Hamming 符号 (Hamming codes)

$c \geq 1$

of the lines in $\mathbf{F_q}^c$ through the origin

$$n = \frac{q^c - 1}{q - 1}$$

Choose a direction vector h_i for each line.

$\longrightarrow$ **No two vectors are colinear.**

$\longrightarrow$ **A linearly dependent system of h_i's consists of at least 3 vectors.**

$H := (h_1 \cdots h_n) \in M(c, n; \mathbf{F}_q)$

$\mathcal{C}$ **: the code with check matrix** H

$\cdots$ **Hamming code** $\longrightarrow d = 3, t = 1$

パリティ検査行列と最小距離
(check matrices and minimum distances)

H : a check matrix of $\mathcal{C}$

the minimum distance $\mathrm{d} =$
(the minimum # of column vectors of H
which are linearly dependent)
(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 $\mathrm{GH}^{\mathsf{T}} = \mathrm{O}$ となるような) G を求めよ。

(3) $w(e) = 1$ なる $e \in \mathbb{F}_2^{\,7}$ を列挙し、そのシンドローム $e\mathrm{H}^{\mathsf{T}}$ 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 $y \in \mathbb{F}_2^{\,7}$ について、シンドローム $y\mathrm{H}^{\mathsf{T}}$ 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。

組織符号 (systematic codes)

$\mathcal{C}$: a systematic code (組織符号)

$\overset{\leftarrow}{\Longleftrightarrow}$ $\mathcal{C}$ has a generator matrix G of the form

$$G = (I_k | P), \text{ where } P \in M(k, n-k; \mathbf{F}_q).$$

$G = (I_k | P)$: gen.matrix ($P \in M(k, n-k; \mathbf{F}_q)$)

$H = \left(-P^T \middle| I_{n-k}\right)$: check matrix

$GH^T = O$

組織符号 (systematic codes)

$$G = (I_k | P), \quad H = \left(-P^T \middle| I_{n-k}\right)$$

$$\varphi_G : {\mathbf{F}_q}^k \xrightarrow{\sim} \mathcal{C} \subset V = {\mathbf{F}_q}^n$$

$$s = (s_1, \ldots, s_k) \longmapsto sG = (s|sP)$$

s : **information symbols(情報桁)**

sP : **check symbols(検査桁)**

Thm

Any linear code is equivalent to a systematic code.

符号の同値 (equivalence of codes)

Two codes $\mathcal{C}, \mathcal{C}' \subset V$ are equivalent (同値)

$$\overset{\leftarrow}{\Longleftrightarrow} \exists \mathrm{f} \in \mathrm{Aut}(\mathrm{V}, \mathrm{d}) : \mathcal{C}' = \mathrm{f}(\mathcal{C})$$

同値な符号は、誤り訂正に関して同様の性質を持つ
Equivalent codes have the same properties w.r.t. error-correction.
(the dimension, the minimum distance)

Good representatives of equivalent classes
= standard forms of linear codes
= systematic codes

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

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

An example of a code-word :

an information word $s = (1\ 0\ 0\ 1)$

$$\longmapsto x = sG = (1\ 0\ 0\ 1\ 1\ 0\ 0)$$

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

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

$$y = (1\ 0\ 1\ 1\ 1\ 0\ 0)$$

と受信されたとせよ。

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

$\longrightarrow y - e_3 = (1\ 0\ 0\ 1\ 1\ 0\ 0)$ **が正しい符号語**

$\longrightarrow$ **情報語は** $(1\ 0\ 0\ 1)$

符号の自己同型 (automorphisms of a code)

To construct a code with many code-words systematically,

the code-words of $\mathcal{C}$ should be distributed as "equally" as possible.

$\longrightarrow$ Use mathematical structures (symmetry) of $V = \mathrm{T}^{\mathrm{n}}$

invariant under translation (平行移動で不変)
$\longrightarrow$ linear codes (線型符号)

符号の自己同型 (automorphisms of a code)

To be more efficient, more “symmetric” !!

