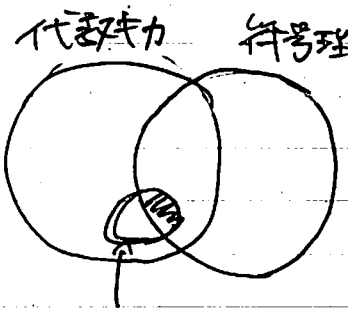
深澤 知 (Satoru Fukasawa)　　Data . . No.

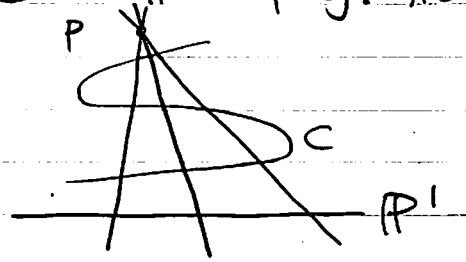
AG codes with many automorphisms from Galois points



§1 Galois points

$k = \bar{k}$, $p = \mathrm{ch}\, k \geq 0$
$C \subset \mathbb{P}^2$: irred. alg. curve of deg. $d > 1$
$k(C)$: C の関数体

$P \in \mathbb{P}^2 \setminus C$
$\pi_P : C \longrightarrow \mathbb{P}^1$; proj. from P



$k(C)/\pi_P^* k(\mathbb{P}^1)$: fin. ext. (of deg. $= d$)

Def (Yoshihara, 1996)
P : (outer) Galois $\overset{\text{def}}{\Longleftrightarrow}$ $k(C)/\pi_P^* k(\mathbb{P}^1)$: Galois ext.

- $G_P := \mathrm{Gal}\left(k(C)/\pi_P^* k(\mathbb{P}^1)\right) \hookrightarrow \mathrm{Aut}(k(C)) \cong \mathrm{Aut}(X)$
  $\varphi : X \longrightarrow C$ normali.

基本問題：ガロア点はいくつあるか？

(1) Yoshihara, Homma, F (~2013):
C: smooth ⇒ 任意標数で確定

(2) Thm (F, Ann. Mat. Pura Appl. 2023)
(他) $p=0$, genus ≥ 1, $d \geq 3$
$\exists$ non-collinear (outer) Galois points
$\Leftrightarrow C \sim X^d + Y^d + Z^d = 0$

Criterion (F, 2018)
X: smooth proj. curve, $Q \in X$
$G_1, G_2 < \mathrm{Aut}(X)$, $G_1 \neq G_2$, $|G_1| = |G_2| < \infty$
(I) (a) $X/G_i \cong \mathbb{P}^1$
(b) $G_1 \cap G_2 = \{1\}$
(c) $\sum_{\sigma \in G_1} \sigma(Q) = \sum_{\tau \in G_2} \tau(Q)$

$\Leftrightarrow$ (II) $\exists \varphi : X \longrightarrow \mathbb{P}^2$: birat. onto its image
$\exists P_1, P_2 \in \mathbb{P}^2 \setminus \varphi(X)$: Galois points s.t.
$G_1 = G_{P_1}$, $G_2 = G_{P_2}$, $Q \in \overline{P_1 P_2}$

§2 Codes, automorphisms

$\mathbb{F}_q$: finite field of q elements
$n \geq 1$: integer
$C \subset \mathbb{F}_q^n$: linear subspace を, (linear) code という.

parameters
- n : length
- $k = \dim C$: dimension
- minimum distance $d := \min\{\mathrm{wt}\, a \mid a \in C \setminus \{0\}\}$ (wt: 0でない成分の個数)

このとき, $[n, k, d]_q$ - code と言う.

Thm (Singleton bound)
$k + d \leq n + 1$

Ex. (Read-Solomon code)
$1 \leq m < q$
$\mathbb{F}_q[x]_{\leq m} = \{$次数 m 以下の多項式$\} = \bigoplus_{i=0}^{m} \mathbb{F}_q \cdot x^i$

$$\begin{array}{ccc} \Phi : \mathbb{F}_q[x]_{\leq m} & \longrightarrow & \bigoplus_{P \in \mathbb{F}_q} \mathbb{F}_q \cdot P \\ \downarrow & & \downarrow \\ f & \longmapsto & (f(P))_{P \in \mathbb{F}_q} \end{array}$$

により, $[q, m+1, \geq q-m]$ - code が得られる.
Singleton bound により, ちょうど $q-m$ である.

automorphisms of codes
$\mathrm{Aut}(C) := \{\sigma \in S_n \mid \sigma(C) = C\}$
$\left(\sigma(a_1, \cdots a_n) = (a_{\sigma(1)}, \cdots, a_{\sigma(n)})\right.$ と考えている.$\left.\right)$

Ex $AGL(1, \mathbb{F}_q) = \{\mathbb{F}_q \to \mathbb{F}_q ;\ x \mapsto ax+b \mid a \in \mathbb{F}_q^\times,\ b \in \mathbb{F}_q\}$
は $\mathbb{F}_q$ の元を入れかえる.
$\sigma \in AGL(1, \mathbb{F}_q)$ に対して

$$\begin{array}{ccc} \mathrm{Im}\,\mathrm{ev} & \longrightarrow & \mathrm{Im}\,\mathrm{ev} \\ \cup & & \cup \\ (f(P))_{P \in \mathbb{F}_q} & \longmapsto & (f(\sigma(P)))_{P \in \mathbb{F}_q} \end{array}$$

線形写像で単射なので, 入っていることだけが重要

という同型が得られ,
$AGL(2, \mathbb{F}_q)$ は $[q, m+1, q-m]$ RS-code に act する.

