

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

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

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

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)

$X^\ell - 1$ 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!!

平方剰余

ℓ : 奇素数

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

a : ℓ を法とする平方剰余 (quadratic residue)

$$\iff \exists x \in \mathbf{Z} : x^2 \equiv a \pmod{\ell}$$

$$\iff a \in (\mathbf{Z}/\ell\mathbf{Z})^{\times 2}$$

そうでないとき

平方非剰余 (quadratic non-residue)

平方剰余

ℓ : 奇素数、 $a \in \mathbb{Z}$ に対し、

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

: 平方剰余記号・Legendre 記号

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

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

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

平方剰余の第 2 補充法則

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

平方剰余符号

以下 $q = 2, n = \ell$: 奇素数とする

$2 : \text{mod } \ell$ 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、 $\langle 2 \text{ mod } \ell \rangle \subset F_\ell^{\times 2} \subsetneq F_\ell^\times$

$Q := F_\ell^{\times 2}$: 平方剰余全体

$N := F_\ell^\times \setminus F_\ell^{\times 2} = uF_\ell^{\times 2}$: 平方非剰余全体
(u : 平方非剰余の1つ)

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

平方剰余符号

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

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

とすると、

$$f_Q(X), f_N(X) \in \mathbf{F}_2[X] \quad \text{となり、}$$

$$X^\ell - 1 = (X - 1)f_Q(X)f_N(X) \quad \text{と分解する}$$

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 → **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
→ **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)

$g, h \in \mathbf{F}_q[X]$: 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)

冪等生成元 (idempotent generator)

$\ell \equiv \pm 1 \pmod{8}$ の時、

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

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

$$\begin{aligned} e_Q(X)^2 &= e_Q(X), & e_N(X)^2 &= e_N(X) \\ 1 + e_Q(X) + e_N(X) &= X^{\ell-1} + \cdots + X + 1 \end{aligned}$$

定理

(ζ_ℓ の取り方に依り)

$\ell \equiv -1 \pmod{8}$ の時、

$$\begin{aligned}(e_Q) &= (f_Q), & (1 - e_Q) &= ((X - 1)f_N) \\(e_N) &= (f_N), & (1 - e_N) &= ((X - 1)f_Q)\end{aligned}$$

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

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

実際

$\mu_b : R \longrightarrow R$: 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 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)

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

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

$$\bar{\mathcal{C}} := \left\{ (x_1, \dots, x_n, x_{n+1}) \mid \begin{array}{l} (x_1, \dots, x_n) \in \mathcal{C} \\ \sum_{i=1}^{n+1} x_i = 0 \end{array} \right\}$$

$: \mathcal{C}$ の**拡大符号** $\subset \mathbf{F}_q^{n+1}$

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

\overline{Q} : Q の拡大符号 $\subset R \times F_2 \simeq F_2^{\ell+1}$ とする

$F_2^{\ell+1}$ の添字集合:

$$\{0, 1, \dots, \ell - 1\} \cup \{\infty\} = \mathbf{P}_1(F_\ell)$$

定理

$$\text{Aut}(\overline{Q}) \supset \text{PSL}_2(F_\ell)$$

特に、 $\text{Aut}(\overline{Q})$ は $\mathbf{P}^1(F_\ell)$ 上推移的

参考: 複素関数論

$\mathbf{C} \cup \{\infty\} = \mathbf{P}_1(\mathbf{C})$: Riemann 球面

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

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

例: $l = 7$

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

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

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

→ $[7, 4, 3]$ -**Hamming** 符号

… 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 $\text{PSL}(2, F_7)$ 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
… **完全符号 (perfect code)**

例: $l = 23$

$$\begin{aligned} & X^{23} - 1 \\ &= (X + 1)(X^{11} + X^9 + X^7 + X^6 + X^5 + X + 1) \\ &\quad (X^{11} + X^{10} + X^6 + X^5 + X^4 + X^2 + 1) \end{aligned}$$

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

→ **Goley 符号**

… **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 → 情報理論
- 確実に → 符号理論
- 安全に → 暗号理論

情報通信を行なう際の要請

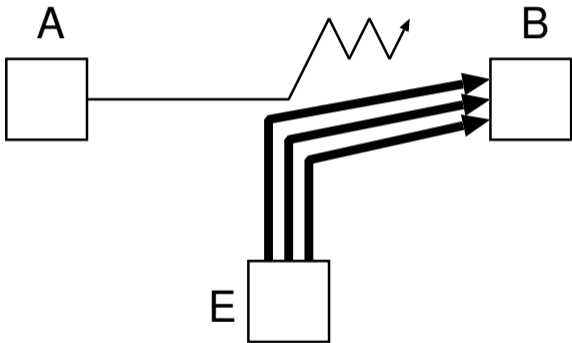
- 効率的に → 情報理論
- 確実に → 符号理論
- 安全に → 暗号理論

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

