第17卷 第5期 电 子 科 学 学 刊 Vol. 17 No. 5
1995 年 9 月 JOURNAL OF ELECTRONICS Sept. 1995

基于 FIA 的代数几何码的译码

任 剑 肖国镇
(西安电子科技大学信息保密所 西安 710071)

摘要 设 C 是亏格为 g 的不可约代数曲线；$C^*(D,G)$ 为 C 上的代数几何码，该码的设计距离为 $d^* = \deg(G) - 2g + 2$. 本文首先从理论上证明所给算法的合理性，然后给出一种基于基本累次算法(FIA) 的译码算法. 该算法是 G. L. Feng 等人(1993)提出的算法的改进.它可对 $\leqslant[(d^* - 1)/2]$ 个错误的接收向量进行译码. 运算量与存贮量约为 G. L. Feng 等人算法的一半，且便于软硬件实现.

关键词 代数几何码，基本累次算法，译码算法

1 引 言

近年来，用代数几何的方法设计好码被公认为是编码学发展中最重要的成果. 它是由苏联数学家 Goppa 首先在古典 Goppa 码的基础上引入的.1982 年，苏联学者 Tsfasman, Vladůt 和 Zink 证明了模曲线上代数几何码的参数优于 Gilbert-Varshamov 界. 1989 年，Justesen 等人[1]首先给出平面代数曲线上代数几何码的译码算法，纠错能力为 $[(d^* - g - 1)/2]$. 随后 Skorobogatov 和 Vladůt[2] 进行了推广，给出任意代数曲线上纠 $[(d^* - g - 1)/2]$ 个错误的译码算法. Pellikaan[3] 给出基于深刻的代数几何知识的译码算法，纠错能力为 $[(d^*-1)/2]$，但复杂度太高 $(O(n^4))$，而且并非完全有效[4,5]，1992 年 Justesen 等人[6]对正则平面曲线，给出纠 $[(d^* - g/2 - 1)/2$ 个错误的译码算法. 最近冯贵良等人[7]又给出纠 $[(d^* - 1)/2]$ 个错误的译码算法. 但他们没有能给出严格的的理论证明，且重复计算和多余存贮较多. 为此本文首先从理论上完善了该算法，然后给出了运算快，存贮少，便于软硬件实现的译码算法.

2 预 备 知 识

设 $\bar{F}_q$ 为 F_q 的代数闭包，射影空间 P^n 为 $\bar{F}_{q+1}$ 在等价关系 $(a_0,a_1,\cdots,a_n) \sim (\lambda a_0, \lambda a_1,\cdots,\lambda a_n),(\lambda \in \bar{F}_q)$ 下的等价类，其元素叫做点. 若 P^n 的点的坐标都在 F_q 中，则称为 F_q 点. 用 $C(F_q)$ 记 C 上 F_q 点的全体. 在 $\bar{F}_q$ 上不可约的代数曲线称为绝对不可约曲线. 以下我们只考虑这种曲线.

一个除子是一个有限形式和 $D = \Sigma n_i P_i$，其中 P_i 为 C 上的点，n_i 为整数. D的阶

1993-11-01 收到，1994-06-03 定稿
任 剑 男，1967 年生，博士生，主要研究编码学与密码学.
肖国镇 男，1934 年生，教授，博士生导师，研究领域主要有信息论、编码学、密码学与应用数学.

定义为 $\deg(D)=\Sigma n_i$. D 的承集定义为 $\mathrm{supp}(D)=\{P_i|n_i\neq 0\}$. 若所有的 n_i 都是正的，则称 D 是有效的，记为 $D\geqslant 0$. 若 P_i 都是 F_q 点，则称 D 为定义在 F_q 上的. 以下我们只考虑这种除子.

C 上的一个有理函数是分式 $f=g/h$，其中 g 和 h 是系数在 F_q 中的同次齐次多项式，$h\neq 0$. g/h 与 g'/h' 称为一致的是指 $gh'-g'h$ 在 C 上恒为 0. 若 $h(P)\neq 0$，则称 f 在 P 点正则. 定义 $(f)=\Sigma m_iQ_i$，其中 Q_i 为 g 或 h 的零点，m_i 为零点的阶. 易知 $\deg(f)=0$. 若存在有理函数 f 使 $D_1-D_2=(f)$，则称除子 D_1,D_2 线性等价. $L(D)=\{f|(f)+D\geqslant 0\}\cup\{0\}$ 为线性空间，维数记为 $l(D)$. 易知，当 $\deg(D)<0$ 时，$L(D)=\{0\}$. $L(0)=F_q$. Riemann-Roch 定理告诉我们 $l(D)=\deg(D)-g+1+l(W-D)$，这里 W 为 C 上的标准除子. 当 $\deg(D)>2g-2$ 时，$l(D)=\deg(D)-g+1$.

