数理解析研究所講究録 1228 巻 2001 年 69-75

有限素体上定義された Modular Code の構成について

杉山 健一 (Kennichi SUGIYAMA)
所属：千葉大学 (Chiba University)

2001 年 2 月 20 日

1 はじめに

通信衛星を用いて情報の交換を行う際に、様々な理由により、伝達される情報に誤りが生じるのは避けられないことである。その誤りを訂正するために考えられた情報伝達手段が符号理論であった。この論説では、まず符号理論の復習をし、どのような符号が良いものとされるかをまず解説する。その後、Ihara, Tsfasman-Vladut-Zink による $\mathbf{F}_{p^2}$ 上の良い符号を modular curve を用いて構成する方法について説明をする。また、彼らの方法と Artin-Schreier 理論とを組み合わせて $\mathbf{F}_p$ 上の良い符号が得られることも併わせて説明させて頂く。

2 符号理論の復習

この章では有限体上定義された曲線を用いて符号を構成する、いわゆる代数幾何符号について復習をする。以下 p は素数とする。

そもそも符号とは 有限体 $\mathbf{F}_q(q = p^f)$ 上の線型空間 V とその部分空間 W の組 (V, W) のことであった。$f = (f_1, \cdots f_n) \in V$ に対し、その weight $wt(f)$ を 0 でない成分 f_i の個数と定義し、W の weight $wt(W)$ を $wt(W) = \mathrm{Min}\{wt(f) \mid f \in W, f \neq 0.\}$ と定める。伝達したい情報に W の元を対応させて情報を送るのであるが、その時、$wt(W)$ は符号の誤り訂正可能な能力を表わしたのであった。よって、V の次元 n を固定した上で (以下、V と $\mathbf{F}_q^n$ を同一視する)、より良い符号とは $\mathbf{F}_q^n$ の部分空間 W で次元が大きく (i.e. 情報伝達量が多い)、また $wt(W)$ が大きい (i.e. 誤り訂正可能な能力が大きい) ものとなる。そのような符号を代数曲線を用いて構成する方法があり、代数幾何符号といわれている。以下この構成方法について解説をする。

X を $\mathbf{F}_q$ 上の滑らかな射影代数曲線とし、その種数を g_X で表わす。ま

た、$X(\mathbf{F}_q)$ で X 上の $\mathbf{F}_q$ 有理点を表わし、$X(\mathbf{F}_q)=\{P_1,\cdots,P_n\}$ とする。$G=\sum_{i=1}^{N}Q_i$ を X 上の effective divisor で $\mathbf{F}_q$ 有理 (i.e. Galois 群の作用で不変) なもので、かつ任意の i について $P_i\notin \mathrm{supp}G$ なものとする。以下の議論では、常に次の仮定をおく。

仮定 $2g_X-2<\deg G(=N)<n$.

$\mathcal{L}(G)$ で G により定まる $\mathbf{F}_q$ 上の linear system とすると、$f\in\mathcal{L}(G)$ は、$P_1,\cdots,P_n$ で正則であることに注意する。従って線型写像

$$\mathcal{L}(G)\xrightarrow{\Phi}\mathbf{F}_q^n, \tag{1}$$

が、$\Phi(f)=(f(P_1),\cdots,f(P_n))$ により定義され、これは次の性質を持つことがわかる。

命題 2.1 仮定の下に次が成立する。

1. Φ は単射で、$\dim\mathrm{Im}\Phi=\deg G-g_X+1$。
2. $wt(\mathrm{Im}\Phi)\geq n-\deg G$。

補足 2.1 $\deg G>2g_X-2$ より例えば、$\deg G=2g_X-1$ と取ると、

- $\dim\mathrm{Im}\Phi=g_X$、
- $wt(\mathrm{Im}\Phi)\geq g_X(\frac{n}{g_X}-2)+1$、

がわかる。従って、この場合 g_X が大きいと情報伝達量が多くなり、さらに $\frac{n}{g_X}$ が大きいと誤り訂正能力が大きくなる。

例 2.1 *(Reed-Solomon 符号)* X として $\mathbf{F}_q$ 上の射影直線 $\mathbf{P}^1_{\mathbf{F}_q}$ を用いる。また、$\mathbf{F}_q$ の元を $\{0,\cdots,q-1\}$ と番号付けて、$\mathbf{P}^1_{\mathbf{F}_q}$ 上の有理点として $P_i=[i:1]$ を用いる。また、$Q=\infty=[1:0]$, として $G=mQ$ ととる。この時 仮定は $-2<m<q$ となり、$\mathcal{L}(G)$ は $\mathbf{F}_q$ を係数に持つ m 次以下の多項式全体となる。線型写像 Φ は

