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**

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

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

$X^\ell - 1 \in \boldsymbol{F}_q[X]$ 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 F_q 上の共役毎にまとまって、
F_q 上の既約因子を成す

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

$X^\ell - 1$ 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!!

平方剰余

ℓ：奇素数

$a \in \boldsymbol{Z}, (a, \ell) = 1$ に対し、　$(a \in (\boldsymbol{Z}/\ell\boldsymbol{Z})^\times)$

a：ℓ を法とする**平方剰余 (quadratic residue)**

$$\overset{\leftarrow}{\Longleftrightarrow} \exists x \in \boldsymbol{Z} : x^2 \equiv a \pmod{\ell}$$

$$\Longleftrightarrow a \in (\boldsymbol{Z}/\ell\boldsymbol{Z})^{\times 2}$$

そうでないとき

平方非剰余 (quadratic non-residue)

平方剰余

ℓ : 奇素数、$a \in Z$ に対し、

$$\left(\frac{a}{\ell}\right) := \begin{cases} +1 & (a : \bmod \ell \text{ で平方剰余}) \\ -1 & (a : \bmod \ell \text{ で平方非剰余}) \\ 0 & (\ell \mid a) \end{cases}$$

: **平方剰余記号・Legendre 記号**

$$\left(\frac{a}{\ell}\right) \equiv a^{\frac{\ell-1}{2}} \pmod{\ell}$$: **Euler の規準**

平方剰余の相互律 (reciprocity law)

p, ℓ : **奇素数 ($p \neq \ell$) に対し、**

$$\left(\frac{\ell}{p}\right)\left(\frac{p}{\ell}\right) = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}}$$

平方剰余の第 1 補充法則

$$\left(\frac{-1}{\ell}\right) = (-1)^{\frac{\ell-1}{2}} = \begin{cases} +1 & (\ell \equiv 1 \mod 4) \\ -1 & (\ell \equiv 3 \mod 4) \end{cases}$$

平方剰余の第 2 補充法則

$$\left(\frac{2}{\ell}\right) = (-1)^{\frac{\ell^2-1}{8}} = \begin{cases} +1 & (\ell \equiv \pm 1 \mod 8) \\ -1 & (\ell \equiv \pm 5 \mod 8) \end{cases}$$

平方剰余符号

以下 $q = 2$, $n = \ell$ **：奇素数とする**

2 **：** $\bmod \ell$ **で平方剰余** $\iff \ell \equiv \pm 1 \pmod 8$

(平方剰余の第 2 **補充法則)**

この時は、 $\langle 2 \bmod \ell \rangle \subset \boldsymbol{F}_\ell{}^{\times 2} \subsetneq \boldsymbol{F}_\ell{}^{\times}$

$Q := \boldsymbol{F}_\ell{}^{\times 2}$ **：平方剰余全体**

$N := \boldsymbol{F}_\ell{}^{\times} \smallsetminus \boldsymbol{F}_\ell{}^{\times 2} = u\boldsymbol{F}_\ell{}^{\times 2}$ **：平方非剰余全体**

(u **：平方非剰余の** 1 **つ)**

Q, N**: 共に Galois 不変で、** $\boldsymbol{F}_\ell = \{0\} \sqcup Q \sqcup N$

平方剰余符号

$$f_Q(X) := \prod_{a \in Q} (X - \zeta_\ell{}^a)$$

$$f_N(X) := \prod_{a \in N} (X - \zeta_\ell{}^a)$$

とすると、

$f_Q(X), f_N(X) \in \boldsymbol{F}_2[X]$ **となり、**

$X^\ell - 1 = (X-1) f_Q(X) f_N(X)$ **と分解する**

平方剰余符号

$$X^\ell - 1 = (X-1) f_Q(X) f_N(X)$$

これから構成される符号 $\longrightarrow$ 平方剰余符号
(quadratic residue code, QR code※)

実際にはこの因数分解を求めるのが面倒
$\longrightarrow$ 冪等生成元 (idempotent generator)
を用いると便利

※ 2 次元バーコードの QR コード ™ とは別物
(QR コードは (株) デンソーウェーブの登録商標です)

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)**

冪等生成元 (idempotent generator)

$\ell \equiv \pm 1 \pmod 8$ **の時、**

$$e_Q(X) := \sum_{a \in Q} X^a, \qquad e_N(X) := \sum_{a \in N} X^a$$

とすると、 $R = \boldsymbol{F}_2[X]/(X^\ell - 1)$ **内で**

$$e_Q(X)^2 = e_Q(X), \quad e_N(X)^2 = e_N(X)$$

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

定理

(ζ_ℓ の取り方に依り)

