数理解析研究所講究録
第786巻 1992年 74-94

代数幾何符号の一般修正復号アルゴリズム

日本電気㈱C&C情報研究所　三浦　晋示（Shinji Miura）

あらまし　代数曲線上に定義される代数幾何符号の復号アルゴリズムとして A.N.Skorobogatov and S.G.Vladut[4] による基本復号アルゴリズムと修正復号アルゴリズムが知られている．本稿では，これらをさらに拡張し訂正能力を高めた一般修正復号アルゴリズムを提案する．

また，R.Pellikaan[5] とS.G.Vladut[6] は基本復号アルゴリズムを並列化した並列基本復号アルゴリズムを提案し$2g \leqq d_{des}$［$4g-2 \leqq m$］の仮定の下で$\lfloor (d_{des}-1)/2 \rfloor$までの訂正を保証した．本稿では，この仮定を除いても，すなわち$1 \leqq d_{des}$［$2g-1 \leqq m$］としても$\lfloor (d_{des}-1)/2 \rfloor$までの訂正を保証できることを示す．なお，このときの時間複雑度のオーダーは$O(n^3)$でおさえられ，計算複雑度のオーダーは$O(n^4)$でおさえられる．ただし，gは曲線の種数，$d_{des}=m-2g+2$は設計最小距離である．

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

pp.35-53(1984).(6)J.P.Hansen "Codes on the Klein quartic" IEEE Trans. Inf. Theory,33,pp.923-925(1987). (7)H.Stichtenoth : "A Note on Hermitian Codes Over GF(q^2)" IEEE Trans. Inf. Theory, 34,No.5,pp.1345-1348(1988). (8H.Stichtenoth : "Self-Dual Goppa Codes" Journal of Pure and Applied Algebra 55.pp.199-211(1988). (9)三浦晋示 "超楕円符号(1),(2)" SITA'90,Inuyama,Japan,December,1989.(10)J.P.Hansen and H.Stichtenoth "Group Codes on Certain Algebraic Curves with Many Rational Points" AAECC,Vol.1,No.1, Springer,1990.(11)R.Pellikaan, B.-Z.Shen, and G.J.M.van Wee "Which Linear Codes are Algebraic-Geometric? " IEEE Trans. Inf. Theory,37,3,(MAY 1991).(12)橋本喜一朗: "数論研究の動向と展望" 数理科学, 325, pp.37-44, 1990.(13)神谷典史, 三浦晋示, 今井秀樹 "任意の平面曲線上に符号を構成する方法" 信学論(A), J74-A,7,pp1067-1074(1991).(14)V.G.Goppa: "Geometry and Codes" : 1988 MIA Kluwer Academic Publishers. (15)J.H.van Lint and G.van der Geer : "Introduction to Coding Theory and Algebraic Geometry" Birkhäuser Verlag,(1988).(16)M.A.Tsfasman and S.G.Vladut: "Algebraic-Geometric Codes" MIA Kluwer Academic Publishers,(1991).(17)C.Moreno: "Algebraic curves over finite fields" Cambridge University Press,(1991).

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されてきている[9],[10]．なかでもその多項式時間限界距離復号法は長い間未解決な問題であったが，その解決に向けて決定的とも言える第一歩を踏み出したのは J.Justesen[3] らであった．その提案は本質をついたものであり，これを契機に復号アルゴリズムの研究は飛躍的に進むことになる．その後，A.N.Skorobogatov[4] らはその一般化に成功し，基本復号アルゴリズムと修正復号アルゴリズムを提案した．これらはいずれも時間複雑度のオーダーは $O(n^3)$で，計算複雑度のオーダーは $O(n^3)$，$O(n^4)$である．これによって任意の代数幾何符号の復号に関して$\lfloor(d_{des}-g-1)/2\rfloor$までの誤り訂正が保証されることになった．また，修正復号アルゴリズムによって，特にだ円または超だ円曲線上の符号の場合には因子Gを適当に定めると$\lfloor(d_{des}-1)/2\rfloor$までの誤り訂正が保証される．なお，これに関しては S. Sakata[8] のアルゴリズムを有効に使った高速化の研究も進められている．ついで，R.Pellikkan[5] は基本復号アルゴリズムを並列化することを提案し，特に Hasse-Weil uper bound を達成する曲線上の符号に関して，$q>3$，$2g \leqq d_{des}$ならば$\lfloor(d_{des}-1)/2\rfloor$までの誤り訂正を保証するアルゴリズムの存在を示した．また，S.G.Vladut[6] は R.Pellikkan の手法に従って任意の曲線上の符号に関して，$q>37$か，種数gが十分大きいときの$q>16$に関して，$2g \leqq d_{des}$ならば$\lfloor(d_{des}-1)/2\rfloor$までの誤り訂正を保証するアルゴリズムの存在を示した．なおこれらはいずれも時間複雑度のオーダーは $O(n^3)$，

$2g \leqq d_{des}$ [$4g-2 \leqq m$] の仮定の下で R.Pellikaan[5] と S.G.Vladut[6] は基本復号アルゴリズムを並列化した並列基本復号アルゴリズムによって $\lfloor (d_{des}-1)/2 \rfloor$ までの訂正を保証できることを示しているが，本稿では，一般に $1 \leqq d_{des}$ [$2g-1 \leqq m$] としても $\lfloor (d_{des}-1)/2 \rfloor$ までの訂正を保証できることを示す[脚注]．このときの時間複雑度のオーダーは $O(n^3)$ でおさえられ，計算複雑度のオーダーは $O(n^4)$ でおさえられる．

