第 14 卷 第 6 期
1992 年 11 月

电 子 科 学 学 刊
JOURNAL OF ELECTRONICS

Vol. 14, No. 6
Nov., 1992

关于 Justesen 代数几何码

陆佩忠　　宋国文
(成都电信技术研究所,成都 610041)

摘要　本文通过建立保持 Hamming 距离的同构，给出了研究 Justesen 等(1989)所构造的代数几何码的一般方法，并取得一些新的结果. 本文在进行译码研究时，首次把同类型的"较小"的代数几何码的码字与错误位置多项式的值相对应，从而清晰地揭示了译码过程，以及纠错能力. 本文还得到一般代数几何码维数的上界和下界. 最后给出了一个容易理解的译码算法. 此算法类似于 RS 码的 Peterson 译码算法。

关键词　代数几何码;错误位置多项式;伴随式矩阵; Riemann-Roch 定理.

一、引　　言

J. Justesen 等[1]构造了一大类代数几何码,统称为 JAG 码. JAG 码是基于平面代数曲线. 文献[1]中给出了一个译 JAG 码的算法. 此算法是通过求解一个系数由伴随式的适当组合排序而构成的齐次线性方程组，得到错误位置多项式. A. N. Skorobogatov 等[2]推广了 Justesen 的思想，给出了基于一般代数曲线的代数几何码的译码算法. 他们的一个很有价值的思想是把错位多项式看成一个多变元的有理函数. 这样就与定义码字所用的有理函数在概念上得到统一. 文献[2]中译码时先要选择除子 D,K, 还要分别求出对应的空间 $L(D-K)$ 和 $L(K)$ 的基. 这在代数几何中尚无一般的方法. 因此这个译码算法只是理论上的,在实际应用中,必须对各自选择的码型作额外处理.

本文的主要思想是用"较小"的代数几何码 S,T 来代替空间 $L(D-K)$, $L(K)$. 这样避开了除子的使用. 而前者的生成元集是已知的. 此方法的显著优点是，把错位多项式的值与码 T 中的码字相对应，从而清晰地揭示了译码过程和纠错能力. 本文首先引进了保距同构的概念，用更一般的方法给出了 JAG 码的参数. 本文得到一般代数几何码维数的上界和下界. 最后给出 JAG 码的译码算法,此算法类似于 RS 码的 Peterson 译码算法.

二、代数几何基础和代数几何码的构造

关于代数几何码的详细介绍参阅文献[3].这里列出一些本文要用到的概念和结论. 这样对不熟悉代数几何的读者,只要承认几个结论,就可以顺利阅读和理解本文的思想和

1991.05.30 收到，1992.01.03 定稿.

方法.

设 $\bar{F}_q$ 是 F_q 的代数封闭域，P^n 是射影空间. P^n 中的分量都是 F_q 中的 $n+1$ 元的元素对称之为有理点. 设 C 是 P^n 中的代数曲线. 本文中的 C 都是在 $\bar{F}_q$ 上平滑且绝对不可约的代数曲线.

Bezout 定理　设 F,G 为射影平面曲线，次数分别是 n,m，且无公共分枝，则 $F\cap G$ 中点数是 nm.

C 上的有理函数 $f=g/h$，这里 g，h 是同次齐次多项式，且 h 在 C 上不恒为 0. 称 $f=g/h$ 在 P 点正则，如果 $h(p)\neq 0$.

C 上的除子 D 是 C 上点的形式有限和：$D=\sum n_iP_i$，$n_i\in Z$. D 的次数 $\deg(D)=\sum n_i$. 支撑点集 $\mathrm{supp}(D)=\{P_i\mid n_i\neq 0\}$. 称 D 是有效的，如果 $n_i\geqslant 0$，对每个 i. 这时记 $D\geqslant 0$.

对每个 C 上的有理函数 $f=g/h$，对应一个除子 $(f)=\sum(n_i-m_i)Q_i$，这里 n_i 是 Q_i 作为 g 的零点的重数，m_i 为 Q_i 作为 h 的零点的重数. 则 $\deg((f))=0$.

称除子 D_1,D_2 线性等价，如果 $D_1-D_2=(f)$，f 为 C 上的某有理函数.

称 $L(D)=\{f\mid(f)+D\geqslant 0\}$ 是除子 D 的相伴有理函数空间. 记

$$l(D)=\dim(L(D)) \tag{1}$$

显然如果 $\deg(D)<0$，则 $L(D)=\varnothing$.

