数理解析研究所講究録
第786巻 1992年 49-73

曲線族 C_a^b, $_rC_a^b$ 上の代数幾何符号の構造

日本電気㈱C&C情報研究所　三浦　晋示（Shinji Miura）

1. まえがき

近年，デジタル通信技術の進歩は著しく，それに伴って誤り訂正符号の応用がますます盛んになってきている．しかし，応用に関する研究ばかりでなく，より良い符号を構成しその復号法を見つけるという符号理論の最も中心的な研究も着実に成果をあげてきている．現在，その核をなすのは代数幾何符号の研究である．代数幾何符号は V.D.Goppa[1] によって発見され，その後の研究で注目すべき多くの性質が明らかになってきている．それにともない最近ではそれらをまとめた教科書も数多く出版されるようになった[14],[15],[16],[17]．それらには代数幾何符号の一般的な性質，復号問題，漸近論などのごく最近までの成果がまとめられている．しかし，それら多くの成果に比較して具体例のあまりに少ない事に気づく．すなわち，よい曲線の探索と符号の具体的な構成はまだほとんど進められていないのが実状である．楕円曲線符号族[3],[5],[9]，超楕円曲線符号族[8],[9]，Schmidt 曲線符号[7],[14]，Hermite 曲線符号[2],[4],[7]，Fermat 曲線符号[2]，The Klein quartic 上の符号[6]，H. Stichtenoth

の曲線符号族[8]，J.P.Hansen らの曲線符号[10]，Modular 曲線符号族，等に関して幾つかの報告があるにすぎない．しかもそれらの内で有理的な座を多数もつ曲線の探索と符号の構成が具体的に示されているのは数例に限られる．さて，一般に代数幾何符号は，曲線が有理的な座を多く持つほど訂正能力は高い．それゆえ，任意の自然数gと有限体Fに対して，種数がgでF有理的な座をなるべく多く持つ曲線の探索が課題となる．さらに，符号の検査行列の具体的な構成手順と，経済的効率的な符号化／復号アルゴリズムを要求される．そこで，復号問題の解決が一般論としてほぼ見えてきた現在，比較的小さい有限体Fと自然数gからなる組の全てに関して，F有理的な座を最大にする種数gの曲線の組織的な探索とそれらのデータベース化は重要な課題である．さらに，符号化／復号アルゴリズムを具体的に作動する際に必要となる有理関数，またそれらから導かれる検査行列，等も同時に導いておく必要がある．

以上の課題をふまえ，本稿では二種類の曲線族 $C_a{}^b$，${}_rC_a{}^b$ を，種数を一定にかつ検査行列が統一的に構成できる中で最も大きな自由度を保つように選定し提案する．ついで，符号の構造を明らかにし，それらの中で有理的な座を最大にする曲線の探索を行なう．構造解明と探索は成功し，新たに数多くの性能のよい符号が発見できた．

2. 準備（代数幾何符号）

$F = GF(q)$ をq元からなる有限体とする．nを自然数とし F^n を線形空間とする．写像 $d: F^n \times F^n \to N$，$d(x, y) = \#\{j: x_j \neq y_j, 1 \leqq j \leqq n\}$ は距離

の公理を満たし，これによりF^nに距離空間としての構造が入る．これをハミング距離と呼ぶ．また，$wt: F^n \to N$, $wt(x)=d(x, 0)$をハミング重みと呼ぶ．一般にF上の線形符号Cとは，ある自然数nに関する線形距離空間F^nの部分空間をいう．集合としては$C \subset F^n$である．このときF^nを受信空間，Cを符号語空間，またその元を符号語と呼ぶ．nを符号長，$k=\dim(C)$を情報次元，$d_{min}=\min\{wt(x): 0 \neq x \in C\}$を最小距離，また，k/nを符号効率，$d_{min}/n$を訂正能力率と呼ぶ．符号理論の中心的な課題の一つとして，一般に有限体Fと符号効率＝k/nを指定したとき，各々のnに対して訂正能力率＝d_{min}/nを大，或は訂正能力率を一定に保つときnを大にする符号語空間Cの具体的構成とその効率的な符号化／復号アルゴリズムの発見がある．さて，XをF上絶対既約な射影曲線とする．Xの種数をgenus(X)または簡単にgと表す．Fの代数的閉包を$\mathbb{F}$とする．$X(F)$をXのF有理点全体の集合，また$X(\mathbb{F})(\supset X(F))$をXの$\mathbb{F}$有理点全体の集合とし以後Xで表わす．$X^*$をXの非特異モデル（正規化）とし$\mu: X^* \to X$をXの特異点の解消を与える双有理射とする．各点$P \in X$に対して$\mu^{-1}(P)$に含まれる$X^*$の点を，Pを中心とする座と呼ぶ．曲線X上のすべての座Pに関して，それらの有限個の整数係数の形式的な和$\Sigma\ n_P \cdot P$をX上の因子という．また，$Aut(X^*/X^*(F))$をX^*の$X^*(F)$上の自己同型群とするとき，任意の$\sigma \in Aut(X^*/X^*(F))$に対して因子$\Sigma\ n_P \cdot P$が，$\Sigma\ n_P \cdot P = \Sigma\ n_P \cdot \sigma(P)$を満たすときに，$\Sigma\ n_P \cdot P$をF有理的な因子という．各因子$H=\Sigma\ n_P \cdot P$に対して，座Pの係数をすべて加えたもの$\Sigma\ n_P$をHの次数といい，deg(H)で表す．$n_P \neq 0$なるPの全体をHの台といい，supp(H)で

表す．また，$n_P \leqq m_P\ (\forall P)$のときに$\Sigma\ n_P \cdot P \leqq \Sigma\ m_P \cdot P$と表し，$0 \leqq H$のときにHを有効因子（あるいは正因子）と呼ぶ．Rat(X)は曲線Xの$\mathbb{F}$上の有理関数体を表し，$\Omega^1(\mathrm{Rat}(X))$は曲線Xの$\mathbb{F}$上の一次微分加群を表すとする．任意の$\mathbb{F}$有理的な因子Hに関して，$L(H)=\{f\in \mathrm{Rat}(X):\ (f)+H\geqq 0 \text{ or } f=0\}$，$\Omega(H)=\{\omega\in \Omega^1(\mathrm{Rat}(X)):\ (\omega)\geqq H \text{ or } \omega=0\}$とおくと，これらはともに，次元の有限な$\mathbb{F}$上の線形空間をなす．それらの$\mathbb{F}$ベクトル空間としての次元をそれぞれ$\dim L(H)=\ell(H)$，$\dim\Omega(H)=\delta(H)$と表す．ただし，ここで(f)，$(\omega)$は有理関数f，有理一次微分$\omega$に付随する因子である．また，$K_X$をXの$\mathbb{F}$有理的な標準因子，すなわち$\omega\ (\neq 0)\in \Omega^1(\mathrm{Rat}(X))$，$K_X=(\omega)$とすると$\delta(H)=\ell(K_X-H)$であり，$\deg(K_X)=2g-2$，$\deg(H)<0$ならば$\ell(H)=0$である．さて，$P_1, P_2, \cdots, P_n$をXの$\mathbb{F}$有理的な座とし，因子Dを$D=P_1+P_2+\cdots+P_n$とする．またGを$\mathbb{F}$有理的な因子とし，$\mathrm{supp}(D)\cap \mathrm{supp}(G)=\varnothing$，$m=\deg(G)$，$n=\deg(D)$とする．写像$\alpha_L$，$\alpha_\Omega$を

