数理解析研究所講究録
第641巻 1988年 155-193

代数幾何符号

電通大情報工学科　水野弘文（Hirobumi Mizuno）

目次

まえがき

情報理論 C.E.Shannon が論文 A Mathematical Theory of Communication を発表した１９８４年に誕生した。

Shannon の符号化定理によれば、雑音のある離散通信路を通して情報を送るとき、その伝送率が、通信路容量をこえない限り、受信者がいくらでも小さい誤り確率で情報を受信できるような符号化の方法が存在する。

符号理論の目標は、伝送すべき情報に組織的かつ効率的に冗長を付加し、通信系や計算機系の信頼度の向上を図ることにある。符号化定理によって存在が保証された望ましい符号を具体的に構成し、そして伝送の途中で発生する誤りを検出訂正するアルゴリズム、通信システムを実現することが問題になる。

誤り訂正符号は大きくわけるとブロック符号とたたみ込み符号の2種類になるが、ここで考察する符号はすべて符号長一定の線形ブロック符号である。符号理論の研究はShannonの情報理論の論文発表とほとんど同時に開始され、その後の40年の間に大きく進歩した。線形符号についてはR.W. Hamming, M.F.E.Golay, R.C Bose, E.R.Berlekamp その他の人達の研究がよく知られており、また日本人の貢献も増えてきている。

Shannonの先生であったN.Wienerは、確率過程の理論を情報科学に応用し、予測理論を作り上げた。それは、送られて来たデータにフィルターをかけて、雑音をとり除き、もとの正しい情報をとり出す方法である。それに対して、Shannonの考えは、雑音によって誤りが混入するという前提の下で、送りたい情報をそのまま送るのではなく、チャンネル（通信路）に送り込む前にあらがじめ加工を施し、通信の途中で誤りが発生しても受信者側でこれをみつけ出し、そしてもとの正しい符号語（加工された情報）を復元し、そして本来の必要な情報をとり出すという方法である。Wienerがアナログ型人間とすると、Shannonはデジタル型人間ということができる。

Hamming符号、BCH符号その他の巡回符号は多項式やイデアルを用いて表現されるが、1970年にV.D.Goppaは有理

関数を用いて記述される新しい線形符号を定義した。それはBCH符号を部分集合として含む広範なクラスの符号で、符号長が十分長いとき、それまでに知られていた符号と比較してすぐれた性質をもっている。この符号は今日Goppa符号と呼ばれている。それから約10年後、Goppaは再び極めて注目すべき一連の論文を発表した。いわゆる代数幾何符号である。そして符号理論と、代数曲線論との間の関係を明らかにした。この新しい代数幾何符号は、一つの代数曲線Cを基底として構成され、したがってすぐれた符号を構成するには、それに都合のよい代数曲線をまず構成しなければならない。例えば、有限体F_q上定義された曲線CのF_q有理点の数がCの種数$g = g(C)$と比較して十分大きいことが望ましい。先に述べたGoppa符号は、代数幾何符号の立場から眺めると、曲線Cの種数が0、すなわち射影直線を基底とする符号に外ならない。

この論文では、第1章でまずHamming符号からGoppa符号までの概略を説明する。続いて第2章で、代数幾何符号に必要な最小限の代数曲線論について述べる。最後の第3章でこの論文の目標である代数幾何符号を定義し、Riemann-Rochの定理を用いてその符号長、次元、最小距離の関係式を導く。しかし、ここでは具体的な符号の構成、その性能の評価など

については省略する。

第Ⅰ章　符号理論入門

Ⅰ.1.　序

有限体 $F_2 = GF(2)$ の2つの元を 0 と 1 で表わす。F_2 の元の列 $u = (u_0, u_1, u_2, u_3)$ を送信する場合を考える。u をメッセージと呼ぶことにする。このベクトル u をそのまま送信するのではなく、更に3つの冗長ビット x_4, x_5, x_6 をつけ加えて7次元ベクトル

$$x = (x_0 , x_1 , x_2 , x_3 , x_4 , x_5 , x_6)$$

をつくる。ここで、x は連立1次同時方程式

$$\begin{cases} x_1 + u_4 + u_6 + u_7 = 0 \\ x_2 + u_4 + u_5 + u_6 = 0 \\ x_3 + u_5 + u_6 + u_7 = 0 \end{cases}$$

すなわち、$Hx^t = 0$ の解であるとする。ただし、H は GF(2) の元つまり0か1を要素とする行列で、

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

である。このとき $Hx^t = 0$ の解全体は F_2^7 の中の線形部分空間Γをつくる。ここで、行列

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

を定義すれば、

$$\phi : u \rightarrow x = u G$$

によって線形写像 $\phi : F_2^4 \rightarrow F_2^7$ が定義される。そして、$\mathrm{Im}\phi = \Gamma$ となる。

例えば、$u = (1011)$ なら $x = \phi(u) = (1011100)$ となる。

送信されたベクトル x が途中で雑音のために誤りを生じて、受信者はベクトル $y = x + e_2 = (1001100)$, $e_2 = (0010000)$ を受信したとすると、

$$s = Hy^t = Hx^t + He_2^t = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

となり、これは行列 H の（0番目から数えて）第2列と一致していることがわかる。こうして受信者は受信ベクトル y が与えられたとき、シンドローム s を計算することにより、受信ベクトル y の第2成分が誤りであることを知り、それを 0 から 1 に訂正してもとの送信ベクトル x を得ることができる。Γ は、これから我々が考察しようとする線形符号の最もかんたんな例になっている。

I.2. 線形符号

有限体 $F_q = GF(q)$ 上の n 次元ベクトル空間 F_q^n において、ベクトル $x = (x_0, x_1, \cdots, x_{n-1})$ に対してそのノルム、あるいは重みを

$$\| x \| = | \{ i \mid 0 \leqq i \leqq n-1, x_i \neq 0 \} |$$

と定義する。このとき F_q^n の 2 点 x, y に対してその間の距離 $d(x,y) = \| x - y \|$ が導入されて、F_q^n は距離空間になる。