2. 準備（代数幾何符号）

「曲線族 $C_a{}^b$，${}_rC_a{}^b$ 上の代数幾何符号の構造」を参照．

3. A.N.Skorobogatov and S.G.Vladutの復号アルゴリズム

以下，受信語 $w \in \mathbb{F}^n$ と，誤りベクトル $e \in \mathbb{F}^n$ を因子のように形式表現して，$w = \Sigma_{j=1}{}^n w_j \cdot P_j$，$(w_j \in \mathbb{F},\ P_j \in supp(D))$，$e = \Sigma_{i=1}{}^e e_i \cdot Q_i$，$(0 \neq e_i \in \mathbb{F},\ Q_i \in supp(D))$ と表わす．まず，線形符号 $C_\Omega(X,D,G) = Image(\alpha_\Omega) \subset \mathbb{F}^n$ に於て受信語 $w \in \mathbb{F}^n$ と $\psi \in L(G)$ に付随するシンドローム $s(w, \psi)$ を次のように定義する．

$$s:\ \mathbb{F}^n \times L(G) \to \mathbb{F} \qquad (1)$$

$$(w, \psi) \quad \to s(w, \psi) = \Sigma_{j=1}{}^n w_j \cdot \psi(P_j)$$

また，シンドローム写像Sを次のように定義する．

$$S:\ \mathbb{F}^n \to L(G)^\vee \qquad (2)$$

$$w \ \to (\psi \to s(w, \psi))$$

sを $Image(\alpha_\Omega) \times L(G) = (Image(\alpha_L))^\perp \times L(G)$ に制限すると，これはゼロ

写像となる．任意の有理関数$\phi \in L(G)$に対して$s(w, \phi) = s(e, \phi)$である．また，受信語$w \in \mathbb{F}^n$が符号語$w \in \mathrm{Image}(\alpha_n)$であるための必要十分条件は$S(w) = 0$である．ただし，$L(G)^{\cup}$は$L(G)$から$\mathbb{F}$への線形写像の全体を表すとする．

ここでは復号アルゴリズムを，［誤り位置導出］と［誤り値導出］の2つの部分に分ける．

［誤り位置導出］；受信語wから，誤り位置の候補$\{Q_{k1}, \cdots, Q_{ks}\} \subset \mathrm{supp}(D)$を導く．ただし，誤り位置$\{Q_1, \cdots, Q_e\}$に関して$\{Q_1, \cdots, Q_e\} \subset \{Q_{k1}, \cdots, Q_{ks}\}$である．

［誤り値導出］；［誤り位置導出］で導かれた誤り位置の候補$\{Q_{k1}, \cdots, Q_{ks}\}$をもとに，誤り値$e_{kj} \in \mathbb{F}$を導く．

ここでは，誤り位置をある有理関数の零点として捉える．誤り位置関数σを定義する．誤り位置関数$\sigma \neq 0$とは次の二つの条件を満足するX上の有理関数とする．ただし一般には一意に定まるとは限らないことに注意せよ．

e.l.f.1. $\sigma \in \mathrm{Rat}(X)$, $\sigma(Q_i) = 0 (1 \leq i \leq e)$, $\sigma(P) \neq \infty (P \in \mathrm{supp}(D))$. (3)

e.l.f.2. $\{P \in \mathrm{supp}(D) : \sigma(P) = 0\}$に対応する検査行列の列ベクトルは一次独立. (4)

ここで，誤り位置関数の極の取り得る範囲を指定する．Fを$\mathbb{F}$有理的な有効因子とする．ただし，$\mathrm{supp}(F) \cap \mathrm{supp}(D) = \emptyset$を仮定する．このとき有理関数$\sigma$，$0 \neq \sigma \in L(F - \sum_{i=1}^{e} Q_i)$は，極をFにのみ持ち条件e.l.f.1を満

たす．さらに後に示すように$\delta(G-F)=0$を仮定するとe.l.f.2も満足する．それ故，$L(F-\Sigma_{i=1}^{\circ} Q_i)$の零でない任意の元は誤り位置関数となる．しかし，$L(F-\Sigma_{i=1}^{\circ} Q_i)$は誤り位置を示す因子$\Sigma_{i=1}^{\circ} Q_i$を直接含むので，その元を導くことは容易ではない．そこで，the error locator map $E_{F,w}$を定義する[5]．

$$E_{F,w}:\ L(F)\rightarrow L(G-F)^{\vee} \qquad (5)$$

$$\sigma \rightarrow (\eta \rightarrow s(w,\sigma\eta))$$

一般には$\mathrm{Ker}E_{F,w}\supset L(F-\Sigma_{i=1}^{\circ} Q_i)$であるが，ある条件の下では$\mathrm{Ker}E_{F,w}=L(F-\Sigma_{i=1}^{\circ} Q_i)\neq(0)$となる．なお，$\mathrm{Ker}E_{F,w}$の元は線形方程式を解くことにより容易に求められる．

有効因子Fに付随する基本復号アルゴリズム[4],[5]

$r=\ell(G)$とし，$\phi_1,\phi_2,\cdots,\phi_r\in L(G)$を基底とする．

① シンドロームベクトル$s=(s(w,\phi_1),s(w,\phi_2),\cdots,s(w,\phi_r))$を導く．$1\leqq j\leqq r$に関して$s(w,\phi_j)=\Sigma_{i=1}^{n} w_i\cdot\phi_j(P_i)\in F$を計算する．$s=0$ならば誤り無しと判定する．

② $\sigma\in\mathrm{Ker}E_{F,w}$，$\sigma\neq 0$を導く．

$\dim L(F)=a$，$\dim L(G-F)=b$とし，

$\phi_1,\phi_2,\cdots,\phi_a\in L(F)$，

$\psi_1,\psi_2,\cdots,\psi_b\in L(G-F)$をそれぞれ基底とする．

シンドローム$s(w,\phi_i\phi_j)$を導く．

$b\times a$行列$H_{b,a}$を$H_{b,a}=(s(w,\phi_i\phi_j))$とする．

$H_{b,a}\cdot {}^t f = 0$, $f = (f_1, f_2, \cdots, , f_a) \in \mathbb{F}^a$, $f \neq 0$, を解く. $\sigma = (\phi_1, \phi_2, \cdots, \phi_a)\cdot {}^t f = \sum_{j=1}^{a} f_j \cdot \phi_j \in L(F)$が$KerE_{F,w}$の元である. ただし, $\sigma \neq 0$なる解が存在しないときは訂正不能とする.