α_L：$L(G)\to \mathbb{F}^n$，

$$f\to (f(P_1), f(P_2), \cdots, f(P_n))$$

α_Ω：$\Omega(G-D)\to \mathbb{F}^n$，

$$\omega\to (\mathrm{res}_{P_1}\omega, \mathrm{res}_{P_2}\omega, \cdots, \mathrm{res}_{P_n}\omega)$$

と定義する．ただし，$\mathrm{res}_P\omega$は留数．

このとき，V.D.Goppa[1],[2]は２つの線形符号を，

$C_L(X,D,G)=\mathrm{Image}(\alpha_L)\subset \mathbb{F}^n$，$C_\Omega(X,D,G)=\mathrm{Image}(\alpha_\Omega)\subset \mathbb{F}^n$，

と定義した．次の事実が知られている[14],[15],[16],[17]．

[定理1](文献(8),(14))

線形符号$C_\Omega(X,D,G)=\mathrm{Image}(\alpha_\Omega)\subset \mathbb{F}^n$の情報次元kと最小距離$d_{min}$は，$k=\dim(\mathrm{Image}(\alpha_\Omega))=\delta(G-D)-\delta(G)=n-\ell(G)+\ell(G-D)$，$d_{min}=\min\{d:\ \delta(G-\Sigma_{j=1}^{d}Q_j)>\delta(G)$，$Q_j$はsupp(D)のある異なるd点$\}$，$\ell(G)-\ell(G-D)+1\geqq d_{min}\geqq\max\{1,m-2g+2\}$．特に，$2g-1\leqq m$ならば$\ell(G)=m-g+1$，$0\leqq m\leqq n-1$ならば$\ell(G-D)=0$である．なお，$\ker\alpha_\Omega=\Omega(G)$である．□

[定理2](文献(8),(14))

線形符号$C_L(X,D,G)=\mathrm{Image}(\alpha_L)\subset \mathbb{F}^n$の情報次元$k^*$と最小距離$d^*_{min}$は，$k^*=\dim(\mathrm{Image}(\alpha_L))=\ell(G)-\ell(G-D)$，

$d^*_{min}=\min\{d^*:\ \ell(G-D+\Sigma_{j=1}^{d^*}Q_j)>\ell(G-D)$，$Q_j$はsupp(D)のある異なる$d^*$点$\}$，$n-\ell(G)+\ell(G-D)+1\geqq d^*_{min}\geqq\max\{1,n-m\}$．なお，$\ker\alpha_L=L(G-D)$である．□

[定理3]　線形符号$C_L(X,D,G)$，$C_\Omega(X,D,G)$が意味をなすのは，$0\leqq m\leqq n+2g-2$の場合に限る．$n+2g-1\leqq m$ならば，$C_L(X,D,G)=\mathbb{F}^n$，$C_\Omega(X,D,G)=(0)$，また，$m\leqq -1$ならば，$C_L(X,D,G)=(0)$，$C_\Omega(X,D,G)=\mathbb{F}^n$である．□

[定理4](文献(14))　線形符号$C_L(X,D,G)$と$C_\Omega(X,D,G)$は互いに双対空間となる．$C_L(X,D,G)=C_\Omega(X,D,G)^\perp$．すなわち，$x\in C_L(X,D,G)$，$y\in C_\Omega(X,D,G)$とすると，$\Sigma_{j=1}^{n}x_j\cdot y_j=0$．□

これらは，次の二つの基本的な定理から導かれる．

[Riemamm-Rochの定理5]$\ell(H)=\delta(H)+\deg(H)-g+1$．□

[留数の定理6]　任意の$\mathbb{F}$上の一次微分ζに対して，$\mathrm{res}_P\zeta\neq 0$なる座Pは有限個に限られ，それら有限個の留数の和は$\Sigma_P\ \mathrm{res}_P\zeta=0(\in\mathbb{F})$を満た

す．ただし，$\sum_P$は座Pのすべてにわたるものとする．□

また，次の事実が知られている．

[定理7](文献(5)) 線形符号$C_L(X,D,G)$と$C_\Omega(X,D,G)$に於て最長符号長はXのF有理的な座の総数nに等しく，

$n \leqq q+1+2g\sqrt{q}$： Hasse-Weil upper bound

$n \leqq q+1+g\lfloor 2\sqrt{q}\rfloor$： Hasse-Weil-Serre upper bound

である．また，$\lim(n\to\infty)g/n \geqq 1/(\sqrt{q}-1) > 1/\lfloor 2\sqrt{q}\rfloor$である．なお，$\lim(n\to\infty)g/n = 1/(\sqrt{q}-1)$を満たす曲線系列として Modular 曲線族が知られている．□

[定理8](文献(11)) 任意の線形符号$C \subset \mathbb{F}^n$は，F上絶対既約な射影曲線Xと，X上のF有理的な因子D,Gを適当に定めると，$C = C_L(X,D,G) = Image(\alpha_L) \subset \mathbb{F}^n$と表現できる．なお，この場合，Xの種数gの最小な表現が最もよく最適表現と呼ぶ．また$C_\Omega(X,D,G)$についても同様なことがいえる．□

3. 平面曲線上の代数幾何符号

ここでは，絶対既約な射影平面曲線の一般形$H_a{}^b$を与え，$H_a{}^b$上の代数幾何符号を具体的に構成するときに必要となる特異点の解消と種数の導出を述べる．ついで，アフィン平面曲線$f(x,y)=0$の原点が$x^a+y^b=0$の原点と同じ型の尖点となるための必要十分条件を与える．

3．1 曲線族$H_a{}^b$

$0 \leqq a \leqq b$なる任意の自然数a, bについて, 曲線$H_a{}^b$を次のように与える. このとき$H_a{}^b$は絶対既約な射影平面曲線の一般形となる.

$H_a{}^b$: $H(X,Y,Z) = \Sigma_{j=0}{}^a H_{b-j}(X,Z)Y^j$, ただし, $H(X,Y,Z)$はX,Y,Zに関する次数がb次で$\mathbb{F}$上絶対既約な斉次多項式とする. すなわち代数的閉包$\mathbb{F}$上でも既約とする. $H_{b-j}(X,Z)$, $(0 \leqq j \leqq a)$はX,Zに関する次数がb-j次の斉次多項式である. また, $H_b(X,Z) \neq 0$, $H_{b-a}(X,Z) \neq 0$とする. 以下簡単のため, $H_a{}^b$は曲線族$H_a{}^b$と呼ぶときは曲線$H_a{}^b$の全体の集合をまた曲線$H_a{}^b$と呼ぶときはその一つの曲線を表すとする. 点$P=(0:1:0)$は, $1 \leqq a \leqq b-2$のときに特異点となる.