§3 AG codes, Stichtenoth's criterion

X : smooth proj. curve / $\mathbb{F}_q$, defined / $\mathbb{F}_q$

- $\mathrm{Div}(X) = \bigoplus_{\text{places } P \subset \mathbb{F}_q(X)} \mathbb{Z} \cdot P$
- $D \in \mathrm{Div}(X)$ に対し,

$$\mathcal{L}(D) = \{ f \in \mathbb{F}_q(X) \setminus \{0\} \mid (f) + D \geq 0 \} \cup \{0\}$$

$$(f) = \sum_P v_P(f)\, P$$

代数幾何では $\mathcal{L}(D)$ は sheaf のように X 上の global sections の空間. Stichtenoth のテキストに合わせた

カタイ "L" の方が…良かった?

AG code

$S \subset X(\mathbb{F}_q)$: fin. set. $\mathrm{supp}(D) \cap S = \emptyset$

evaluation map

$$\Phi : \mathcal{L}(D) \longrightarrow \bigoplus_{P \in S} \mathbb{F}_q \cdot P$$

$$f \longmapsto (f(P))_{P \in S}$$

の像 $\Phi(\mathcal{L}(D))$ を AG code という.

上の Reed-Solomon code は, $X = \mathbb{P}^1$, $S = \mathbb{P}^1(\mathbb{F}_q) \setminus \{(1:0)\}$, $D = m \cdot (1:0)$ として得られる

Q. 代数曲線の aut $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(X)$ が符号の aut を自然に誘導しないだろうか?

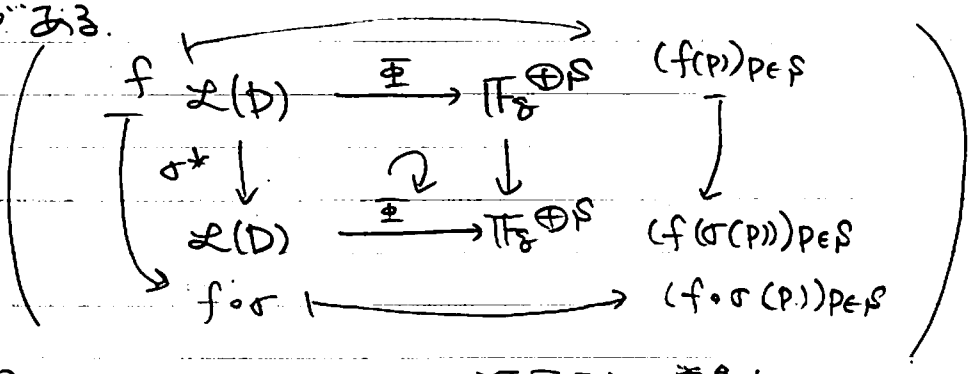
Stichtenoth's conditions

$$\begin{cases} \bullet\ \sigma(S) = S \\ \bullet\ \sigma(D) = D \end{cases} \quad - \circledast$$

$$\mathrm{Aut}(S, D) := \{ \sigma \in \mathrm{Aut}_{\mathbb{F}_q}(X) \mid \sigma(S) = S,\ \sigma(D) = D \}$$

Prop (Stichtenoth, 1990)

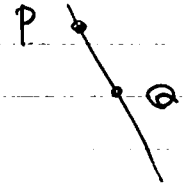
(a) 自然な準同型 $\mathrm{Aut}(S, D) \longrightarrow \mathrm{Aut}(\Omega(\mathcal{L}(D)))$ がある.



(b) $\#S > 2g(X)+2$ なら, (a) の準同型は単射.

Q. ㊟ (のうち, 特に $\sigma(D)=D$) にはどのような(幾何学的)意味があるか?

㊟ が0点による自己同型は㊟をみたす典型例



$$D=\sum_{\sigma\in G_P}\sigma(Q)$$

今回の結果 2つの Galois pts そもそも plane curve / $\mathbb{F}_q$ が得られれば, "aut つきの code" が得られる.