③ $\{P \in supp(D) : \sigma(P) = 0\} = \{Q_{k1}, Q_{k2}, \cdots, Q_{ks}\}$を導く.

$supp(D) = \{P_1, P_2, \cdots, P_n\}$に対して$\sigma(P_j)$を計算し, $\sigma(P_j) = 0$ならば, $P_j \in \{P \in supp(D) : \sigma(P) = 0\}$とする.

④ 誤りベクトル $e = \sum_{i=1}^{s} e_{ki} \cdot Q_{ki}$を導く.

$1 \leqq i \leqq r$, $1 \leqq j \leqq s$, $\phi_i(Q_{kj})$を導く.

$N_{r,s}$を, i,j成分が$\phi_i(Q_{kj})$で与えられるr×s型の行列とする. 線形方程式$N_{r,s}\cdot {}^t e = {}^t s$, $e = (e_{k1}, e_{k2}, \cdots, e_{ks}) \in \mathbb{F}^s$を解く. ただし, sはシンドロームベクトル. ここで改めて, $e = \sum_{i=1}^{s} e_{ki} \cdot Q_{ki}$とおく. 線形方程式が解を持たないかあるいは一意に定まらない場合は訂正不能とする.

⑤ 訂正を実行する.

$wt(e) \leqq \lfloor (d_{min}-1)/2 \rfloor$ならば, eをエラーベクトルと推定して訂正を実行する. $wt(e) > \lfloor (d_{min}-1)/2 \rfloor$ならば, 訂正不能とする.

①, ②, ③が［誤り位置導出］の部分, ④が［誤り値導出］の部分で⑤が訂正を実行する部分である.

以下, $t = \lfloor (d_{min}-1)/2 \rfloor$とし, エラーパターン $e = \sum_{i=1}^{e} e_i \cdot Q_i$ (ただし, $e \leqq t$) を固定する. ここで, 有効因子Fに付随する基本復号アルゴリズムを詳しく解析する.

［定理9］ $\mathbb{F}$有理的な有効因子Fに付随する基本復号アルゴリズムがエラー

パターン $e=\Sigma_{i=1}^{e} e_i \cdot Q_i$ を正しく訂正するための必要十分条件は,

(a.1) $L(F-\Sigma_{i=1}^{e} Q_i) \neq (0)$

(b.1) $\ker E_{F,w} = L(F-\Sigma_{i=1}^{e} Q_i)$

(c.1) 任意の σ ($\neq 0$) $\in \ker E_{F,w}$ に対して,

$\{P \in \mathrm{supp}(D) : \sigma(P)=0\}$ に対応する検査行列

の列ベクトルは一次独立

をすべて満たすことである. (証明略) ■

また, 定理に関連して,

(a.3) $\deg(F) \geqq e+g$

(a.2) $\ell(F) > e$

(a.1) $L(F-\Sigma_{i=1}^{e} Q_i) \neq (0)$

(b.4) $\deg(G-F) \geqq 2g-1+e$ $[d_{des}-1 \geqq \deg(F)+e]$

(b.3) $\delta(G-F-\Sigma_{i=1}^{e} Q_i) = 0$

$[\ell(K_X-G+F+\Sigma_{i=1}^{e} Q_i) = 0]$

(b.2.3) $\delta(G-F) = \delta(G-F-\Sigma_{i=1}^{e} Q_i)$

$[\ell(K_X-G+F) = \ell(K_X-G+F+\Sigma_{i=1}^{e} Q_i)]$

(b.2.2) $\ell(G-F)-\ell(G-F-\Sigma_{i=1}^{e} Q_i) = e$

(b.2.1)

$0 \to L(G-F-\Sigma_{j=1}^{e} Q_j) \to L(G-F) \to F^{e} \to 0$ exact

$\eta \to (\eta(Q_1), \cdots, \eta(Q_e))$

(b.1)' $L(F-\Sigma_{i=1}^{e} Q_i) \to L(F) \to L(G-F)^{\vee}$ exact

$\sigma \to (\eta \to s(w, \sigma\eta))$

(b.1)　$\ker E_{F,w} = L(F - \Sigma_{i=1}^{e} Q_i)$

(c.4)　$\deg F < d_{des}$

(c.4)'　$\deg F < d_{min}$

(c.3)　任意の $\sigma(\neq 0) \in \ker E_{F,w}$ に対して,

$\#\{P \in \mathrm{supp}(D) : \sigma(P) = 0\} < d_{des}$

(c.2)　任意の $\sigma(\neq 0) \in \ker E_{F,w}$ に対して,

$\#\{P \in \mathrm{supp}(D) : \sigma(P) = 0\} < d_{min}$

(c.1)　任意の $\sigma(\neq 0) \in \ker E_{F,w}$ に対して,

$\{P \in \mathrm{supp}(D) : \sigma(P) = 0\}$ に対応する検査行列の列ベクトルは一次独立

とおくと, 次の事実を得る. ただし, K_X は X の F 有理的な標準因子を表すとする.

[補題10]　(a.3) ⇒ (a.2) ⇒ (a.1),

(b.4) ⇒ (b.3) ⇒ (b.2.3) ⇔ (b.2.2) ⇔ (b.2.1) ⇒ (b.1)' ⇔ (b.1),　(c.4) ⇒ (c.3) ⇒ (c.2) ⇒ (c.1),　(c.4) ⇒ (c.4)' ⇒ (c.2) ⇒ (c.1).

(証明)　自明でない (b.2.1) ⇒ (b.1)' のみを示す.

(b.2.1) ⇒ (b.1)' : $\ker E_{F,w} \supset L(F - \Sigma_{i=1}^{e} Q_i)$ は明かである, ⊂ を示す.