Riemann-Roch 定理　$l(D)=\deg(D)-g+1+l(K-D)$，这里 K 是 C 上某除子的线性等价类. g 是 C 的亏格.

设 C 的次数是 d，如果 C 是正则的，则亏格 $g=(d-1)(d-2)/2$. 如果 $D=0$，则 $l(K)=g$. 令 $D=K$，则 $\deg(K)=2g-2$. 如果 $l(K-D)\neq 0$，则称 D 是特殊的. 如果 $\deg(D)>2g-2$，则 $l(D)=\deg(D)-g+1$. 如果 $g=1$，则 C 是椭圆曲线. 如果 $g=0$ 则 $C=P^1$.

对 C 上任一有理点 p，存在局部参数 μ_p. μ_p 是有理函数，且在 p 点是单零点.[2]

下面我们来定义代数几何码.

设 C 为代数曲线，g 为亏格，$P=\{P_1,\cdots,P_n\}$ 为 C 上的有理点集. D 是 C 的除子，且 $\mathrm{supp}(D)\cap P=\varnothing$，设 $2g-2<\deg(D)\leqslant n+g-1$.

作线性变换 v：$L(D)\to F_q^n$，使 $v(f)=(f(P_1),\cdots,f(P_n))$，则由 $\{C,P,D\}$ 导出两个代数几何码 $G_D=v(L(D))$ 和 $H_D=(v(L(D)))^{\perp}$. 本文主要是对 H_D 进行译码. 设 $f_1,\cdots,f_m$ 是 $L(D)$ 的一组基. 由 Riemann-Roch 定理，$m=\deg D-g+1$. 显然

$$H=\begin{bmatrix} f_1(P_1) & f_1(P_2)\cdots f_1(P_n)\\ f_2(P_1) & f_2(P_2)\cdots f_2(P_n)\\ \cdots\cdots & \\ f_m(P_1) & f_m(P_2)\cdots f_m(P_n)\end{bmatrix} \tag{2}$$

是 G_D 的生成矩阵，同时又是 H_D 的校验矩阵.

设 c 为 H_D 的任一码字，r 为收到的码字，$r=c+e$，e 为错码向量，对任意 $f\in L(D)$，定义伴随式：

$$S(r,f)=\sum_{i=1}^{n} r_i f(p_i) \tag{3}$$

则

$$S(r,f)=\sum_{i=1}^{n}(e_i+c_i)f(p_i)=\sum_{i=1}^{n} e_i f(p_i)+\sum_{i=1}^{n} c_i f(p_i) \tag{4}$$

故

$$S(r,f)=\sum_{i=1}^{n} e_i f(p_i)=S(e,f) \tag{5}$$

对任意 $a\in F_q^n$，则 $a\in H_D$，当且仅当 $S(a,f_i)=0$，$i=1,\cdots,m$。

定理 1 (1) H_D 的极小距离 $d(H_D)\geqslant a-2g+2$，这里 $a=\deg D$，令 $s=a-2g+1$，称 $s+1$ 为设计码距。(2) $\dim(H_D)$ 满足：

$$n-a+2g-1\geqslant \dim(H_D)\geqslant n-a+g-1 \tag{6}$$

证明 (1) 对 P 中任意 s 个点 $p_{i_1},\cdots,p_{i_s}$，作映射 v'：$L(D)\to F_q^s$，使 $v'(f)=(f(p_{i_1}),\cdots,f(p_{i_s}))$，则

$$\dim(v'(L(D)))=\dim(L(D))-\dim\left(L(D)-\sum_{j=1}^{s} p_{i_j}\right)$$

上式成立是因为 $\mathrm{supp}(D)\cap P=\emptyset$。这时 $\deg\left(L(D)-\sum_{j=1}^{s} p_{i_j}\right)=a-s=2g-1>2g-2$。由 Riemann-Roch 定理知，$\dim(L(D))=a-g+1$，$\dim\left(L(D)-\sum_{j=1}^{s}\times p_{i_j}\right)=a-s-g+1$。故 $\dim(v'(L(D)))=a-g+1-(a-s-g+1)=s$，因此 v' 是映上的线性变换，所以 $(v'(L(D))^{\perp}=0$，H_D 的极小 Hamming 距离$\geqslant s+1=a-2g+2$。

