数理解析研究所講究録
第802巻 1992年 62-67

楕円曲線に基づく符号について

今井 潤 (Jun Imai)
NTT コミュニケーション科学研究所
NTT Communication Science Laboratories

概要

代数曲線の因子を用いて符号を構成する際、従来では、曲線の方程式の標準型を選び、次に、その係数や次数を任意に変化させて曲線を1つ決め、そしてその曲線の有理点の情報から符号を構成しており、どの様な性質を持つ符号が生成されるかは、全く予測できなかった。本研究では、楕円曲線に関して、望ましい有理点の情報から逆に代数曲線のクラスを決定する方法と、その曲線を用いて符号を構成する方法，そして，構成された符号のクラスが従来の符号のクラスに対して如何なる位置関係にあるかという問題についての考察を楕円曲線の特殊な性質を用いて行なった.

1 まえがき

ここで扱う符号とは線形符号（群符号）、或はそれに同型な有限群に限定する。従来、誤り訂正符号として定義されているものには（1）巡回符号 （2）BCH符号 （3）Classical Goppa 符号 （4）代数幾何学的符号、等がある。群のカテゴリーとして、次のような包含関係が成立する。

- (1) ⊃ (2), (3) ⊃ (2), (4) ⊃ (3)

（1）もしくは（2）の符号の良い点は、その構造の明快さにある。最も実用的な（2）の符号に関して言えば、その実用性は、種々の制約条件に合わせて、好みのパラメータを持つ符号を構成できる（最適とはいかないが）ことにある。もちろん復号法も比較的容易である。一方（3）、（4）の符号はBCH符号の定義を一般化することによって、符号のクラスを広げ、より良いパラメータを持つものを研究対象に入れることができるという利点がある。しかし実際に求めるパラメータを持つ符号を構成することは難しく、また復号アルゴリズムも一般化の度合に比例して複雑なものになってくる。

2 問題設定とその背景

「如何なる曲線を選べば、どの様な性質を持つ符号が構成できるか」という事をここでは問題にする。とは言うものの，”代数曲線の因子を適当に選ぶことによって，（代数曲線上の）関数体の元から成るある部分線形空間（あるいは代数曲線上の1次微分型式から成るある部分線形空間）を規定し，次にこの空間をGoppaの定義した埋め込み写像（有理化写像）によって，基礎体上の線形空間として実現する”という方法は採らなかった．従来の研究では、曲線の標準型を一つ決め、次に適当な因子を選ぶことによって、符号を構成する線形空間を決める。そして次に、その符号のパラメータ、すなわち（n， r， d）＝（符号長、検査記号数、最小距離）、の満たすいくつかの関係式を、曲線の標準型中のいくつかのパラメータ、曲線の有理点の個数、係数体の拡大次数、曲線の種数、曲線の生成因子から決まる各種の量等によって表現するというものであった。
そこで今回の研究では，楕円曲線を用いることによって，巡回符号を真に含み，しかも代数幾何学的符号に必ずしも含まれない符号のクラスを定義し，そして，それらの性質を計る評価尺度をも与えた．また逆に，この評価尺度に関して，ある与えられた条件を満たすような符号を構成するという，一種の逆問題を考察することによって，符号構成段階で設計思想を導入する方法に先鞭をつけた．曲線を楕円曲線に制限するのは、問題を容易にするためと、従来の研究の蓄積の豊富さ、楕円曲線固有の有用な性質の存在等の理由による。
代数幾何的符号の欠点は、その定義の複雑さ、符号の性質を左右する因子の多さ、そして定義の一般性の高さからくる復号手続きの復雑さである。これらの諸問題を解決するためにはBCH符号に見られるような簡単明瞭かつ便利な

代数的構造を代数幾何学的符号にも持ち込むことが一つの方法であると考えられるが，これについては今後の研究課題として残し，今回は取り扱わない.

3 符号のガロア表現

巡回符号が生まれてから、符号は体のガロア理論を背景として、有限体 F_q 上の多項式環から作られる有限生成環 $F_q[X]/(X^m-1), q=p^n$ の ideal の形で表現される加法群として与えられ、その生成元である、生成多項式がその符号の性質を左右する因子であった。ここでは、更にすすんで、符号を特徴付ける数学的概念を導入する。

Definition 3.1 ガロア群 $Gal(\overline{F_q}/F_q)$ の、生成多項式の解（F_q 有理点）を基底とする表現空間への表現を符号に付随したガロア表現という。