§4 AG codes from Gala's points

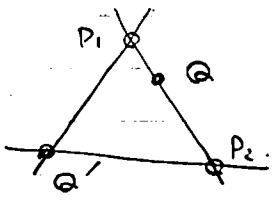
§1のCriterionを $/\mathbb{F}_q$ に拡張しつつ、次を得る。

Thm X: smooth proj. curve, $Q, Q' \in X(\overline{\mathbb{F}_q})$
$G_1, G_2 \subset \mathrm{Aut}_{\mathbb{F}_q}(X)$, $G_1 \neq G_2$, $|G_1| = |G_2| \ (< \infty)$

(a) $X/G_i \cong \mathbb{P}^1$

(b) $G_1 \cap G_2 = \{1\}$

(c) $\sum_{\sigma \in G_1} \sigma(Q) = \sum_{\tau \in G_2} \tau(Q')$ $(/\overline{\mathbb{F}_q})$ で、
この div. D は defined $/\mathbb{F}_q$



(d) $Q' \in X(\mathbb{F}_q)$, $Q' \notin \mathrm{supp}(D)$, $\#S > |G_1|$
(ここで、$S := \langle G_1 \cdot G_2 \rangle \cdot Q'$)

たいてい成立

$\Rightarrow$ 次が成立。

(1) evaluation map

$$\Phi : \mathcal{L}(D) \longrightarrow \bigoplus_{R \in S} \mathbb{F}_q \cdot R \ ; \ f \longmapsto (f(R))_{R \in S}$$

は単射で、min. distance $\geq \#S - |G_1|$

genusの条件不要

(2) $\exists$ inclusion $\langle G_1, G_2 \rangle \hookrightarrow \mathrm{Aut}(\Phi(\mathcal{L}(D)))$

Ex. $X = \mathbb{P}^1$, q: odd, $q \geq 5$ とする。 $m = \frac{q-1}{2}$ とする。

$$G_1 = \left\{ \begin{pmatrix} s^i & 0 \\ 0 & 1 \end{pmatrix} \;\middle|\; 0 \leq i \leq m-1 \right\} \quad (s: \text{原始 } m \text{ 乗根})$$

$$G_2 = \left\{ \begin{pmatrix} s^i & (-s^i) \\ 0 & 1 \end{pmatrix} \;\middle|\; 0 \leq i \leq m-1 \right\}$$

$Q = (1:0)$, $Q' = (0:1)$, $D = mQ$

- (X, G_1, G_2, Q, Q') は (a) ~ (d) をみたす。
得られる code は $[q, \frac{q+1}{2}, \frac{q+1}{2}]$-RS code であり、
$\langle G_1, G_2 \rangle \cong \mathbb{F}_q \rtimes \left(\mathbb{Z}/\left(\frac{q-1}{2}\right)\mathbb{Z}\right)$ である。

(P.f. of Thm)

(1) $\forall f \in \mathcal{L}(D)\setminus\{0\}$ が S 上で 0 にならなければよい.

$\#\{f\text{ の zero}\} \le \deg(D) = |G_1| < \#S$ より OK.

(条件(d))

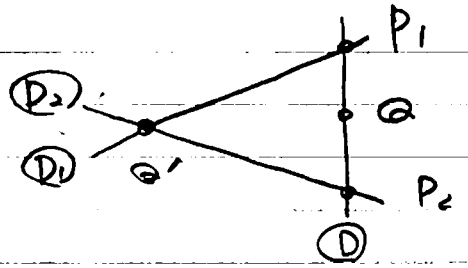
(2) $\gamma \in \langle G_1, G_2\rangle \Rightarrow \gamma \in \mathrm{Aut}(S, D)$ は,

S が orbit であること, Galois pt の def よりわかる.

$\forall \gamma \in \langle G_1, G_2\rangle \setminus \{1\}$, $\gamma|_S \neq 1$ を示せばよい.

$\gamma|_S = 1$ と仮定.

(a)(b)(c) より ガロア点が2つある状況



$\Lambda : \varphi : X \longrightarrow \mathbb{P}^2$ に対応する linear system

$\gamma^*\Lambda = \Lambda$

γ は linear transform. に拡張される.

$\rightsquigarrow \gamma = 1$ と丁寧に示す. □

§5 A generalization

このような $e_{\geq 1}$ は必ず存在. $e_{\geq 2}$ とは限らない.

(G_1, G_2, Q, Q') : 定理の仮定をみたす

$D = \sum_{\sigma \in G_1} \sigma(Q) = eD_0 \quad \left(D_0 = \sum_{R \in \mathrm{supp}(D)} R\right)$ と書けたとき,

$\frac{m|G_1|}{e} < \#S$ となる m について,

$\Phi : \mathcal{L}(mD_0) \longrightarrow \mathbb{F}_q^{\oplus S}$ によって code がつくれ,

$\langle G_1, G_2 \rangle \hookrightarrow \mathrm{Aut}(\Phi(\mathcal{L}(mD_0)))$ となる.

- $\mathrm{supp}(D) = \{Q\}$ のときは one-point code と考えることができる.
  ↝ Reed-Solomon code,
  Hermitian code,
  ....
  と recover
- one-pt code + aut と考えることは,
  Thm(C) の設定に近い.
  ↝ 2つの Galois pts という設定は,
  これまでの符号理論研究と相性がよい.