F_q^n の k 次元部分空間Γを [n, k]線形符号 と定義する。$\phi \in Hom(F_q^k, F_q^n)$ が単射なら $\Gamma = Im\phi$ は [n, k]線形符号になる。ϕ を行列 $G = G_\phi$ で表現して

$$\phi : u \rightarrow uG, \quad u \in F_q^k$$

とするとき、G を線形符号 Γ_ϕ の生成行列という。

$\phi \in Hom(F_q^n, F_q^r)$ が全射のとき $\Gamma_\phi = Ker\phi$ は F_q^n の $k = n-r$ 次元部分空間になるから、これを線形符号と考えることもできる。ϕ の表現行列を $H = H_\phi$ とすると

$$\Gamma_\phi = \{ x \in F_q^n \mid Hx^t = 0 \}$$

となる。この場合 H を Γ_ϕ のパリティ検査行列と呼ぶ。

また [n, k]線形符号 Γ に対して、n を符号長、k を次元、r = n-k を検査点数と呼ぶ。線形符号Γの各元を符号語という。2つの異なる符号語 x, y の間の距離の最小値

$$d = \min_{x, y \in \Gamma,\ x \neq y} d(x, y)$$

をΓの最小距離という。線形符号の場合にはそれはΓの最小重み

$$\min_{0 \neq x \in \Gamma} \| x \|$$

に等しい。

線形符号Γのパリティ検査行列H と Γの最小距離d に関して次の定理が容易に証明される。

定理1. 検査行列 H のどの δ-1 個のベクトルも線形独立ならば d ≧ δ

符号語 x ∈ Γ が送られ、伝送の途中で誤りe が生じて、ベクトル y = x + e を受信したとする。H をパリティ検査行列とするとき、e = 0 なら $Hy^t = Hx^t = 0$ であるが、e ≠ 0 の場合には

$$s = Hy^t = He^t \neq 0$$

となる。eを誤りベクトル、sを受信ベクトルyのシンドロームという。

Γの最小距離dに対してd ≧ 2t+1ならば、Γはt重誤り訂正可能である。すなわち、‖e‖ ≦ tならば受信ベクトルyからシンドロームsを求め、もとの送信ベクトルxを確定することができる。

行列Hの階数がrならば、線形独立な列ベクトルの最大個数はrに等しいから、定理1からr ≧ d-1したがって、

定理2　[n,k]線形符号Γの最小距離をdとすると

$$d \leqq n - k + 1$$

特に等号が成り立つ場合、ΓはMaximum Distance Separable (MDS) 符号と呼ばれる。

I.3. 巡回符号

nをqと互いに素な自然数とし、n | q-1とする。

$\alpha \in GF(q^m)$を1の1つの原始n乗根とし、αを根にもつ次数n-1以下の多項式

$$c(X) = c_0 + c_1 X + \cdots + c_{n-1} X^{n-1} \in F_q[X]$$

の集合をΓとする。ベクトル $c = (c_0, c_1, \cdots, c_{n-1})$ と多項式 $c(X)$ を対応させることによって、Γを F_q^n の内の部分空間と同一視し、Γを線形符号と考えることにしよう。さて $c(X) \in \Gamma$ のとき $c(\alpha) = 0$，すなわち

$$c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1} = 0$$

この式に α をかけて $\alpha^n = 1$ に注意すると

$$c_{n-1} + c_0\alpha + c_1\alpha^2 + \cdots + c_{n-2}\alpha^{n-1} = 0$$

となる。すなわち $c(X)$ の係数を巡回させてできる多項式

$$c'(X) = c_{n-1} + c_0X + c_1X^2 + \cdots + c_{n-2}X^{n-1}$$

もまたΓに属する。そこで

定義　ベクトル $c = (c_0, c_1, \cdots, c_{n-1})$ が符号語なら、

$$c' = (c_{n-1}, c_0, c_1, \cdots, c_{n-2})$$

もまた符号語となるときΓを巡回符号という。

あるいはまた、剰余環 $R_n = F_q[X]/(X^n-1)$ のイデアルΓを巡回符号であると定義することもできる。

α を前のように $GF(q^m)$ の元で、1の原始n乗根とするとき、

$$\alpha, \alpha^2, \alpha^3, \cdots, \alpha^{\ell-1}$$

をすべて根にもつ n-1 次以下の多項式全体は、F_q 上のベクト

ル空間になる。R_n で考えれば、それらの多項式はイデアルΓ（の各剰余類の代表元）になる。このようにして得られる巡回符号を BCH 符号 と呼ぶ。

定理3　上に定義した BCH 符号 Γ は、最小距離 $d \geq \ell$ および次元 $k \geq n - m(\ell-1)$ をもつ。

巡回符号は具体的な構成も、符号化、復合化のアルゴリズムも簡単で、実用上重要な符号の一つであるが、符号長 n が大きくなるにつれて、漸近的に悪くなる、すなわち $n \to \infty$ のとき $R = k/n$, $\delta = d/n$ のどちらかが、0 に近づくという欠点がある。

I.4. Goppa符号

BCH 符号は、1959 年に、Hocquenghem が発見し、続いて1960年に、Bose と Chaudhuri がそれとは独立に発見した多重誤り訂正符号で、それは巡回符号になる。BCH 符号を含む巡回符号は、剰余環 $R_n = F_q[x]/(x^n-1)$ の中のイデアルとしての構造をもち、多くの研究がなされた。　これに対して、Goppa は有理式を用いて線形符号を表現するという新しい方

法を開発した。それはGoppa符号と呼ばれ、極めて大きな注目を集めた。

さて、Goppa符号を定義しよう。

体 F_q の m 次拡大体を $K = GF(q^m)$ とし、$g(z) \in K[z]$ を t 次の多項式とする。$D = \{ \alpha_1, \alpha_2, \cdots, \alpha_n \} \subset K$ は $g(z)$ の根を含まないような K の部分集合とする。ベクトル $c = (c_1, c_2, \cdots, c_n) \in F_q^n$ に対して有理関数

$$\phi_c(z) = \sum_{i=1}^{n} \frac{c_i}{z - \alpha_i}$$

を対応させる。このとき

定義　Goppa符号 $\Gamma(D, g)$ は

$$\phi_c(z) \equiv 0 \pmod{g(z)}$$

をみたすようなベクトル $c = (c_1, c_2, \cdots, c_n)$ のつくる F_q^n の部分空間である。$g(z)$ を $\Gamma(D, g)$ の生成多項式と呼ぶ。