Example 3.1 $F:=F_q$,
$m \geq 2$ を $(q, m)=1$ である自然数、
$\zeta = \zeta_m$ を（Fの代数的閉包に含まれる）1の原始m乗根、
$K := F(\zeta)$,
ζ を根に持つ既約多項式を生成元とする符号に付随したガロア表現を ρ,
$Ker(\rho)$ に対応するガロア拡大を κ
とおくと以下が成立する。

$$K \simeq \kappa,$$

$$f := [K : F] = [F(\zeta) : F] = \textit{the order of } q \textit{ modulo } m \textit{ in } (Z/(m))^*$$

$$G(K/F) \simeq < q(mod\ m) > \simeq Im(\rho)$$

すなわち $G(K/F)$ は $q\ (mod\ m)$ の生成する $(Z/(m))^*$ の巡回部分群に同型である。

4 符号概念の拡張

前節では、符号を特徴付ける概念として、ガロア表現なるものを考えた。これを用いると、符号の持つ性質・群構造の複雑さなどをある程度知る事ができる。
例えば、次の事が成立する。

Theorem 4.1 有限体 F_q *(char=p)*
上に構成される伝統的な巡回符号に付随するガロア表現を ρ とするとき、
$Im(\rho)$ は巡回群となる。

Proof.
定義より、巡回符号の生成多項式の最小分解体のガロア群を調べればよい。
$Gal(K/F_q)$, （但し K は生成多項式の最小分解体）は、位数 $[K : F_q]$ の巡回群となっているので、定理の主張は成立する。 ∎
従って、巡回符号の特殊性はガロア表現の像に反映されている。
次に、巡回符号をガロア表現の意味で拡張することを考える。

Definition 4.1 k を完全体（有限体は完全体）、$\overline{k}$;k の代数的閉包
$K := k(x_1, x_2, ..., x_n)$ を k 上の n 変数有理関数体,
a_1,a_2,...,a_n をn個の k 上代数的独立な元,
$F := k(a_1, a_2, ..., a_n)$,
$f(X) := X^n + a_1X^{n-1}+, ..., +a_n$
とする。
このとき有限生成環 $F[X]/(X^m-1)$ のイデアル
を拡張された巡回符号と呼ぶ。

このとき，次の問題が基本的である.

Problem 4.1 *G*; 与えられた有限群
このとき、ある拡張された巡回符号が存在して、それに付随した $Gal(\overline{k}/k)$ のガロア表現 ρ に対して次が成立するか.
$Im(\rho) \simeq G$

Proposition 4.1 上の *Definition* の記号のもとで、次が成立する。
イデアル $(f(X))$ に対応するガロア表現を ρ とするとき、

$$Im(\rho) \simeq S_n$$

但し、S_n は n 次対称群

Proof.
多項式 $f(X)$ の F に関する最小分解体を $K' := F(\alpha_1, \alpha_2, ..., \alpha_n)$,$f(X) = \prod_{i=1}^{n}(X - \alpha_i)$ とする.
このとき,
$a_1 = -\sum_{i=1}^{n} \alpha_i, a_2 = \sum_{i<j}^{n} \alpha_i\alpha_j, ..., a_n = (-1)^n\alpha_1\alpha_2...\alpha_n$.
より, $K' = F(\alpha_1, ..., \alpha_n) = k(a_1, ..., a_n, \alpha_1, ...\alpha_n) = k(\alpha_1, ...\alpha_n)$.
また, $g(x) := \prod_{i=1}^{n}(X - x_i) = X^n + \overline{a_1}X^{n-1} + ... + \overline{a_n}$ とするとき, $F' := k(\overline{a_1}, ..., \overline{a_n}) \subseteq K$ とおけば, K/F' は $n!$ 次のガロア拡大であり, そのガロア群は $Gal(K/F') \simeq S_n$ である.
このとき容易に, K' から K の上への k 同型 $\varphi : K' \longrightarrow K$ であって,
$\varphi(\alpha_i) = x_i, (1 \leq i \leq n)$ となるものが存在することが示せるので, K/F' と K'/F はガロア拡大で, $Gal(K/F') \simeq Gal(K'/F) \simeq S_n$ である. 従って, 求める結果を得る. ∎

従って, 上記の問題に対する解答としては 最も簡単な巡回群に対する場合, すべての有限群を, その部分群として持つ対称群に対しては肯定的である. ここでこの問題に対する理解を深めるために有限単純群の分類定理について説明する.
有限単純群の分類が完成されたのは１９８１年頃といわれており, それは次のような定理としてまとめられている.

Theorem 4.2 任意の有限単純群は次の群のどれかと同型である.