(2) 由于 $G_D\cong L(D)/[L(D-\sum p_i)]$，故 $\dim(H_D)=n-\dim(G_D)=n+l(D-\sum p_i)-l(D)=n-a+g-1+l(D-\sum p_i)\geqslant n-a+g-1$。另一方面，$H_D$ 的 Hamming 距离$\geqslant s+1$，故矩阵H的任意 s 列线性无关，故H的秩$\geqslant s$，$\dim(G_D)\geqslant s$，$\dim(H_D)=n-\dim(G_D)\leqslant n-s=n-a+2g-1$。

文献[3]中已有定理1的部分结果，但我们的证明更简明。维数的上界是我们新得到的结果。特别在 $g=0$ 时，$\dim H_D=n-a+1$，且 $d(H_D)\geqslant a+2$。

三、Justesen 码的构造

下设 C 为射影空间 P^2 上的平面曲线，记 C 是由一个系数在 F_q 上的三变元 m 次齐次多项式的零点组成。$P=\{p_1,\cdots,p_n\}$ 是 C 的有理点集，且 p_i 的第 1 个非零分量值是 1。对 $j\geqslant m-2$，设 V_j 是 $F[x,y,z]$ 中 j 次齐次多项式全体以及 0 所组成的向量空间。构造如下两种线性码：

$$G_j=\{(f(p_1),\cdots,f(p_n))\mid f\in V_j\} \tag{7}$$

$$H_j = G_j^{\perp} \tag{8}$$

现在要建立 G_j, H_j 与前面定义的 AG 码 G_D, H_D 之间的联系. 先看特殊情形. 设 V_j 中含有 1 个 j 次齐次多项式 f_0, 使 $f_0(p_i) \neq 0$, $i = 1, \cdots, n$. 令 $D = \sum n_i Q_i$, 其中 Q_i 是 $\boldsymbol{C} \cap f_0$ 中的点, n_i 为重数. 由 Bezout 定理知 $\deg D = mj$. 设 $n > mj$

定理 2　设 G_D, H_D 是由上述 $\{\boldsymbol{C}, P, D\}$ 导出的 AG 码, G_j, H_j 是由(7),(8)式所定义的 JAG 码. 定义如下同态:

σ: $G_j \to G_D$ 使 $\sigma(f(p_1), \cdots, f(p_n)) = (f(p_1)/f_0(p_1), \cdots, f(p_n)/f_0(p_n))$, 则 σ 是同构且保持 Hamming 重量.

证明　$f(p_i)/f_0(p_i) = 0$, 当且仅当 $f(p_i) = 0$, 故 σ 保持 Hamming 重量. 设 $f \in \mathrm{Ker}(\sigma)$, 则 $f(p_i) = 0$, $f/f_0 \in L\left(D - \sum_{i=1}^{n} p_i\right)$. 因 $\deg D = mj < n$, 故 $f/f_0 = 0$, f 在 $\boldsymbol{C}$ 上恒为 0, 故 σ 是单射. 若 f 在 $\boldsymbol{C}$ 上恒为 0, 当且仅当 f 是 $\boldsymbol{C}$ 的倍数. 令 $I = \{f \in V_j \mid f$ 为 $\boldsymbol{C}$ 的倍数$\}$, 则 $\dim(I) = \binom{j-m+2}{2}$. 显然 $V_j/I \cong G_j$, 故 $\dim G_j = \binom{j+2}{2} - \binom{j-m+2}{2} = \deg D - g + 1$. 由于 $G_D \cong L(D)/L(D - \sum p_i)$, 由 Riemann-Roch 定理知, $\dim(G_D) = \deg D - g + 1 = \dim G_j$, 因此 σ 是同构.

同样, 我们有下面的结论.

定理 3　下面的映射 δ 是保持 Hamming 重量的同构. δ: $H_j \to H_D$ 使

$$\delta(h_1, \cdots, h_n) = (h_1 f_0(p_1), \cdots, h_n f_0(p_n))$$

推论 1　当 V_j 中有不以 $\{p_i\}$ 为零点的多项式时, 且 $n > mj$, $j \geq m - 2$, 则

$$d(H_j) \geq mj - 2g + 2$$

下面我们要取消对 V_j 的限制.

引理 1　在有限射影几何 $PG(2, q)$ 中存在一条直线 l, 使 l 不与 $p_1, \cdots, p_n$ 中任一点相切.

证明　见文献[1]中注 1.