$\ell \equiv -1 \pmod 8$ **の時、**

$$(e_Q) = (f_Q), \quad (1 - e_Q) = ((X-1)f_N)$$
$$(e_N) = (f_N), \quad (1 - e_N) = ((X-1)f_Q)$$

$$\mathcal{Q} := (e_Q) = (f_Q),\ \mathcal{N} := (e_N) = (f_N)$$

とおくと、 $\mathcal{Q}, \mathcal{N}$ は互いに同値な符号

実際

$$\mu_b : R \longrightarrow R \quad \text{：等距離環同型}$$
$$X \longmapsto X^b$$

により、

$$\mu_b(\mathcal{Q}) = \begin{cases} \mathcal{Q} & (b \in Q) \\ \mathcal{N} & (b \in N) \end{cases}$$

定理

$\ell \equiv \pm 1 \pmod 8$ **の時、**

QR code $\mathcal{Q}$ **の最小距離** d **について、**

- $d \equiv 1 \pmod 2$ **(実は更に** $d \equiv 3 \pmod 4$**)**
- $d^2 \geq \ell$ **(square root bound)**

($\ell \equiv -1 \pmod 8$ **なら更に** $d^2 - d + 1 \geq \ell$**)**

拡大符号 (extended code)(再掲)

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

$\mathcal{C}$: $[n, k, d]$-符号 $\subset V$ に対して

$$\overline{\mathcal{C}} := \left\{ (x_1, \ldots, x_n, x_{n+1}) \,\middle|\, \begin{array}{c} (x_1, \ldots, x_n) \in \mathcal{C} \\ \sum_{i=1}^{n+1} x_i = 0 \end{array} \right\}$$

: $\mathcal{C}$ の拡大符号 $\subset \boldsymbol{F}_q{}^{n+1}$

$\overline{\mathcal{C}}$: $[n+1, k, d]$-符号

$\overline{\mathcal{Q}}$: $\mathcal{Q}$ **の拡大符号** $\subset R \times \boldsymbol{F}_2 \simeq {\boldsymbol{F}_2}^{\ell+1}$ **とする**

${\boldsymbol{F}_2}^{\ell+1}$ **の添字集合:**

$$\{0, 1, \ldots, \ell - 1\} \cup \{\infty\} = \mathbf{P}_1(\boldsymbol{F}_\ell)$$

定理

$$\mathrm{Aut}(\overline{\mathcal{Q}}) \supset \mathrm{PSL}_2(\boldsymbol{F}_\ell)$$

特に、$\mathrm{Aut}(\overline{\mathcal{Q}})$ **は** $\mathbf{P}^1(\boldsymbol{F}_\ell)$ **上推移的**

参考: 複素関数論

$\boldsymbol{C} \cup \{\infty\} = \mathrm{P}_1(\boldsymbol{C})$: **Riemann 球面**

$\mathrm{PGL}_2(\boldsymbol{C}) = \mathrm{GL}_2(\boldsymbol{C})/\boldsymbol{C}^\times \curvearrowright \mathrm{P}_1(\boldsymbol{C})$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z := \dfrac{az+b}{cz+d}$: **一次分数変換で作用**

例: $l = 7$

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

$$f_Q(X) = X^3 + X + 1$$

$$e_Q(X) = X^4 + X^2 + X = X f_Q(X)$$

$\longrightarrow$ $[7, 4, 3]$-**Hamming 符号**

$\cdots$ **パリティ検査 bit を付け加えた拡張符号は**
位数 168 **の単純群** $\mathrm{PSL}(2, \boldsymbol{F}_7)$ **を**
自己同型群に持つ $[8, 4, 4]$-**符号**

Hamming の球充填上界

(F_2 上の線型符号の場合)

F_2 上の $[n, k, 2t+1]$-符号について

$$\sum_{s=0}^{t} \binom{n}{s} \leq 2^{n-k}$$

$[n, k, 2t+1] = [7, 4, 3]$ は上で等号成立の場合

$\cdots$ 完全符号 (perfect code)

例: $l = 23$

$$X^{23} - 1$$
$$= (X+1)(X^{11} + X^9 + X^7 + X^6 + X^5 + X + 1)$$
$$(X^{11} + X^{10} + X^6 + X^5 + X^4 + X^2 + 1)$$

$$e_Q(X) = X + X^2 + X^4 + X^8 + X^{16} + X^9$$
$$+ X^{18} + X^{13} + X^3 + X^6 + X^{12}$$

$\longrightarrow$ **Goley 符号**

$\cdots$ **Matthew 群** M_{23} **を自己同型群に持つ**

$[23, 12, 7]$-**符号**

(これも完全符号)