“symmetry of a code”

$\cdots$ automorphisms of a code

(符号の自己同型)

等距離線型自己同型 (linear isometry)

$\mathrm{V} = (\mathrm{V}, \mathrm{d})$: a metric linear space
(距離付き線型空間)

$\mathrm{f} : \mathrm{V} \longrightarrow \mathrm{V}$: a **linear isometry**
(**等距離線型自己同型**, **isometric linear autom.**)

$\Longleftrightarrow$ f : a linear autom. preserving distances
$(\mathrm{d}(\mathrm{f}(\boldsymbol{x}), \mathrm{f}(\boldsymbol{y})) = \mathrm{f}(\boldsymbol{x}, \boldsymbol{y}))$

For d : Hamming distance,
$\Longleftrightarrow$ f : a linear autom. preserving weights
$(w(\mathrm{f}(\boldsymbol{x})) = w(\boldsymbol{x}))$

等距離線型自己同型 (linear isometry)

$\mathrm{Aut}(\mathrm{V}, \mathrm{d})$: **the group consisting of all the linear isometries of** $V = (\mathrm{V}, \mathrm{d})$

$\mathrm{Aut}(\mathrm{V}, \mathrm{d})$ **is generated by the following two kinds of autom's:**

- **permutations of components (成分 (文字の場所) の置換)**
- **non-zero const. multipl'ns of a component (或る成分の非零定数倍)**

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

符号の同値 (equivalence of codes)

Two codes $\mathcal{C}, \mathcal{C}' \subset \mathrm{V}$ are equivalent (同値)

$$\overset{\leftarrow}{\Longleftrightarrow} \exists \mathrm{f} \in \mathrm{Aut}(\mathrm{V}, \mathrm{d}) : \mathcal{C}' = \mathrm{f}(\mathcal{C})$$

同値な符号は、誤り訂正に関して同様の性質を持つ
Equivalent codes have the same properties
w.r.t. error-correction.
(the dimension, the minimum distance)

符号の自己同型 (automorphisms of a code)

$\mathcal{C}$: **a linear code** $\subset V = \mathbf{F}_q{}^n$

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

$$\overset{\leftarrow}{\Longleftrightarrow} \mathrm{f} \in \mathrm{Aut}(V, \mathrm{d}) \text{ s.t. } \mathrm{f}(\mathcal{C}) = \mathcal{C}$$

$$\mathrm{Aut}(\mathcal{C}) := \{\mathrm{f} \in \mathrm{Aut}(V, \mathrm{d}) \,|\, \mathrm{f}(\mathcal{C}) = \mathcal{C}\}$$

: $\mathcal{C}$ **の自己同型群**

(the automorphism group of $\mathcal{C}$**)**

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

符号の自己同型 (automorphisms of a code)

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

In particular, when $q = 2$**,**

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

$\longrightarrow$ **対称群の有限体上の線型表現の問題に**
(linear representations of symmetric groups over finite fields)

A typical case:

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

$\cdots$ **巡回符号 (cyclic codes)**

巡回符号 (cyclic codes)

A linear code $\mathcal{C}$ is a cyclic code (巡回符号)

$$\overleftarrow{\Longleftrightarrow} \ \sigma = (1\ 2\ \cdots\ n) \in \mathrm{Aut}(\mathcal{C})$$

$$\Longleftrightarrow \Big((c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C} \Longrightarrow (c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C} \Big)$$

巡回符号 (cyclic codes)

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

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

$$\longrightarrow V : \textbf{a free } R\textbf{-module of rank } 1$$

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

$$(1, 0, \ldots, 0) \leftrightsquigarrow 1$$

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

巡回符号 (cyclic codes)

V : **a free** R**-module of rank** $1 \supset \mathcal{C}$

$$\mathcal{C} \text{ : cyclic } \Longleftrightarrow \mathcal{C} \text{ : a sub-} R \text{-module of } V$$

under identification $V \simeq R$

$$\Longleftrightarrow \mathcal{C} \text{ : an ideal of } R$$

R : **a commutative ring**

$$I \text{ : an ideal of } R \overset{\leftarrow}{\Longleftrightarrow} \begin{cases} \bullet\ 0 \in I \\ \bullet\ \forall a, b \in I : a + b \in I \\ \bullet\ \forall a \in I, \forall r \in R : ra \in I \end{cases}$$

