“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 $\longrightarrow$ 線型符号

もっと “対称性” が高いと良いのでは ？

“対称性” $\longrightarrow$ 符号の自己同型

符号の自己同型

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

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

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

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

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

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**

$\Longleftrightarrow$ f : 線型自己同型で距離を保つ

$(d(f(\boldsymbol{x}), f(\boldsymbol{y})) = f(\boldsymbol{x}, \boldsymbol{y}))$

d : Hamming 距離の場合には、

$\Longleftrightarrow$ f : 線型自己同型で重みを保つ

$(w(f(\boldsymbol{x})) = w(\boldsymbol{x}))$

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 $\cdots \mathrm{Aut}(V, d)$

$\mathrm{Aut}(V, d)$ **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)

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

符号の同値 (再掲)

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

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

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

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

特に、$q = 2$ のときは、

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

$\longrightarrow$ **対称群の有限体上の線型表現の問題に**

典型的な場合:

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

$\cdots$ **巡回符号 (cyclic code)**

巡回符号

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

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

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

巡回符号

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

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

により、V : 階数 1 の自由 R-加群

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

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

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

巡回符号

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、

$$I : R \text{ の ideal} \overset{\leftarrow}{\iff} \begin{cases} \bullet\ \forall a, b \in I : a + b \in I \\ \bullet\ \forall a \in I, \forall r \in R : ra \in I \end{cases}$$

巡回符号

$\mathcal{C}$ **: 巡回符号**

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

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

($\boldsymbol{F}_q[X]$ **: PID なので** $\exists g \in R : \widetilde{I} = (g)$**)**

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

$X^n - 1 \in \boldsymbol{F}_q[X]$ **の分解が判れば、**

巡回符号が分類・構成できる !!

巡回符号

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

$$\mathcal{C} := gR \text{：巡回符号} \simeq \boldsymbol{F}_q[X]/(h)$$
$$= \{c(X) \in R | h(X)c(X) = 0 \text{ in } R\}$$

g：**生成元多項式 (generator polynomial)**

h：**検査多項式 (check polynomial)**

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

$\longrightarrow$ **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)

$m, n \in \boldsymbol{Z}$: **互いに素のとき**

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

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

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

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

ここに、 $a, b \in \boldsymbol{Z}$ **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)

$g, h \in \boldsymbol{F}_q[X]$: **互いに素のとき**

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

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

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

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

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

有限体

$\boldsymbol{Z/mZ}$ **：体 (**0 **以外の元が全て可逆)**

$$\Longleftrightarrow m = p \text{ **：素数**}$$

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

$F(X) \in \boldsymbol{F}_p[X]$ **：既約** $\Longrightarrow$ $\boldsymbol{F}_p[X]/(F)$ **：体**

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

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

Frobenius 自己同型・有限体の Galois 群

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

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

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

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

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

$$\varphi_p(x) = x \Longleftrightarrow x \in \boldsymbol{F}_p$$

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

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

$q = 2$, $n = \ell$: **奇素数のとき、**

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

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

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

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

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

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

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

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

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

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

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

右辺の因子が $\boldsymbol{F}_q$ 上の共役毎にまとまって、
$\boldsymbol{F}_q$ 上の既約因子を成す

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

$q = p^f, \quad \ell$：素数 $\neq p$

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

$\mathrm{Gal}(F/\boldsymbol{F}_q) = \langle \varphi_q \rangle, \quad \varphi_q = {\varphi_p}^f : x \longmapsto x^q$

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

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

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

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

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

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

: $\boldsymbol{F}_q$ 上の既約分解

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

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

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

$X^\ell - 1$ が

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

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

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

: $\boldsymbol{F}_q$ 上の既約分解

巡回符号 (再掲)

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

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

g：**生成元多項式、** h：**検査多項式**

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

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

$X^\ell - 1$ の分解と巡回符号

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

$g(X)$	$\mathcal{C} = (g)$	k	d	t
1	V	ℓ	1	0
$X-1$	**パリティ検査**	$\ell - 1$	2	0
$\dfrac{X^\ell - 1}{X-1}$	**繰返し符号**	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

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

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

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

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

$X^\ell - 1$ の分解と巡回符号

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

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

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

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