Weil **界引理**　$|\#C(F_q)-(q+1)|\leqslant g[2\sqrt{q}]$.

3　代数几何码的构造和译码理论基础

设 C 是一亏格为 g 的代数曲线，$P_1,P_2,\cdots,P_n$，Q 是 C 上的 F_q 有理点. $D=P_1+P_2+\cdots+P_n$，$G=mQ$，$m>\max\{2g,4g-2\}$. 线性码 $C^*(D,G)$ 是线性映射 α^*: $\Omega(G-D)\to F_q^n$，$\alpha^*(\eta)=(\mathrm{Res}_{P_1}(\eta),\mathrm{Res}_{P_2}(\eta),\cdots,\mathrm{Res}_{P_n}(\eta))$ 的象，其对偶码 $C(D,G)$ 为线性映射 $\alpha:L(G)\to F_q^n$，$\alpha(f)=(f(P_1),f(P_2),\cdots,f(P_n))$ 的象. 从而 $C^*(D,G)$ 的校验矩阵为

$$H=\begin{bmatrix} f_1(P_1) & f_1(P_2)\cdots f_1(P_n)\\ f_2(P_1) & f_2(P_2)\cdots f_2(P_n)\\ \vdots & \vdots\quad\ \vdots\\ f_r(P_1) & f_r(P_2)\cdots f_r(P_n)\end{bmatrix},$$

其中 $f_1,f_2,\cdots,f_r$ 为 $L(G)$ 的基.

由文献[8]知，$C^*(D,G)$ 的参数为

$$d^*=m-2g+2,\quad k^*=m-g+1,$$
$$v\leqslant[(d^*-1)/2]=[(m+1)/2]-g.$$

取除子 $H=(m+g)Q$，$F=[(m+1)/2]Q$，则 $\deg(F)=[(m+1)/2]\leqslant(m+1)/2<m$，$\deg(H-F)=m+g-[(m+1)/2]\leqslant m/2+g<m$.

若 $L(o_iQ)\neq L((o_i-1)Q)$，则存在一函数 ϕ_{o_i} 在 Q 点有 o_i 阶极点，称 o_i 为非空隙. 对非空隙有如下引理.

引理[9]

$$o_0=0,$$
$$0<o_1<\cdots<o_{g-1}<2g,$$
$$o_i=i+g,\quad i=g,\quad g+1,\cdots,m.$$

从而可以选取 $L(H)$ 的基 $f_1,f_2,\cdots,f_{m+1}$，使得 $f_i=\phi_{o_i-1}$，$i=1,2,\cdots,m+1$. 显然 $f_1,f_2,\cdots,f_{m+1-g}$ 为 $L(G)$ 的基，$f_1,f_2,\cdots,f_l(l=[(m+1)/2]-g+1)$ 为 $L(F)$ 的基，$f_1,f_2,\cdots,f_t(t=m+1-[(m+1)/2])$ 为 $L(H-F)$ 的基.

设 u 为接收码字，c 为发送码字，e 为错误向量，$E_1,E_2,\cdots E_v$ 为错误位置，$v\leqslant$

$[(d^*-1)/2]$，定义

$$s_i=\sum_{\mu=1}^{\nu}e_\mu\phi_i(E_\mu),\quad S_{ij}=\sum_{\mu=1}^{\nu}e_\mu\phi_{o_{i-1}}\cdot\phi_{o_{j-1}}(E_\mu),$$

则对 $1\leqslant i\leqslant m-g+1$，$s_i=\sum_{j=1}^{n}u_i\phi_i(P_j)$。

令

$$S=\begin{bmatrix}S_{11}&S_{12}\cdots S_{1l}\\S_{21}&S_{22}\cdots S_{2l}\\\vdots&\vdots&\vdots\\S_{s1}&S_{s2}\cdots S_{sl}\end{bmatrix},$$