1. 素数位数の群
2. ５次以上の交代群
3. １６の系列からなるリー型の群
4. ２６個の散在型単純群

ここで, リー型の群とは, ９系列のシュバレイ群, ４系列のスタインバーグ群, 鈴木群, ２系列の李群を意味する. また散在型単純群とは, ある特定の系統的な規則に基づいて構成されないような群で, 種々の分野で別々に発見されてきた特に大きな位数を持つ単純群のことである. その中で, 符号理論と関係の深いものは, マシュー群 M_{24} (これはスタイナーシステムＳ（５, ８, ２４）の自己同型群）と *Conway* の $\bullet O$ （これは, *Leech* 格子の自己同型群）である.

Definition 4.2 *(type of code)*
Prop 4.1 で考えた符号に対して *type* A_{n-1} という名称を与えることにする. これは, A_{n-1} のワイル群 $W(A_{n-1})$ が対称群 S_n に同型であることによる.

この定理から, 問題 4.1 に対する解答は, 有限群として上記定理中の（３）, （４）の単純群に対して, 確かめればよい. しかしこの解答を与えることは非常に難しい. だが, Ｇが巡回群や対称群以外のある群に対してこの問題を解けることを以下の節で, 示す. それには, 楕円曲線の代数的サイクルに対する Mordell-Weil lattice の理論を用いる.

5 Mordell-Weil lattice 理論

Definition 5.1 *(Mordell-Weil gourp)*
K;体
K 上の楕円曲線　E/K とは，次のような標準的な方程式で定義される代数曲線である．

$$y^2 = x^3 + Ax + B, (A, B \in K, 4A^3 + 27B^2 \neq 0)$$

また

$$E(K) := \{P = (x, y) \in E \mid x, y \in K\} \cup O, where\ O = \infty$$

を E の K ー有理点と呼ぶ．$E(K)$ は O を単位元とするアーベル群の構造を持つ．この群を *Mordell-Weil* 群と呼び，今世紀初頭より数論や代数幾何の研究対象として研究されているが，なかなか奥の深い対象である．また $E(K)_{tor}$ を $E(K)$ のねじれ部分群とする．

Definition 5.2 （代数的サイクル）
代数多様体 X の（余次元 d の）既約部分多様体 Z_i の整係数一次結合 $Z := \sum n_i Zi$ を，X 上の（余次元 d の）代数的サイクルという．それらの全体を $Z^d(X)$ と書く．また各 Z にそのコホモロジー類を対応させるサイクル写像 $\gamma : Z^d(X) \to H^{2d}(X)$ の像 $C^d(X)$ も代数的サイクルと呼ぶ．とくに，正標数において $H^{2d}(X) = C^d(X)$ となるとき，X は余次元 d で超特異的という．

さて代数的サイクル E(K) に適当な内積を定義して，この群を格子 (lattice) として考えようという研究が Mordell-Weil lattice の理論と呼ばれるものであり，これは代数学，群論，数論，代数幾何等の色々な分野の諸現象間の，これまで見過ごされていた興味深い関係を我々に示してくれる理論である．

Definition 5.3 (T.Shioda) *(Mordell-Weil lattice (MWL))*
紙数の関係で，正確な定義は原典にあたっていただくとして，ここでは定義のあらすじを述べるだけにとどめる．
定義体 $K = k(t)$; 体 k 上の 1 変数代数関数体とする．一般には K は，ある代数曲線 C/k の関数体 $k(C)$ でよい．
まず K 上の楕円曲線 E に対し，自然に構成される楕円曲面（小平ー *Néron model*）$f : S \to C$ を考え，その *Néron-Severi group* を $NS(S)$ とする．この楕円曲面はそのファイバーをとれば，K 上の楕円曲線とみなすことができ，断面のなす群は $E(K)$ と同型になる．いま T を，零断面 (O) とファイバーの規約成分全体で生成される $NS(S)$ の部分群とするとき，$E(K) \cong NS(S)$ が成立する．そしてこの同型を用いて次のような準同型が一意的に定義できる．

$$\varphi : E(K) \to NS(S) \otimes Q,\ such\ that\ Im(\varphi) \perp T,\ \varphi(P) \equiv (P) mod T \otimes Q,\ Ker(\varphi) = E(K)_{tor}$$