$$\Phi(f)=(f(0),\cdots,f(q-1))$$

で与えられ、$\dim\mathrm{Im}(\Phi)=m+1$, $wt(\mathrm{Im}\Phi)\geq q-m$ となる。

以上の説明より、次の動機には説明を要しないだろう。

動機 $\mathbf{F}_q$ 上の射影代数曲線 X で、その種数 g_X ならびに $\frac{|X(\mathbf{F}_q)|}{g_X}$ の大きいものを構成したい。(一般に、集合 A の濃度を $|A|$ で表わすことにする。)

3 様々な評価

以下、次の記号を用いる。

記号 3.1 • $N_q(g) = \sup_X\{|X(\mathbf{F}_q)|\}$ 、ここで X は $\mathbf{F}_q$ 上の射影代数曲線でその種数が g となるものを走らせる。

• $\alpha(q) = \limsup_{g\to\infty} \frac{N_g(q)}{g}$。

これらの不変量について次に評価が知られている。

事実 3.1 *1. (Drinfeld-Vladut)* $\alpha(q) \leq \sqrt{q} - 1$.

2. (Kresch-Wetrell-Zieve) 勝手な q に対し、$\lim_{g\to\infty} N_q(g) = \infty$ が成立する。

また、$f = 2$ の時は、伊原先生、Tsfasman-Vladut-Zink, Garcia-Stichtenoth によりそれぞれ独立に次の事実が示されている。

事実 3.2 $\mathbf{F}_{p^2}$ 上定義された射影代数曲線の列 $\{X_l\}_l$ で、$\lim_{l\to\infty} g_{X_l} = \infty$、でかつ、$\lim_{l\to\infty} \frac{|X_l(\mathbf{F}_{p^2})|}{g_{X_l}} = \sqrt{q} - 1$ を満すものが存在する。従って、$q = p^2$ の場合は、*Drinfeld-Vladut* による評価は *best possible* となる。

補足 3.1 伊原先生、*Tsfasman-Vladut-Zink* は、次の章で見るように、*modular* 曲線の理論を用いた。一方で、*Garcia-Stichtenoth* は *Artin-Schreier* 理論を用いている。

我々の問題意識は Drinfeld-Vladut による評価が $q = p$、つまり基礎体が有限素体の場合にも best possible となるか、というものである。この問題を扱う前に (我々の議論においても必要であるため)、伊原先生、Tsfasman-Vladut-Zink による曲線の構成を次の章で復習することにする。

4 Modular Curves を用いた符号の構成 (After Ihara, Tsfasman-Vladut-Zink)

今、N を自然数で p と互いに素なものとする。また、$\Gamma_0(N)$ を Hecke 合同部分群；

$$\Gamma_0(N) = \{\gamma \in SL_2(\mathbf{Z}) \mid \gamma \equiv \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mathrm{mod} N\} \tag{2}$$

とし、この群でポアンカレ上半平面をわって得られるリーマン面にカスプを添加してコンパクト化したものを $X_0(N)(\mathbf{C})$ と書く。この時、$X_0(N)(\mathbf{C})$ は、$\mathbf{Z}[\frac{1}{N}]$ 上の滑らかで自然なモデルを持つことが知られている。このモデルを mod p reduction したものを $X_0(N)_{\mathbf{F}_p}$ で表す。この章では、前章における理論をこの $X_0(N)_{\mathbf{F}_p}$ 及びその上の $\mathbf{F}_{p^2}$ 有理点 $X_0(N)_{\mathbf{F}_p}(\mathbf{F}_{p^2})$ に対して適用する。まず $|X_0(N)_{\mathbf{F}_p}(\mathbf{F}_{p^2})|$ の下からの評価を求めよう。