则对 S 中的项 S_{ij}，当 $o_{i-1}+o_{j-1}=p\leqslant m$ 时，S_{ij} 容易求出，而当 $o_{i-1}+o_{j-1}>m$ 时，S_{ij} 为未知，又 $S_{1l}=\sum_{\mu=1}^{\nu}e_\mu\phi_{o_{l-1}}\cdot\phi_{o_{l-1}}(E_\mu)$，而 $o_{l-1}+o_{1-1}=m+g$，从而 S 中未知元为 $s_{m+1},s_{m+2},\cdots,s_{m+g}$。

对线性方程组

$$SX'=0,\quad X=(x_1,x_2,\cdots,x_l),\tag{1}$$

我们有如下结论。

定理 1 在上述条件下，(1)式必有非零解。

证明 因为 $\deg(F-E_1-\cdots-E_\nu)=[(m+1)/2]-\nu\geqslant[(m+1)/2]-[(m+1)/2]+g=g$，由 Riemann 定理，$l(F-E_1-\cdots-E_\nu)\geqslant\deg(F-E_1-\cdots-E_\nu)+1-g\geqslant g+1-g=1$。从而存在 $f\in L(F-E_1-\cdots-E_\nu)\backslash\{0\}$，设 $f=x_1f_1+x_2f_2+\cdots+x_lf_l$，则 $x_1,x_2,\cdots,x_l$ 不同时为 0，且

$$\begin{aligned}\sum_{i=1}^{l}S_{ij}x_i&=\sum_{i=1}^{l}\sum_{\mu=1}^{\nu}e_\mu\phi_{o_{i-1}}\cdot\phi_{o_{j-1}}(E_\mu)x_i\\&=\sum_{i=1}^{l}\sum_{\mu=1}^{\nu}e_\mu f_i(E_\mu)\cdot f_j(E_\mu)x_i\\&=\sum_{\mu=1}^{\nu}e_\mu f_i(E_\mu)\cdot\sum_{i=1}^{l}f_j(E_\mu)x_i\\&=\sum_{\mu=1}^{\nu}e_\mu f_i(E_\mu)f(E_\mu)=0.\end{aligned}$$

所以，$(x_1,x_2,\cdots,x_l)$ 为(1)式的非零解。 证毕

定理 2 设 $(x_1,x_2,\cdots,x_l)$ 是(1)式的解，令 $f=x_1f_1+x_2f_2+\cdots+x_lf_l$，则 $f\in L(F-E_1-\cdots-E_\nu)$。

证明 由 Riemann-Roch 定理和 $\deg\left(H-F-\sum_{\mu=1}^{\nu}E_\mu\right)\geqslant m+g-[(m+1)/2]-[(m+1)/2]+g>2g-2$ 可得

$$l(H-F)=\deg(H-F)+1-g=m+1-[(m+1)/2],$$

$$l\left(H-F-\sum_{\mu=1}^{\nu}E_\mu\right)=\deg\left(H-F-\sum_{\mu=1}^{\nu}E_\mu\right)+1-g$$
$$=m+1-[(m+1)/2]-\nu,$$

从而 $l(H-F)-l\left(H-F-\sum_{\mu=1}^{\nu}E_\mu\right)=\nu$.

考虑 $\beta: L(H-F)\to F_q^\nu$, $\beta(f)=(f(E_1),f(E_2),\cdots,f(E_\nu))$, 则 $\ker(\beta)=L\left(H-F-\sum_{\mu=1}^{\nu}E_\mu\right)$, 故 $\dim \mathrm{Image}(\beta)=\nu$. 因而 β 为满射. 我们可以选择 $L(H-F)$ 的基 $f_1,f_2,\cdots,f_l$, 满足 $f_i(E_\mu)=\delta_{i\mu}$. 这时我们有

$$0=\sum_{i=1}^{l}\left(\sum_{\mu=1}^{\nu}e_\mu f_i f_i(E_\mu)\right)x_i=\sum_{\mu=1}^{\pi}e_\mu f_i(E_\mu)\sum_{i=1}^{l}f_i(E_\mu)x_i$$
$$=\sum_{\mu=1}^{\nu}e_\mu f_i(E_\mu)f(E_\mu)=e_i f(E_i),$$