定理4　Goppa符号 $\Gamma(L, g)$ の符号長 n、次元 k および最小距離 d は関係式

$$k \geqq n - m \deg(g)$$

$$d \geqq \deg(g) + 1$$

を満足する。

第Ⅱ章　代数曲線

Ⅱ.1.　アフィン代数曲線

体Fの代数的閉包を $\bar{F}$ とする。多項式 $f(X,Y)\in F[X,Y]$ に対して $f(a,b)=0$ をみたす点 $P=(a,b)$, $a,b,\in\bar{F}$ を $f(x,y)$ の零点という。$f(X,Y)$ の零点全体の集合

$$V(f)=\{\ (a,b)\ \mid\ a,b\in\bar{F}\ ;\ f(a,b)=0\ \}$$

を多項式 f で定まるアフィン代数曲線という。また、単に曲線 $f(X,Y)=0$,あるいはもっと簡単に曲線 f ということもある。特に $V(f)$ の点 (a,b) は、$a,b\in F$ のとき F 有理的である、あるいは F 点であるという。

曲線 f の点 $P=(a,b)$ に対して

$$\left(\frac{\partial f}{\partial X}\right)_p=\left(\frac{\partial f}{\partial Y}\right)_p=0$$

となるとき、P は f の特異点であるという。そうでない点は単純点という。f のすべての点が単純点なら、曲線 f は非特異、またはなめらかであるという。

多項式 $f(X,Y)$ が $\bar{F}[X,Y]$ において既約のとき曲線 f は既約であるということにする。

Ⅱ.2. 射影代数曲線

$F(x_0, x_1, x_2)$ を次数 $n > 0$ の同次多項式とする。射影平面 P^2 の点 $P = [a_0, a_1, a_2]$ が

$$F(P) = F(a_0, a_1, a_2) = 0$$

をみたすとき、P はこの同次多項式 F の零点という。

$F(\lambda a_0, \lambda a_1, \lambda a_2) = \lambda^n F(a_0, a_1, a_2)$ であるから、零点は同次座標のとり方によらない。

$$F(x) = F(x_0, x_1, x_2)$$

の零点全体の集合を射影平面代数曲線という。

$f(X, Y) = F(1, x, y)$ とおけば、$F(x_0, x_1, x_2)$ に対して非同次多項式 $f(X, Y)$ が対応する。逆に $f(X, Y)$ が与えられたとき、その次数を n として

$$F(x_0, x_1, x_2) = x_0^n f\left(\frac{x_1}{x_0}, \frac{x_2}{x_0}\right)$$

とおけば、n 次同次多項式 $F(x_0, x_1, x_2)$ が得られる。

曲線 F の点 P において、$F(x_0, x_1, x_2)$ のすべての r-1 階導関数の値が 0 になり、かつ r 階導関数の中には 0 でないものが存在するとき、P は曲線 f の r 重点という。

例. 曲線 $F \equiv x_0 x_2^2 - x_1^3 - x_0 x_1^2$ は、

点 P = [1, 0, 0] において $\frac{\partial F}{\partial x_0} = x_2^2 - x_1^2$,

$\frac{\partial F}{\partial z_1} = -3x_1^2 - 2x_0x_1$, $\frac{\partial F}{\partial z_2} = 2x_0x_2$

がすべて 0 になり、しかも $\frac{\partial^2 F}{\partial x_2^2} = 2 \neq 0$ であるから、

P は F の 2 重点である。

F に対応するアフィン代数曲線は

$$f = Y^2 - X^2 - X^3$$

で与えられる。

II.3. 特異点、曲線の種数

アフィン代数曲線 C : f(X, Y) = 0 においては、点 P が C の r 重点ならば、P での f(X, Y) の r-1 階までの導関数がすべて 0 で、かつ r 階導関数の中に 0 でないものがある。

多項式 f(X, Y) を P = (a, b) を中心として Taylor展開すると

$$f(X, Y) = \sum_{i=0}^{n} \sum_{j=0}^{n} \binom{i}{j} \frac{\partial^i f(a, b)}{\partial X^j \partial Y^{i-j}} (X-a)^j (Y-b)^{i-j}$$

点 P を通る直線は

$$L : X = a + \lambda t, \quad Y = b + \mu t$$

と表され、L は比 $\lambda : \mu$ によってきまる。曲線 C と L との交点は $f(a+\lambda t, b+\mu t) = 0$ を t に関して解くことによっ

て求まる。さて P = (a, b) が C の r 重点であることに注意すると

$$f(a+\lambda t, b+\mu t) = t^r \sum_{i=0}^{r} \binom{r}{j} \frac{\partial^r f(a,b)}{\partial X^i \partial Y^{r-i}} \lambda^i \mu^{r-i} + \cdots$$

となり、t = 0 は少くとも r 重根になる。

$$\sum_{i=0}^{r} \binom{r}{j} \frac{\partial^r f(a,b)}{\partial X^i \partial Y^{r-i}} \lambda^i \mu^{r-i}$$

は λ, μ についての r 次同次式であるから、それを 0 にするような λ : μ は重複度を考慮してちょうど r 個存在する。そのような λ, μ によってきまる直線 L を点 P での C への接線という。