$X_0(N)$ は 楕円曲線 E とその N 等分点の成す部分群 Γ の対 (E,Γ) をパラメトライズすることに注意して、

$$\Sigma_0(N) = \{(E,\Gamma) \mid E \quad \text{is a supersingular elliptic curve over} \quad \overline{\mathbf{F}_p}\}, \quad (3)$$

とおく。ここで $\overline{\mathbf{F}}_p$ 上の楕円曲線が supersingular とは p 倍写像が純非分離であるときにいう。(E が supersingular の時、点 (E,Γ) を supersingular 点という。) 一般に $\Sigma_0(N) \subset X_0(N)(\mathbf{F}_{p^2})$ が知られており、また $\Sigma(N)$ は Hasse 不変量といわれる $\mathbf{F}_p$ 上の重み $p-1$ の保型形式 A の 0 点 (multiplicity free) であることもわかっている。よって、$g_0(N)$ を $X_0(N)$ の種数、$c_0(N)$ を $X_0(N)$ のカスプの個数として、良く知られた公式

$$\deg A = (p-1)(g_0(N)-1) + \frac{p-1}{2}c_0(N), \quad (4)$$

を用いることにより、

$$\mid X_0(N)_{\mathbf{F}_p}(\mathbf{F}_{p^2}) \mid \geq \mid \Sigma_0(N) \mid = \deg A = (p-1)(g_0(N)-1) + \frac{p-1}{2}c_0(N), \quad (5)$$

という評価を得る。$\lim_{N\to\infty} g_0(N) = \infty$ 及び $\lim_{N\to\infty} \frac{c_0(N)}{g_0(N)} = 0$ より

$$\liminf_{N\to\infty} \frac{\mid X_0(N)(\mathbf{F}_{p^2}) \mid}{g_0(N)} \geq p-1, \quad (6)$$

が得られる。以上により、$q = p^2$ の時は、Drinfeld-Vladut による評価式は best possible であることがわかった。

5 An Artin-Schreier Tower

前章で Drinfeld-Vladut による評価は $q = p^2$ の時は、Best Possible であることがわかった。それでは、$q = p$、つまり 定義体が有限素体の場合はどうであろうか。これがこれからの問題である。この問題を扱う際に有効な手段として、曲線の Artin-Shreier 理論がある。この章ではこの理論について解説しよう。

まず一般論から。

事実 5.1 k を $\mathbf{F}_p$ の有限次拡大とし、F を k 上の一変数関数体とする。今 $u \in F$ がどんな $w \in F$ を用いても $u = w^p - w$ と書けないとする。F' で F の *Artin-Schreier* 拡大

$$F' = F(y), y^p - y = u$$

は次の性質を満たす。

1. F'/F は p 次の巡回拡大

2. $\mathbf{P}_F$ で F の付値全体の成す集合を表わすとする。$P \in \mathbf{P}_F$ に対し整数 m_P を次の要領で与えることにする；

   もし $z \in F$ で p が $\mathrm{ord}_P(u-(z^p-z))$ を割り切らないものがとれたとすると、$m_P = -\mathrm{ord}_P(u-(z^p-z))$ と置く。また、ある $z \in F$ を用いて $\mathrm{ord}_P(u-(z^p-z)) \geq 0$ とできるのなら $m_P = -1$ とおく。*(m_P は well-defined であるとが知られている。)*

   以上の準備のもとに、P が F'/F で不分岐であるための必要十分条件は $m_P = -1$ である。また、P が F'/F で完全分岐するための必要十分条件は $m_P > 0$ である。
3. もし $Q \in \mathbf{P}_F$ で $m_Q > 0$ となるものがあったとすると、k は F' 内で代数的閉である。また $g'(resp.g)$ で $F'(resp.F)$ の種数を表わすものとすると、公式