从而由 $e_i\neq 0$ 可得 $f(E_i)=0$. 故 $f\in L(F-E_1-\cdots-E_\nu)$. 证毕

综上所述，对(1)式的解 $(x_1,x_2,\cdots,x_l)$, 令 $f=x_1f_1+x_2f_2+\cdots+x_lf_l$, 且设 $Q_1,Q_2,\cdots,Q_s$ 为 f 的所有零点，则 $\{Q_1,Q_2,\cdots,Q_s\}$ 包含所有的错位. 设 $Q_i=E_i$, $i=1,2,\cdots,\nu$. 由伴随式的定义知

$$\sum_{i=1}^{s}f_j(Q_i)z_i=s_j,\quad j=1,2,\cdots,\quad l(G)=m+1-g. \tag{2}$$

显然 $(e_1,e_2,\cdots,e_\nu,0,\cdots,0)$ 为(2)式的一个解，设 $(z_1,z_2,\cdots,z_s)$ 为(2)式的另一解，则 $(z_1-e_1,z_2-e_2,\cdots,z_\nu-e_\nu,z_{\nu+1},\cdots,z_s)$ 可由增加零分量而成为一码字，其 Hamming 重量为 s. 由于 $f\in L(F-Q_1-\cdots-Q_s)\backslash\{0\}$, 所以 $\deg(F)-s\geqslant 0$, 即 $s\leqslant\deg(F)=[(m+1)/2]$ (注意 $m>4g-2$) $<m-2g+2=d^*$, 矛盾！从而(2)式有唯一解. 这样我们有如下定理.

定理 3　若除子 $G=mQ$, 其中 $m>\max\{2g,4g-2\}$, $H=(m+g)Q$, $F=[(m+1)/2]Q$, $\nu\leqslant[(m+1)/2]-g$, 则(2)式有唯一解.

上述三个定理保证了在 $s_{m+1},s_{m+2},\cdots,s_{m+g}$ 已知时，译码算法可以通过求(1)式的解来得出错位，由(2)式的解作为错误向量而实现. 下面我们来研究如何求 $s_{m+1},s_{m+2},\cdots,s_{m+g}$.

4　基于 FIA 的 $s_{m+1},s_{m+2},\cdots,s_{m+g}$ 的 g 次迭代求法和译码算法

FIA 算法[10]可解决如下问题：

设

$$A=\begin{bmatrix}a_{11}&a_{12}&\cdots&a_{1N}\\a_{21}&a_{22}&\cdots&a_{2N}\\\vdots&\vdots&&\vdots\\a_{M1}&a_{M2}&\cdots&a_{MN}\end{bmatrix}$$

为一矩阵，找出最小的 l 和 $c_1,c_2,\cdots,c_l$ 使

$$a_{i,l+1}+c_1a_{i,l}+\cdots+c_la_{i,1}=0,\ i=1,2,\cdots,M.$$

对第 j 列，定义 $C^{(i-1,j)}(x)=\sum_{k=0}^{j-1}c_k^{(i-1,j)}x^k$，其中 $c_0^{(i-1,j)}=1$，满足对 $h\leqslant i-1$，

$$[C^{(i-1,j)}(x)\cdot a^{(h)}(x)]_j=a_{h,j}+c_1^{(i-1,j)}a_{h,j-1}+\cdots+c_{j-1}^{(i-1,j)}a_{h,1}=0.$$

这里 $a^{(h)}(x)=1+a_{h,1}x+a_{h,2}x^2+\cdots+a_{h,N}x^N$，$[f(x)]_j$ 为 $f(x)$ 中 x^j 的系数，第 j 列的起始多项式为 $C^{(0,j)}(x)$，$C^{(0,1)}(x)=1$ 为第 1 列的起始多项式。令

$$d_{i,j}=[C^{(i-1,j)}(x)\cdot a^{(i)}(x)]_j=a_{i,j}+c_1^{(i-1,j)}a_{i,j-1}+\cdots+c_{j-1}^{(i-1,3)}a_{i,1}.$$

若对第 j 列，$i=1,2,\cdots,r-1$，$d_{i,j}=0$，则 $C^{(0,j)}(x)=C^{(1,j)}(x)=\cdots=C^{(r-1,j)}(x)$. 若 $d_{r,j}\neq 0$，且不存在 u，$1\leqslant u<j$，$C^{(u)}(x)=C^{(r-1,u)}(x)$，定义第 j 列的最后多项式为 $C^{(r-1,j)}(x)$ 在 $a_{r,j}$ 处置“×”，然后转向第 $j+1$ 列。令 $C^{(0,j+1)}(x)=C^{(j)}(x)-C^{(r-1,j)}(x)$ 若存在 u，$1\leqslant u<j$，使 $C^{(u)}(x)=C^{(r-1,u)}(x)$，令