由引理 1, V_j 中存在 f_0, 使 $\mathrm{ord}_{p_i}(f_0) \leqslant 1$, 这只要将 l 中的变量上升 j 次幂即可. 令 D 是 f_0 与 $\boldsymbol{C}$ 的切割除子, 则 $D = \sum n_i P + D'$, 其中 $0 \leqslant n_i \leqslant 1$, 且 $\mathrm{supp}(D') \cap P = \varnothing$. 令 μ_{p_i} 为 $\boldsymbol{C}$ 在 p_i 点局部参数, 即 μ_{p_i} 以 p_i 为单零点的有理函数. 我们构造类似的同构:

σ': $G_j \to G'_D$ 使 $\sigma'(f(p_1), \cdots, f(p_n)) = (\mu_{p_1}^{n_1} f/f_0(p_1), \cdots, \mu_{p_n}^{n_n} f/f_0(p_n))$ 其中 G'_D 的定义如下:

设 v' 是线性变换, 即

v': $L(D) \to F_q^n$ 使 $v'(f) = (\mu_{p_1}^{n_1} f(p_1), \cdots, \mu_{p_n}^{n_n} f(p_n))$

其中 $f \in L(D)$, 此时 $G'_D = v'(L(D))$, $H'_D = (G'_D)^{\perp}$.

δ': $H_j \to H'_D$ 使 $\delta'(c_1, \cdots, c_n) = (f_0/\mu_{p_1}^{n_1}(p_1)c_1, \cdots, f_0/\mu_{p_n}^{n_n}(p_n)c_n)$

对上述的 $G'_D, H'_D, v', \sigma', \delta'$ 我们可以得到与定理 1, 定理 2 和定理 3 相同的结论. 详见文献[2]. 以后我们不再对 V_j 限制, 假定存在 f_0, 使 $f_0(p_i) \neq 0$, $i = 1, \cdots, n$.

四、一些著名的码

例 1 传统意义下的 Reed-Solomen 码

令 C 由 $z=y$ 一次多项式定义. 有理点 $p_i=(\alpha^{i-1},1,1)$ $i=1,2\cdots,n$, 其中 α 是 F_{q^n} 中的 n 次本原单位根. 令 $Q=(0,1,1)$. 令除子 $D=tQ$, 其中 $t<n$. 定义 $G=\{(f(p_1),\cdots,f(p_n))|f\in L(D)\}$, 此时 $\dim(G)=l(D)-l(D-\sum p_i)=\deg D-g+1=t+1$. 显然 $\{y^i/x^i|i=0,\cdots,t\}$ 是 $L(D)$ 的 $t+1$ 个元素,且易证明是线性无关的, 因而构成 $L(D)$ 的基. 由于 p_i 的 y, z 坐标都为 1, 故 $L(D)$ 中的元素 f 可看作 $F[x]$ 中次数$\leqslant t$ 的多项式. 这样 G 就可看作 RS 码,且 $d(G)=n-t$.

例 2 BCH 码

C 仍为 $y=z$ 所定义, $p_i=(\alpha^{i-1},1,1)$, $i=1,\cdots,n$, $Q_1=(1,0,0)$, $Q_2=(0,1,1)$. 令 $D=(d-1)Q_1-Q_2$, 则 $l(D)=\deg D-g+1=d-1$. 显然, x^i/y^i, $i=1,\cdots,d-1$ 是 $L(D)$ 的基. H_D 是由 $\{C,P,D\}$ 导出的 AG 码. 校验矩阵 $H=(f_i(p_j))=(\alpha^{ij})$, $i=1,\cdots,d-1$. 且 $d(H_D)\geqslant \deg D-2g+2=d$. 把 H_D 限制在 F_q 上时,便得到由 $\alpha,\alpha^2,\cdots,\alpha^{d-1}$ 所定义的 BCH 码.

例 3 Goppa 码

设 $g(z)$ 为 F_{q^m} 上次数为 t 的多项式, $L=\{r_0,\cdots,r_{n-1}\}\subset F_{q^m}$, $|L|=n$, 且 $g(r_i)\neq 0$, $i=0,\cdots,n-1$. Goppa 码 $\Gamma(L,g)$ 定义为

$$\Gamma(L,g)=\left\{c=(c_0,\cdots,c_{n-1})\in F_q^n\ \middle|\ \sum_{i=0}^{n-1}\frac{c_i}{z-r_i}\equiv 0\ \mathrm{mod}\, g(z)\right\} \tag{9}$$