誤り訂正符号には、他にも、

- **Reed-Muller 符号**
- **BCH 符号**
  (Bose, Ray-Chaudhuri, Hocquenghem)
- **Reed-Solomon 符号**
- **Goppa 符号**

など、重要なものがあるが、

本講義ではここまで

情報通信を行なう際の要請

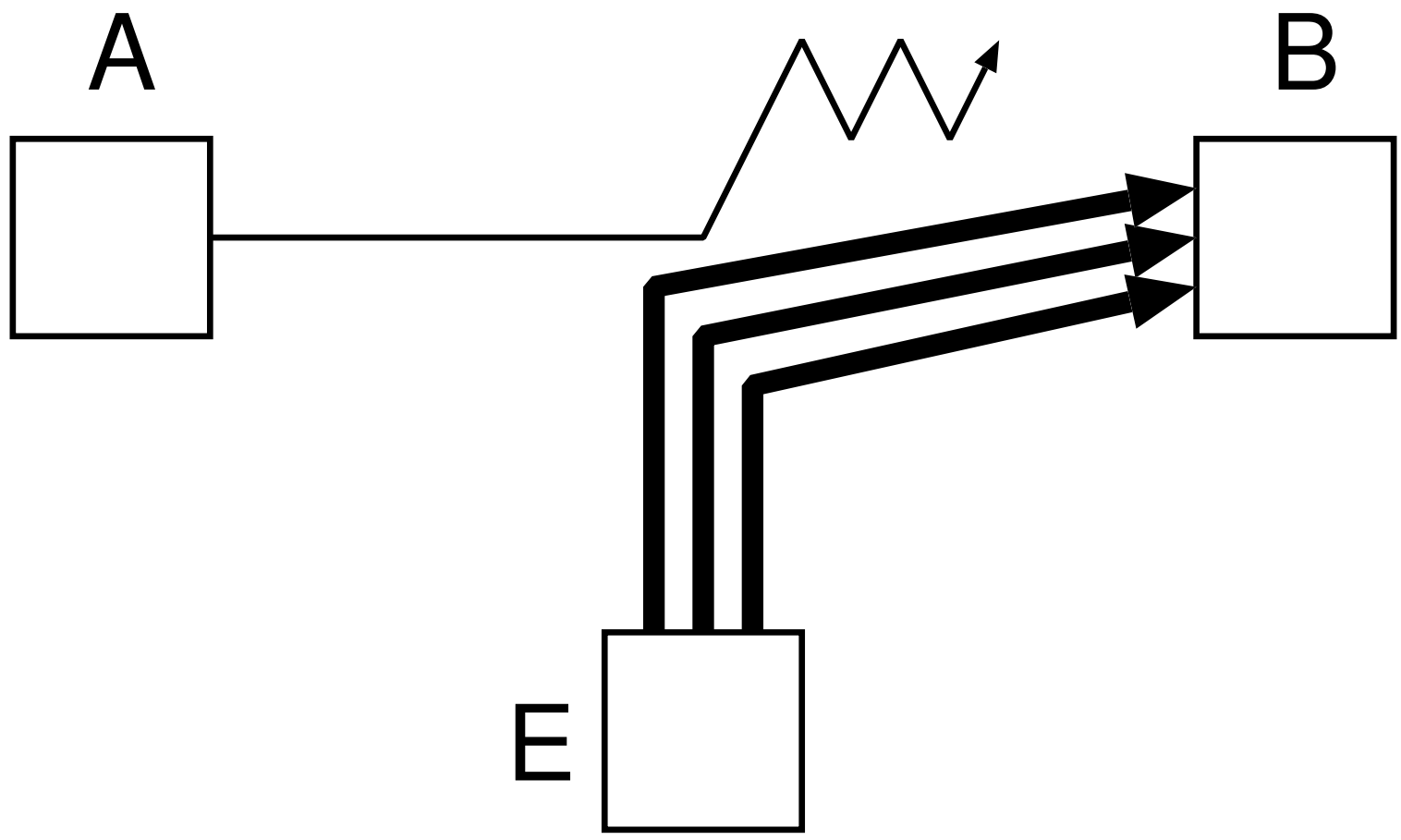
- **効率的に** $\longrightarrow$ **情報理論**
- **確実に** $\longrightarrow$ **符号理論**
- **安全に** $\longrightarrow$ **暗号理論**

安全な情報伝達を阻害するもの

- 妨害 (DoS 攻撃など)
- 盗聴
- 改竄
- なり済まし

など

DoS (Denial of Service) 攻撃



DoS (Denial of Service) 攻撃