$$C^{(r,j)}(x)=C^{(r-1,j)}(x)-(d_{r,j}/d_{r,u})\cdot C^{(u)}(x)x^{j-u}.$$

易知，第 j 列有“×”，当且仅当该列不可由前 $j-1$ 列线性表示。现在我们考虑如下形式的矩阵 S^*

$$\begin{bmatrix}
S_{11} & S_{12} & S_{13} & S_{14} & S_{15} & S_{16} & S_{17} & S_{18} & S_{19}\\
S_{21} & S_{22} & S_{23} & S_{24} & S_{25} & S_{26} & S_{27} & ⓐ & \# \\
S_{31} & S_{32} & S_{33} & S_{34} & S_{35} & S_{36} & ⓐ & \# & \# \\
S_{41} & S_{42} & S_{43} & S_{44} & ⓐ & \# & \# & \# & \# \\
S_{51} & S_{52} & S_{53} & S_{54} & \# & \# & \# & \# & \# \\
S_{61} & S_{62} & ⓐ & \# & \# & \# & \# & \# & \# \\
S_{71} & S_{72} & \# & \# & \# & \# & \# & \# & \#
\end{bmatrix}$$

这里ⓐ和#未知，ⓐ右边和下边的元为#，左边和上边的元已知，若#为所在行(或列)中的第一个未知元，则它左边(或上边)的元已知，右边(或下边)的元为#. 我们的目的是考察若 S_{ij} 为ⓐ时，是否存在唯一的值ⓐ，使第 j 列的前 i 项可由前 i 项线性表示。若答案是肯定的，如何求这一值？为此我们先证明如下的定理。

定理 4 设 A 为对称矩阵，则第 i 行 j 列处的ⓐ可唯一确定，当且仅当第 j 行第 i 列处的ⓐ可唯一确定，且二者相等。这里我们假定这两处都为ⓐ，我们把第 i 行 j 列处的ⓐ记为 $ⓐ_{ij}$。

证明 $ⓐ_{ij}$ 可唯一确定等价于存在唯一的 $ⓐ_{ij}$ 使

$$\mathrm{Rank}\begin{pmatrix}
a_{11} & \cdots & a_{1,j-1} & a_{1j}\\
\vdots & & \vdots & \\
a_{i-1,1} & \cdots & a_{i-1,j-1} & a_{i-1,j}\\
a_{i1} & \cdots & a_{i,j-1} & ⓐ_{ij}
\end{pmatrix}=\mathrm{Rank}\begin{pmatrix}
a_{11} & \cdots & a_{1,j-1}\\
\vdots & & \vdots\\
a_{i-1,1} & \cdots & a_{i-1,j-1}\\
a_{i1} & \cdots & a_{i,j-1}
\end{pmatrix}$$

等价于存在唯一 $ⓐ_{ij}$ 使

$$\mathrm{Rank}\begin{pmatrix}
a_{11} & \cdots & a_{i-1,1} & a_{i1}\\
\vdots & & \vdots & \vdots\\
a_{1,j-1} & \cdots & a_{i-1,j-1} & a_{i,j-1}\\
a_{1j} & \cdots & a_{i-1,j} & ⓐ_{ij}
\end{pmatrix}=\mathrm{Rank}\begin{pmatrix}
a_{11} & \cdots & a_{i-1,1} & a_{i1}\\
\vdots & & \vdots & \vdots\\
a_{1,j-1} & \cdots & a_{i-1,j-1} & a_{i,j-1}
\end{pmatrix}.$$

由于 A 对称可知上式等价于 $@_{ji}$ 可唯一确定，且 $@_{ji}=@_{ij}$。　　证毕

对第 3 节我们考虑的代数几何码，作如下的矩阵，对我们有用的仅是满足 $o_{i-1}+o_{j-1}\leqslant m+g$ 的 S_{ij}，因而我们只写出这些元，可得

$$S^*=\begin{bmatrix} S_{11} & S_{12} & \cdots S_{1l} & S_{1,l+1}\cdots S_{1,m-g} & S_{1,m-g+1} \\ S_{21} & S_{22} & \cdots S_{2l} & S_{2,l+1}\cdots S_{2,m-g} & \\ \vdots & \vdots & \vdots & \vdots & \\ S_{t-1,1} & S_{t-1,2}\cdots S_{t-1,l} & S_{t-1,l+1} & & \\ S_{t1} & S_{t2} & \cdots S_{tl} & & \end{bmatrix}.$$