3. 2 特異点の解消と種数の導出

ここでは, 文献(13)に従って特異点を持つことを許した射影平面曲線上に代数幾何符号を構成する際に必要な特異点の解消法と種数公式を確認する. まず blowing up を定義する. 有限体$\mathbb{F} = GF(q)$を固定する. Xを既約多項式$f(x,y) \in \mathbb{F}[x,y]$で定義されたアフィン平面曲線とする. X上の原点$P=(0,0)$における重複度を$r = e(P,X)$とする. このとき,

$$h_0(x,t) = f(x,xt)/x^r$$

$$h_1(s,y) = f(sy,y)/y^r$$

とおくと, これらはそれぞれ, xとt, sとy, に関する既約多項式をなす. $h_0(x,t)$をf(x,y)のy変換, $h_1(s,y)$をf(x,y)のx変換と呼ぶ. そこで, これらの定義するアフィン平面曲線をそれぞれ,

$$X^*{}_0 = \{(x,t) \in \mathbb{F}^2 : h_0(x,t) = 0\}$$

$X^*_1 = \{(s,y) \in \mathbb{F}^2 : h_1(s,y) = 0\}$, とおき, 点$(x,t) \in X^*_0 - V(t)$と点$(s,y) \in X^*_1 - V(s)$とを関係$x = sy$, $xt = y$によって同一視するとX^*_0とX^*_1とを貼り合わせた曲線$X^* = X^*_0 \cup X^*_1$を得る. ただし,

$V(t) = \{(x,t) \in \mathbb{F}^2 : t=0\}$

$V(s) = \{(s,y) \in \mathbb{F}^2 : s=0\}$

とする. そして正則射τ: $X^* \to X$を, $(x,t) \in X^*_0$のときは$\tau(x,t) = (x,xt)$, $(s,y) \in X^*_1$のときは$\tau(s,y) = (sy,y)$と定義する. τは$X^* - \{V(X) \cup V(Y)\}$と$X - \{0\}$の正則同型を与え, $\tau\{V(X) \cup V(Y)\} = \{0\}$である. このように定義された$\tau$: $X^* \to X$をアフィン平面曲線Xの原点を中心とした blowing up と呼ぶ. また, 点Pが一般の場合には原点を点Pに写す平行移動をπ: $\mathbb{F}^2 \to \mathbb{F}^2$とし, $\pi^{-1}(X)$の原点を中心とした blowing up をμ: $X^* = X^*_0 \cup X^*_1 \to \pi^{-1}(X)$と表すとき, $\pi\mu$: $X^* = X^*_0 \cup X^*_1 \to X$をXの点Pを中心とした blowing up と呼ぶ. なお, アフィン平面曲線Xの原点を中心とした blowing up τ: $X^* = X^*_0 \cup X^*_1 \to X$で, 新しく発生する特異点は$X^*_0$上では$V(x)$, X^*_1上では$V(y)$の上に限られることが示される. またX^*_0とX^*_1に包含関係の存在するときはτ: $X^* \to X$は, τ: $X^*_0 \to X$あるいはτ: $X^*_1 \to X$に一致する. このための必要十分条件は, それぞれ,

$X^*_0 \cap V(t) = \varnothing \quad \Leftrightarrow$

$\{(0,y) \in \mathbb{F}^2 : f(0,y) = 0, \ y \neq 0\} = \varnothing$ かつ $h_1(0,0) \neq 0$

$X^*_1 \cap V(s) = \varnothing \quad \Leftrightarrow$

$\{(x,0) \in \mathbb{F}^2 : f(x,0) = 0, \ x \neq 0\} = \varnothing$ かつ $h_0(0,0) \neq 0$

である．また，点Pが正則点なら$\tau^{-1}(P)$は一点でかつ正則点である．特異点のときは$\tau^{-1}(P)=\{P_1,\cdots,P_s\}$とおくと$s\leqq e(P,X)$であるが，各点$P_i$は$X^*$の正則点とは限らない．特に$P_i$が$X^*$の特異点のときに，$P_i$をPに無限に近いXの特異点という．同じく$P_i$に無限に近い特異点もPに（位数2で）無限に近い特異点という．以下くり返す．一般に特異点Pと Pに無限に近い特異点は共に高々有限個であり，それ故高々有限回の blowing up によってアフィン平面曲線の全ての特異点は解消される．なお，Cを射影平面曲線とするとCは2つのアフィン平面曲線の貼り合わせとして表せるので，この場合でも特異点の解消は高々有限回の blowing up によってできる．なおこのとき，非特異モデルは高々有限個の非特異なアフィン平面曲線の貼り合わせとして表現されることに注意せよ．また，blowing up は$\mathbb{F}$有理性（$\mathbb{F}$有理点を有理点に写す）も保存するので，$\mathbb{F}$有理的な座の構造，非特異モデルの各々のアフィン平面曲線と元の曲線の有理関数の対応関係なども明らかになる．さらに，曲線の種数は次の公式から一般的に導かれる．（射影平面曲線に関する J.Plücker の公式）Cを次数がdの射影平面曲線とする．このとき，$\mathrm{genus}(C)=(d-1)(d-2)/2-\sum_Q \nu_Q(\nu_Q-1)/2$である．ただし，$\sum_Q$はC上の無限に近い特異点（Cの特異点も含める）の全てに関する和であり，ν_Qは点Qの重複度とする．また，PをCの特異点とするとき$\varepsilon_P=\sum_Q \nu_Q(\nu_Q-1)/2$とおく．ただし，ここでの$\sum_Q$はPに無限に近い特異点の全てに関する和である．このとき，J.Plücker の公式は，$\mathrm{genus}(C)=(d-1)(d-2)/2-\sum_P \varepsilon_P$と表される．ここで，$\sum_P$はCの特異点の全てに関する和である．また，尖点の定義を本論文では次の意味で使用

する．Pを曲線Xの特異点とする．Pを中心に blowing up してμ： $X_1 \to X$を得るとき$\mu^{-1}(P)=\{P_1\}$と一点しかないとする，さらにP_1で blowing up してμ_1： $X_2 \to X_1$を得るとき$\mu_1^{-1}(P_1)=\{P_2\}$と一点しかないとする，・・・．このようにつねにPに無限に近い位数 i の特異点P_iが常に一点しかでてこないとき，PをXの尖点（cusp）という．

[例1] a，bを互いに素な自然数とする．a＜bとする．

$Z^{b-a}Y^a+X^b$の特異点P＝(0:0:1)に於けるε_Pを計算する．

b/aの正則連分数展開を，

$b = k_0 a + a_1$,

$a = k_1 a_1 + a_2$,

・・・

$a_{q-2} = k_{q-1} a_{q-1} + 1$,

$a_{q-1} = k_q 1$, とする．ただし，$k_j > 0$, $a_{j-1} > a_j > 0 (1 \leqq j \leqq q)$．$k_0 > 0$, $a_0 = a$とする．アフィン平面曲線X：y^a+x^bの特異点は原点のみである．Xの特異点の解消は次のように実行される．なお，この場合 blowing up を2枚のアフィン平面曲線の貼り合わせとして表わしていくとき，いつでもそれらには必ず包含関係があることを注意しておく．また新しく発生する特異点は原点のみである．すなわち，Pは尖点である．

y^a+x^bにy変換をk_0回施して，$y^a+x^{a_1}$を得る．重複度はa_1である．これに，x変換をk_1回施して，$y^{a_2}+x^{a_1}$を得る．重複度はa_2である．・・・・．さらに，qの奇偶に従って，y変換をk_{q-1}回あるいはx変換をk_{q-1}回施して，$y^{a_{q-1}}+x$あるいは$y+x^{a_{q-1}}$を得る．特異点解消おわり．$\sum_{j=0}^{q-1} k_j a_j^2 = ba-$

a_{q-1}, $\sum_{j=0}^{q-1} k_j a_j = b+a-a_{q-1}-1$に注意すると, $\varepsilon_P = \sum_Q \nu_Q(\nu_Q-1)/2 = \sum_{j=0}^{q-1} k_j a_j(a_j-1)/2 = (b-1)(a-1)/2$である. 同様に, $Z^{b-a}Y^a+X^b$の特異点$P=(0:1:0)$に於けるε_Pは, $\varepsilon_P = (b-1)(b-a-1)/2$である. すなわち, 次の補題が示された.