但し，$P \in E(K)$ に対し，P に対応する断面を (P) と書いている．さて，代数曲面 S には，交点理論によって S 上の因子 D, D' に対し交点数 $(D.D')$ が定義されこれが $NS(S)$ 上に *bilinear pair* を誘導する．そこで，上記の写像 φ によって，$E(K)$ を $NS(S)$ に埋め込むことによって $E(K)$ 上に *symmetric bilinear form* を交点数を用いて次のように定義する．

$$\langle P, P' \rangle := -(\varphi(P).\varphi(P'))$$

これを *height pairing* という．このとき，$E(K)/E(K)_{tor}$ は $\langle\ ,\ \rangle$ に関して　*positive lattice* になり，また，

$$E(K)^0 := \{P \in E(K); ((P)\Theta_{v,0}) = 1,\ for\ all\ reducible\ fiber\ and\ \Theta_{v,0}\ with\ (\Theta_{v,0}(O)) = 1\}$$

は $\langle\ ,\ \rangle$ に関して　*positive even integral lattice* となる．これらを各々 *Mordell-Weil lattice* および *narrow Mordell-Weil lattice* $(E(K)^0$ と書く$)$ という．

次の節ではこのMWLから生じるガロア表現を用いて問題 4.1 を解くことを試みる．

6 Mordell-Weil lattice 理論の適用

k_0 を完全体，$\lambda := (p_i, q_j), (0 \leq i, j \leq s), (s = 2, 3, 4)$ を k_0 上代数的独立とする．$k_{0\lambda} := k_0(\lambda) = k_0(p_i, q_j)$ $k := \overline{k_{0\lambda}}$ をその代数的閉包，$G = Gal(k/k_{0\lambda})$ とする．$K_0 = k_0(t)$, $K = k(t)$ を各々 k_0,k の関数体とする．このとき次が成立する．

Theorem 6.1 $\lambda=(p_i,q_j),(0\le i,j\le s),(s=2,3,4)$ を k_0 上代数的独立とする．このとき
$k_0(\lambda)[X]/(X^m-1)$ の巡回符号として下記のような多項式 $\Phi_r(X;\lambda)\in k_0(\lambda)[X]$ で生成されるイデアルをとれば，
それに付随したガロア表現 ρ_λ に対し，

$$Im(\rho_\lambda)=W(E_r),(r=6,7,8)$$

となる．
ここで，$\Phi_r(X;\lambda)$ は次のような多項式である．

$$\Phi_r(X;\lambda)=\begin{cases} a\ polynomial\ of\ degree\ 27, & for\ r=6\\ a\ polynomial\ of\ degree\ 56, & for\ r=7\\ a\ polynomial\ of\ degree\ 240, & for\ r=8\end{cases}$$

Proof. (construction of $\Phi_r(X;\lambda)$)
r=6, 7, 8 に対して，次のような楕円曲線 E_λ を選んでやる．

$E_\lambda: y^2=x^3+p(t)x+q(t)$
このとき p(t), q(t) は各々下記のようなものである．

$$p(t)=\begin{cases}\sum_{i=0}^{2}p_it^i, & \text{for r=6}\\ p_0+p_1t+t^3, & \text{for r=7}\\ \sum_{i=0}^{3}p_it^i, & \text{for r=8}\end{cases},\quad q(t)=\begin{cases}\sum_{j=0}^{2}q_jt^j, & \text{for r=6}\\ \sum_{j=0}^{4}q_jt^j, & \text{for r=7}\\ \sum_{j=0}^{3}q_jt^j+t^5, & \text{for r=8}\end{cases}$$

するとこのとき，E_λ の MWL に対して次が成立する．

$$E_\lambda(k(t))\cong E_r^*,\ (dual\ lattice\ of\ E_r)$$

そこで，この MWL の，lattice E_r^* としての性質を利用して $\Phi_r(X;\lambda)$ を以下のように定義する．

$$\Phi_r(X;\lambda)=\prod_{P\in I}(X-sp'_\infty(P))$$

ここで，sp'_∞ は特異ファイバー $f^{-1}(\infty)$ に対して定義された specialization map, I は $E_\lambda(k(t))\cong E_r^*$ の minimal vector 全体である．その個数を評価する事によって $\Phi_r(X;\lambda)$ の次数は定理の主張と一致することがわかる．
さらに，$\Phi_r(X;\lambda)$ の $k_0(\lambda)$ 上の最小分解体が下記の Theorem における κ に一致し，しかもそのガロア群が $W(E_r)$ となることも示せる．従って定理の主張は，すべて示された． ∎

（注 1） Theorem 6.1 で定義した符号に対して type E_r, $(r=6,7,8)$ という名称を与えることにする．理由は，Def4.2 と同じである．

（注 2） G は E(K) にも作用し，G の表現 $\overline{\rho}: G\to Aut(E(K))$ が自然に定義され，しかも hight pairing の定義から

$$\langle P^\sigma,Q^\sigma\rangle=\langle P,Q\rangle,(\sigma\in G,\ P,Q\in E(K))$$