P が C の単純点、すなわち r = 1 のときは

$$f_X(a,b)\lambda + f_Y(a,b)\mu = 0$$

射影平面で考えて P = [a₀, a₁, a₂] = [1, a, b] とし、f(X, Y) = F(1, X, Y) とすると、Eulerの恒等式：

$$x_0 F_{x_0} + x_1 F_{x_1} + x_2 F_{x_2} = n F$$

から

$$a f_X(P) + b f_Y(P) = - F_{x_0}(P)$$

となる。これらの関係式によって、射影平面曲線

C : f(x) = 0 の単純点 P = [a₀, a₁, a₂] での接線は

$$x_0 \frac{\partial F}{\partial x_0}(a) + x_1 \frac{\partial F}{\partial x_1}(a) + x_2 \frac{\partial F}{\partial x_2}(a) = 0$$

で与えられる。

$r > 1$ の場合、 r 重点 P での r 本の接線がすべて異なるならば、P は曲線 C の通常特異点であるという。

曲線 C が既約ならば、その特異点の個数は有限で、それらを $P_1, P_2, \cdots\cdots, P_k$、かつ点 P_i の重複度を r_i とすると、C の次数を n とするとき

$$\sum_{i=1}^{k} \frac{1}{2} r_i(r_i-1) \leqq \frac{1}{2}(n-1)(n-2)$$

が成立つ。非負整数

$$g = \frac{1}{2}(n-1)(n-2) - \sum_{i=1}^{k} \frac{1}{2} r_i(r_i-1)$$

を C の種数という。

種数 $g = 0$ の曲線を有理曲線という。この場合 C の座標はパラメータ t の有理関数 $\phi(t), \phi(t)$ を用いて

$$X = \phi(t), \quad Y = \phi(t)$$

と表わされる。ここで t はアフィン直線上を動く。

前にあげた曲線 $Y^2 - X^2 - X^3 = 0$ は原点 $(0,0)$ で通常の2重点をもち、それ以外には特異点をもたない3次既約曲線であるから $g = \frac{1}{2}(3-1)(3-2) - \frac{1}{2}\,2(2-1) = 0$ となり、有理曲線である。そして、パラメータ表示

$$X = t^2 - 1, \quad Y = t^3 - t$$

をもつ。

Ⅱ.4. 因子

n 次既約曲線 $C : F(x_0, x_1, x_2) = 0$ は高々通常の特異点だけをもつものとする。このとき、十分次元の高い射影空間の中のなめらかな曲線 X および X から C の上への有理写像

$$\Phi : X \to C$$

で、C の特特異点を除いた部分では 1 対 1 となるものが存在する。X を C の非特異点モデルという。P が C の r 重点ならば $\Phi^{-1}(P)$ は X の r 個の異なる点からなる：

$$\Phi^{-1}(P) = \{ P^{(1)}, P^{(2)}, \cdots, P^{(r)} \}$$

したがって、C の r 重点には、r 個の異なる点が重なっていると考えられる。$P^{(1)}, P^{(2)}, \cdots, P^{(r)}$ を、C の点 P を中心とする r 個の place と呼ぶ。P が単純点ならば

$$\Phi^{-1}(P) = \{ P^{(1)} \}$$

であり、点 $P \in C$ と、P を中心とする place とは同一視してもさしつかえない。

曲線 C の place の形式的な有限和

$$D = \Sigma\ n_i P_i, \quad n_i \in Z$$

を因子と呼ぶ。係数の和 $\Sigma_i n_i$ を D の次数と呼び、deg D

と表わす。

曲線Cの place P での局所パラメータを t とすると、C の座標は P の近傍で t のベキ級数として表わされる。

例　　$Y^2 = X^2 + X^3$

は原点 P = (0,0) を中心とする2つの異なる place をもつ。それらの place でのこの曲線のパラメータ表示は次のようになる：

$$P^{(1)} : \quad X = 2t + t^2 , \quad Y = 2t + 3t^2 + t^3$$

$$P^{(2)} : \quad X = -2t + t^2 , \quad Y = 2t - 3t^2 + t^3$$

II.5. 有理関数，交わりの重複度

同じ次数の同次多項式 $A(x_0, x_1, x_2)$, $B(x_0, x_1, x_2)$ があって、$B(x) \not\equiv 0 \pmod{F(x)}$ とする。このとき対応

$$P \rightarrow \phi(P) = \frac{A(P)}{B(P)}$$

によって曲線 C : F = 0 の有理関数 ϕ が定義される。

ϕ は $B(P) \neq 0$ のとき点 P で正則である。与えられた place P で正則な C 上の関数の集合 $\theta_P(C)$ は P に於ける局所環である。この場合、P での局所パラメータと呼ばれる元 $t \in \theta_P(C)$ が存在して、任意の関数は $\phi(t) = u\, t^{\nu}$ と表され、u は $\theta_P(C)$ の単元である。ν を関数 ϕ の P での位数と呼び、

$ord_P(\phi)$ とかく。$\nu > 0$ ならば ϕ は P で ν 位の零点を持つ、また $\nu < 0$ なら $-\nu$ 位の極を持つという。

2つの曲線 C : $f(X,Y) = 0$, D : $g(X,Y) = 0$ が1点 $P = (a,b)$ で交わるとき、その点 P での C , D の交点数 $I_P(C,D)$ が次のように定義される。P を中心とする C の1つの place を $P^{(i)}$ $(1 \leqq i \leqq r)$ とし、$P^{(i)}$ における C の局所パラメータを t をする。$P^{(i)}$ での C のパラメータ表示を

$$X = x(t) , \quad Y = y(t)$$

とし、t に関する $g(x(t),y(t))$ の位数

$$ord_{P^{(i)}}(D) = ord_t(g(x(t),y(t)))$$

を place $P^{(i)}$ での曲線 D の位数と呼ぶ。そして、点 P での C と D の交わりの重複度を

$$I_P(C,D) = \sum_{i=1}^{n} ord_{P^{(i)}}(D)$$

と定義する。このとき次の定理が成り立つ。

定理5.(Bezout) m 次曲線 C と n 次曲線 D が共通の成分を持たないとき、

$$\sum_{P \in C \cap D} I_P(C,D) = m\,n$$

が成り立つ。

Ⅱ.6. 平面代数曲線の線形系と曲線上のlinear series

次数 ℓ の x_0, x_1, x_2 に関する単項式

$$x_0^{\ell},\ x_0^{\ell-1}x_1,\ x_0^{\ell-1}x_2,\ \cdots,\ x_2^{\ell}$$

は全部で $N+1 = \frac{1}{2}(\ell+1)(\ell+2)$ 個ある。

それらを $M_0, M_1, \cdots, M_N$ とすれば、任意の ℓ 次同次多項式は

$$g(x) = \sum_{i=0}^{N} a_i M_i$$

と表され、従ってそれら全体は N 次元射影空間をなす。すなわち ℓ 次射影平面代数曲線と P^N の点が1対1に対応し、それらの曲線全体は P^N によってパラメータ表示される。

