

“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

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 $\dots \text{Aut}(\mathcal{C})$

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

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

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

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)**

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

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

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 $\supset \mathcal{C}$ に対し、

\mathcal{C} : 巡回符号 $\iff \mathcal{C}$: 部分 R -加群

$V \simeq R$ と同一視するとき

$\iff \mathcal{C} : R$ 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 $\exists g \in R : \tilde{I} = (g)$)

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

$X^n - 1 \in \mathbf{F}_q[X]$ 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

代数学からの準備

中国式剰余定理 (孫子の定理)

$m, n \in \mathbf{Z}$: 互いに素のとき

$$\mathbf{Z}/mn\mathbf{Z} \simeq \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$$

$$x \bmod mn \iff (x \bmod m, x \bmod n)$$

$$bn \bmod mn \iff (1 \bmod m, 0 \bmod n)$$

$$am \bmod mn \iff (0 \bmod m, 1 \bmod n)$$

ここに、 $a, b \in \mathbf{Z}$ は $am + bn = 1$ を満たす
(Euclid の互除法)

中国式剰余定理 (孫子の定理・多項式版)

$g, h \in \mathbf{F}_q[X]$: 互いに素のとき

$$\mathbf{F}_q[X]/(gh) \simeq \mathbf{F}_q[X]/(g) \times \mathbf{F}_q[X]/(h)$$

$$f \bmod (gh) \iff (f \bmod (g), f \bmod (h))$$

$$bh \bmod (gh) \iff (1 \bmod (g), 0 \bmod (h))$$

$$ag \bmod (gh) \iff (0 \bmod (g), 1 \bmod (h))$$

ここに、 $a, b \in \mathbf{F}_q[X]$ は $ag + bh = 1$ を満たす
(Euclid の互除法)

有限体

$\mathbf{Z}/m\mathbf{Z}$: 体 (0 以外の元が全て可逆)

$\iff m = p$: 素数

$\mathbf{F}_p := \mathbf{Z}/p\mathbf{Z}$: p 元体

$F(X) \in \mathbf{F}_p[X]$: 既約 $\implies \mathbf{F}_p[X]/(F)$: 体

$\deg F = f$ のとき、 $\#(\mathbf{F}_p[X]/(F)) = p^f =: q$

$\mathbf{F}_q^\times = \langle g \rangle$ ($\exists g \in \mathbf{F}_q^\times$) : 位数 $(q - 1)$ の巡回群

Frobenius 自己同型・有限体の Galois 群

$q = p^f$, $a, b \in \mathbf{F}_q$ のとき、

$$(a + b)^p = a^p + b^p$$

$$(ab)^p = a^p b^p$$

$\varphi_p : \mathbf{F}_q \longrightarrow \mathbf{F}_q$: 体自己同型

$x \longmapsto x^p$ (**Frobenius 自己同型**)

$$\varphi_p(x) = x \iff x \in \mathbf{F}_p$$

$$\text{Gal}(\mathbf{F}_q/\mathbf{F}_p) = \langle \varphi_p \rangle, \quad \varphi_p^f = 1$$

$X^\ell - 1 \in \mathbf{F}_q[X]$ 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

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

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

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

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

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

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

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

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

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

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

$X^\ell - 1 \in F_q[X]$ の既約分解

$q = p^f$, 以下簡単のため ℓ : 素数 $\neq p$ とする

ζ_ℓ : 1 の原始 ℓ 乗根 $\in \overline{F}_q$

$$X^\ell - 1 = \prod_{a=0}^{\ell-1} (X - \zeta_\ell^a) \quad \text{in} \quad \overline{F}_q[X]$$

右辺の因子が F_q 上の共役毎にまとまって、
 F_q 上の既約因子を成す

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

$$q = p^f, \quad \ell : \text{素数} \neq p$$

$$\zeta_\ell : 1 \text{ の原始 } \ell \text{ 乗根} \in \overline{\mathbf{F}_q}, \quad F := \mathbf{F}_q(\zeta_\ell)$$

$$\text{Gal}(F/\mathbf{F}_q) = \langle \varphi_q \rangle, \quad \varphi_q = \varphi_p^f : x \mapsto x^q$$

$$[F : \mathbf{F}_q] = \text{ord}(q \bmod \ell) =: t$$

$$\zeta_\ell^a \text{ の } \mathbf{F}_q \text{ 上の共役} : \zeta_\ell^a, \zeta_\ell^{aq}, \dots, \zeta_\ell^{aq^{t-1}}$$

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

$$f_a(X) := \prod_{i=0}^{t-1} (X - \zeta_\ell^{aq^i}) \in \mathbf{F}_q[X]$$

($t = \text{ord}(q \bmod \ell)$ in $(\mathbf{Z}/\ell\mathbf{Z})^\times$)

$$X^\ell - 1 = (X - 1) \prod_{a \in \mathbf{F}_\ell^\times / \langle q \bmod \ell \rangle} f_a(X)$$

: \mathbf{F}_q 上の既約分解

(($X - 1$) と t 次式 $\frac{\ell - 1}{t}$ 個との積に分解)

$X^\ell - 1 \in F_q[X]$ の既約分解

$t = \text{ord}(q \bmod \ell)$ in $(\mathbf{Z}/\ell\mathbf{Z})^\times$

$X^\ell - 1$ が

$(X - 1)$ と t 次式 $\frac{\ell - 1}{t}$ 個との積に分解

例えば、 $\langle q \bmod \ell \rangle = (\mathbf{Z}/\ell\mathbf{Z})^\times$ の時は、

$$X^\ell - 1 = (X + 1)(X^{\ell-1} + X^{\ell-2} + \cdots + X + 1)$$

: F_q 上の既約分解

巡回符号 (再掲)

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

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

g : 生成元多項式、 h : 検査多項式

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

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

$X^\ell - 1$ 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
$X - 1$	パリティ検査	$\ell - 1$	2	0
$\frac{X^\ell - 1}{X - 1}$	繰返し符号	1	ℓ	$\left\lfloor \frac{\ell - 1}{2} \right\rfloor$
$X^\ell - 1$	(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

$\langle q \bmod \ell \rangle \subsetneq (\mathbf{Z}/\ell\mathbf{Z})^\times$ となるような ℓ を選べ!!