mid u \bullet c = 0, \forall c \in C\}.$$

Theorem. Let C be a linear code of length n over $\mathbb{F}_q$. Then
(i) $|C| = q^{\dim(C)}$, i.e., $\dim(C) = \log_q |C|$.
(ii) $C^\perp$ is a linear code and $\dim(C) + \dim(C^\perp) = n$.
(iii) $(C^\perp)^\perp = C$.

Hamming weight (汉明重量)

- Definition. Let C be a code (not necessarily linear). The minimum Hamming weight of C, denoted by wt(C), is the smallest of the weights of the nonzero codeword of C.

- Theorem. Let C be a linear code over F_q. Then d(C)=wt(C).

Proof. Recall that for any words $\mathbf{x}, \mathbf{y}$, we have $d(\mathbf{x}, \mathbf{y}) = wt(\mathbf{x} - \mathbf{y})$.
By definition, there exist $\mathbf{x}', \mathbf{y}' \in C$ such that $d(\mathbf{x}', \mathbf{y}') = d(C)$, so

$$d(C) = d(\mathbf{x}', \mathbf{y}') = wt(\mathbf{x}' - \mathbf{y}') \geq wt(C),$$

since $\mathbf{x}' - \mathbf{y}' \in C$.
Conversely, there is a $\mathbf{z} \in C \setminus \{0\}$ such that $wt(C) = wt(\mathbf{z})$, so

$$wt(C) = wt(\mathbf{z}) = d(\mathbf{z}, 0) \geq d(C).$$

Why we prefer linear codes over nonlinear codes

- As a linear code is a vector space, it can be described completely by using a basis.
- The distance of a linear code is equal to the smallest weight of its nonzero codewords.
- The encoding and decoding procedures for a linear code are faster and simpler than arbitrarily nonlinear codes.

Generator matrix and Parity-check matrix(生成矩阵和校验矩阵)

- Definition. (i) A generator matrix for a linear code C is a matrix G whose rows form a basis for C.

(ii) A parity-check matrix H for a linear code C is a generator matrix for the dual code.

- Definition. (i) A generator matrix of the form $(I_k \mid X)$ is said to be in standard form.

(ii) A parity-check matrix in the form $(Y \mid I_{n-k})$ is said to be in standard form.

- Lemma. Let C be an [n,k]-linear code over F_q, with parity-check matrix H. Then

$$v \in C \Leftrightarrow vH^T = 0.$$

In particular, given a kXn matrix G, then G is a generator matrix for C if and only if the rows of G are linearly independent and $GH^T = O$.

Let β_i denote the ith row of H for $1 \leq i \leq n-k$.
If $\mathbf{v} \in G$, then $\mathbf{v} \cdot \beta_i = 0$ for $1 \leq i \leq n-k$, which means $vH^T = 0$.
If $\alpha_1, \cdots, \alpha_k$ are rows of G, we have $\alpha \cdot H^T = 0$ and so $GH^T = 0$.
Conversely, if $\mathbf{v} \cdot \beta_i = 0$, then for any $\mathbf{y} = \sum_{i=1}^{n-k} d_i\beta_i \in G^\perp$, we have

$$\mathbf{v} \cdot \mathbf{y} = 0.$$

Thus $\mathbf{v} \in (G^\perp)^\perp = G$.
Similarly, we can prove the last part.

- Theorem Let C be a linear code and let H be a parity-check matrix for C. Then

(i) C has distance $\geq d$ if and only if any d-1 columns of H are linearly independent; and

(ii) C has distance $\leq d$ if and only if H has d columns that are linearly dependent.

Let $\mathbf{v} = (v_1, \cdots, v_n) \in C$ be a codeword of weight $e > 0$. Suppose the nonzero coordinates are in the positions $i_1, i_2, \cdots, i_e$. Let $\mathbf{c}_j$, $1 \le j \le n$ denote the ith column of H.

