代数幾何符号とモジュラー曲線

(第 19 回 津田塾大学 数学史シンポジウム)

平松 豊一 (法政大学)　斎藤 正顕 (工学院大学)　松田 修三 (法政大学)

2008 年 10 月 11 日

§1. はじめに

1.1 情報理論の主テーマは符号化 (encoding) で, そのうち信頼性の向上を扱うのが符号理論である (通信路符号化という). 伝達される情報はブロックにして符号化される. その基礎理論は, 1948 年に

C.E. Shannon : A Mathematical Theory of Communication

で確立された :

通信路符号化定理 (Shannon の第 2 基本定理)

符号伝送率が, 通信路が伝送できる情報量を表す通信路容量より小さいなら, ブロックの長さが十分長い符号を使うかぎり復号誤りの確率をいくらでも小さくして情報を伝送することができる.

上で云う誤り訂正できる能力を備えた良い符号を構成することが問題になる. それには代数的手法が有効である (最近では, LDPC 符号). また効率的に復号 (decoding) することも大切な factor の 1 つである.

1.2 GF(2) 上の n 次元線形空間を V とする. V 内の k 次元部分空間を 2 元 (n,k) 線形符号といい, C とかく. (n,k) 符号 C の元 x ($x \neq 0$) の 0 でない成分の個数を x の重みといい, その最少なものを C の (最小) 重みといい, $d(C)$ ($= d$) で表す. このとき, C は $t = \left[\dfrac{d-1}{2}\right]$ 個またはそれ以下の誤りを訂正できる.

さて, 良い符号の条件とは? n, k が与えられたとき, 重み d が出来るだけ大きいことが望ましい (このとき, 復号誤り確率がより小さくなる). 具体的に述べる. (n,k) 符号 C の基ベクトルを行とする行列を C の生成行列といい, G で表す. このとき,

$$\phi : \mathrm{GF}(2)^k \ni u \longmapsto x = uG \in \mathrm{GF}(2)^n$$

なる線形写像 ϕ を符号化といい, $\phi(u) = x$ が C の元 : 符号語である. 即ち

$$C = \mathrm{Im}\,\phi = \{\, uG : u \in \mathrm{GF}(2)^k \,\}.$$

そして, 与えられた n, k に対し

$$d \leqq n - k + 1 \quad \text{(Singleton 限界)}$$

が成立する. この d を最大にするような ϕ : rank k の $k \times n$ 行列 G を決めることが問題である. このことをもう少し分析してみよう. n が与えられたとき, k が大きい方が効率がよく, また d が大きい方が誤り訂正能力が高く従って信頼性が増すことになる. しかし, 上の Singleton 限界は k と d が独立に勝手な値をとることが出来ないことを示している. つまり, k と d は trade off の関係にある.

§2. 代数幾何符号

1970 年になると, 従来多項式を用いて定義されていた符号が有理式を用いて定義される Goppa 符号として一般化される :

A new class of linear error-correcting codes

Goppa は, 更に 1 0年間の思索を続け, 1980 年になって, 代数幾何符号を発見した :

V.D. Goppa : Geometry and Codes, Kluwer, 1988.

2.1 pを素数とし, $q=p^{\ell}$ $(\ell \geqq 1)$, $m \in \mathbb{Z}^{+}$ とする. そして,

$$h(z) \in \mathrm{GF}(q^m)[x], \quad \text{monic},$$
$$D \subset \mathrm{GF}(q^m) - \{\, h(z)=0 \text{ の根} \,\},$$
$$n = \#D, \quad D = \{\alpha_1, \ldots, \alpha_n\}$$

とする.

$$\mathrm{GF}(q)^n \ni a = (a_1, \ldots, a_n) \mapsto \sum_{i=1}^{n} \frac{a_i}{z-\alpha_i} \in \mathrm{GF}(q^m)(z)$$

なる対応 $\phi_a(z)$ が次の条件

$$\phi_a(z) \equiv 0 \mod g(z)$$

をみたすとする. 即ち, a の台を

$$A = \{\, i : a_i \neq 0 \,\}$$

とし

$$\sigma_a(z) = \prod_{i \in A} (z-\alpha_i),$$
$$\eta_a(z) = \sum_{i \in A} a_i \prod_{\substack{i \in A \\ j \neq i}} (z-\alpha_j)$$