[補題9] a, bを互いに素な自然数とする. $a<b$とする. $Z^{b-a}Y^a+X^b$の特異点$P=(0:1:0)$に於けるε_Pは, $\varepsilon_P = (b-1)(b-a-1)/2$である. □

3. 3 アフィン平面曲線$f(x,y)=0$の原点が$x^a+y^b=0$の原点と同じ型の尖点となるための必要十分条件

[補題10] a, bを互いに素な自然数とする.

アフィン平面曲線$x^a+y^b+x^cy^d$（c, d; 非負整数）の原点が曲線x^a+y^bの原点と同じ型の尖点になるための必要十分条件は, $ab \leqq ad+bc$が成り立つことである. (証明略). ■

[主補題11] a, bを互いに素な自然数とする.

$f_{a0}\cdot x^a \neq 0$と$f_{0b}\cdot y^b \neq 0$を項として持つアフィン平面曲線$f(x,y)$の原点が曲線x^a+y^bの原点と同じ型の尖点になるための必要十分条件は, $f(x,y)$に現われる項$f_{cd}\cdot x^cy^d \neq 0$に関して$ab \leqq ad+bc$（c, d; 非負整数）が成り立つことである. (証明)補題10から導かれる. ■

4. 曲線族$T_a{}^b$上の代数曲線符号

曲線$H_a{}^b$に於て, さらに条件$H_{b-j}(X,0)=0, (1 \leqq j \leqq a)$, $H_b(X,0) \neq 0$を仮定したときの$H_a{}^b$を$T_a{}^b$と表す. このとき曲線$T_a{}^b$は, Zに関する無限遠

点として高々一点P＝(0:1:0)を持ち，さらに，div(Z)＝b·Pを満たす．ただし，div(Z)は，Zに付随する因子を表すが，ここでは点Pが特異点である場合も許した表示とする．射影平面曲線H_a^bのF有理点全体からなる集合を$H_a^b(F)$と表すと，次の事実が示される．

[定理12]（曲線T_a^bのF有理点）

$T_a^b(F)=\{P\}\cup\{(x:y:1)\mid H(x,y,1)=0,\ x,y\in F\}$である．□

4．1　曲線族C_a^b

[定理13] a，bを互いに素な自然数とする．ただし，a＜b．H_a^b: $H(X,Y,Z)=\Sigma_{j=0}^{a} H_{b-j}(X,Z)Y^j$，ただし，$H_{b-a}(0,Z)\neq 0$，$H_b(X,0)\neq 0$，に於て点P＝(0:1:0)が$Y^aZ^{b-a}+X^b$の点Pと同じ型の尖点になるための必要十分条件は，$f(j)=\lceil(b-a)j/a\rceil$とおくとき，$Z^{f(j)}\mid H_{b-j}(X,Z)$，$0\leqq j\leqq a$である．なおこのとき，Pは座として扱ってよい．

(証明)主補題11から導かれる．■

ただし，実数sに対してs≧0のときは$\lceil s\rceil$はs以上の整数の中で最小なものを表わし，s＜0のときは$\lceil s\rceil$は0を表わす．また，$\lfloor s\rfloor$はs≧0のときはs以下の整数の中で最大なものを表わし，s＜0のときは0を表わすとする．多項式F，Hに対してF∣HはHがFで割り切れることを示す．曲線H_a^bが定理の仮定を満たし，さらに点Pを除いて特異点が存在しないときのH_a^bをC_a^bと表す．

4．1．1　曲線族C_a^b上の代数幾何符号の構造

曲線族C_a^bに関しては次の事実が示される.

[命題15] 曲線族C_a^bは曲線族T_a^bに含まれ曲線C_a^bの$\mathbb{F}$有理的な座は$C_a^b(\mathbb{F})=\{P\}\cup\{(x:y:1)\mid H(x,y,1)=0,\ x,y\in\mathbb{F}\}$に一致する. □

[定理14] 曲線C_a^bの種数は,

$$\mathrm{genus}(C_a^b)=(b-1)(b-2)/2-(b-1)(b-a-1)/2$$
$$=(b-1)(a-1)/2$$ である.

(証明)補題9から$\varepsilon_P=(b-1)(b-a-1)/2$である. ■

[定理15] 曲線C_a^bに関して,

$\mathrm{div}(X)=(b-a)\cdot P+\sum_{j=1}^{a}(0:\kappa_j:1)$,

$\mathrm{div}(Y)=\sum_{j=1}^{b}(\lambda_j:0:1)$,

$\mathrm{div}(Z)=b\cdot P$である. ただし, div( )は因子. また, κ_j ($\in\overline{\mathbb{F}}$, $1\leqq j\leqq a$)は$H(0,\kappa,1)=\sum_{j=0}^{a}\kappa^j H_{b-j}(0,1)=0$の解で, λ_j ($\in\overline{\mathbb{F}}$, $1\leqq j\leqq b$)は$H(\lambda,0,1)=H_b(\lambda,1)=0$の解である. なお, $\overline{\mathbb{F}}$は$\mathbb{F}$の代数的閉包である. また, 有理関数x, yを$x=X/Z$, $y=Y/Z$とおくと,

$\mathrm{div}(x)=\sum_{j=1}^{a}(0:\kappa_j:1)-a\cdot P$,

$\mathrm{div}(y)=\sum_{j=1}^{b}(\lambda_j:0:1)-b\cdot P$.

特に, $\mathrm{order}_P(x)=-a$, $\mathrm{order}_P(y)=-b$である. □

$\Gamma_a^b=\{x^k y^j:\ 0\leqq j\leqq a-1, 0\leqq k\}\subset \mathrm{Rat}(X)$, $\Gamma_a^b(m)=\{x^k y^j:\ 0\leqq j\leqq a-1, 0\leqq k, ak+bj\leqq m\}\subset\Gamma_a^b$とおく. また, 写像$\tau$: $\mathrm{Rat}(X)\setminus\{0\}\to\mathbb{N}$を$\tau(f)=-\mathrm{order}_P(f)$とする. このとき$\tau$: $\Gamma_a^b\to\mathbb{N}$は単射である. $\Lambda_a^b=\mathbb{N}-\tau(\Gamma_a^b)=\{ak+(bj \bmod a):\ 0\leqq k\leqq \lfloor bj/a\rfloor-1, 0\leqq j\leqq a-1\}$とおく. ただし$\mathbb{N}$は0を含む自然数全体の集合とする.

[補題16]　$\#\Lambda_a{}^b=(a-1)(b-1)/2$.