仮定から任意の $j \in \{1,2,\cdots,e\}$ に対して, $\eta(Q_j) \neq 0$, $\eta(Q_i) = 0$, $i \in \{1,2,\cdots,e\} \setminus \{j\}$ なる $\eta \in L(G-F)$ の存在が保証される. $\sigma \in \ker E_{F,w}$ とすると $s(w, \sigma\eta) = 0$ である. $s(w, \sigma\eta) = s(e, \sigma\eta) = \Sigma_{i=1}^{e} e_i \cdot \sigma(Q_i)\eta(Q_i) = e_j \cdot \sigma(Q_j)\eta(Q_j) = 0$ から $\sigma(Q_j) = 0$ が導かれる. すなわち, $\ker E_{F,w} = L(F - \Sigma_{i=1}^{e} Q_i)$ である. ■

また, 次の興味深い事実は神谷 (日電) が導いた.

[補題11] (c.1)' $\delta(G-F)=0$

とすると, (b.3)⇒(c.1)'⇒(c.1)である.

(証明) 自明でない(c.1)'⇒(c.1)のみを示す.

(c.1)'⇒(c.1): (c.1)を否定すると, ある$\sigma(\neq 0)\in \ker E_{F,w}\subset L(F)$に関して, $\{P\in \mathrm{supp}(D):\ \sigma(P)=0\}=\{Q_{k1},\cdots,Q_{ks}\}$とおくとき, $\alpha_\Omega(\omega)\neq 0$なる, $\omega\in\Omega(G-\Sigma_{j=1}^{s}Q_{kj})\subset\Omega(G-D)$が存在する. このとき, $0\neq\sigma\omega\in\Omega(G-F)$である. すなわち, $\delta(G-F)\neq 0$である. ■

次ぎに, A.N.Skorobogatov and S.G.Vladut[4] の修正復号アルゴリズムを復習する. まず対象とする代数幾何符号を次のように限定する. 因子Gはある有効因子Hを使ってG=b·H(bは自然数)と表せるとする. そして, 基本復号アルゴリズムの手順②をHに依存して次のようにかえるのである.

②' $\mathrm{Ker}E_{a\cdot H,w}\neq(0)$なる最小の自然数aに関して

$\sigma\in\mathrm{Ker}E_{a\cdot H,w}$, $\sigma\neq 0$を導く.

このとき, 彼らは次の事実を得ている. ただし, deg(H)=hとする. S(H)を, $S(H)=\max\{\lfloor(j\cdot h+h+1)/2\rfloor-\ell(j\cdot H):\ 0\leq j\}$とすると, 修正復号アルゴリズムは$\lfloor(d_{des}-1)/2\rfloor-S(H)$までの訂正を保証できる. また, Hが超だ円ワイヤルトラス因子ならばS(H)=0である. なお著者は次節で, さらに精度のよい評価式を, より一般的な一般修正復号アルゴリズムを対象に提案する.

4. 一般修正復号アルゴリズム

一般修正復号アルゴリズムを提案する. 基本復号アルゴリズムに於ける

手順②を次のようにかえたものを一般修正復号アルゴリズムと呼ぶ.

まず, Λを因子Dと互いに素なF有理的な有効因子からなる任意の集合とする. なお一般にΛは因子Gに依存する必要はない.

② $^{\bullet}\mathrm{Ker}E_{H,w} \neq (0)$なる次数最小の因子$H \in \Lambda$に関して$\sigma \in \mathrm{Ker}E_{H,w}$, $\sigma \neq 0$を導く. ただし, $\sigma \neq 0$の存在しないときは訂正不能とする.

以下, $m > 2g-2$を仮定する. $d_{des} = m-2g+2 \geq 1$である.

ここで, 各々の$H(\neq 0) \in \Lambda$に対して$H' \in \Lambda$を$H' \leqq H (H' \neq H)$なるなかで次数$\deg(H')$の最大なものを表すとする. ただしH'はHに対して一意に定まるとは限らないことに注意せよ. またNはゼロを含む自然数全体の集合とする.

以下, $\Lambda \ni 0$, $\#\Lambda \geq 2$を仮定する.

ここで, Λから導かれる自然数$S^{\bullet}(\Lambda)$を次のように定める.

$$S^{\bullet}(\Lambda) = \min \{S^{\bullet} \in \mathbf{N}:\ 0 \geq \lfloor (m-2\deg(H')+1-S^{\bullet})/2 \rfloor - \ell(G-H-H'),\ \forall H(\neq 0) \in \Lambda,\ \forall H' \in \Lambda \text{ s.t. } \ell(G-H-H') > 0,\ \lfloor (m-2\deg(H')+1-S^{\bullet})/2 \rfloor > 0\}. \quad (6)$$

なお特に$S^{\bullet} = m-1$, $S = m-1$とすると, 条件文は成立するので, 一般に$m-1 \geq S^{\bullet}(\Lambda) \geq 0$が導かれる. また,

$\lfloor (m-2\deg(H')+1-S^{\bullet})/2 \rfloor = \lfloor (d_{des}-1-S^{\bullet})/2 \rfloor + g - \deg(H')$に注意せよ. なお$S^{\bullet}(\Lambda)$は, Clifford's theorem から導かれた値である. $\delta(F) > 0$なる任意のF有理的な因子Fに関して$\ell(F)-1 \leqq \deg(F)/2$.

以上の準備の下で次の定理が成立する.