とおくとき, $\phi_a(z) = \eta_a(z)/\sigma_a(z)$ が成立し, 与えられた条件は

$$g(z) \mid \eta_a(z)$$

となる. そして, このようなベクトル a の作る $\mathrm{GF}(q)^n$ の部分空間を Goppa 符号といい, $\Gamma(D,g)$ とかく. また, $g(z)$ をその生成多項式という. これは, よく知られている BCH 符号の拡張に当たっており, 次の性質をもつ :

$$n \leqq q^m - s_0, \qquad n-k \leqq m \deg g(z),$$
$$d \leqq \deg g(z) + 1,$$

ここで,

$$s_0 = \#\{\, \alpha \in \mathrm{GF}(q^m), \quad g(\alpha) = 0 \,\}.$$

Remark 1. 符号理論は 1950 年のハミング符号に始まり, 1959 年から 1961 年にかけては BCH 符号と RS 符号, そしてその復号法としてピーターソン法が現れた. その後, Goppa 符号, 代数幾何符号とおよそ 10 年毎に現れ, 1982 年にはモジュラー曲線から生ずる代数幾何符号が発表された ([4]) :

M.A. Tsfasman, S.G. Vlădut and Th. Zink : Modular curves, Shimura curves, and Goppa codes, better than the Varshamov-Gilbert bound, Math. Nachrichten, **109**.

2.2 代数幾何符号

2.2.1 L 型 (D,G) 符号　　C を GF(q) 上の絶対既約非特異な射影曲線とし, その種数を g とする. $P_1,\ldots,P_n$ を GF(q) 上の有理的な C 上の点とし, 次の 2 つの divisors を導入する :

$$D=\sum_{i=1}^{n}P_i,$$

$$G=\sum_{i=1}^{\ell}m_iQ_i:\ \mathrm{GF}(q)\text{ 上の有理的な点のみからなる台をもち, 各点 }Q_j\text{ はどの }P_i\text{ とも異なる}$$

そして, C の GF(q) 上の有理関数全体を GF$(q)(C)$ とし,

$$L(G)=\{\,f\in \mathrm{GF}(q)(C):(f)+G\geqq 0\,\}\cup\{0\}$$

とおく. $L(G)$ は $GF(q)$ 上の有限次元ベクトル空間で, R-R 定理より

$$\dim L(G):=d(G)=\deg G-g+1+d(G-D).$$

さて,

$$\begin{array}{ccc}\phi_L:L(D) & \longrightarrow & \mathrm{GF}(q)^n\\ \cup & & \cup\\ f & \longmapsto & \phi_L(f)=(\,f(P_1),\ldots,f(P_n)\,)\end{array}$$

なる対応の像 $\mathrm{Im}\,\phi_L$ を C 上の L 型 (D,G) 符号（または functional 符号）といい,

$$\Gamma_L(D,G;C)\quad(=(n,k_L))$$

とかく. また, その最少距離を d_L とかく. R-R 定理より

定理 1. $\deg G<n$ とする. そのとき,

(1)　$k_L\geqq \deg G-g+1$,

(2)　$d_L\geqq n-\deg G=\delta_1$

が成立する. また, $\deg G>2g-2$ なら (1) で $=$ が成り立つ. 更に, $r=k_L/n$, $\delta=d_L/n$ とおくとき (2) は

$$\delta+r\geqq 1-\frac{g-1}{n}$$

と表される.

Remark 2. δ_1 を設計最小距離という. また, r を符号伝送率（または, 情報率, 符号化率, 伝送速度）といい, δ を相対距離という. δ and / or r を最大にするには？

2.2.2 Ω 型 (D,G) 符号

$$\left\{(\,c_1,\ldots,c_n\,)\in \mathrm{GF}(q)^n\ :\ \sum_{i=1}^{n}c_if(P_i)=0\text{ for all }f\in L(D)\right\}$$

なる GF(q) 上の線形符号を C 上の Ω 型 (D,G) 符号といい,

$$\Gamma_\Omega(D,G;C)\quad(=(n,k_\Omega))$$

とかく. また, その最少重みを d_Ω とかく. Ω 型の上の定義より, L 型と Ω 型は互いに双対である.