设 C 仍由 $y=z$ 所定义, $p_i=(r_i,1,1)$, $i=0,\cdots,n-1$, 此时 $g=0$, 令 t 次齐次多项式 $g(x/z)z^t$ 与 C 的交点 $Q_1,\cdots,Q_t$. 令 $D=\sum_{i=1}^{t}Q_i$ 是 C 上的除子. 此时

$$\mathrm{supp}(D)\cap P=\varnothing,\quad l(D)=\deg D-g+1=t+1$$

显然, $\{x^iy^{t-i}/[g(x/y)y^t]|i=0,1,\cdots,t\}$ 构成 $L(D)$ 的一组基. 导出的 AG 码为 H_D. 令 $h_i=x^iy^{t-i}/[g(x/y)y^t]$, 则 $c\in H_D$, 当且仅当 $S(c,h_i)=0$, $i=0,\cdots,t$. 因而相应的校验矩阵为

$$H=\begin{bmatrix}1 & 1 & \cdots & 1\\ r_0 & r_1 & \cdots & r_{n-1}\\ \cdots & \cdots & \cdots & \cdots\\ r_0^t & r_1^t & \cdots & r_{n-1}^t\end{bmatrix}\begin{bmatrix}\frac{1}{g(r_0)} & & 0\\ & \ddots & \\ 0 & & \frac{1}{g(r_{n-1})}\end{bmatrix} \tag{10}$$

将 H_D 码限制在 F_q 上,即得著名的 Goppa 码 $\Gamma(L,g)$. 此时

$$\dim(H_D)=n-\deg(D)+2g-1=n-t+1$$

且 $d(H_D)\geqslant \deg D-2g+2=t+2$, 故 $\Gamma(L,g)$ 的极小距离 $d_\Gamma\geqslant \deg(g(z))+2$.

注意, 我们得到 d_Γ 比文献[5]中的下界大 1。

五、Justesen 码的译码

先给出对 BCH 码的新的译码算法. 不仿设 d 为偶数. 令 $K_d=\{x/y,\cdots,x^{d-1}/y^{d-1}\}$ 为例 2 中 $L(D)$ 的基,作 $D'=(d/2-1)Q_1-Q_2$, 则 $K_{d/2}$ 是 $L(D')$ 的基. 设 $H_{d/2}=\{1,x/y,\cdots,x^{d/2}/y^{d/2}\}$, 则 $K_{d/2}\cdot H_{d/2}=K_d$. 若 $r=c+e$ 为收到的码字, e 为出错向量,且 $W(e)<d/2$. 则必存在一个有理函 σ 是 $H_{d/2}$ 中元素的线性组合,且是错误位置的有理函数. 这只要注意到 p_i 的 y, z 坐标上的值是 1, 以及 $W(e)<d/2$ 便知. 把 $K_{d/2}$ 和 $H_{d/2}$ 中的元素按顺序分别表示成 $k_1,\cdots,k_{d/2-1}$ 和 $h_0,h_1,\cdots,h_{d/2}$. 设

$$s_{ij}=S(r,k_ih_j),\quad i=1,\cdots,d/2-1,\quad j=0,\cdots,d/2 \tag{11}$$

求齐次线性方程组

$$\sum_{j=0}^{d/2}s_{ij}x_j=0,\quad i=1,\cdots,d/2-1 \tag{12}$$

如果上述错误位置有理函数 $\sigma(x,y,z)=\sum_{i=0}^{d/2}y_ih_i$, 则可证明 $(y_0,\cdots,y_{d/2})$ 是方程组(12)式的解. 这是因为

$$\sum_{j=0}^{d/2}s_{ij}y_j=\sum_{j=0}^{d/2}S(r,k_ih_j)y_j=\sum_{j=0}^{d/2}S(e,k_ih_j)y_j \tag{13}$$

故

$$\sum_{j=0}^{d/2}s_{ij}y_j=\sum_{j=0}^{d/2}\left(\sum_{s=1}^{n}e_sk_i(P_s)h_j(P_s)\right)y_j=\sum_{s=1}^{n}e_sk_i(P_s)\left(\sum_{j=0}^{d/2}y_jh_j\right)(P_s)$$

故

$$\sum_{j=0}^{d/2}s_{ij}y_j=\sum_{s=1}^{n}e_sk_i(P_s)\sigma(P_s),\quad i=1,\cdots,d/2-1 \tag{14}$$