巡回符号 (cyclic codes)

$\mathcal{C}$: **a cyclic code**

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

$\longleftrightarrow$ **an ideal** $\widetilde{I}$ **of** $\mathbf{F}_q[X]$ **s.t.** $\widetilde{I} \supset (X^n - 1)$

($\exists f \in R : \widetilde{I} = (f)$**, for** $\mathbf{F}_q[X]$ **is a PID)**

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

Classification of cyclic codes

$\longleftrightarrow$ **decomposition of** $X^n - 1 \in \mathbf{F}_q[X]$

巡回符号 (cyclic codes)

For a decompsition $X^n - 1 = g(X)h(X) \in \mathbf{F}_q[X]$**,**

$$\mathcal{C} := gR \text{ : a cyclic code } \simeq \mathbf{F}_q[X]/(h)$$
$$= \{c(X) \in R \mid h(X)c(X) = 0 \text{ in } R\}$$

g : **生成元多項式 (generator polynomial)**

h : **検査多項式 (check polynomial)**

How decomposes $X^n - 1 \in \mathbf{F}_q[X]$ **?**

$\longrightarrow$ **Galois Theory of finite fields**

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

$q = 2$, $n = \ell$: **an odd prime**

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

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

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

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

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

$$X^{17} - 1 = (X+1)(X^8+X^5+X^4+X^3+1)$$
$$(X^8+X^7+X^6+X^4+X^2+X+1)$$

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

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

$$X^{23} - 1 = (X+1)$$
$$(X^{11} + X^9 + X^7 + X^6 + X^5 + X + 1)$$
$$(X^{11} + X^{10} + X^6 + X^5 + X^4 + X^2 + 1)$$
$$X^{29} - 1 = (X+1)(X^{28} + X^{27} + \cdots + X + 1)$$
$$X^{31} - 1 = (X+1)(X^5 + X^2 + 1)(X^5 + X^3 + 1)$$
$$(X^5 + X^3 + X^2 + X + 1)$$
$$(X^5 + X^4 + X^2 + X + 1)$$
$$(X^5 + X^4 + X^3 + X + 1)$$
$$(X^5 + X^4 + X^3 + X^2 + 1)$$
$$X^{37} - 1 = (X+1)(X^{36} + X^{35} + \cdots + X + 1)$$

巡回符号 (cyclic codes)

For a decompsition $X^n - 1 = g(X)h(X) \in \mathbf{F}_q[X]$**,**

$\mathcal{C} = (g)$ **: a cyclic code** $\subset V = \mathbf{F}_q[X]/(X^\ell - 1)$

g **: 生成元多項式 (generator polynomial)**

h **: 検査多項式 (check polynomial)**

$n = \dim_{\mathbf{F}_q} V = \ell$

$k = \dim_{\mathbf{F}_q} \mathcal{C} = \deg h = \ell - \deg g$

$X^\ell - 1$ の分解と巡回符号

$$X^\ell - 1 = g(X)h(X) \in \mathbf{F}_q[X]$$

$g(X)$	$\mathcal{C} = (g)$	k	d	t
1	V	ℓ	1	0
$X - 1$	**parity-check**	$\ell - 1$	2	0
$\dfrac{X^\ell - 1}{X - 1}$	**repetition**	1	ℓ	$\left\lfloor \dfrac{\ell - 1}{2} \right\rfloor$
$X^\ell - 1$	(0)	0	—	—

$X^\ell - 1$ の分解と巡回符号

$$X^\ell - 1 = g(X)h(X) \in \mathbf{F}_q[X]$$

$\mathcal{C} = (g)$: **巡回符号** $\subset V = \mathbf{F}_q[X]/(X^\ell - 1)$

$X^\ell - 1$ の程よい分解がないと、
新しい (良い) 符号が得られない