となるので，$\overline{\rho}$ は lattice automorphism group への homomorphism になっており，証明中の I は G-invariant な $E_\lambda(K)$ の有限集合となっている．

（注 3） G の $E_\lambda(K)$ 上のガロア表現 $\overline{\rho_\lambda}$ の像は，各々，

$$Aut(E_\lambda k(t))\supset Aut(E_r)=\begin{cases}W(E_r), & \text{for r=8, 7}\\ W(E_r)\cdot\{\pm1\}, & \text{for r=6}\end{cases}$$ に含まれる．このとき次が知られている．

Theorem 6.2 (T. Shioda) $\lambda=(p_i,q_j)$ が k_0 上代数的独立なる仮定の下に以下が成立する．
(1) $Im(\overline{\rho_\lambda})=W(E_r)$
(2) $Ker(\overline{\rho_\lambda})$ に対応する $k_0(\lambda)$ の拡大を κ とすると $\kappa=k_0(\lambda)(u_1,...,u_r)=k_0(u_1,...,u_r)$,
ここで，$u_i=sp'(P_i)$, $\{P_i\}_{i=1,...r}$ は *lattice* $E_\lambda(k(t))$ の *minimal vector* であるような生成元，
sp' は *specialization map*. このとき $u_i,(i=1,...,r)$ は k_0 上代数的独立である．
(3) $k_0[u_1,...,u_r]^{W(E_r)}=k_0[p_i,q_j]$

7 むすび

本稿では，関数体上の楕円曲線に関するMWLの有意義な性質を符号理論へ応用するために，代数的符号のクラスに限定して，議論をしてきた．これまでにわかった事実を結果としてまとめると以下のようになる．

1. 巡回符号に代表される代数的符号を含む，新しい符号のクラスを定義し，拡張された巡回符号と名づけた．そして，このクラスの符号の性質を計る新しい尺度として，符号に付随したガロア表現なる概念を導入し，これを用いて，新しい符号のクラスが従来の巡回符号のクラスを真に包含することを示した．

2. 適当な有限群を与えて，それをガロア表現の像として持つような符号を求めるという，符号の逆構成問題を提示し，それに対する部分的な解答を与えた．

3. 上記の問題に対する解として特徴的なものに対し，その分類名称を与えることを提案した．

4. 上記の問題に対する解法として，一般的ではないが，”半単純リー環の root lattice に関連の深い，（適当な関数体上定義された）楕円曲線を選び，次にその有理点上のガロア表現 $\bar{\rho}$ を調べ，$Ker(\bar{\rho})$ に対応する拡大体を求め，そして，MWLの理論を用いて，その拡大体を最小分解体として持つような代数方程式を決定する．”という方法を提案した．

5. このようにして定義された符号は，従来の代数的符号が代数的拡大の範囲内で構成されていたのに対し，必ずしも代数的でない拡大体の範囲内でも構成される．また，一度構成した符号の代数的独立な元に適当な値を代入する事により，符号を有理化することも可能である．

このようにして，楕円曲線が，拡張された意味での代数的符号の構成に応用できた原因は，MWLの理論がガロア群の表現を強烈に意識している点にある．従って，次に生ずる問題として，この理論が代数幾何学的符号の構成に応用できるかということが挙げられる．この点については現時点では不明な点が多いが，興味を惹かれる現象は，あるsupersingular curve のMWLが，sphere packing problem の良い解を与えるという事実である．このことから著者は，MWLがConway と Goppa に相撲をとらせるための良い土俵となるのではないかと考えている．

8 補

実をいうと本文の内容は、著者の研究の進展の結果、かなりの加筆訂正の必要なものになっていますが、残念ながら著者の怠慢のために原稿提出期日までに、訂正版の原稿が仕上がりませんでした。従って内容のわかりにくさは、著者に全面的に責任があります。本論文の内容に興味を持たれる方は、著者まで、御連絡頂ければ、増補大訂正版のプレプリントをお送りします。（かなり内容が変わっております。）

参考文献

[1] Conway, J., Sloan, N. *Sphere Packings, Lattices and Groups*, Springer-Verlag, 1988.

[2] Shioda, T. *The Galois representation of type E_8 arising from certain Mordell-Weil groups*, Proc. Japan Acad., 65A(1989), 195-197.

[3] Shioda, T. *Mordell-Weil lattices and Galois representation*, Preprint.

[4] Serre, J-P. *Lectures on the Mordell-Weil Theorem*, Veiweg 1989.

[5] Imai, J. *Galois Representation and Coding Theory*, preprint