

## Hamming 符号 (Hamming codes)

$$c \geq 1$$

# of the lines in  $\mathbb{F}_q^c$  through the origin

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

Choose a direction vector  $\mathbf{h}_i$  for each line.

→ No two vectors are colinear.

→ A linearly dependent system of  $\mathbf{h}_i$ 's  
consists of at least 3 vectors.

$$H := (\mathbf{h}_1 \cdots \mathbf{h}_n) \in M(c, n; \mathbb{F}_q)$$

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

... **Hamming code** →  $d = 3, t = 1$

## パリティ検査行列と最小距離

(check matrices and minimum distances)

$H$  : a check matrix of  $C$

the minimum distance  $d =$

(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  $GH^T = 0$  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  $y \in \mathbb{F}_2^7$  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。

## 組織符号 (systematic codes)

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

$\iff \mathcal{C}$  has a generator matrix  $G$  of the form  
 $G = (I_k | P)$ , where  $P \in M(k, n - k; \mathbb{F}_q)$ .

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

$H = (-P^T | I_{n-k})$  : **check matrix**

$$GH^T = 0$$

## 組織符号 (systematic codes)

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

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

$$\mathbf{s} = (s_1, \dots, s_k) \longmapsto \mathbf{s}G = (\mathbf{s} | \mathbf{s}P)$$

$\mathbf{s}$  : **information symbols**(情報桁)

$\mathbf{s}P$  : **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)

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

同値な符号は、誤り訂正に関して同様の性質を持つ

**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  $s = (1 \ 0 \ 0 \ 1)$**

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

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

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。

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

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

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

→ 情報語は  $(1\ 0\ 0\ 1)$



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

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。

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

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

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

→ 情報語は  $(1\ 0\ 0\ 1)$

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

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。

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

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

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

→ 情報語は  $(1\ 0\ 0\ 1)$

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

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。

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

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

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

→ 情報語は  $(1\ 0\ 0\ 1)$

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

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。

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

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

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

→ 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.

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

invariant under translation (平行移動で不変)  
→ 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”

... automorphisms of a code  
(符号の自己同型)

## 符号の自己同型 (automorphisms of a code)

To be more efficient, more “symmetric” !!

“symmetry of a code”

... **automorphisms** of a code  
(符号の**自己同型**)

## 等距離線型自己同型 (linear isometry)

$V = (V, d)$  : a metric linear space

(距離付き線型空間)

$f : V \longrightarrow V$  : a **linear isometry**

(等距離線型自己同型, **isometric linear autom.**)

$\iff f$  : a linear autom. preserving distances  
( $d(f(\mathbf{x}), f(\mathbf{y})) = d(\mathbf{x}, \mathbf{y})$ )

For  $d$  : Hamming distance,

$\iff f$  : a linear autom. preserving weights  
( $w(f(\mathbf{x})) = w(\mathbf{x})$ )



## 等距離線型自己同型 (linear isometry)

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

$\text{Aut}(V, d)$  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)

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

## 符号の同値 (equivalence of codes)

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

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

同値な符号は、誤り訂正に関して同様の性質を持つ  
**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  $\subset V = \mathbb{F}_q^n$

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

$$\iff f \in \text{Aut}(V, d) \text{ s.t. } f(\mathcal{C}) = \mathcal{C}$$

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

:  $\mathcal{C}$  の自己同型群

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

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

## 符号の自己同型 (automorphisms of a code)

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

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

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

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

A typical case:

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

… 巡回符号 (cyclic codes)

## 符号の自己同型 (automorphisms of a code)

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

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

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

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

**A typical case:**

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

… 巡回符号 (cyclic codes)

## 符号の自己同型 (automorphisms of a code)

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

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

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

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

**A typical case:**

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

... 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)

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

$$\iff \left( (c_0, c_1, \dots, c_{n-1}) \in \mathcal{C} \right. \\ \left. \implies (c_{n-1}, c_0, \dots, c_{n-2}) \in \mathcal{C} \right)$$

## 巡回符号 (cyclic codes)

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

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

→  **$V$  : a free  $R$ -module of rank 1**

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

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

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



## 巡回符号 (cyclic codes)

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

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

under identification  $V \simeq R$

$\iff \mathcal{C}$  : an ideal of  $R$

---

$R$  : a commutative ring

$I$  : an ideal of  $R \iff \left\{ \begin{array}{l} \bullet 0 \in I \\ \bullet \forall a, b \in I : a + b \in I \\ \bullet \forall a \in I, \forall r \in R : ra \in I \end{array} \right.$

## 巡回符号 (cyclic codes)

$\mathcal{C}$  : a cyclic code

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

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

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

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

Classification of cyclic codes

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

## 巡回符号 (cyclic codes)

$\mathcal{C}$  : a cyclic code

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

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

$(\exists f \in R : \tilde{I} = (f), \text{ for } \mathbb{F}_q[X] \text{ is a PID})$

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

**Classification of cyclic codes**

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

## 巡回符号 (cyclic codes)

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

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

$g$  : 生成元多項式 (generator polynomial)

$h$  : 検査多項式 (check polynomial)

---

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

→ Galois Theory of finite fields

## 巡回符号 (cyclic codes)

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

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

$g$  : 生成元多項式 (generator polynomial)

$h$  : 検査多項式 (check polynomial)

---

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

→ Galois Theory of finite fields

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

---

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

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

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

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

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

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

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

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

## $X^\ell - 1 \in \mathbb{F}_q[X]$ 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 decomposition  $X^n - 1 = g(X)h(X) \in \mathbb{F}_q[X]$ ,**

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

**$g$  : 生成元多项式 (generator polynomial)**

**$h$  : 检查多项式 (check polynomial)**

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

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



## $X^\ell - 1$ の分解と巡回符号

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

$g(X)$	$\mathcal{C} = (g)$	$k$	$d$	$t$
1	$V$	$\ell$	1	0
$X - 1$	<b>parity-check</b>	$\ell - 1$	2	0
$\frac{X^\ell - 1}{X - 1}$	<b>repetition</b>	1	$\ell$	$\left\lfloor \frac{\ell - 1}{2} \right\rfloor$
$X^\ell - 1$	$(0)$	0	—	—

## $X^\ell - 1$ の分解と巡回符号

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

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

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