射影平面 P^2 上に k 個の点 P_1, P_2, $\cdots$, P_k をとり、P^2 の0-サイクル

$$A = \sum_{i=1}^{k} r_i P_i$$

を考える。P^2 上の ℓ 次曲線の中で、点 P_i において少なくとも重複度が r_i 以上であるような曲線はサイクル A を通るということにする。このとき、A を通る ℓ 次曲線全体

$$V(A;\ell) = \{ H \mid m_{p_i}(H) \geq r_i,\ 1 \leq i \leq k \}$$

$m_{p_i}(H)$: 曲線 H の点 P_i での重複度

は P^N の中の部分空間になる。その次元は

$$\dim V(A;\ell) \geqq \frac{1}{2}\ell(\ell+3) - \sum_i \frac{1}{2} r_i(r_i+1)$$

C : f = 0 を m 次既約曲線とする。V(A;ℓ) の各曲線 H はCと交わって次数 ℓm の因子を切断する。このようにして得られる因子の集合を C 上の liner series という。Liner series は g で表わす習慣がある。

サイクル $A = \sum_{i=1}^{k} r_i P_i$ の成分 P_i のいくつかが曲線C上の点である場合には、P_i を中心とするCのplace は linear series のすべての因子 D に含まれる。一般に、因子 B が linear series g のすべての因子に含まれるとき、因子 B は g の固定部分という。このとき各 D∈G から B を除いて得られる因子の集合

$$g' = g - B = \{ D-B \mid D \in g \}$$

もまた linear series という。各因子 D ∈G の次数を n とすると、g の因子の次数は n′ = n - deg B となる。

前に述べたように、ℓ次射影平面曲線全体は $N = \frac{1}{2}\ell(\ell+3)$ 次元の射影空間をなす。これはサイクル A が 0 の場合で、V = V(0;ℓ) と表される。

W を V の r 次元の線形部分空間とし、W に属する各 ℓ 次

曲線がC上に切断する因子の集合を考える。それが固定部分Bを持つならば、それを除いて $g' = g - B$ はもはや固定部分を含まないようにすることができる。Wに属する ℓ 次曲線Hと、Hによって C上に切断される因子 D との対応が1対1ならば、linear series g および $g' = g - B$ の次元は r であると定義する。また $\deg(D-G) = n$ ならば g' の次数は n である。次数が n、次元が r の linear series を g^r_n と書き表す。

Linear series g^r_n に対して、$g^r_n \subsetneqq g^s_n$ となるようなC上の linear series g^s_n が存在しないとき、g^r_n は完備であるという。

II.7. Riemann-Roch の定理

曲線Cは通常の特異点だけを持つと仮定する。曲線Cに対して、曲線Aが次の条件をみたすとき、AはCに対して随伴であるという。Cが点Qで重複度 $r_Q = m_Q(C) > 1$ を持つとき、$m_Q(A) \geqq r_Q - 1$。Cの次数を m とする。このとき ℓ ($< m$) 次随伴曲線全体は次元

$$r \geqq \frac{1}{2}\ell(\ell+3) - \sum_Q \frac{1}{2} r_Q(r_Q-1)$$

の線形系をなす。Cの定義方程式を $f(x_0, x_1, x_2) = 0$ とする

とき、もし $\ell \geqq m$ ならば f を法として線形独立な ℓ 次同次多項式だけを考える必要があるから、この場合は

$$r \geqq \frac{1}{2}\ell(\ell+3) - \frac{1}{2}\sum_{Q}\frac{1}{2}r_Q(r_Q-1) - \frac{1}{2}(\ell-m)(\ell-m+3)$$

となる。$\ell = m-3$ 次の随伴曲線を特別随伴曲線と呼ぶ。

Q を曲線 C の通常の r 重点をすると、Q を中心とする r 個の C の place $Q^{(1)}, Q^{(2)}, \cdots, Q^{(r)}$ がある。$Q_1, Q_2, \cdots, Q_k$ を C のすべての重複点とし、Q_i を中心とする place を $Q_i^{(1)}, Q_i^{(2)}, \cdots, Q_i^{(r_i)}$ とする。そして、因子

$$E = \sum_{i=1}^{k}(r_i-1)(Q_i^{(1)} + \cdots + Q_i^{(r_i)})$$

を考える。このとき C の随伴曲線 A と C との交わりとして C の因子 (AC) が定義される。それらはすべて E を固定部分として含む。$\deg E = \sum_{i=1}^{k} r_i(r_i-1)$ であるから、次随伴曲線によって C 上に切断される因子を (AC) とすると、固定部分を除いてできる linear series g の次数は

$$n = \ell(\ell+3) - \deg E$$

となる。特に A が特別随伴曲線、すなわち $\ell = m-3$ のとき、g_n^r の次数は $n = m(m-3) - \sum_{i=1}^{k} r_i(r_i-1)$

曲線 C の種数を g とすると、

$$g = \frac{1}{2}(m-1)(m-2) - \sum_{i=1}^{k} \frac{1}{2} r_i(r_i-1)$$

であったから、因子 $(AC)-E \in g_n^r$ の次数は $2g-2$ 。

因子 $K = (AC)-E$ をCの標準因子という。また、Kを含む完備 linear series g_n^r の次元 r は

$$r \geqq \frac{1}{2} m(m-3) - \sum_{i} \frac{1}{2} r_i(r_i-1) = g-1$$

であるが、この場合実は等号が成り立ち、$r = g-1$ となることが証明される。Linear series g_{2g-2}^{g-1} をCの標準 linear series と呼ぶ。