By the above theorem, C contains a nonzero word $\mathbf{v} = (v_1, \cdots, v_n)$ of weight e if and only if

$$\mathbf{v}H^T = v_{i_1}\mathbf{c}_{i_1}^T + \cdots + v_{i_e}\mathbf{c}_{i_e}^T,$$

which is true if and only if there are e columns of H that are linearly dependent over $\mathbb{F}_q$.

To say that the distance of C is $\ge d$ is equivalent to saying that C does not contain any nonzero word of weight $\le d-1$, which is in turn equivalent to that any $d-1$ columns of H are linearly independent.

Corollary. Let C be a linear code and H be a parity-check matrix for C. Then the following statement are equivalent:

(i) C has distance d;
(ii) any d-1 columns of H are linearly independent and H has d columns that are linearly dependent.

Equivalence of linear codes

Definition. Two (n,M)-code over F_q are equivalent If one can be obtained from the other by a combination of operations of the following types:

(i) Permutation of the n digits of the codewords;

(ii) Multiplication of the symbols appearing in a fixed position by a nonzero scalar.

- For example.

Let q=3 and n=3. Consider the ternary code

C={000,011,022}

Permuting the first and second positions, followed by multiplying the third position by 2, we obtain the equivalence code

C'={000, 102, 201}.

定义：设H 是一个 F_2 上的 $m\times(2^m-1)$阶矩阵，其列由 F_2 上的所有 2^m-1 个非零m维列向量组成，以H 为校验矩阵的二元Hamming码定义为

$$C=\{c\in F_2^{2^m-1} \mid Hc^T=0\}.$$

定理：上述定义的二元汉明码为 $[2^m-1, 2^m-1-m, 3]$.

- 例. 参数为 [7 , 4 , 3] 的二元汉明码的校验矩阵为

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

设 $x=(x_1,\ldots,x_7)$是C的一个码字， 则 $x=(x_1,\ldots,x_7)\in C \Leftrightarrow Hx^T=0.$ 我们有

$$x_5=x_1+x_2+x_3$$

$$x_6=x_1+x_2+x_4$$

$$x_7=x_2+x_3+x_4.$$

则任意的x都可以写成

$$x = x_1(1000110) + x_2(0100111) + x_3(0010101) + x_4(0001011).$$

令

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

由于G的行线性无关，所以G是C的一个生成矩阵。

Singleton界和MDS码

- 定理： 设 $C \subseteq F_q^n$ 是一个参数为[n,k] 的线性码，则C的最小距离 $d \le n-k+1$.
- 证明： 设参数为 [n,k] 的线性码C的校验矩阵为H, 则H为一个秩为n-k的 $(n-k)\times n$ 的矩阵，因此H中任意n-k + 1列都线性相关，故结论成立。

MDS码

- 定义: 一个参数为[n,k] 的线性码C, 若满足 d(C)=n-k+1, 则称为MDS码。

注： MDS码是存在的，广义Reed-Solomon码就是MDS码。

循环码

循环码是采用循环特性界定的一类线性码， 编码设备不太复杂， 检纠错能力较强。

循环码的定义

- 定义：设 F_q 是一个有限域，令 $C \subseteq F_q^n$为一个线性码，我们说一个线性码C是循环的，如果对任意的 $c=(c_0,\ldots,c_{n-1})\in C$, c 的循环右移

$$c'=(c_{n-1},c_0,\ldots,c_{n-2})\in C.$$

例 参数为 [7 , 4 , 3] 的二元 Hamming码就是一个循环码。

循环码的表示

- 多项式表示
- 矩阵表示

- 定义 设F是一个域，多项式集合F[x]定义为

$$F[x]=\{r_0+r_1x+\ldots+r_nx^n \mid r_i\in F, n\in N\}$$

集合F[x]中有自然的加法和乘法，因此为一个环，称为多项式环。

定义 设 $C\subseteq F_q^n$是一个线性码， $c=(c_0,c_1,\ldots,c_{n-1})\in C$

码字c的码多项式定义为

$$c(x)=c_0+c_1x+\ldots+c_{n-1}x^{n-1}.$$

- 令 $\pi: \quad F_q^n \quad \to \quad F_q[x]/(x^n-1)$

$$(r_0,\ldots,r_{n-1}) \quad \mapsto \quad r_0 + r_1 x + \ldots + r_{n-1}x^{n-1}$$