   $g' = pg + \frac{p-1}{2}(-2 + \sum_{P \in \mathbf{P}_F}(1+m_P)\mathrm{deg}P)$

   が成立する。

X を $\mathbf{F}_p$ 上の滑らかな射影代数曲線とし、f を X における $\mathbf{F}_p$ 上定義された有理関数とする。更に、P_f で f の極全体の成す集合を表わすものとする。$P \in P_f$ で p が $\mathrm{ord}_P f$ を割らないものがあったとすると、X 上のどんな有理関数 g を用いても $f = g^p - g$ と書けないことがすぐにわかる。したがって、上記の事実より Artin-Schreier 拡大

$$Y = \{T^p - T\} \xrightarrow{\pi} X \tag{7}$$

は p 次巡回拡大で点 P で完全分岐することがわかる。P 上の (唯一つの) 点を Q と書くと、Y 上の有理関数 $g = T \cdot \pi^* f$ は $\mathbf{F}_p$ 上定義され、Q で極を持ちその位数は p で割り切れないことが直ちに分る。この構成を順次繰り返して、$\mathbf{F}_p$ 上の滑らかな射影代数曲線 X_n、X_n における $\mathbf{F}_p$ 上の有理関数 f_n、X_n の点 P_n から成る三つ組 $\{(X_n, f_n, P_n)\}_{n \geq 0}$ が得られる：

- $X_0 = X$, $f_0 = f$, $P_0 = P$.
- $X_n = \{T_n^p - T_n = f_{n-1}\} \xrightarrow{\pi_n} X_{n-1}$.
- $f_n = T_n \cdot \pi^* f_{n-1}$.

f_n は P_n で極を持ちその位数は p で割り切れないことが分る。また、これより拡大 $X_n = \{T_n^p - T_n = f_{n-1}\} \xrightarrow{\pi_n} X_{n-1}$ は P_{n-1} 上完全分岐することも分る。従って、点 P_n を

- P_n は P_{n-1} 上の唯一つの点、

と定義する。次に、X_n の $\mathbf{F}_p$ 有理点の個数の下からの評価を求めよう。そのために

$$\Sigma_0 = \{x \in X_0(\mathbf{F}_p) \mid f_0(x) = 0\}, \tag{8}$$

を考える。また、$\Sigma_n = \pi_{n-1}^{-1}(\Sigma_{n-1})$ と定めると、$\Sigma_n \subset X_n(\mathbf{F}_p)$ で $X_n \xrightarrow{\pi_n} X_{n-1}$ は Σ_{n-1} 上エタールでとなる。従って特に

$$| X_n(\mathbf{F}_p) | \geq | \Sigma_n | = p^n | \Sigma_0 | \tag{9}$$

を得る。一方、g_n で X_n の種数を表わすとすると、**事実 5.1** より

$$g_n = p^n \cdot g_0 + (p^n - 1)(\frac{1}{2} | P_f | - 1) - \frac{p-1}{2}\{(p+1)^n - p^n\} \cdot \sum_{P \in P_f} \mathrm{ord}_P(f) \tag{10}$$

が得られる。以上より次の命題が得られた。

命題 5.1 $\liminf_{n\to\infty} \frac{(p+1)^n |X_n(\mathbf{F}_p)|}{p^n \cdot g_n} \geq -\frac{2|\Sigma_0|}{(p-1)\sum_{P\in P_f} \mathrm{ord}_P(f)}$.

6 $\mathbf{F}_p$ 上定義された符号の構成

この章では、$\mathbf{F}_p$ 上の滑らかな射影代数曲線 X とその上の $\mathbf{F}_p$ 上定義された有理関数 f で、任意の $P \in P_f$ について p が $\mathrm{ord}_P f$ を割らないものの構成ならびに、このような対 (X, f) に対し Σ_0 の個数を具体的に求めることを目標にする。

まず、N と p を 奇素数で $N > p$ なるものとする。X として modular 曲線 $X_0(N)$ の mod p reduction をとることにする。

次に f の構成について述べる。m を 12 と $p-1$ の最小公倍数とする。すると $A^{\frac{m}{p-1}}$ (A は Hasse 不変量) は重み m の保型形式なり、f を $f = \frac{A^{\frac{m}{p-1}}}{\Delta^{\frac{m}{12}}}$ (Δ は重み 12 の Jacobi 形式) と定めると、f はカスプ 0 と ∞ で極を持ち、それぞれの位数は

$$\mathrm{ord}_\infty(f) = -\frac{m}{12}, \quad \mathrm{ord}_0(f) = -\frac{mN}{12}, \tag{11}$$