Cの正因子Dに対して、Dを含む完備 linear series g を $|D|$ とかく。特に標準因子Kに対しては

$$|K| = g_{2g-2}^{g-1}$$

曲線C の正因子Dが与えられたとき、 Dを通る特別随伴曲線全体のつくるベクトル空間の次元を $i(D)$ とかいて、Dの

特別指数という。それらの随伴曲線はCと交わって g^{g-1}_{2g-2} の部分 linear series を与え、それは D を固定部分として含む。このとき、$g^{g-1}_{2g-2} - D = |K-D|$ の次元は $i(D)-1$ である。

さて、Riemann-Rochの定理 を述べる。

定理6. D を代数曲線C上の因子とするとき、完備 linear series $|D|$ に対して

$$\dim |D| = \deg D - g + i(D)$$

が成り立つ。ここで、$i(D)$ は因子D の特別指数であり、$\deg D > 2g-2$ なら $i(D) = 0$。また、K をC の標準因子とする時、

$$i(D) = \dim |K - D| + 1$$

因子 $D = \Sigma\, n_P P$ に対して $\mathrm{ord}_P \phi \geqq -n_P$ となるようなC上の有理関数 ϕ の全体は有限次元ベクトル空間になる。それを $L(D)$ とかく。このとき、

$$|D| = \{ D_1 = D+(\phi) \geqq 0 \ ; \ \phi \in L(D) \}$$

となり、$|D|$ はベクトル空間 $L(D)$ に付随する射影空間になっている。

$\ell(D) = \dim L(D)$ とかけば、$\ell(D) = \dim |D| + 1$

であるから Riemann-Roch の定理は

$$\ell(D) = \deg D - g + 1 + \ell(K-D)$$

となる。

II.8. Abel微分と留数定理

この節では、複素数体を基礎の体として話を進める。

既約平面代数曲線 $C : f(X,Y) = 0$

があるとき、関係 $f(z,u)$ によって z の関数 $u = u(z)$ が定まる。$f(X,Y)$ が Y について n 次の多項式とすると、一つの $X = z$ に対して一般に n 個の $Y = u$ の値 $u^{(1)}, \cdots, u^{(n)}$ が定まり、$u(z)$ は z の多価関数になる。そこで、$F(z,u) = 0$ をみたす z, u の組 (z, u) を一つの点を考え、同じ z の値に対して $u^{(1)} \neq u^{(2)}$ となるときは $(z, u^{(1)})$ と $(z, u^{(2)})$ は別の点であると定義する。このような点全体の集合 $\{(z,u) \mid f(z,u) = 0\}$ に適当に位相を導入することによって、複素 z 平面、あるいはそれに無限遠点 ∞ を添加して得られる複素射影直線 $P^1(\mathbb{C})$ 上の n 重被覆面としての Riemann面 R が得られる。このとき体 $\mathbb{C}(z,u)$ の各元は R 上の1価解析関数になる。R は位相幾何学的には連結で向きづけ可能な閉曲面の構造を持ち、その局面の種数 g が、前に定義

した代数曲線Cの種数に等しいことが証明される。$\mathbb{C}(z,u)$の元$\Phi(z,u)$をR上の有理関数という。

またR上の複素積分

$$\int_{(z_0,u_0)}^{(z,u)} \Phi(z,u)\,dz$$

をR上の、または曲線C上のabel積分、そして

$$\omega = \Phi(z,u)\,dz$$

をabel微分、または単にC上の微分という。

Cの特別随伴曲線で線形独立なものはg個存在するから、それらを$\phi^{(1)}(X,Y),\cdots,\phi^{(g)}(X,Y)$としよう。任意の特別随伴曲線$\phi(X,Y)$はそれらの1次結合として表わされる。さて、

$f_Y(X,Y) = \dfrac{\partial}{\partial Y} f(X,Y)$　とかくとき

$$\omega = \frac{\phi(z,u)}{f_Y(z,u)}\,dz$$

と表わされるabel微分ωはCのすべてのplaceにおいて極をもたない。すなわち、いたるところ正則である。このような微分をC上の第1種微分と呼ぶ。第1種微分全体はg次元ベクトル空間をなす。それをΩと表わす。微分ωのplace Pでの位数を$\mathrm{ord}_P\omega$とかくと、有限個のplaceにおいてのみ$\mathrm{ord}_P\omega > 0$となり、ωの因子$(\omega) = \Sigma_P(\mathrm{ord}_P\omega)P$が定義

される。これは前に定義したCの標準因子 $K = (AC)-E$ に等しい。

Riemann面R上に点 $P_1, P_2, \cdots, P_k$ が得られたとき、これらk個の点で少なくとも1位の零点を持つ第1種微分 ω が存在するならば、因子 $D = P_1 + P_2 + \cdots + P_k$ は special であるという。また、そのような微分で、線形独立なものの最大個数がiのとき、$i = i(D)$ を D の特別指数という。

次に、ω を任意の微分とし、点 $Q \in R$ において極を持つとする。QでのRの局所パラメータをtとすると、ω は Q の近傍で

$$\omega = (c_{-\nu} t^{-\nu} + \cdots + c_{-1} t^{-1} + c_0 + c_1 t + \cdots) dt$$

の形に表わされる。このとき c_{-1} を ω の Q での留数と呼び、$\mathrm{Res}_Q \omega$ とかく。それは局所パラメータtの取り方にはよらない。ω がRのすべての点で留数0を持つならば、ω は第2種の微分と呼ばれる。0でない留数をもつとき、第3種微分と呼ばれる。ω を第3種微分とし、点 $Q_1, Q_2, \cdots, Q_k$ で極をもち、それ以外の点では正則とする。このとき次の留数定理が成り立つ。