[定理12] $\exists H^{\bullet} \in \Lambda$, $\ell(G-H^{\bullet}-H^{\bullet\prime}) > 0$, $\deg(H^{\bullet}) \geq g + \lfloor (d_{des}-1-S^{\bullet}(\Lambda))/2 \rfloor$とする. このとき,

$\lfloor (d_{des}-1-S^*(\Lambda))/2 \rfloor \geqq e$ならば, $\ker E_{H,w} \neq (0)$,

$\ell(G-H-H') > 0$を満たす$H(\neq 0) \in \Lambda$は存在し, そのうち次数$\deg(H)$の最小な$H(\neq 0) \in \Lambda$に対して,

(a.1) $L(H-\Sigma_{i=1}^{e} Q_i) \neq (0)$,

(b.3) $\delta(G-H-\Sigma_{i=1}^{e} Q_i) = 0$

$[\ell(K_X-G+H+\Sigma_{i=1}^{e} Q_i) = 0]$,

が成り立つ. また, $d_{des} > g+1$, $\exists H^* \in \Lambda$, $\deg(H^*) = g+\lfloor (d_{des}-1-g)/2 \rfloor$のときは, $\lfloor (d_{des}-1-g)/2 \rfloor \geqq e$ならば, $\ker E_{H,w} \neq (0)$, $\ell(G-H-H') > 0$を満たす$H(\neq 0) \in \Lambda$は存在し, そのうち次数$\deg(H)$の最小な$H(\neq 0) \in \Lambda$に対して,

(a.1) $L(H-\Sigma_{i=1}^{e} Q_i) \neq (0)$,

(b.3) $\delta(G-H-\Sigma_{i=1}^{e} Q_i) = 0$

$[\ell(K_X-G+H+\Sigma_{i=1}^{e} Q_i) = 0]$,

が成り立つ. なお, いずれの場合も(b.3)から, (b.1)と(c.1)の成立も保証される.

(証明) $\ker E_{H,w} \neq (0)$, $\ell(G-H-H') > 0$を満たす次数$\deg(H)$の最小な$H(\neq 0) \in \Lambda$に対して, $\lfloor (d_{des}-1-S^*(\Lambda))/2 \rfloor \geqq e$の仮定のもと, $\ell(K_X-G+H+\Sigma_{i=1}^{e} Q_i) = 0$を示す. このとき, $\ker E_{H,w} = L(H-\Sigma_{i=1}^{e} Q_i)$で, $L(H-\Sigma_{i=1}^{e} Q_i) \neq (0)$はあきらか. まず, $\lfloor (m-2\deg(H')+1-S^*(\Lambda))/2 \rfloor > 0$を示す. 否定して$0 \geqq \lfloor (m-2\deg(H')+1-S^*(\Lambda))/2 \rfloor$とすると,

$\deg(H') \geqq \lfloor (m+1-S^*(\Lambda))/2 \rfloor = \lfloor (d_{des}-1-S^*(\Lambda))/2 \rfloor + g \geqq e+g$, $\ker E_{H',w} \supset L(H'-\Sigma_{i=1}^{e} Q_i) \neq (0)$, $\ell(G-H'-H'') > 0$. これはHの最小性に矛盾する. それ故, $0 \geqq \lfloor (m-2\deg(H')+1-S^*(\Lambda))/2 \rfloor - \ell(G-H-H')$が保証される.

次に，$\ell(K_X-G+H+\Sigma_{i=1}^{n} Q_i)>0$と仮定して矛盾を導く．

このとき，有効因子Jが存在して，$K_X-G+H+\Sigma_{i=1}^{n} Q_i \sim J$が成り立つ．ただし，～は線形同値を表す．$2g-2-m+\deg(H)+e=\deg(J)$である．

$(0)=\ker E_{H',w} \supset L(H'-\Sigma_{i=1}^{n} Q_i)$から，

$\ell(H'-\Sigma_{i=1}^{n} Q_i)=0$がいえ，$H'-\Sigma_{i=1}^{n} Q_i \sim K_X-J-G+H+H'$より，$\ell(K_X-J-G+H+H')=0$，すなわち，$\ell(K_X-G+H+H') \leqq \deg(J)$が導かれる．ここで，Jが有効因子であるとの仮定が使われている．他方，$S^*(\Lambda)$の定義によると，$\ell(G-H-H') \geqq \lfloor (m-2\deg(H')+1-S^*(\Lambda))/2 \rfloor$．それゆえ，$\ell(K_X-G+H+H')=\ell(G-H-H')-m+\deg(H)+\deg(H')+g-1 \geqq \lfloor (m-2\deg(H')+1-S^*(\Lambda))/2 \rfloor-m+\deg(H)+\deg(H')+g-1=\lfloor (d_{des}-1-S^*(\Lambda))/2 \rfloor-m+\deg(H)+2g-1 \geqq e-m+\deg(H)+2g-1 \geqq \deg(J)+1$．矛盾である．

また，$d_{des}>g+1$，$\exists H^* \in \Lambda$，$\deg(H^*)=g+\lfloor (d_{des}-1-g)/2 \rfloor$ならば，$\lfloor (d_{des}-1-g)/2 \rfloor \geqq e$とすると，$\ell(G-H^*-H^{**})>0$，$\ker E_{H^*,w} \supset L(H^*-\Sigma_{i=1}^{n} Q_i) \neq (0)$である．それ故，$\ker E_{H,w} \neq (0)$，$\ell(G-H-H')>0$を満たす$H(\neq 0) \in \Lambda$は存在し，そのうち次数$\deg(H)$の最小な$H(\neq 0) \in \Lambda$に対して，$\deg(H^*) \geqq \deg(H)$である．

$\deg(K_X-G+H+\Sigma_{i=1}^{n} Q_i) \leqq 2g-2-m+g+\lfloor (d_{des}-1-g)/2 \rfloor+e<0$から，$\ell(K_X-G+H+\Sigma_{i=1}^{n} Q_i)=0$である．このとき，$\ker E_{H,w}=L(H-\Sigma_{i=1}^{n} Q_i)$で，$L(H-\Sigma_{i=1}^{n} Q_i) \neq (0)$はあきらか．■

ここで，一般修正復号アルゴリズムの手順②*を，次の②**に代えておく．

② **$\mathrm{Ker}E_{H,w} \neq (0)$，$\ell(G-H-H')>0$なる次数最小の因子$H(\neq 0) \in \Lambda$に関

して$\sigma \in Ker E_{H,w}$, $\sigma \neq 0$を導く. ただし, $\sigma \neq 0$の存在しないときは訂正不能とする.

