

“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

$\iff f : V \longrightarrow V : \text{等距離線型同型で } f(\mathcal{C}) = \mathcal{C}$

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

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

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

\mathcal{C} : 巡回符号

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

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

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

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

により、 V : 階数 1 の自由 R -加群

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

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

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

\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、

$\mathfrak{a} : R$ の **ideal** \iff

- $\forall a, b \in \mathfrak{a} : a + b \in \mathfrak{a}$
- $\forall a \in \mathfrak{a}, \forall r \in R : ra \in \mathfrak{a}$

C : 巡回符号

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

$\longleftrightarrow \mathfrak{a} \supset (X^n - 1)$ なる $\mathbf{F}_q[X]$ の **ideal** \mathfrak{a}

($\mathbf{F}_q[X]$: PID なので $\exists f \in R : \mathfrak{a} = (f)$)

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

$X^n - 1 \in \mathbf{F}_q[X]$ の分解が判れば、
巡回符号が分類・構成できる !!

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