定理8. 微分 ω のすべての留数の和は0になる:

$$\Sigma_Q \mathrm{Res}_Q \omega = 0$$

第Ⅲ章　代数幾何符号

Ⅲ.1.　序

まえがきで述べたように、V.D.Goppa は代数幾何学の概念や結果を符号理論の言葉に翻訳し、２つの理論の間の関連を明らかにした。それまでにも、符号理論は抽象代数学、有限幾何学、組合せ理論、数論等の方法を応用して発展してきたのであるが、更に代数幾何学と結びつくことにより極めて大きい発展の可能性が開けてきたと言うことができる。

Ⅲ.2.　L 型（D，G）-符号

この章では、代数曲線 C は有限体 F_q 上定義され、種数 g を持つとする。P_1，P_2，…，P_n を F_q 上有理的な C の点とし、因子 $D = \sum_{i=1}^{n} P_i$ を定義する。また因子 $G = \Sigma\ m_i Q_i$ は F_q に関して有理的で、各 Qj はどの P_i（$1 \leq i \leq n$）とも異なるとする。体 F_q に関して有理的な C 上の関数全体は体 $F_q(C)$ をなすが、その中で

$$L(G) = \{ f \in F_q(C) \mid (f) + G \geq 0 \}$$

は F_q 上の有限次元ベクトル空間をなす。その次元 $\ell(G)$ は

Riemann-Rochの定理により

$$\ell(G) = \deg G - g + 1 + i(G)$$

で与えられる。L(G) から F_q^n の中への線形写像

$$\phi_L : L(G) \to F_q^n$$ を

$$\phi_L(f) = (f(P_1), f(P_2), \cdots, f(P_n))$$

によって定義する。このとき、$\mathrm{Im}\phi_L$ を曲線C上のL型(D,G)-符号と呼び、$\Gamma_L(D,G;C)$ と表わす。

定理8. $\deg D > \deg G$ とする。このとき $\Gamma_L(D,G;C)$ の符号長n, 次元 k_L, 最小距離 d_L の間に次の関係が成り立つ:

(1) $\quad k_L \geqq \deg G - g + 1$

ここで、$\deg G > 2g - 2$ なら等号が成り立つ。

(2) $\quad d_L \geqq n - \deg G$

(証明) $f \in L(G)$ に対して、$f \in \mathrm{Ker}\phi$ ならば $f \in L(G-D)$。$\deg(G-D) < 0$ だから $f = 0$。したがって ϕ は単射になり、$\dim\Gamma_L(D,G;C) = \ell(G)$。一方 Riemann-Rochにより $\ell(G) = \deg G - g + 1 + i(G)$。したがって(1)を得る。

もし $\deg G > 2g-2$ なら、標準因子Kの次数は $2g-2$

であるから、Gを含む標準因子は存在せず、$i(G) = 0$となる。したがって等号が成り立つ。

次に、ベクトル$\phi(f) \neq 0$の重みがdとすると、fは$n-d$個の点$P_{i_1}, \cdots, P_{i_{n-d}}$で0になる。したがって

$$f \in L(G - P_{i_1} - \cdots - P_{i_{n-d}})$$

すなわち、$(f) \geqq P_{i_1} + \cdots + P_{i_{n-d}} - G$

両辺の因子の次数を考えれば $0 \geqq n - d - \deg G$。

ここで、もし$d < n - \deg G$とすると$n - d - \deg G > 0$となり矛盾。したがって、任意の符号語$\phi(f)$の重み$\geqq n - \deg G$となる。よって(2)が成り立つ。 Q.E.D.

Ⅲ.3. Ω型(D,G)-符号

前節と同様に、F_q上定義された既的射影平面代数曲Cを考える。C上の微分ωは、$F_q(C)$の元u,zによって$\omega = u\,dz$と表されるときF_q有理的ということにする。この節では、F_q有理的な微分全体のつくるベクトル空間をΩと表わすことにしよう。DをC上のF_q有理的因子とするとき、

$$\Omega(D) = \{ \omega \in \Omega \mid (\omega) \geqq D \}$$

はF_q上有限次元のベクトル空間になる。その次元は、

Riemann-Roch により

$$\dim \Omega(D) = \ell(D) - \deg D + g - 1$$

因子 $D = \sum_{i=1}^{n} P_i$ および G を前節と同様とし、上式の D の D の代わりに G - D を代入すれば、deg D = n に注意して、

(3) $$\dim \Omega(G-D) = n - \deg G + g - 1 + \ell(G-D)$$

ベクトル空間 $\Omega(G-D)$ から F_q^n への線形写像 ϕ_Ω を

$$\phi_\Omega(\omega) = (\operatorname{Res}_{p_1}\omega, \cdots, \operatorname{Res}_{p_n}\omega)$$

と定義する。写像 $\phi_\Omega : \Omega(G-D) \to F_q^n$ の像 $\operatorname{Im}\phi_\Omega$ を曲線 C 上の Ω 型 (D, G)-符号とよび、$\Gamma_\Omega(D, G; C)$ と書く。

定理9　曲線 C および C の因子 D, G は前と同様とする。このとき、もし

$$2g - 2 < \deg G < n + g - 1$$

ならば、C 上の Ω 型 (D, G)-符号 $\Gamma_\Omega(D, G; C)$ の符号長 n_Ω、次元 k_Ω、最小距離 d_Ω の間に次の関係が成り立つ：

(4) $$k_\Omega \geqq n - \deg G + g - 1$$

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

更に、$\deg G < n$ なら (4) において等号が成り立つ。

（証明）　$\omega \in \Omega(D, G; C)$ は点 P_1, P_2, …, P_n において高々1位の極をもち、それ以外の点では正則である。　もし $\phi_\Omega(\omega) = 0$ すなわち $\omega \in \mathrm{Ker}\,\phi_\Omega$ ならば、ω は極をもたず、したがって第1種微分になり、$\omega \in \Omega(G)$ すなわち $(\omega) \geqq G$。　もし $\omega \neq 0$ なら、標準因子 $K = (\omega)$ の次数は $2g - 2$ であるから、$2g - 2 \geqq \deg G$ となり仮定と矛盾する。ゆえに $\omega = 0$。　すなわち $\mathrm{Ker}\,\phi_\Omega = 0$ となり、ϕ_Ω は単射である。ゆえに $k_\Omega = \dim\, \Omega(G-D)$

ここで (3) に注意すれば (4) が得られる。更に $\deg G < n$ なら、$\deg(G-D) < 0$ であるから $\ell(G-D) = 0$ となり等号が成り立つ。

$\omega \in \Omega(G-D)$ に対して $\phi_\Omega(\omega) \in \Gamma_\Omega(D, G; C)$ の重みを d とする。ω は d 個の点 P_{i_1}, P_{i_2}, …, P_{i_d} だけで1位の極をもつから、$\omega \in \Omega(G - P_{i_1} - \cdots - P_{i_d})$，したがって、$\deg(\omega) = 2g - 2 \geqq \deg G - d$ すなわち $d \geqq \deg G - 2g + 2$ となり (5) が示された。

Q.E.D.