(証明)　$\#\Lambda_a{}^b=\Sigma_{j=1}{}^{a-1}\lfloor bj/a\rfloor=(a-1)(b-1)/2$. ■

すなわち，$\#\Lambda_a{}^b=\mathrm{genus}(C_a{}^b)$. それゆえ，$\Gamma_a{}^b(m)\subset L(m\cdot P)$に注意すると集合$\Lambda_a{}^b$は曲線$C_a{}^b$の点Pに於ける空隙系列（gap sequence）をなすことが示される．$\tau(\Gamma_a{}^b)$はその構造から，Nを0を含む自然数全体からなる加法的単位半群としたとき，自然数0，$a=-\mathrm{order}_P(x)$，$b=-\mathrm{order}_P(y)$で生成されるNの部分半群を成す事が示される．また，点Pは Weierstrass point である．なお，自然数kが曲線上の点Pに於ける空隙値（gap value）であるとは，$L(k\cdot P)=L((k-1)\cdot P)$を満たす場合をいう．すなわち，点Pのみで極を持ち，Pに於ける位数が-kと等しい有理関数の存在しない場合をいう．そして，空隙値の全体を空隙系列（gap sequence）と呼ぶ．一般に空隙値は$\{1,2,\cdots,2g-1\}$に含まれ，その総数は曲線の種数gに一致することが知られている．また，点Pに於ける空隙系列が$\{1,2,\cdots,g\}$に等しくないとき，Pは Weierstrass point であると呼ばれる．

[定理17]　$\Lambda_a{}^b\subset N$は曲線$C_a{}^b$の点Pに於ける空隙系列である．□

[定理18]　$\Gamma_a{}^b(m)=\{x^k y^j:\ 0\leqq j\leqq a-1, 0\leqq k, ak+bj\leqq m\}$は，曲線$C_a{}^b$上の線形空間$L(m\cdot P)$の基底となる．□

[注意1]　実は曲線族$C_a{}^b$はさらに拡張できて，曲線族$C_a{}^{b\cdot m}$とする事ができる．$m=b$の場合が$C_a{}^{b\cdot m}=C_a{}^b$である．mを自然数とし，a，bを互いに素な自然数とする．ただし，$a<b\leqq m$.

$H_{a+m-b}{}^m$: $H(X,Y,Z)=\Sigma_{j=0}{}^{a+m-b}H_{m-j}(X,Z)Y^j$，ただし，$H_{b-a}(0,Z)\neq 0$，$H_b(X,0)\neq 0$，に於て点$P=(0:1:0)$が$Y^aZ^{b-a}+X^b$の点Pと同じ型の尖点になる

ための必要十分条件は，$f(j)=\lceil(b-a)(b-m+j)/a\rceil$とおくとき，$Z^{f(j)} \mid H_{m-j}(X,Z)$，$0\leqq j\leqq a+m-b$で，これが成立したとせよ．なおこのとき，Pは座として扱ってよい．ここで，さらに点Pを除いて特異点が存在しないときのH_{a+m-b}^{m}を$C_a^{b,m}$と表す．$\mathrm{genus}(C_a^{b,m})=(m-1)(m-2)/2-(b-1)(b-a-1)/2$である．$C_a^{b,m}$が本来は，特異点としてアフィン平面曲線$z^{b-a}+x^b$の原点と同じ型の尖点をただ一つもつ射影平面曲線族の最も一般的な定式化である．しかし，これを採用しなかったのは，$m>b$のときは定理18に相当する命題が成立しないからである．$C_a^{b,m}$の例としては，例えば標数2の上の$C_5^{7,9}$：$Z^2Y^7+X^7Y^2+X^8Y+Z^9$があげられる．

4．1．2　超だ円符号

ここで標数が2の有限体上の超だ円曲線曲線，すなわちC_2^{2g+1}の，点P以外に特異点をもたないための必要十分条件を与えよう．次が成り立つ．

[定理19]　標数が2の有限体上の曲線C_2^{2g+1}に於て，

$g\geqq 2$のとき，$P=(0:1:0)$は特異点である．また，$H_{2g}(\lambda,1)=0$，なる$\lambda\in \mathbb{F}$に対して，$\mu=\sqrt{H_{2g+1}(\lambda,1)}\in \mathbb{F}$と置くとき，$H_X(\lambda,\mu,1)=0$ならば，点$(\lambda:\mu:1)$も特異点である．なおこれら以外には特異点はない．□

4．1．3　既知の曲線と曲線族C_a^bの関係

①　$a=2$，$b=3$，$H_3(X,0)=X^3$と制限したときの曲線C_2^3は楕円曲線の（体の標数に依存しない）Weierstrass の標準形そのものである．これに関しては，Y.Driencort[3]らの詳しい報告がある．

② $a=2$, $b=2g+1$と制限したC_2^{2g+1}は種数がgの超楕円平面曲線の（体の標数に依存しない）一般形を与える．なお，このとき$P=(0:1:0)$は hyperelliptic Weierstrass point である．また，$\mathbb{F}=GF(q^{2m})$上の($q=2^e$, mは奇数)，C_2^{q+1}: $Y^2Z^{q-1}+YZ^q+X^{q+1}$, はHasse-Weil upper bound を達成し特に性質のよい曲線である．これらに関しては，一部文献(8)と，文献(9)に詳しい報告がある．

③ H. Stichtenoth[9] は Kummer 拡大として$\mathbb{F}=Gf(q)$上，$y^e=f(x)$．ただし，$f(x)=q_1(x)\cdots q_r(x)$，$q_i(x)\in\mathbb{F}[x]$は，既約でかつ互いに素，また$\deg(f(x))=m$とするとき，$g.c.d(e,m)=1$，$q\equiv 1 \bmod e$，を考察している．これらは，射影化するとC_e^m，あるいはC_m^eに含まれる．

④ $b=a+1$としたC_a^{a+1}は非特異となるが，この場合のC_a^{a+1}は Hasse-Weil upper bound に達する F.K.Schmidt の曲線を含む．$\mathbb{F}=GF(q)$上の$y^m=x^p+x$，ただし，$m>2$，$m\mid(p+1)$，$q=p^2$，pは素数のべきである．$m\leqq p$のときはC_m^pに，また$m=p+1$のときは$x^m=y^p+y$としてC_p^mに含まれ，これは Hermitian curves $X^m+Y^m+Z^m$ と双有理同型である．これらに関しては，H.J.Tiersma[4]と H.Stichtenoth[7] に詳しい報告がある．なお，一般の Fermat curves $X^n+Y^n+Z^n$も$X\to X+(\sqrt[n]{(-1)})Y$と座標変換すればC_{n-1}^nに帰着される．また The Klein quartic $Y^3Z+X^3Y+Z^3X$[6]は$C_2^{3,4}$に含まれる．

⑤ H. Stichtenoth[8] は Artin-Schreier 拡大として$\mathbb{F}=Gf(q)$上，$f(y)=h(x)$，$f(y)\in\mathbb{F}[y]$，$h(x)\in\mathbb{F}[x]$．ただし，$\mathbb{F}$の標数を$p=\mathrm{char}\,\mathbb{F}$とするとき，

(1)　$h(x)=\sum_{i=0}^{r} c_i\cdot x^{\wedge}(p^i)$,　$c_0\neq 0$,　$c_r\neq 0$,

(2)　$\{x\in \mathbb{F} : f(x)=0\}$は$\mathbb{F}$の位数が$m=p^r$の加法的部分群をなす,

(3)　$\deg(f)=e\neq 0 \bmod q$,

(4)　$(y)_\infty=m\cdot P_\infty$,　$(dy)=((m-1)(e-1)-2)\cdot P_\infty$,　$\mathrm{genus}=(m-1)(e-1)/2$,　とする平面曲線上の符号の構造を考察している．これらも，射影化するとC_e^mに含まれる．