从而

$$\sum_{j=0}^{d/2}s_{ij}y_j=0$$

反之, 若 $(y_0,\cdots,y_{d/2})$ 是方程组(12)式的解, 则由(14)式, 设 $E_1,\cdots,E_t$ 为错误位置, 此时 $(\cdots,e_{i_1}\sigma(E_1),\cdots,e_{i_t}\sigma(E_t),0,\cdots)$ 构成 AG 码 $H_{D'}$ 的一个码字, 由于 $d(H_{D'})\geqslant d/2$, 再由 $W(e)<d/2$, 因而 $\sigma(E_1)=\cdots=\sigma(E_t)=0$, 即 σ 是错误位置有理函数. 此算法类似于 Peterson 算法.[5]

上述算法可推广到其它代数几何码的译码, 其主要思想是用"较小"的码字来代替错位有理函数. 上述 BCH 码的纠错能力很清楚,就是 $[(d-1)/2]$.

下面给出 Justesen 码的译码.

如文献[1]中那样, 先设有理点集 P 中的点形为 $(1,\alpha,\beta)$, 设 $f_0=x^j\in V_j$, f_0 与 C 的交点作成的除子为 D, 则 $\mathrm{supp}(D)\cap P=\varnothing$, 且 $\deg(D)=mj$. 显然 $\Phi=\{y^{i_1+i_2}/x^{i_1+i_2}\,|\,i_1+i_2\leqslant j\}$ 是 $L(D)$ 的生成元集. 由于

$$l(D)=\deg D-g+1=mj-(m-1)(m-2)/2+1$$

$$-\binom{j+2}{2}-\binom{j-m+2}{2}$$

故 $\Phi(\mathrm{mod}C)$ 构成 $L(D)$ 的基.

设 $0<j'<j$, $0<j''<j$, 且 $j'+j''=j$. 令 $K=V_{j'}$, $H=V_{j''}$ 各自定义出 JAG 码 $H_{j'}$, $H_{j''}$. 如同(11),(12)式定义 s_{ij} 和方程组

$$\sum_{i=1}^{k} s_{ij}x_i=0,\quad j=1,\cdots,h \tag{15}$$

称矩阵 $S=(s_{ij})$ 是伴随式矩阵. 设 a 是最小的 j' 使方程组(15)式有非零解. 显然 $a\leqslant[j/2]+1$.

引理 2 设 $j''\geqslant m-3$, $E_1,\cdots,E_s$ 为错误位置, 且 $s\leqslant j''m-2g+2$, 若 $(y_1,\cdots,y_k)$ 是(15)式的解, 则 $g_y=\sum_{i=1}^{k} y_ik_i$ 是错误位置多项式, 即 $g_y(E_i)=0$, $i=1,\cdots,s$.

引理 3 若 $m(j''-j')<g$, 则 $V_{j'}$ 中必有 $g_y\neq 0$, 使 $g_y(E_i)=0, i=1,\cdots,s$, 其中 $s<j''m-2g+2$.

证明 设 D' 是由 $x^{j'}$ 与 C 的交点作成的除子, 则 $\forall f\in V_{j'}$. 若 $f(E_i)=0$, $i=1,\cdots,s$, 当且仅当 $f\in L\left(D'-\sum_{i=1}^{s}E_i\right)$, 由 Riemann-Roch 定理, $l\left(D'-\sum_{i=1}^{s}E_i\right)\geqslant \deg D'-s-g+1=mj'-g+1-s\geqslant mj'-g+1-(mj''-2g+1)=g-m\times(j''-j')>0$, 故存在 $g_y\neq 0$, 使 $g_y\in L\left(D'-\sum_{i=1}^{s}E_i\right)$.

引理 3 解决了存在性问题.

引理 4 若 $g_y\in V_{j'}$, 且 $g_y\neq 0$, 使 $g_y(E_i)=0, i=1,\cdots,s$, 令 $g_y=y_1k_1+\cdots+y_kk_k$, 则 $(y_1,\cdots,y_k)$ 是(15)式的非零解.

引理 5 设 $j=j'+j''$, 且 $j''\geqslant m-2$, $g_y\in V_{j'}$, 且 g_y 不是 C 的倍数, 则 g_y 在 C 上的交点数 $u<d(H_j)$.

证明 由 Bezout 定理 $u\leqslant mj'=mj-mj''=mj-2g+2-(mj''-2g+2)\leqslant d(H_j)-(mj''-2g+2)<d(H_j)$.

综合引理 2,3,4,5 我们得到如下对 JAG 码的译码算法. 取 $j=j'+j''$, 使 $j''-j'<g/m$.