Ⅲ.4. (D,G)-符号の双対性

有限体 $F = F_q$ 上の n 次元ベクトル空間 F_q^n に属する2つのベクトル $a = (a_1, \cdots, a_n)$, $b = (b_1, \cdots, b_n)$ に対して、それらのスカラー積 $a \cdot b$ を

$$a \cdot b = a_1 b_1 + \cdots + a_n b_n$$

と定義する。$a \cdot b = 0$ のとき、a と b は直交するという。ユークリッド空間の場合と異なり、$a \neq 0$ でも $a \cdot a = 0$ となる場合が生ずる。

V を F^n の部分空間とするとき、V のすべてのベクトルと直交するベクトルは全体は F^n の部分空間 W をなす。それを V の双対空間と呼び、$V^{\perp}$ とかくことにする。

$$V^{\perp} = \{ x \in F^n \mid \forall y \in V \text{ に対し、} x \cdot y = 0 \}$$

Γ が F^n 上の [n,k] 線形符号で、そのパリティ検査行列を H、生成行列を G とすると、Γ の双対空間 $\Gamma^{\perp}$ は H を生成行列、G をパリティ検査行列とする [n,n-k] 線形符号になる。$\Gamma^{\perp}$ を Γ の双対符号という。

定理10. $2g-2 < \deg G < n$ のとき、L 型 (D,G)-符号 $\Gamma_L(D,G;C)$ と Ω 型 (D,G)-符号 $\Gamma_{\Omega}(D,G;C)$ は互いに双対である。

（証明） $\phi_L(f) = (f(P_1), \cdots, f(P_n)) \in \Gamma_L(D, G; C)$

$$\phi_\Omega(\omega) = (\mathrm{Res}_{p_1}\omega, \cdots, \mathrm{Res}_{p_n}\omega) \in \Gamma_\Omega(D, G; C)$$

に対して、それらの内積を考えると

$$(\phi_L(f), \phi_\Omega(\omega)) = \sum_{i=1}^{n} f(P_i)\,\mathrm{Res}_{P_i}\omega = \sum_{i=1}^{n} \mathrm{Res}_{P_i}(f\omega)$$

さて、$f \in L(G)$, $\omega \in \Omega(G-D)$ であるから、微分 $f\omega$ に対して、その因子を考えると

$$(f\omega) = (f) + (\omega) \geqq -G + (G-D) = -D$$

すなわち $f\omega \in \Omega(-D)$ となり、$f\omega$ は D の成分である n 個の点 $P_1, P_2, \cdots, P_n$ において高々1位の極を持ち、それ以外の点では正則である。したがって、留数定理によって

$$\sum_{i=1}^{n} \mathrm{Res}_{P_i}(f\omega) = 0$$

ゆえに $\Gamma_L(D, G; C)$ の各元 $\phi_L(f)$ と $\Gamma_\Omega(D, G; C)$ の各元 $\phi_\Omega(\omega)$ とは直交している。また、定理8、定理9により

$$k_L = \deg G - g + 1, \quad k_\Omega = n - \deg G + g - 1$$

したがって $C_L^{\perp} = C_\Omega$ Q.E.D.

文献

1. C.E.Shannon: A mathematical theory of Communica-

tion. Bell System Tech.J.27(1948), 379-423, 623-656

2. R.W.Hamming: Error Detecting and Error Correcting Codes ibid. 29(1950) 147-160

3. M.J.E.Golay: Notes on digital coding, proc. IEEE 37(1949) 657

4. A.Hocquenghem: Codes correcteurs d'erreurs, Chiffres, 2(1959) 147-156

5. R.C.Bose and D.K.Ray-Chaudhuri: On a class of error correcting binary group codes, Inform. Contr., 3(1969) 68-79

6. : Further results on error correcting binary group codes. ibid. 3(1969) 279-290

7. I.S.Reed and G.Solomon: Polynomial codes over certain finite fields, J.SIAM Appl. Math., 8(1960) 300-304

8. H.F.Mattson and G.Solomon: A new treatment of Bose-Chaudhuri codes, J.SIAM Appl. Math. 9(1961) 654-669

9. E.R.Berlekamp: Algebraic Coding Theory, McGraw-

Hill, 1968

10. V.D.Goppa: A new class of linear correcting codes, Problemy Peredachi Informatsii, 6, no.3(1970) 24-30

11. :A rational representation of codes and (L,g)-codes, ibid.7, no.3 (1971) 41-49

12. :Binary symmetric channel capacity is attained with irreducible codes, ibid.10 No.1(1974) 111-112

13. :Codes constructed on the base of (L,g)-codes ibid.8 No.2(1972) 107-109

14. :Correction of arbitrary noise by irreducible codes, ibid.10 no.3 (1974) 277-278

15. V.D.Goppa: Codes on Algebraie Curves. Soviet math. Dvkl. 24(1981) 170-172

16. :Algebraico-Geometive Codes Math. USSR Izvestia 21(1983) 75-91

17. :Codes and Information Rusian Math. Surveys 39:1(1984)

87-141

18. M.A.Tsfasman: Goppa codes What are Better than the Varshamor-Gilbert Bound. Prob, Inform. Transmission 18(1982) 163-166