4．2　曲線族${}_rC_a^b$

[定理21]　a，b，rを非負整数とする．ただし，$a<b$，$a+r<b$，aとb，$a+r$とb，$r+1$とbは互いに素とする．H_{a+r}^b：$H(X,Y,Z)=\sum_{j=0}^{a+r} H_{b-j}(X,Z)Y^j$，ただし，$H_{b-a-r}(0,Z)\neq 0$，$H_{b-r-1}(0,Z)\neq 0$，$H_b(X,0)\neq 0$，に於て，点$P=(0:1:0)$が$Y^{a+r}Z^{b-a-r}+X^b$の点Pと，また点$Q=(0:0:1)$が$Y^{r+1}Z^{b-r-1}+X^b$の点Qとそれぞれ同じ型の尖点になるための必要十分条件は，$f(j)=\lceil (b-a-r)j/(a+r)\rceil$，$g(j)=\lceil b(r+1-j)/(r+1)\rceil$とおくとき，$X^{g(j)}Z^{f(j)} \mid H_{b-j}(X,Z)$，$0\leqq j\leqq a+r$である．なおこのとき，P，Qは座として扱ってよい．

(証明)主補題11から導かれる．■

曲線H_{a+r}^bが定理の仮定を満たし，さらに点P,Qを除いて特異点が存在しないときのH_{a+r}^bを${}_rC_a^b$と表す．

4．2．1　曲線族${}_rC_a^b$上の代数幾何符号の構造

曲線族${}_rC_a^b$に関しては次の事実が示される．

[命題22]　曲線族${}_rC_a^b$は曲線族T_{a+r}^bに含まれ，曲線

${}_rC_a^b$のF有理的な座は${}_rC_a^b(F)=\{P\}\cup\{(x:y:1)\mid H(x,y,1)=0,\ x,y\in F\}$に一致する. □

[定理23] 曲線${}_rC_a^b$の種数は, $genus({}_rC_a^b)=(b-1)(b-2)/2-(b-1)(b-a-r-1)/2-(b-1)r/2=(b-1)(a-1)/2$である.

(証明)$P=(0:1:0)$, $Q=(0:0:1)$とすると, 補題9から,

$\varepsilon_P=(b-1)(b-a-r-1)/2$, $\varepsilon_Q=(b-1)r/2$である. ■

[定理24] 曲線${}_rC_a^b$に関して,

$div(X)=(b-a-r)\cdot P+(r+1)\cdot Q+\sum_{j=1}^{a-1}(0:\kappa_j:1)$,

$div(Y)=b\cdot Q$,

$div(Z)=b\cdot P$である. ただし$\kappa_j(\in\mathbb{F}, 1\leqq j\leqq a-1)$は, $\sum_{j=0}^{a-1}H_{b-j-r-1}(0,1)\kappa^j=0$の解である. また, 有理関数x, yを$x=X/Z$, $y=Y/Z$とおくと,

$div(x)=(r+1)\cdot Q+\sum_{j=1}^{a-1}(0:\kappa_j:1)-(a+r)\cdot P$,

$div(y)=b\cdot Q-b\cdot P$.

特に, $order_P(x)=-(a+r)$, $order_P(y)=-b$である. □

つぎに, 曲線${}_rC_a^b$の点(座)Pに於ける空隙系列(gap sequence)を求めよう. これにより, 線形空間$L(m\cdot P)$の基底も導かれる. 自然数$j=1,2,\cdots,r,\cdots,r+a$に対して, 自然数値をとる関数$I(j)$を, $I(j)=\min\{i: jb\leqq i(r+1)\}$すなわち, $I(j)=\lceil jb/(r+1)\rceil$とする. $1\leqq j\leqq r$なるjに関しては, $I(j)<b$, $r+1\leqq j\leqq r+a$なるjに関しては, $b\leqq I(j)$となることを注意せよ. このとき, x, y, $h_j=x^{I(j)}/y^j$, $(1\leqq j\leqq r)$は点Pを唯一の極として持つ有理関数となる. $h_r=x^{I(r)}/y^r$, $h_{r-1}=x^{I(r-1)}/y^{r-1}$, $\cdots$, $h_1=x^{I(1)}/y$, $1, y, y^2, \cdots, y^{a-1}$を初項として, 公比をxとした等比数列の集合を${}_r\Gamma_a^b$と

する．また，そのうち点Pに於ける位数が-m以上のものの集合を${}_r\Gamma_a{}^b(m)$とおく．${}_r\Gamma_a{}^b=\{x^ky^j:\ 0\leqq j\leqq a-1, 0\leqq k\}\cup\{x^kh_j:\ 1\leqq j\leqq r, 0\leqq k\}\subset Rat(X)$，${}_r\Gamma_a{}^b(m)=\{x^ky^j:\ 0\leqq j\leqq a-1, 0\leqq k, (a+r)k+bj\leqq m\}\cup\{x^kh_j:\ 1\leqq j\leqq r, 0\leqq k, -order_P(x^kh_j)\leqq m\}\subset{}_r\Gamma_a{}^b$である．また，写像$\tau$: $Rat(X)\setminus\{0\}\to N$を$\tau(f)=-order_P(f)$とする．このとき$\tau$: ${}_r\Gamma_a{}^b\to N$は単射である．${}_r\Lambda_a{}^b=N\setminus\tau({}_r\Gamma_a{}^b)$とおく．

[補題25] $\#{}_r\Lambda_a{}^b=(a-1)(b-1)/2$.

(証明) $\#{}_r\Lambda_a{}^b=(a+r-1)(b-1)/2-\{\Sigma_{j=1}{}^r\ b-I(j)\}=(a+r-1)(b-1)/2-r(b-1)/2=(a-1)(b-1)/2$. ■

すなわち，$\#{}_r\Lambda_a{}^b=genus({}_rC_a{}^b)$．それゆえ，${}_r\Gamma_a{}^b(m)\subset L(m\cdot P)$に注意すると集合${}_r\Lambda_a{}^b$は曲線${}_rC_a{}^b$の点Pに於ける空隙系列（gap sequence）をなすことが示される．$\tau({}_r\Gamma_a{}^b)$はその構造から，Nを0を含む自然数全体からなる加法的単位半群としたとき，自然数0，$a+r=-order_P(x)$，$b=-order_P(y)$，$(a+r)I(j)-jb=-order_P(h_j)$, $(1\leqq j\leqq r)$，で生成されるNの部分半群を成す事が示される．また，点Pは Weierstrass point である．

[定理26] ${}_r\Lambda_a{}^b\subset\square N$は曲線${}_rC_a{}^b$の点Pに於ける空隙系列である．□

[定理27] ${}_r\Gamma_a{}^b(m)$は，曲線${}_rC_a{}^b$上の線形空間$L(m\cdot P)$の基底となる．□

[注意2] 注意1と同様に，曲線族${}_rC_a{}^b$はさらに拡張できて，曲線族${}_rC_a{}^{b,m}$とする事ができる．$m=b$の場合が${}_rC_a{}^{b,m}={}_rC_a{}^b$である．m，a，b，rを非負整数とする．ただし，$a<b$，$a+r<b\leqq m$，aとb，a+rとb，r+1とbは互いに素とする．$H_{a+r+m-b}{}^m$: $H(X,Y,Z)=\Sigma_{j=0}{}^{a+r+m-b}\ H_{m-j}(X,Z)Y^j$，ただし，$H_{b-a-r}(0,Z)\neq0$，$H_{b-r-1}(0,Z)\neq0$，$H_b(X,0)\neq0$，に於て，点$P=(0$

