

Hamming 符号

$$c \geq 1$$

$$F_q^c \text{ 内で原点を通る直線の本数 } n = \frac{q^c - 1}{q - 1}$$

ここから方向ベクトル h_i を 1 本ずつ選ぶと
どの 2 本も同一直線上にない
→ h_i 達の線型従属系は最小 3 本

$$H := (h_1 \cdots h_n)$$

C : H をパリティ検査行列とする符号

… **Hamming 符号** → $d = 3, t = 1$

パリティ検査行列と最小距離 (再掲)

$H : C$ のパリティ検査行列 とするとき

最小距離 $d =$
(H の線型従属な列ベクトルの個数の最小値)

演習問題

- (1) 3 次の 2 元 Hamming 符号 \mathcal{H} は $[7, 4]$ -符号である。パリティ検査行列 (の一つ) H を構成せよ。
- (2) \mathcal{H} の生成行列 (の一つで $GH^T = 0$ となるような) G を求めよ。
- (3) $w(e) = 1$ なる $e \in F_2^7$ を列挙し、そのシンδροーム eH^T との対照表を作れ。
- (4) 符号語 $x \in \mathcal{H}$ を適当に一つ生成し、適当に 1 箇所だけ変えた (誤りを入れた) 語 $y \in F_2^7$ について、シンδροーム yH^T を計算せよ。また、正しく復号すると元の $x \in \mathcal{H}$ が得られることを確かめよ。

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

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

符号語の例：

情報語 $s = (1 \ 0 \ 0 \ 1)$

$$\longmapsto \mathbf{x} = \mathbf{s}G = (1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0)$$

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

e	eH^T
e_1	(1 1 1)
e_2	(1 1 0)
e_3	(1 0 1)
e_4	(0 1 1)
e_5	(1 0 0)
e_6	(0 1 0)
e_7	(0 0 1)

符号語 $x = (1 0 0 1 1 0 0)$ が
1箇所誤って

$$y = (1 0 \mathbf{1} 1 1 0 0)$$

と受信されたとせよ。

$$yH^T = (1 0 1) = e_3H^T$$

→ $y - e_3 = (1 0 \mathbf{0} 1 1 0 0)$ が正しい符号語

→ 情報語は (1 0 0 1)

さて、“良い”符号であるためには、

符号語が“均等”に散らばっているのが
望ましかった。

平行移動で重なる → 線型符号

もっと“対称性”が高いと良いのでは？

“対称性” → 符号の自己同型

等距離線型自己同型 (再掲)

$V = (V, d)$: 距離付き線型空間

$f : V \longrightarrow V$: 等距離線型自己同型

$$\iff f : \text{線型自己同型で距離を保つ} \\ (d(f(\mathbf{x}), f(\mathbf{y})) = d(\mathbf{x}, \mathbf{y}))$$

d : **Hamming** 距離の場合には、

$$\iff f : \text{線型自己同型で重みを保つ} \\ (w(f(\mathbf{x})) = w(\mathbf{x}))$$

等距離線型自己同型 (再掲)

$V = (V, d)$ の等距離線型自己同型全体は
群を成す $\cdots \text{Aut}(V, d)$

$\text{Aut}(V, d)$ は次の 2 種で生成される:

- 符号語の位置の置換
(生成行列の列の置換)
- 或る位置の非零定数倍
(生成行列の或る列の非零定数倍)

$$\text{Aut}(V, d) = \mathfrak{S}_n \wr \mathbf{F}_q^\times = \mathfrak{S}_n \times (\mathbf{F}_q^\times)^n$$

符号の同値 (再掲)

符号 $\mathcal{C}, \mathcal{C}' \subset V$ が同値 (**equivalent**)

$$\iff \exists f \in \text{Aut}(V, d) : \mathcal{C}' = f(\mathcal{C})$$

同値な符号は、
誤り訂正に関して同様の性質を持つ

符号の自己同型

$\mathcal{C} : \text{符号} \subset V = \mathbf{F}_q^n$

$f : \mathcal{C}$ の自己同型 (**automorphism**)

$\iff f : V \longrightarrow V : \text{等距離線型自己同型で}$
 $f(\mathcal{C}) = \mathcal{C}$

その全体は群を成す $\dots \text{Aut}(\mathcal{C})$

$$\text{Aut}(\mathcal{C}) \subset \text{Aut}(V, d) = \mathfrak{S}_n \wr \mathbf{F}_q^\times$$

符号の自己同型

$$\text{Aut}(\mathcal{C}) \subset \text{Aut}(V, d) = \mathfrak{S}_n \wr \mathbf{F}_q^\times$$

特に、 $q = 2$ のときは、

$$\text{Aut}(\mathcal{C}) \subset \text{Aut}(V, d) = \mathfrak{S}_n$$

→ 対称群の有限体上の線型表現の問題に

典型的な場合:

$$\sigma = (1 \ 2 \ \cdots \ n) \in \text{Aut}(\mathcal{C}) \text{ のとき}$$

... 巡回符号 (cyclic code)