第 1 步 求伴随式 $S(e,f)$, $f\in V_j$.

第 2 步 根据矩阵 $S=(s_{ij})$ 相对于 k_ih_j 的排序, 将第 1 步中求出的伴随式填入 S.

第 3 步 求方程组 $S\cdot X=0$ 的解 $(y_1,\cdots,y_k)$, 求得 $g_y=y_1k_1+\cdots+y_kk_k$.

第 4 步 将有理点集 P 中的点逐一代入 g_y, 求出错误位置 $E_1,\cdots,E_s$.

第 5 步 求方程组 $\sum_{i=1}^{s} e_if(E_i)=S(e,f)$, $f\in V_j$, 得到唯一的解 $e_1,e_2,\cdots,e_s$.

引理 6 用上述算法, 当 m 为奇数时, 可纠 $(d-g+1)/2-m/2$ 个错, 当 m 为偶数

时，可纠 $(d-g+1)/2-3m/4$ 个错．这里 d 为 H_j 的设计码距，即 $d=mj-2g+2$．

证明　取 $i''=[(j+(m-3)/2)/2]$，则 $(j''-j')m=(2[(j+(m-3)/2)/2]-j)m=(m-3)m/2-2\Delta m<g$．这里 $0\leqslant\Delta<1$，实际上 $\Delta=0$，$1/4$，$2/4$ 或 $3/4$，因此 $mj''-2g+2=(d-g+1)/2-\Delta m\geqslant(d-g+1)/2-3m/4$．

为提高算法的纠错能力，要在 V_j 中保证存在错位多项式的前题下减小 i'，增大 j''，使得 $mj''-2g+2$ 尽可能地接近 $d/2$．比较引理 3，我们提出一个猜想．

猜想　设 $j=i'+j''$，m 是平面曲线 $\boldsymbol{C}$ 的次数，$E_1,\cdots,E_s$ 是 $\boldsymbol{C}$ 上任意 s 个有理点，$s\leqslant(mj-2g+2-m)/2$，若 $m(j''-i')<2g$，则 $V_{j'}$ 中有 $g_y\neq0$，使 $g_y(E_i)=0$，$i=1,\cdots,s$．

如果此猜想成立，则我们的算法的纠错能力可达到 $[(d-m)/2]$ 个错．因为这时可取 $j''=[(m-3+j)/2]$．而当 $(m-3+j)/2$ 是整数时，纠错能力可达到 $[(d-1)/2]$．

例 4　设 $F=GF(8)$，$\boldsymbol{C}$：$x^3y+y^3z+z^3x=0$，故 $g=3$ 则根据 J. P. Serre 上界，$n=24$，有 24 个有理点：

$$Q_1=(1,0,0),\quad Q_2=(0,1,0),\quad Q_3=(0,0,1),\quad Q_4=(1,1,\alpha),$$
$$Q_5=(1,1,\alpha^2),\quad Q_6=(1,1,\alpha^4),\quad Q_7=(1,\alpha,\alpha^4),\quad Q_8=(1,\alpha,\alpha^5),$$
$$Q_9=(1,\alpha,1),\quad Q_{10}=(1,\alpha^2,1),\quad Q_{11}=(1,\alpha^2,\alpha),\quad Q_{12}=(1,\alpha^2,\alpha^3),$$
$$Q_{13}=(1,\alpha^3,\alpha^3),\quad Q_{14}=(1,\alpha^3,\alpha^4),\quad Q_{15}=(1,\alpha^3,\alpha^6),\quad Q_{16}=(1,\alpha^4,\alpha^6),$$
$$Q_{17}=(1,\alpha^4,1),\quad Q_{18}=(1,\alpha^4,\alpha^2),\quad Q_{19}=(1,\alpha^3,\alpha^2),\quad Q_{20}=(1,\alpha^5,\alpha^3),$$
$$Q_{21}=(1,\alpha^5,\alpha^5),\quad Q_{22}=(1,\alpha^6,\alpha^5),\quad Q_{23}=(1,\alpha^6,\alpha^6),\quad Q_{24}=(1,\alpha^6,\alpha).$$