:1:0)が$Y^{a+r}Z^{b-a-r}+X^b$の点Pと，また点Q＝(0:0:1)が$Y^{r+1}Z^{b-r-1}+X^b$の点Qとそれぞれ同じ型の尖点になるための必要十分条件は，

$f(j)=\lceil (b-a-r)(b-m+j)/(a+r)\rceil$,

$g(j)=\lceil b(r+1-j)/(r+1)\rceil$とおくとき，

$X^{g(j)}Z^{f(j)} \mid H_{b-j}(X,Z)$, $0\leqq j\leqq a+r+m-b$で，これらが成立したとせよ．なおこのとき，P，Qは座として扱ってよい．ここで，さらに点P，点Qを除いて特異点が存在しないときの$H_{a+r+m-b}^{m}$を${}_rC_a^{b,m}$と表す．$\mathrm{genus}({}_rC_a^{b,m})=(m-1)(m-2)/2-(b-1)(b-a-r-1)/2-(b-1)r/2$である．${}_rC_a^{b,m}$が本来は，特異点としてアフィン平面曲線$y^a+x^b$の原点と同じ型の尖点をただ二つもつ射影平面曲線族の最も一般的な定式化である．

4．3　点P以外に特異点を持たない曲線

T_a^bに於てFの標数を2とするとき，点P＝(0:1:0)以外に特異点を持たない曲線としては，例えば次がある．ただし，T_a^bとしての制約に注意せよ．いずれもF上絶対既約となる．

①　T_a^b: $H(X,Y,Z)=Z^{b-a}Y^a+\Sigma_{i=1}^{[a/2]}H_{b-2i}(X,Z)Y^{2i}+H_b(X,Z)$，ただし，a（≧3）は奇数，$H_b(X,Z)=0$は重複因子を持たない．この仮定の下の$T_a^b$は$C_a^b$に含まれる．

②　T_a^b: $H(X,Y,Z)=\Sigma_{i=1}^{a/2}H_{b-2i}(X,Z)Y^{2i}+Z^{b-1}Y+H_b(X,Z)$，ただし，a（≧2）は偶数．

③　T_a^b: $H(X,Y,Z)=\Sigma_{i=1}^{a/2}H_{b-2i}(X,Z)Y^{2i}+Z^{b-c-1}Y^c+H_b(X,Z)$，ただし，a（≧2）は偶数，cは$1\leqq c\leqq a$なる奇数，$H_b(X,Z)=0$は重複因子を持

たない.

5. 有理点を多数もつ曲線の探索

種数gとFを一定にすると, F有理的な座の総数が多いほど曲線はよい符号を生成する. そこで, 有理的な座を多数持つ曲線の探索が課題となる. しかし, 有理的な座の総数に関して, 上限, すなわち最大値のあることは知られているものの, それがどのような値で, また, どのような曲線のときに上限に達するかは一般的には知られていない. そのため, 定理7で与えた上界式に達する曲線の探索が一つの目安になってくる.

ただし, 漸近的には $\lim(n\to\infty) g/n \geqq 1/(\sqrt{q}-1) > 1/\lfloor 2\sqrt{q} \rfloor > 1/2\sqrt{q}$

なのでgを無限に大きくしたときはそれらの上界式に達する曲線は存在しないことが示される.

5. 1 Hasse-Weil upper bound に達する曲線の例

以下は, 曲線の非特異モデルの有理点数が Hasse-Weil upper bound に達する例である.

[例2] $F = GF(2^{2e})$上, 超だ円曲線 C_{2^b}: $Z^{b-2}Y^2+Z^{b-1}Y+X^b$, $b = 2^e+1$. または, C_{2^b}: $Z^{b-2}Y^2+Z^{b-1}Y+X^b+tZ^b$, $t \in GF(2^e)$, $b = 2^e+1$. $genus(C_{2^b}) = (b-1)(2-1)/2 = 2^{e-1}$. $\#_r C_{2^b}\cdot(GF(2^{2e})) = 2^{2e}+1+2\cdot 2^{e-1}\cdot 2^e = 2^{2e+1}+1$.

[例3] $F = GF(2^4)$上, ${}_rC_{2^5}$: $Z^{3-r}Y^{r+2}+Z^{4-r}Y^{r+1}+X^5$, $r = 0, 1, 2$.

$genus({}_rC_{2^5}) = 2$. $\#_r C_{2^5}\cdot(GF(2^4)) = 33$.

[例4] $F = GF(2^6)$上, ${}_rC_{2^9}$: $Z^{7-r}Y^{r+2}+Z^{8-r}Y^{r+1}+X^9$, $r = 0, 3, 6$.

genus($_rC_2^9$)=4. $\#_rC_2^{9*}(GF(2^6))=129$.

[例5] $\mathbb{F}=GF(2^8)$上. $_rC_2^{17}$: $Z^{15-rY^{r+2}}+Z^{16-rY^{r+1}}+X^{17}$, $r=0,1,2,\cdots,13,14$. genus($_rC_2^{17}$)=8. $\#_rC_2^{17*}(GF(2^8))=513$. $_rC_3^{17}$: $Z^{14-rY^{3+r}}+Z^{15-rY^{2+r}}+Z^{16-rY^{1+r}}+X^{17}$, $r=5,8$. genus($_rC_3^{17}$)=16. $\#_rC_3^{17*}(GF(2^8))=769$. $_rC_4^{17}$: $Z^{13-rY^{4+r}}+Z^{16-rY^{1+r}}+X^{17}$, $r=0,6,12$. genus($_rC_4^{17}$)=24. $\#_rC_4^{17*}(GF(2^8))=1025$.

[例6] $\mathbb{F}=GF(2^{10})$上. $_rC_2^{11}$: $Z^{9-rY^{r+2}}+Z^{10-rY^{r+1}}+X^{11}$, $r=0,1,2,3,4,5,6,7,8,9$. genus($_rC_2^{11}$)=5. $\#_rC_2^{11*}(GF(2^{10}))=1345$. C_3^{11}: $Z^8Y^3+X^{11}+Z^{11}$. genus(C_3^{11})=10. $\#C_3^{11*}(GF(2^{10})=1665$. $_rC_3^{11}$: $Z^{8-rY^{3+r}}+Z^{9-rY^{2+r}}+Z^{10-rY^{1+r}}+X^{11}$, $r=0,7$. genus($_rC_3^{11}$)=10. $\#_rC_3^{11*}(GF(2^{10}))=1665$. $_rC_4^{11}$: $Z^{7-rY^{4+r}}+Z^{10-rY^{1+r}}+X^{11}$, $r=0,1,2,\cdots,6$. genus($_rC_4^{11}$)=15. $\#_rC_4^{11*}(GF(2^{10}))=1985$.