记 S^* 中 s_{m+1} 为 $@,s_{m+2},\cdots,s_{m+g}$ 为#，其余已知。文献[7]已对如下矩阵作了类似的代换

$$\bar{S}=\begin{bmatrix} S_{11} & \cdots S_{1,m-g+1} \\ \vdots & \vdots \\ S_{m-g+1,1} & \cdots S_{m-g+1,m-g+1} \end{bmatrix},$$

且有如下结果：在 $\bar{S}$ 中，若 $s_{m+1},\cdots,s_{m+w-1}$ 已求出，$1\leqslant w\leqslant g$，用@代替 s_{m+w}，则必有至少一个@可求出，且在可求出者中，等于 s_{m+w} 者数目最多。由定理 4，我们有如下的定理。

定理 5　在 S^* 中只考虑 $j\geqslant i$ 的 $@_{ij}$ 时，若 $s_{m+1},\cdots,s_{m+w-1}$ 已求出，$1\leqslant w\leqslant g$，用@代替 s_{m+w}，则至少有一个@可唯一确定。若根据所确定的值是否相同进行分组，则确定同一值数目最多的组所对应的值为 s_{m+w}；若有两组数目相同，则必有一组含一对角元，这时另一组对应的值即为 s_{m+w}，且只有这两种情况。

现在我们给出如下改进的译码算法：

第 1 步　建立空表 C,D,E,F；$1\to j,r$；$1\to C^{(j)}(x)$；

第 2 步　计算 $d_{r,j}=[C^{(j)}S^{(r)}(x)]_j$；

第 3 步　若 $d_{r,j}=0$，则

(1) 若 $j=m-g+1$，$S_{r+1,j}$ 为@或#时，停机。

(2) 若 $S_{r+1,j}$ 为@，但 $r+1\leqslant j$，考察是否存在 $d_{r+1,u}\in D$，$1\leqslant u<j$，若无，则 $-\sum_{h=1}^{j-1}C_h^{(j)}S_{r+1,h}\to @_{r+1,j}$ 且贮存于 E，$C^{(j)}(x)$ 贮存于 F，$C^{(j)}(x)\to C^{(j+1)}(x)$，$j+1\to j$，$1\to r$，返回第 2 步；若有或 $r+1>j$，直接 $C^{(j)}(x)\to C^{(j+1)}(x)$，$j+1\to j$，$1\to r$，返回第 2 步；

(3) 若 $S_{r+1,j}$ 为#，$C^{(j)}(x)\to C^{(j+1)}(x)$，$j+1\to j$，$1\to r$，返回第 2 步；

(4) 若以上几条都不成立，$r+1\to r$，返回第 2 步；

第 4 步　若 $d_{r,j}\neq 0$，则

(1) 若存在 $d_{r,u}\in D$，$1\leqslant u<j$，$C^{(j)}(x)-\frac{d_{r,j}}{d_{r,u}}C^{(u)}(x)\cdot x^{j-u}\to C^{(j)}(x)$，返回第 3 步；

(2) 若不然，贮存 $d_{r,j}$ 于 D，贮存 $C^{(j)}(x)$ 于 C，在 S^* 中的 $S_{r,j}$ 处标一“×”$C^{(j)}(x)\to C^{(j+1)}(x)$，$j+1\to j$，$1\to r$，返回第 2 步。

在上述算法之后，所有满足 $j \geqslant i$ 且可唯一确定的 $@_{i,j}$ 已被求出，存贮于 E 中。根据定理 5 可求出 s_{m+1}，代入 S^* 中。用同样的方法可求出 $s_{m+2},\cdots,s_{m+g}$，且在每次求 $s_{m+2},\cdots,s_{m+g}$ 时，我们可以利用前面已算好的结果，而不必重新开始计算。