定理 2. $\deg G > 2g-2$ とする. このとき,

(1) $k_\Omega = n - \deg G + g - 1 + \dim L(G-D)$,

(2) $d_\Omega \geqq \deg G + 2 - 2g = \delta_2$

が成立する.

Remark 3. (1) δ_2 を Γ_Ω の設計最小距離という.

(2) n を大きくすると, Γ_L では, d_L が大きくなり, Γ_Ω では k_Ω が大きくなる. 従って, 効率のよい符号が得られる. d_L, d_Ω の exact value は?

(3) すべての線形符号は weakly algebraic-geometric code としての表現をもつ ([3]) . 従って, より優れた良い線形符号を得るには如何なる divisors を選ぶかにかかわる.

例 1

$C = \mathbb{P}^1(\mathrm{GF}(q))$ $(: g = 0)$

$P_i = (\alpha_i : 1)$, $Q_i = (\gamma_i : 1)$ $(\alpha_i, \gamma_i \in \mathrm{GF}(q))$

γ_i : 与えられた $g(z)$ の零点

m_i : その重複度

とし,

$$D = \sum_{i=1}^{n} P_i, \quad G = \sum_{i=1}^{\ell} m_i Q_i$$

としたときの Ω 型 (D, G) 符号が Goppa 符号に相当する.

2.3 底曲線を直線から曲線に変更することによって, 有理点がより多くなり符号長が長くなるが, その長さ n は最大 $N(C)$ までとり得る. ここで, $N(C)$ は $\mathrm{GF}(q)$ 上有理的な C 上の点の総数を表す. この $N(C)$ に関しては, 次の Hasse-Weil 限界がある :

$$|N(C) - q - 1| \leqq 2g\sqrt{q}.$$

ここで,

$$A(q) = \lim_{g(C)\to\infty} \sup \frac{N(C)}{g(C)}$$

とおく. 上の不等式より

$$A(q) \leqq 2\sqrt{q}$$

が成立する. この不等式は下記のように良くなる :

$$A(q) \leqq \frac{1}{2}(\sqrt{8q+1} - 1) \quad \text{(Ihara, 1982)}$$

$$\leqq \sqrt{q} - 1 \quad \text{(Vlădut-Drinfeld, 1983)}$$

更に, C がモジュラー曲線で $q = p^{2m}$ なら, 上の不等式で $=$ が成立する. また,

$$\text{予想 (Manin, 1982) : } A(p^{2m+1}) = p^m - 1.$$

$m = 1$ のときは, Zink によって証明された.

§3. モジュラー曲線符号

3.1 合同部分群 Γ ($\subset \mathrm{SL}_2(\mathbb{Z})$) に対し, Γ の下での orbits からなる商空間

$$\Gamma\backslash\mathfrak{H}^+ = \left\{ \Gamma\tau : \tau \in \mathfrak{H}^+ \right\}$$

をモジュラー曲線といい, $X(\Gamma)$ とかく. $X(\Gamma)$ はリーマン面の構造をもつ. さて, $q = p^2$ ($p \neq 2$), $(N, p-1) = 1$ とし, $\widetilde{X}_0(N)$ を Hecke の合同部分群 $\Gamma_0(N)$ に関するモジュラー曲線の reduction mod p とする. $\widetilde{X}_0(N)$ は $\mathrm{GF}(p)$ 上の非特異曲線である. この $\widetilde{X}_0(\Gamma)$ を底曲線とする代数幾何符号 C をモジュラー曲線符号という. これについて, 次の 1) , 2) が成立する.

1) $\widetilde{X}_0(N)$ の $\mathrm{GF}(q)$ 上有理的な点の総数に関し

$$\#E\left(\widetilde{X}_0(N) : \mathrm{GF}(q)\right) \geqq \frac{1}{12}(p-1)(N+1)$$

が成立する.

2) $$\lim_{N\to\infty} \frac{g\left(\widetilde{X}_0(N)\right)}{\#E\left(\widetilde{X}_0(N) : \mathrm{GF}(q)\right)} = \frac{1}{p-1}.$$

定義体を固定し, $g \to \infty$ とすることにより モジュラー曲線族から符号列を作り漸近的特性を得る. まず定理 1 より

$$r \geqq 1 - \delta - \gamma, \quad \gamma = \frac{g-1}{n}.$$

$\left[\frac{N}{12}\right] - 1 \leqq g \leqq \left[\frac{N}{12}\right] + 1$ (Hurwitz-Zenthen) より, $N \to \infty$ のとき $g \to \infty$ で, 上の 2) より

$$r \geqq 1 - \delta - \frac{1}{\sqrt{q}-1}$$

となる. この符号 C は, $q \geqq 7^2$ で Varshamov-Gilbert 下昇式をこえる ([2]) .