$_rC_2^{33}$: $Z^{31-rY^{r+2}}+Z^{32-rY^{r+1}}+X^{33}$, $r=0,3,6,12,15,18,24,27,30$. genus($_rC_2^{33}$)=16. $\#_rC_2^{33*}(GF(2^{10}))=2049$.

[例7] $\mathbb{F}=GF(2^{12})$上. $_rC_2^{13}=Z^{11-rY^{r+2}}+Z^{12-rY^{r+1}}+X^{13}$, $r=0,1,2,3,4,5,6,7,8,9,10$. genus($_rC_2^{13}$)=6. $\#_rC_2^{13*}(GF(2^{12}))=4865$. $_rC_3^{13}$: $Z^{10-rY^{3+r}}+Z^{11-rY^{2+r}}+Z^{12-rY^{1+r}}+X^{13}$, $r=2,3,6,7$. genus($_rC_3^{13}$)=12. $\#_rC_3^{13*}(GF(2^{12}))=5633$. $_rC_4^{13}$: $Z^{9-rY^{4+r}}+Z^{11-rY^{2+r}}+Z^{12-rY^{1+r}}+X^{13}$, $r=0,2$. genus($_rC_4^{13}$)=18. $\#_rC_4^{13*}(GF(2^{12}))=6401$. C_5^{13}: $Z^8Y^5+Z^9Y^4+Z^{12}Y+X^{13}$. genus($C_5^{13}$)=24. $\#C_5^{13*}(GF(2^{12}))=7169$.

$_rC_2^{65}=Z^{63-rY^{r+2}}+Z^{64-rY^{r+1}}+X^{65}$, $r=0,1,2,5,6,7,10,15,16,17,20,21,22,26,27,30,31,32,35,36,40,41,42,45,46,47,52,55,56,57,60,61,62$.

genus($_rC_2^{65}$) = 32.　$\#_rC_2^{65*}(GF(2^{12})) = 8193$.

5. 2　Hasse-Weil-Serre upper bound に達する曲線の例

以下は曲線の非特異モデルの有理点数が Hasse-Weil upper bound には達しないが Hasse-Weil-Serre upper bound には達する興味深い例である. $\mathbb{F} = GF(2^e)$に於てeが奇数であることも興味を惹く.

[例8]　$\mathbb{F} = GF(2^3)$上.

$_rC_2^7$: $Z^{5-r}Y^{r+2}+Z^{6-r}Y^{r+1}+X^7$,　$r = 1,3$.

genus($_rC_2^7$) = 3.　$\#_rC_2^{7*}(GF(2^3)) = 24$.

Hasse-Weil-Serre upper bound : $q+1+g\lfloor 2\sqrt{q}\rfloor = 24$.

Hasse-Weil upper bound　　: $q+1+2g\sqrt{q} \doteqdot 25.976\cdots$.

The Klein quartic $C_2^{3,4}$: $Y^3Z+X^3Y+Z^3X$.

genus($C_2^{3,4}$) = 3.　$\#C_2^{3,4}(GF(2^3)) = 24$.

[例9]　$\mathbb{F} = GF(2^{11})$上.

$_rC_2^{23}$: $Z^{21-r}Y^{r+2}+Z^{22-r}Y^{r+1}+X^{23}$,　$r = 3,5,8,12,15,17$.　genus($_rC_2^{23}$) = (23-1)(2-1)/2 = 11.

$\#_rC_2^{23*}(GF(2^{11})) = 2048+1+5\lfloor 2\cdot\sqrt{2048}\rfloor = 3039$.

Hasse-Weil-Serre upper bound : $q+1+g\lfloor 2\sqrt{q}\rfloor = 3039$.

Hasse-Weil upper bound　　: $q+1+2g\sqrt{q} \doteqdot 3044.6\cdots$.

計算複雑度のオーダーは$O(n^4)$である．ただし，そのときの並列化にともなう因子群の有効な探索法は未解決な問題として残されている．なお，実数sに対して$\lfloor s \rfloor$はs≧0のときはs以下の整数の中で最大なものを，s<0のときは0を表すとした．

他方，R.Pellikkan[7]らは，任意の線形符号は代数幾何符号として表現できることを証明した．このとき最小距離d_{min}を保証する設計最小距離d_{des}はほぼ$d_{des}+g \geqq d_{min} \geqq d_{des}$として表現される．これとさきの S.G.Vladut の結果を使うと，任意の線形符号を代数幾何符号として表現するとき$2g \leqq d_{des}$であるならば多少の例外を除き$\lfloor (d_{des}-1)/2 \rfloor$までの誤り訂正を保証するアルゴリズムの存在が示されたことになる．ただし，表現の存在証明に使用された曲線の種数gは$n \ll g$（$n \to \infty$）であり，前提条件の$2g \leqq d_{des}$は意味を失う．それ故，前提条件$2g \leqq d_{des}$を外すこと，最適な表現を与える曲線の探索，種数gの最小値の評価は重要な課題として残されている．

そこで本稿ではこれらの課題をふまえて，与えられたエラーパターンを有効因子Fに付随する基本復号アルゴリズムが正しく訂正するための必要十分条件を詳しく考察し，それを基に一般修正復号アルゴリズムを提案する．一般修正復号アルゴリズムは，基本復号アルゴリズムと修正復号アルゴリズムをさらに一般的に拡張したものである．次いで，この一般修正復号アルゴリズムが，基本復号アルゴリズムあるいは修正復号アルゴリズムに比較してより訂正能力の高い復号器を構成できることを示し，さらにその訂正能力を保証する評価式を与える．なお，ここで与える評価式は修正復号アルゴリズムの評価式[4]よりも精度はよいことが示される．また，

7. むすび

射影平面曲線がアフィン平面曲線x^a+y^bの原点と同じ型の尖点を持つための必要十分条件を与え，特異点としてそのような尖点をただ一つもつ曲線すべてからなる曲線族$C_a^{b,m}$と，ただ二つもつ曲線のすべてからなる曲線族$_rC_a^{b,m}$を定式化し，特にm＝bとした場合の代数幾何符号の構造を明らかにした．また，曲線族C_a^b，$_rC_a^b$は Hasse-Weil upper bound を達する曲線を多数含むことを具体例を挙げて示した．ただし，組織的な探索は行なっていない．今後の課題としては，例えば曲線族C_a^b，$_rC_a^b$を使って，比較的小さい有限体Fと自然数gの全ての組に対して 有理的な座を多数もつ曲線の探索を組織的に行ないそのデーターベース化を完成することがあげられる．また，構造の簡単な曲線族C_a^b，$_rC_a^b$に固有の符号化／復号アルゴリズムの高速化があげられる．

文　献

(1)V.D.Goppa: “Codes on algebraic curves”,Soviet Math.Dokl.pp.170-172(1981).(2)V.D.Goppa: “Algebraic-Geometrical codes ”,Math.U.S.S.R Izvestiya,21,pp.75-91(1983).(3) Y.Driencourt and J.F.Michon: “Elliptic codes over fields of characteristic 2” Journal of Pure and Applied Algebra 45.pp.15-39(1987).(4)H.J.Tiersma: “Remarks on Codes from Hermitian Curves” IEEE Trans. Inf. Theory,33,No.4,pp.605-609(1987). (5)J.W.P.Hirschfeld : “Liner codes and algebraic curves” in: Geometrical Combinatorics,Pitman, Boston,