巡回符号

線型符号 \mathcal{C} が **巡回符号 (cyclic code)**

$$\iff \sigma = (1\ 2\ \cdots\ n) \in \text{Aut}(\mathcal{C})$$

$$\iff \begin{array}{l} \lceil (c_0, c_1, \dots, c_{n-1}) \in \mathcal{C} \\ \implies (c_{n-1}, c_0, \dots, c_{n-2}) \in \mathcal{C} \rceil \end{array}$$

巡回符号

$$\sigma = (1 \ 2 \ \cdots \ n) \in \mathfrak{S}_n, \quad \sigma^n = 1$$

$$\mathbf{F}_q[\langle \sigma \rangle] \simeq \mathbf{F}_q[X]/(X^n - 1) =: R \curvearrowright V = \mathbf{F}_q^n$$

により、 V : 階数 1 の自由 R -加群

$$V = \mathbf{F}_q^n \simeq R$$

$$(1, 0, \dots, 0) \rightsquigarrow 1$$

$$(c_0, c_1, \dots, c_{n-1}) \rightsquigarrow c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}$$

巡回符号

V : 階数 1 の自由 R -加群 $\supset C$ に対し、

C : 巡回符号 $\iff C$: 部分 R -加群

$V \simeq R$ と同一視するとき

$\iff C$: R の **ideal**

R : 可換環 に対し、

I : R の **ideal** \iff $\left\{ \begin{array}{l} \bullet \forall a, b \in I : a + b \in I \\ \bullet \forall a \in I, \forall r \in R : ra \in I \end{array} \right.$

巡回符号

C : 巡回符号

$\longleftrightarrow R = \mathbf{F}_q[X]/(X^n - 1)$ の **ideal** I

$\longleftrightarrow \tilde{I} \supset (X^n - 1)$ なる $\mathbf{F}_q[X]$ の **ideal** \tilde{I}

($\mathbf{F}_q[X]$: PID なので $\exists f \in R : \tilde{I} = (f)$)

$\longleftrightarrow f|(X^n - 1)$ なる $f \in \mathbf{F}_q[X]$

$X^n - 1 \in \mathbf{F}_q[X]$ の分解が判れば、
巡回符号が分類・構成できる !!

巡回符号

$X^n - 1 = g(X)h(X) \in \mathbf{F}_q[X]$ のとき、

$$\begin{aligned} C := gR : \text{巡回符号} &\simeq \mathbf{F}_q[X]/(h) \\ &= \{c(X) \in R \mid h(X)c(X) = 0 \text{ in } R\} \end{aligned}$$

g : 生成元多項式 (**generator polynomial**)

h : 検査多項式 (**check polynomial**)

$X^n - 1 \in \mathbf{F}_q[X]$ の分解はどうなるのか？

→ 有限体の拡大・**Galois** 理論

$X^\ell - 1 \in \mathbf{F}_q[X]$ の既約分解

$q = 2, n = \ell$: 奇素数のとき、

$$X^3 - 1 = (X + 1)(X^2 + X + 1)$$

$$X^5 - 1 = (X + 1)(X^4 + X^3 + X^2 + X + 1)$$

$$X^7 - 1 = (X + 1)(X^3 + X + 1)(X^3 + X^2 + 1)$$

$$X^{11} - 1 = (X + 1)(X^{10} + X^9 + \cdots + X + 1)$$

$$X^{13} - 1 = (X + 1)(X^{12} + X^{11} + \cdots + X + 1)$$

$$X^{17} - 1 = (X + 1)(X^8 + X^5 + X^4 + X^3 + 1)$$

$$(X^8 + X^7 + X^6 + X^4 + X^2 + X + 1)$$

$$X^{19} - 1 = (X + 1)(X^{18} + X^{17} + \cdots + X + 1)$$

$X^\ell - 1 \in \mathbf{F}_q[X]$ の既約分解

$$X^{23} - 1 = (X + 1)$$

$$(X^{11} + X^9 + X^7 + X^6 + X^5 + X + 1)$$

$$(X^{11} + X^{10} + X^6 + X^5 + X^4 + X^2 + 1)$$

$$X^{29} - 1 = (X + 1)(X^{28} + X^{27} + \cdots + X + 1)$$

$$X^{31} - 1 = (X + 1)(X^5 + X^2 + 1)(X^5 + X^3 + 1)$$

$$(X^5 + X^3 + X^2 + X + 1)$$

$$(X^5 + X^4 + X^2 + X + 1)$$

$$(X^5 + X^4 + X^3 + X + 1)$$

$$(X^5 + X^4 + X^3 + X^2 + 1)$$

$$X^{37} - 1 = (X + 1)(X^{36} + X^{35} + \cdots + X + 1)$$