以上まとめると次の定理が証明されたことになる.

[定理13] Λに付随する一般修正復号アルゴリズムは$\lfloor (d_{des}-1-S^*(\Lambda))/2 \rfloor$までの誤り訂正を保証できる. また, $TS(\Lambda)=\min\{g, S^*(\Lambda)\}$とすると, $\lfloor (d_{des}-1-TS(\Lambda))/2 \rfloor$までの誤り訂正を保証できる. ただし, $TS(\Lambda)=g$の場合は, $\exists H^* \in \Lambda$, $\ell(G-H^*-H^{*\prime})>0$, $\deg(H^*)=g+\lfloor (d_{des}-1-TS(\Lambda))/2 \rfloor$を, $TS(\Lambda)=S^*(\Lambda)$の場合は,

$\exists H^* \in \Lambda$, $\ell(G-H^*-H^{*\prime})>0$, $\deg(H^*) \geqq g+\lfloor (d_{des}-1-TS(\Lambda))/2 \rfloor$を仮定する.

(証明) 定理12から導かれる. ■

また, $S^*(\Lambda)$に関して一般に次の事実が示される.

[定理14] $g \geqq 1$ならば$S^*(\Lambda) \leqq g+h-2$である. ただし,

$$h=\max\{\deg(H)-\deg(H') : \forall H(\neq 0) \in \Lambda, \ \forall H' \in \Lambda \ \text{s.t.} \ \ell(G-H-H')>0, \ \lfloor (m-2\deg(H')+1-S^*(\Lambda))/2 \rfloor > 0\} \tag{7}$$

とする. 特に$\exists H(\neq 0) \in \Lambda$, $\exists H' \in \Lambda$, $\lfloor (m-2\deg(H')+1-(g+h-2))/2 \rfloor > 0$, $\ell(G-H-H')=m-\deg(H)-\deg(H')-g+1=1$, $\deg(H)-\deg(H')=h$のときは, $S^*(\Lambda)=g+h-2$である. それ以外ならば$S^*(\Lambda)=0$か$S^*(\Lambda)<g+h-2$である.

(証明) $\forall H(\neq 0) \in \Lambda$, $\forall H' \in \Lambda$ s.t. $\ell(G-H-H')>0$, $\lfloor (m-2\deg(H')+1-S^*(\Lambda))/2 \rfloor > 0$に関して$\ell(G-H-H') \geqq \lfloor (m-2\deg(H')+1-S^*(\Lambda))/2 \rfloor > 0$に注意する.

$\ell(G-H-H') \geqq \max\{1, m-\deg(H)-\deg(H')-g+1\}$である.

m-deg(H)-deg(H')-g+1≦0のときは，m-deg(H)-deg(H')+1≦g．それ故，h+g≧deg(H)-deg(H')+g≧m-2deg(H')+1．このとき，⌊(h+g-2-S*(Λ)/2⌋≧⌊(h+g-S*(Λ)/2⌋-1≧⌊(m-2deg(H')+1-S*(Λ))/2⌋-1≧⌊(m-2deg(H')+1-S*(Λ))/2⌋-ℓ(G-H-H')がいつでも成り立つので，S*(Λ)≦g+h-2である．またg+h＞2ならばS*(Λ)≦g+h-3である．m-deg(H)-deg(H')-g+1≧1のときは，m-deg(H)-deg(H')≧g．それ故，h≧deg(H)-deg(H')≧g-m+2deg(H)．ℓ(G-H-H')≧m-deg(H)-deg(H')-g+1．このとき，⌊(g+h-1-S*(Λ))/2⌋≧⌊(2g-m+2deg(H)-1-S*(Λ))/2⌋≧⌊(m-2deg(H')+1-S*(Λ))/2⌋-ℓ(G-H-H')がいつでも成り立つので，S*(Λ)≦g+h-2である．■

[系15] g≧1，∃H*∈Λ，ℓ(G-H*-H*')＞0，deg(H*)≧g+⌊(d_{des}-S*(Λ))/2⌋，で特にh＝1ならばS*(Λ)≦g-1が成立ち，この場合はΛに付随する一般修正復号アルゴリズムは一般的に⌊(d_{des}-g))/2⌋までの誤り訂正を保証できる．□

ここで，Pを有理点としΛ＝{P,2P,3P,･･･}とした場合のS*(Λ)を考察する．一般に，ℓ(G)＝r，deg(G)＝mとするとき，r＝ℓ(G)≧ℓ(G-P)≧･･･≧ℓ(G-(m+1)P)＝0となる．また，ℓ(G-jP)＝ℓ(G-(j+1)P)またはℓ(G-(j+1)P)+1なので，{a∈ℕ; ℓ(G-aP)＝ℓ(G-(a+1)P)+1}はちょうどr個存在する．これを順に並べ{a_1,a_2,･･･,a_r}とおき，点Pでの G 空隙系列と呼ぶ．{a_1,a_2,･･･,a_r}≠{0,1,･･･,r-1}のときに，点Pを G Weierstrass point と呼ぶ．なお，G＝mPのときは，{a_1,a_2,･･･,a_r}≠{0,1,･･･,r-2,m}のときにPは Weierstrass point と呼ばれたことに注意せよ．

PがG Weierstrass point あるいは，G＝mPでPが Weierstrass point のと

きに，$S^*(\Lambda)$は小さい値となる．

次に一般の場合にもどってFを因子Dと互いに素な$\mathbb{F}$有理的な有効因子，ΛをFの部分有効因子からなる集合族の部分族とする．ただし，$\Lambda \ni 0, F$とする．次の事実が示される．