下面我们对上述译码算法的复杂度与 Feng 等人[7]的译码的复杂度作一比较。

译码的复杂度主要决定于（1）构造 S^* 的复杂度；（2）求 s_{m+1} 的复杂度；（3）求 $s_{m+2},\cdots,s_{m+g}$ 的复杂度。

现分别以 $C(i)$ 记第 i 步的复杂度，$i=1,2,3$。我们所给算法与 Feng 等人的算法具有相同的 $C(1)$，即为 $O(mn)$，也就是存在一固定的常数 C_1，其运算次数为 $C_1(mn)$。对 $C(2)$，Feng 等人的复杂度为 $O((m-g+1)^3)$，而我们所给算法的复杂度为 $O((m+1)/2(m-g+1)^2)$。由于这两个算法的方法在这里是完全一致的，因而存在一固定的常数 C_2，使 Feng 等人的运算次数为 $C_2(m-g+1)^3$，而我们的运算次数为 $C_2[(m+1)/2](m-g+1)^2$。同样，对 $C(3)$，存在常数 C_3，使 Feng 等人的运算次数为 $C_3(g-1)(m-g+1)^2$，而我们的运算次数为 $C_3(g-1)[(m+1)/2]\cdot(m-g+1)$，由于当 $m \approx n$ 且很大时，我们所给算法的第 2 步与第 3 步的复杂度均为 Feng 等人算法的一半，而第 1 步则远小于第 2，3 步的复杂度，因而可忽略不计。由此说明：当 $m \approx n$ 且很大时，我们的算法复杂度为原来 Feng 等人算法的一半。存贮空间节约一半是因为我们是对 $[(m+1)/2]\times(m-g+1)$ 矩阵进行讨论，而 Feng 等人是对 $(m-g+1)\times(m-g+1)$ 矩阵进行讨论而实现的。

5 结 束 语

代数几何码的译码是目前研究的热点，文献[7]给出一种能对 $G=mQ$ 时 $C^*(D,G)$ 进行译码的有效方法，但文献[7]未能给出严格的理论证明，如文献[7]中只要求 $M>2g$，而我们这里要求 $m>\max\{4g-2,2g\}$。事实上，若仅有条件 $m>2g$，则定理 3 中的唯一性在文献[7]中是无法保证的；另外，当 m 很大时，我们的算法会减少大量的重复计算和重复存贮。

致谢 作者对王新梅教授的帮助、鼓励和有益的讨论表示衷心的感谢。

参 考 文 献

[1] Justesen J, Larsen K J, Jensen H E, et al. IEEE Trans. on IT, 1989, IT-35(7): 811—821.
[2] Skorogatov A N, Vladut S G. IEEE Trans. on IT, 1990, IT-36(9): 1051—1060.
[3] Pellikann R. IEEE Trans. on IT, 1989, IT-35(11): 1228—1232.
[4] Brigand D L B. Decoding of codes on hyperelliptic curves, LNCS 514, Eurocode'90, Proc. International Symposium on Coding Theory and Application. Udine, Italy: Nov. 1990, 126—134.
[5] Rotillon D, Thiongly J A. Decoding of codes on the klein quartic, LNCS, Eurocode'90, Proc. International Symposium on Coding Theory and Application. Udine, Italy: Nov. 1990, 135—149.
[6] Justesen J, Larsen K J, Jesen H E, et al. IEEE Trans. on IT, 1992, IT-38(1): 111—119.
[7] Feng G L, Rao T R N. IEEE Trans. on IT, 1993, IT-39(1): 37—45.
[8] Vanlint J H. Algebraic geometric codes, Coding Theory and Design Theory, IMA Volumes in Mathematics and Its Applications, Vol. 20, Springer-Verlag, 1988, 137—162.

[9] Fulton W. Algebraic Curves. New York: Benjamin, 1969.
[10] Feng G L, Tzeng K K. IEEE Trans. on IT, 1991, IT-37(9): 1274—1287.

ON THE DECODING OF ALGEBRAIC GEOMETRIC CODES BASED ON FIA

Ren Jian　　Xiao Guozhen

(*Institute of Information Security, Xidian University, Xi'an* 710071)

Abstract　Supposing C is an irreducible algebraic curve of genus g, $C^*(D, G)$ is an algebraic geometric code of designed minimum distance $d^* = \deg G - 2g + 2$. This paper, first, proves that the given algorithm is reasonable theoretically, then gives a decoding algorithm based on Fundamental Iterative Algorithm (FIA), which is a modification of the algorithm proposed by G. L. Feng, et al. (1993) and can correct any received code of $(d^* - 1)/2$ or less errors with complexity only one half of that of the algorithm proposed by G. L. Feng, et al. The procedure can be implemented easily by hardware or software.

Key words　Algebraic geometric code, Fundamental iterative algorithm, Decoding algorithm