Remark 4. $q = p^m$ ($p \neq 2$) でも 2) は成立する:

Manin and Vlădut (1985)

また, $p = 2$ のときの研究には

山西・三浦 (1987).

Remark 5. 符号の限界 (不等式) :

1) 構成した符号の評価 : 必要条件による評価式

例えば, S-限界式

2) すぐれた符号構成のヒント : 十分条件による評価式 :

i.e. 限界式をみたすような符号の存在性

例えば, V-G 限界式 : これはよい下界式をもつ :

$$\varphi(\delta) = \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta)\log_q(1-\delta)$$

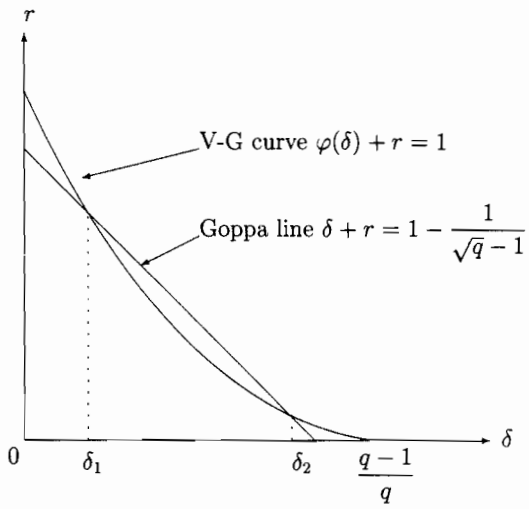
とするとき,

$$\varphi(\delta) + r \geqq 1 \quad (\delta = \frac{d}{n},\ r = \frac{k}{n})$$

さて, $q \geqq 7^2$ のとき

$$\varphi(\delta) + r = 1, \quad r + \delta = 1 - \frac{1}{\sqrt{q} - 1}$$

は解 δ_1, δ_2 をもち, その間で V-G 限界を越える r, δ をもつモジュラー曲線符号を構成することが可能である.



3.2 ここで, $q = p^2$ $(p \neq 2)$ の場合の 2) の証明の概略を述べる : Moreno ([2]) .
まず, モジュラー曲線から良い符号が得られる根拠は次の 2 つである.

1. モジュラー曲線の存在 ;
2. その zeta 関数がよく知られている : GF(p^2) 上の有理点の個数が Hecke 作用素の trace として表現でき, tr ($T(p^2)$) が計算できる (Eichler-Selberg の跡公式) .

さて, $p \nmid N$ として, GF(p) 上の $\widetilde{X}_0(N)$ の zeta 関数は

$$Z(\widetilde{X}_0(N), t) = \frac{\prod_{i=1}^{g}(1 - b_i(p)t + pt^2)}{(1-t)(1-pt)}$$

とかかれる (Eichler-Shimura の合同式) . ここで,

$S_2(\Gamma_0(N))$: $\Gamma_0(N)$ に関する重さ 2 の cusp forms の作る space,
$\{f_1, \ldots, f_g\}$: $S_2(\Gamma_0(N))$ の normalized eigenforms

とするとき, f_i の p 番目の Fourier 係数が $b_i(p)$ である.
$N =$ 素数とするとき, 上の結果より

$$\#E\left(\widetilde{X}_0(N) : \mathrm{GF}(p)\right) = p + 1 - \sum_{i=1}^{g} b_i(p),$$

$$\#E\left(\widetilde{X}_0(N) : \mathrm{GF}(p^2)\right) = p^2 + 1 - \sum_{i=1}^{g} b_i^2(p) + 2pg$$

が成立する. $b_i(p^2) = b_i(p)^2 - p$ だから,

$$\#E\left(\tilde{X}_0(N) : \mathrm{GF}(p^2)\right) = p^2 + 1 - \sum_{i=1}^{g} b_i(p^2) + pg.$$