[定理16] Λに付随する一般修正復号アルゴリズムは，Fに付随する基本復号アルゴリズムよりも訂正能力はよい．すなわち，$\ker E_{F,w} = L(F-\Sigma_{i=1}^{\circ} Q_i) \neq (0)$ならば，$\ker E_{H,w} = L(H-\Sigma_{i=1}^{\circ} Q_i) \neq (0)$であり，たとえ$\ker E_{F,w} \supsetneq L(F-\Sigma_{i=1}^{\circ} Q_i)$であっても，$\ker E_{H,w} = L(H-\Sigma_{i=1}^{\circ} Q_i) \neq (0)$を期待できる．

(証明) $\ker E_{F,w} \cap L(H) = \ker E_{H,w}$，$L(F-\Sigma_{i=1}^{\circ} Q_i) \cap L(H) = L(H-\Sigma_{i=1}^{\circ} Q_i)$から導かれる．■

5. $\lfloor (d_{des}-1)/2 \rfloor$誤り訂正の復号アルゴリズム

基本復号アルゴリズムを文献(5)のアイデアに従って並列化する．有効因子$F_1, F_2, \cdots, F_s$に付随する並列基本復号アルゴリズムとは，各F_jに付随する基本復号アルゴリズムを並列に実行するものである．

R.Pellikaan[5]とS.G.Vladut[6]は$2g \leqq d_{des}$ [$4g-2 \leqq m$] を仮定すると並列基本復号アルゴリズムが$\lfloor (d_{des}-1)/2 \rfloor$までの訂正を保証できることを示している．ここでは，一般に$1 \leqq d_{des}$ [$2g-1 \leqq m$] としても並列基本復号アルゴリズムが$\lfloor (d_{des}-1)/2 \rfloor$までの訂正を保証できることを示す．$\mathbb{D}_k = \{F:$ FはX上の$\deg(F) = k$なる有効因子$\}$，$\mathbb{D}_k^s$をs重のカルテシアン積とする．$k<0$のときは$\mathbb{D}_k = \varnothing$とする．$\mathrm{Pic}(X)$を，$X$上の$\mathbb{F}$有理的な因子全体の主

因子を法とした類のなす加法群とする．これをXの Picard group と呼ぶ．以下，因子はすべてF有理的とする．Fを因子とするとき，そのPic(X)に於ける類を[F]と表す．Pic(X)の元のうち次数が0であるもの全体はPic(X)の部分群をなすがこれを$Pic^0(X)$と表す．$Pic^0(X)$はXの Jacobian とも呼ばれるのでここではJ(X)で表すことにする．sをs≧2なる自然数とする．写像Ψ_k^sを次のように定義する．

$$\Psi_k^s : \mathbb{D}_k^s \to J(X)^{s-1} \qquad (8)$$

$$F=(F_1,\cdots,F_s)\to([F_1-F_2],\cdots,[F_{s-1}-F_s])$$

[補題17](文献(5)) $0\leqq a\leqq b$ならば，$\mathrm{Image}\Psi_a^s\subset \mathrm{Image}\Psi_b^s$である．また，$\Psi_g^s$は全射，すなわち$\mathrm{Image}\Psi_g^s=J(X)^{s-1}$である．また，$(\#\mathbb{D}_k)^s<(\#J(X))^{s-1}$ならば，$\Psi_k^s$は全射でない，なお，$\#\mathbb{D}_k<\#J(X)$ならば，$\log\#J(X)/(\log\#J(X)-\log\#\mathbb{D}_k)<s$なる自然数sに対して$(\#\mathbb{D}_k)^s<(\#J(X))^{s-1}$，すなわち$\Psi_k^s$は全射でない．□

[補題18](文献(5)) もしXが$\mathbb{F}_q$上の a maximal curve とすると，Ψ_{g-1}^{2g}は全射ではない．ただしq＞4とする．□

[補題19](文献(6)) q≧37のときは，あるsが存在してΨ_{g-1}^sは全射ではない．ただしsは符号長nに関して高々多項式のオーダーである．□

[補題20](文献(6)) q≧16のときは，種数gが十分大きいときにはあるあるsが存在してΨ_{g-1}^sは全射ではない．ただしsは符号長nに関して高々多項式のオーダーである．□

さて，次の事実が示される．

[定理21] $\Psi_{g-1}{}^{s}$は全射でないと仮定する. ただし, $1 \leqq d_{des}$ [$2g-1 \leqq m$] とする. このとき, 並列基本復号アルゴリズムで, $\lfloor (d_{des}-1)/2 \rfloor$までの訂正が保証される.

(証明) 補題22を参照. ■

[注意1] R.Pellikaan[5]とS.G.Vladut[6]は$\Psi_{g-1}{}^{s}$は全射でなくかつ$2g \leqq d_{des}$ [$4g-2 \leqq m$] ならば, 並列基本復号アルゴリズムで$\lfloor (d_{des}-1)/2 \rfloor$までの訂正を保証できることを示した. なお, 条件$4g-2 \leqq m$は(c.4) $\deg(F_j) < d_{des}$を保証するためのものである. また, R.Pellikaan[5]は$\Psi_{g-1}{}^{s}$が全射でないsはいつでも存在し, そのときのsはnの高々多項式のオーダーであろうとの予想を提起している.

定理21は次の補題から導かれる. なお, 補題22は補題11から(c.4)の成立を要求しない.

[補題22] $\Psi_{g-a}{}^{s}$は全射でないと仮定する. ただし, $g \geqq a \geqq 1$. また$d_{des} \geqq a$ [$m \geqq 2g-2+a$] とする. $u = \lfloor (d_{des}-a)/2 \rfloor$とおくと, $\Psi_{g+u}{}^{s}$は全射である. そこで$F = (F_1, \cdots, F_s) \in \mathbb{D}_{g+u}{}^{s}$, $\mathrm{supp}(F_j) \cap \mathrm{supp}(D) = \emptyset$, $1 \leqq j \leqq s$, を$\Psi_{g+u}{}^{s}(F)$がImage$\Psi_{g-a}{}^{s}$に含まれないものとする. このとき, $e \leqq u$とすると, 少なくともひとつのi($1 \leqq i \leqq s$)が存在して,

(a.3) $\deg(F_i) \geqq g+e$

(b.3) $\delta(G-F_i-\Sigma_{j=1}{}^{e} Q_j) = 0$

[$\ell(K_X-G+F_i+\Sigma_{j=1}{}^{e} Q_j) = 0$]

である. すなわち, この場合は(a.1), (b.1), (c.1)のすべてが保証される.