となる。これより、(X, f) は **命題 5.1** の仮定を満たすことがわかる。また f の零点は supersingular 点 と一致し、前章のおける Σ_0 は $\mathbf{F}_p$ 有理な supersingular 点全体 $\Sigma_0(N)(\mathbf{F}_p)$ となる。

次に $\Sigma_0(N)(\mathbf{F}_p)$ の個数を求めよう。一般にレベル $\Gamma_0(M)$、重みが 2 の正則カスプ形式の成す空間を $S_2(\Gamma_0(M))$ であらわすことにする。自然な写像

$$S_2(\Gamma_0(N)) \times S_2(\Gamma_0(N)) \longrightarrow S_2(\Gamma_0(pN)) \tag{12}$$

の cokernel を $S_2(\Gamma_0(pN))_{p-new}$ と書くことにすると、$S_2(\Gamma_0(pN))_{p-new}$ は Hecke 作用素 T_p で保たれ、次の公式が成り立つことがわかる。

定理 6.1 $| \Sigma_0(N)(\mathbf{F}_p) | = \mathrm{Tr}[T_p \mid S_2(\Gamma_0(pN))_{p-new}] + 1$。

特に、$S_2(\Gamma_0(N)) = \{0\}$ の時は、

$| \Sigma_0(N)(\mathbf{F}_p) | = \mathrm{Tr}[T_p \mid S_2(\Gamma_0(pN))] + 1$。

従って問題は $\mathrm{Tr}[T_p \mid S_2(\Gamma_0(pN))_{p-new}]$ あるいは $\mathrm{Tr}[T_p \mid S_2(\Gamma_0(pN))]$ を求めることに帰着されるがこれは Eichler-Selberg-土方 による跡公式を用いて求められる。具体的には、

定理 6.2 p と N を奇素数で $N > p$ なるものとする。さらに、$S_2(\Gamma_0(N)) = \{0\}$ と仮定すると次の等式が成立する。

$$|\Sigma_0(N)(\mathbf{F}_p)| = 1 + p - \frac{1}{p-1}\sum_{f\in\mathbf{N}, f|(p-1)} \varphi(\frac{p-1}{f})$$
$$- \sum_{s\in\mathbf{Z}, s^2-4p<0}\{1 + (\frac{s^2-4p}{N})\}\sum_{f\in\mathbf{N}, f|t} h(\frac{s^2-4p}{f^2})/w(\frac{s^2-4p}{f^2}).$$

ここで次の記号を用いた。

- $(\frac{\cdot}{\cdot})$ は *Legendre* 記号.
- φ は *Euler* 関数.
- 負の整数 d に対し, $h(d)$ *(resp.* $w(d)$*)* は $\mathbf{Q}(\sqrt{d})$ の整数環の類数 *(resp.* 単数の位数*)* を表わす。
- $s^2 - 4p < 0$ なる整数 s に対し, 正の整数 t を次の要領で定める：

$$\begin{cases} t^2 m = s^2 - 4p, & \text{もし } 0 > m \equiv 1(4), \\ 4t^2 m = s^2 - 4p, & \text{もし } 0 > m \equiv 2, \text{ あるいは } 3(4). \end{cases}$$

ここで m は *square free* の整数である。

これと **命題 5.1** とを併わせて $\mathbf{F}_p$ 上の滑らかな射影代数曲線の族 $\{X_n\}_n$ で

$$\liminf_{n\to\infty} \frac{(p+1)^n |X_n(\mathbf{F}_p)|}{p^n \cdot g_n} \geq$$
$$\frac{24}{m(p-1)(1+N)}\{1 + p - \frac{1}{p-1}\sum_{f\in\mathbf{N}, f|(p-1)} \varphi(\frac{p-1}{f})$$
$$- \sum_{s\in\mathbf{Z}, s^2-4p<0}\{1 + (\frac{s^2-4p}{N})\}\sum_{f\in\mathbf{N}, f|t} h(\frac{s^2-4p}{f^2})/w(\frac{s^2-4p}{f^2})\}$$

なるものが構成された。