其中 α 是 F 中的本原元，x^3+x+1 为 α 的极小多项式．

设 $j=3$，则 H_j 的码距 $d\geqslant mj-2g+2=8$．实际上 H_j 是一个 $(24,14,8)$ 线性码，详见文献[1]．令 $j'=1$，$i''=2\geqslant m-2$，$m(j''-i')=4<2g=6$．当出错个数 $s\leqslant mj-2g+2-m=2$ 时，设 $r=(0,a,0,a^2,0,\cdots,0)$ 是收到的码。$H=\{x^2,xy,xz,y^2,yz,z^2\}$，$K=\{x,y,z\}$．

$$\text{位置矩阵}=\begin{bmatrix}x^3&x^2y&x^2z\\x^2y&xy^2&xyz\\x^2z&xyz&xz^2\\xy^2&y^3&zy^2\\xyz&y^2z&yz^2\\xz^2&yz^2&z^3\end{bmatrix},\quad\text{故伴随矩阵 }S=\begin{bmatrix}\alpha^2&\alpha^2&\alpha^3\\\alpha^2&\alpha^2&\alpha^3\\\alpha^3&\alpha^3&\alpha^4\\\alpha^2&\alpha^2+\alpha&\alpha^3\\\alpha^3&\alpha^3&\alpha^4\\\alpha^4&\alpha^4&\alpha^5\end{bmatrix}$$

求出方程的一组解为 $y_1=\alpha$，$y_2=0$，$y_3=1$，故 $g_y=\alpha x+z$，求得 $E_1=Q_2$，$E_2=Q_4$，$E_3=Q_{11}$，$E_4=Q_{24}$，再求解方程组

$$s(e,x^3)=0\cdot e_1+\alpha e_2+\alpha^3e_3+e_4=\alpha^3$$
$$s(e,y^3)=e_1+e_2+\alpha^6e_3+\alpha^4e_4=\alpha+\alpha^2$$

$$s(e,x^2y)=0\circ e_1+e_2+\alpha^2e_3+\alpha^6e_4=\alpha^2$$

$$s(e,z^3)=0\cdot e_1+\alpha^3e_2+\alpha^3e_3+\alpha^3e_4=\alpha^5$$

求得 $e_1=\alpha$, $e_2=\alpha^2$, $e_3=e_4=0$ 故译成的码 $c=r-e=0$.

上例中不满足引理 3, 但满足猜想条件.

例 5 接上例,令 $j=4$, $r=(0,a,0,a^2,0,\cdots,0)$, 令 $j'=2$, $j''=2$,则 $(j''-j')m=0<3$, 故 $K=H=V_2=\{x^2,xy,y^2,xz,yz,z^2\}$ 中存在错位多项式, 对应的伴随矩阵是:

$$S=\begin{bmatrix} a^2 & a^2 & a^2 & a^3 & a^3 & a^4 \\ a^2 & a^2 & a^2 & a^3 & a^3 & a^4 \\ a^2 & a^2 & a^4 & a^3 & a^3 & a^4 \\ a^3 & a^3 & a^3 & a^4 & a^4 & a^5 \\ a^3 & a^3 & a^3 & a^4 & a^4 & a^5 \\ a^4 & a^4 & a^4 & a^5 & a^5 & a^6 \end{bmatrix}$$

求出 $\{x^2+xy,\ ax^2+xz,\ ax^2+yz,\ a^2x^2+z^2\}$ 是错位多项式理想的生成元集,求公共根得 Q_2,Q_4 为全部两个解.

参 考 文 献

[1] J. Justesen et al., *IEEE Trans. on IT* **IT-35**(1989)4, 811—821.

[2] A. N. Skorobogatov, S. G. Vladut, *IEEE Trans. on IT*, **IT-36**(1990)5, 1051—1060.

[3] S. Iitaka, Algebraic Geometry, New York: Springer-Verlag, (1982), pp. 185—187.

[4] R. Blahut, Theory and Practice of Error Control Codes, MA: Addison-Wesley, (1983), pp. 180—200.

ON JUSTESEN'S ALGEBRAIC GEOMETRY CODES

Lu Peizhong Song Guowen

(Chengdu Research Institute of Telecommunication Techniques, Chengdu 610051)

Abstract An isomorphism preserving Hamming weight between two algebraic geometry (AG) codes is presented to obtain the main parameters of Justesen's algebraic geometry (JAG) codes. To deduce a simple approach to the decoding algorithm, a code word in a "small" JAG code is used to correspond to error-locator polynomial. By this means, a simple decoding procedure and the ability of error correcting are explored obviously. The low and up bounds of the dimension of AG codes are also obtained.

Key words Algebraic geometry codes; Error-locator polynomial, Syndrome matrix; Riemann-Roch theorem