一方, Hecke 作用素 $T(p^2)$ の $S_2(\Gamma_0(N))$ 上の trace は

$$\mathrm{tr}\,(T(p^2)) = g + p^2 + 1 - \sum \left\{1 + \left(\frac{D}{N}\right)\right\} \frac{h(D)}{w(D)}$$

で与えられる. ここで, $\sum$ は次の組 (s, f) をわたる :

$$-2p < s < 2p, \qquad f > 0, \qquad \frac{s^2 - 4p^2}{f^2} \equiv 0, 1 \mod 4.$$

従って,

$$\#E\left(\tilde{X}_0(N) : \mathrm{GF}(p^2)\right) = g(p-1) + \sum \left\{1 + \left(\frac{D}{N}\right)\right\} \frac{h(D)}{w(D)}.$$

$N \to \infty$ のとき, $g \to \infty$ だから

$$\#E\left(\tilde{X}_0(N) : \mathrm{GF}(p^2)\right) = g(p-1) + O(1) \quad \text{as } N \to \infty$$

となり, 2) が示せた.

Remark 6. $\tilde{X}_0(N)$ は intractable 故, 今の所 モジュラー符号 C の effective な構成はむずかしい.

3.3 モジュラー曲線符号の例を与える ([1]) .

例 2 フェルマー曲線

$$X^3 + Y^3 + Z^3 = 0$$

を考える.

$$x = \frac{3Z}{X+Y}, \quad y = \frac{9X - Y}{2X + Y} + \frac{1}{2},$$

と変換して, 楕円曲線

$$C : y^2 - y = x^3 - 7$$

を得る. C を $\mathrm{GF}(q)$ 上で考える. C はモジュライ空間として, モジュラー曲線 $\tilde{X}_0(3^3)$ のモデルと考えられる (Serre) .

$$\dim S_2(\Gamma_0(3^3)) = 1,$$

その生成元は

$$\begin{aligned}\eta(3z)^2\,\eta(9z)^2 &= q\prod_{n=1}^{\infty}(1-q^{3n})^2(1-q^{9n})^2 \\ &= \sum_{n=1}^{\infty} a(n)q^n \qquad (q = e^{2\pi iz}, \quad \mathrm{Im}\,(z) > 0\,),\end{aligned}$$

ここで, $\eta(z)$ は Dedekind のエータ関数を表す. また,

$$\begin{aligned}&\#E\,(C : \mathrm{GF}(p)\,) = p + 1 - a(p) \qquad (p \neq 3\,), \\ &\#E\left(C : \mathrm{GF}(2^\ell)\right) = 2^\ell + 1 - \alpha_1^\ell - \overline{\alpha}_1^\ell \qquad (\alpha_1 = \sqrt{-2}\,)\end{aligned}$$

を得る. さて,

$$\mathrm{GF}(2^2) = \{0, 1, \alpha, \beta\}, \qquad \beta = 1 + \alpha = \alpha^2$$

とおく. $\mathrm{GF}(2^3)$ 上有理的な C の点は次で与えられる :

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	Q
X	1	α	1	0	β	0	α	1	0
Y	0	0	1	α	0	β	1	α	1
Z	1	1	0	1	1	1	0	0	1

$D = \sum_{i=1}^{8} P_i$, $G = 2Q$ とおくとき, 定理 1 より, $\widetilde{X}_0(27)$ に関するモジュラー曲線符号 $\Gamma_L(D, G; C) = (8, 2)$ を得る. また, $d_L = 6$ である.

Remark 7. モジュラー曲線 $X_0(N)$ の種数 $g = 1$ なのは

$$N \in \{11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\}$$

のときに限る.

参考文献

[1] T. Hiramatsu and G. Köhler, *Coding Theory and Number Theory*, MAIA **554**, Kluwer Academic Publishers, 2003.

[2] C. Moreno, *Algebraic curves and finite fields*, Cambridge Univ. Press, 1991.

[3] R. Pellikaan, B.-Z. Shen and G.J. van Wei, "Which linear codes are algebraic-geometric ?," IEEE Trans. IT, **37** (1991), 583–602.

[4] M.A. Tsfasman and S.G. Vlădut, *Algebraic-Geometric codes*, Kluwer Academic Publishers, 1991.