- 定理 $C \subseteq F_q^n$ 是循环码当且仅当 $\pi(C)$是 $F_q[x]/(x^n-1)$.的一个理想。
- $F_q[x]/(x^n-1)$.的理想均为主理想， 即理想中的每个元素都是由一个元素的倍式组成。所以 $\pi(C)$ 是一个主理想，必然能找到一个生成这个主理想的、次数最低的、首一的多项式g(x), 使得

$$\pi(C) = (g(x)) = \{r(x)g(x) \in F_q[x]/(x^n-1) \mid r(x) \in F_q[x]/(x^n-1)\}.$$

- 把 $\pi(C)$的生成元g(x) 称为循环码C的生成多项式，所有的码多项式都是g(x)的倍式。
- 定理 设参数为[n,k]的循环码 $C \subseteq F_q^n$的生成多项式g(x) 一定是 $x^n - 1$因式，反之，若g(x)是 $x^n - 1$的次数 为n-k 的次数 的因式，则g(x) 一定能生成参数为 [n,k] 的循环码。

- 如果要找一个参数为[n, k]的循环码，就是要寻找一个能除尽 $x^n - 1$ 的n-k次首一多项式 g(x), 由g(x) 生成的主理想就是一个参数为[n, k] 的循环码。

- 如果要找一个参数为[n, k]的循环码，就是要寻找一个能除尽 x^n-1 的n-k次首一多项式 g(x),由g(x)生成的主理想就是一个参数为[n, k] 的循环码。
- 对应的码C为

$$\mathrm{C} \coloneqq \left\{g(x)a(x): a(x) \in \frac{F_q[x]}{x^n-1}, \deg(a(x) \leq k-1)\right\}$$

- 例 构造一个参数为[7，3]的循环码。

由于 $x^7-1=(x+1)(x^3+x+1)(x^3+x^2+1)$，取 $g(x)=(x+1)(x^3+x+1)$， 由g(x)生成的循环码便是一个参数为［7，3］二元循环码。

循环码的矩阵表示

- 设参数为[n，k]的循环码$C\subseteq F_q^n$的生成多项式g(x)，则 $x^n-1=g(x)h(x),\deg(g(x))=n-k,\deg(h(x))=k.$ 则$g(x),xg(x),\ldots,x^{k-1}g(x)$是$\pi(C)$ 在 F_q 上的一组基，其线性组合可以把所有的 q^k 个码的多项式产生出来。因此这组基所对应的k个n维向量作为行构成的 $k\times n$阶矩阵G是循环码C的生成矩阵。

- 因此码C的生成矩阵为

$$G=\begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & \cdots & g_{n-k-1} & g_{n-k} \end{bmatrix}$$

- 设 $h(x)=h_0+h_1x+\ldots+h_{k-1}x^{k-1}+h_kx^k$,由 $x^n-1=g(x)h(x),x^1,\ldots,x^{n-1}$ 可知

$$
\begin{aligned}
&g_{n-k}h_k=1\\
&g_0h_0=-1\\
&g_0h_1+g_1h_0=0\\
&g_0h_2+g_1h_1+g_2h_0=0\\
&\vdots\\
&g_{n-1}h_0+g_{n-2}h_1+\ldots+g_{n-k}h_{k-1}=0
\end{aligned}
$$

其中约定 $g_i=0,i=n-k+1,\ldots,n-1,h_j=0,j=k+1,\ldots,n-1.$

- 码C的校验矩阵为

$$H=\begin{bmatrix} h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & \cdots & h_1 & h_0 \end{bmatrix}$$

- 例 上述参数为［7，3］的二元循环码中，

  $g(x)=(x+1)(x^3+x+1)$， $h(x)=x^3+x+1$，则可以写出G,H.