(証明) $\Psi_{g-a}{}^{s}$は全射ではないことから, $F=(F_1,\cdots,F_s)\in \mathbb{D}_{g+u}{}^{s}$, $supp(F_j)\cap supp(D)=\emptyset$, $1\leqq j\leqq s$, で$\Psi_{g+u}{}^{s}(F)$が$\Psi_{g-a}{}^{s}$の像に含まれないものは存在する. $Q=(Q_1,\cdots,Q_e), Q_1,\cdots,Q_e\in supp(D)$とする. ここで, すべてのi$(1\leqq i\leqq s)$に対して$\Omega(G-F_i-\Sigma_{j=1}{}^{e}\ Q_j)\neq(0)$を仮定して矛盾を導く. 任意のi$(1\leqq i\leqq s)$に対して0ではない有理一次微分$\omega_i\in\Omega^1(Rat(X))$で$(\omega_i)\geqq G-F_i-\Sigma_{j=1}{}^{e}\ Q_j$を満たすものが存在する. 他方, ゼロでない有理一次微分に付随する因子は主因子を法とするとそのすべてが一致する. これをK_Xと表す. 標準因子である. $E_i=(\omega_i)-G+F_i+\Sigma_{j=1}{}^{e}\ Q_j\geqq 0$とおく. $deg(E_i)=2g-2-m+g+u+e\leqq 2g-2-m+g+2u\leqq -d_{des}+g+2\lfloor(d_{des}-a)/2\rfloor\leqq g-a$から, E_iは次数がg-a以下($degE_i=b$とする)の有効因子である. すなわち, iに依存しないで$[E_i-F_i]=K_X-[G-\Sigma_{j=1}{}^{e}\ Q_j]$である. すなわち, 任意の$i_1$, i_2, $1\leqq i_1, i_2\leqq s$, に関して$[E_{i1}-E_{i2}]=[F_{i1}-F_{i2}]$である. それゆえ, $\Psi_b{}^{s}(E)=\Psi_{g+u}{}^{s}(F)$である. これは, $Image\Psi_b{}^{s}\subset Image\Psi_{g-a}{}^{s}$に矛盾する. すなわち, 少なくともひとつのi$(1\leqq i\leqq s)$に関して$\Omega(G-F_i-\Sigma_{j=1}{}^{e}\ Q_j)=(0)$である. ■

6. むすび

代数曲線符号の A.N.Skorobogatov and S.G.Vladut による基本復号アルゴリズムを詳しく解析して, 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一般修正復号アルゴリズムを提案した. そして, 一般修正復号アルゴリズムに従うと, 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従った復号器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た．さらに，その訂正能力を保証する評価式を与えた．また，一般に条件$2g \leqq d_{des}$を外して$1 \leqq d_{des}$［$2g-1 \leqq m$］としても並列基本復号アルゴリズムが$\lfloor (d_{des}-1)/2 \rfloor$までの訂正を保証できることを示した．なお，このアルゴリズムの時間複雑度のオーダーは$O(n^3)$以下で，計算複雑度のオーダーは$O(n^4)$でおさえられる．ただし，$\lfloor (d_{des}-1)/2 \rfloor$誤り訂正を保証する並列基本復号アルゴリズムを得るためには$\Psi_{g+u^s}(F)$が$\mathrm{Image}\Psi_{g-1^s}$に含まれない$F=(F_1,\cdots,F_s)\in \mathbb{D}_{g+u^s}$，$\mathrm{supp}(F_j)\cap \mathrm{supp}(D)=\varnothing$，$1 \leqq j \leqq s$，を求める必要がある．しかし，これは存在は示されているものの具体的な探索手法は今後の課題である．また，$\lfloor (d_{min}-1)/2 \rfloor$までの誤り訂正が最終の目標であるが，この解決も今後の課題である．

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) J.Justesen,K.J.Larsen,H.E.Jensen,A.Havemose,T.Hoholdt: “Construction and Decoding of a Class of Algebraic Geometry Codes”, IEEE Trans. Inf. Theory,IT-35,4,pp811-821,(1989).

(4) A.N.Skorobogatov and S.G.Vladut, “On the decoding of algebraic-geometric codes .”IEEE Trans. Inf. Theory,IT-36,5, (1990).

(5) Ruud Pellikaan, “On a decoding Algorithm for Codes on

Maximal Curves." IEEE Trans. Inf. Theory, IT-35, 6, (1989).

(6) S.G.Vladut, "On the decoding of algebraic-geometric codes over F_q for $q \geqq 16$." IEEE Trans. Inf. Theory, IT-36, 6, (1990).

(7) R.Pellikaan, B.-Z.Shen, and G.J.M.van Wee "Which Linear Codes are Algebraic-Geometric? " IEEE Trans. Inf. Theory, IT-37, 3, (MAY 1991).

(8) S.Sakata: "A Fast Versin of the Modified Skorobogatov-Vladut Algorithm to Decode Some Codes from Algebraic Curves " NOVEMBER, 1991.preprint.

(9) J.H.van Lint and G.van der Geer : "Introduction to Coding Theory and Algebraic Geometry" 1988 Birkhäuser Verlag.

(10) M.A.Tsfasman and S.G.Vladut "Algebraic-Geometric Codes" : 1991 MIA Kluwer Academic Publishers.

(11) 三浦晋示「代数曲線符号の一般的な復号法(1),(2)」電子情報通信学会, ＩＴ研究会, 1990.3.15

(12) 三浦晋示「代数曲線符号の復号アルゴリズムについて」電子情報通信学会, ＩＴ研究会, 1991.1.23