从多项式理想的观点译 Goppa 码 [1]

岳殿武 胡正名*

(南京邮电学院电信工程系 南京 210003)
*(北京邮电大学信息工程系 北京 100088)

摘 要 从多项式理想的观点出发，本文给出了译 Goppa 码新的方法，该方法能纠正 $t=\lfloor (d-1)/2 \rfloor$ 个错误，其中 d 是 Goppa 码的真正最小距离。

关键词 Goppa 码，译码，理想论，Gröbner 基

中图号 TN911.22

1 引 言

从多项式理想的观点来译线性码的思想最初是由 A. Brinton Cooper Ⅲ [1](1990) 提出来的。在文献 [1] 中，他给出了用 Gröbner 基来译 BCH 码的代数方法。Xuemin Chen 等人随后 (1994) 将文献 [1] 的思想方法系统地推广到循环码上去，并且他们所得到的译码方法能纠错误数达到最好情况，即能纠 $t=\lfloor (d-1)/2 \rfloor$ 个随机错误，其中 d 是循环码的真正最小距离 [2,3]。利用 Xuemin Chen 等人的思想方法，本文得到了译 Goppa 码统一的代数方法，该方法纠错能力也能达到最好情况。

下面将给出 Goppa 码基本概念和基本性质 [4]。

记 $K=\mathrm{GF}(q^m)$。令 $L=\{\alpha_1,\alpha_2,\ldots,\alpha_n\}\subset K$。再令 $G(z)$ 是 K 上的一个多项式满足：$G(z)\neq 0$，当 $z=\alpha_i, i=1,2,\cdots,n$; $\deg(G(z))=r\leq n$。那么 Goppa 码 $\Gamma(L,G)$ 就是满足下式的 $\mathrm{GF}(q)$ 上的 n 元向量 $a=(a_1,a_2,\cdots,a_n)$ 全体：

$$\sum_{i=1}^{n}\frac{a_i}{(z-\alpha_i)}\equiv 0 \bmod (G(z)). \tag{1}$$

Goppa 码 $\Gamma(L,G)$ 的校验矩阵 H 为

$$H=\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \cdots & \alpha_n^{r-1} \end{bmatrix}\cdot\begin{bmatrix} G(\alpha_1)^{-1} & & & \\ & G(\alpha_2)^{-1} & & \\ & & \ddots & \\ & & & G(\alpha_n)^{-1} \end{bmatrix}. \tag{2}$$

设 $a=(a_1,\cdots,a_n)$ 是通过有扰信道发送的码字，$v=(v_1,\cdots,v_n)$ 是接收向量。设产生错误向量为 $e=(e_1,\cdots,e_n)$，则有 $v=a+e$。令发生错误位置为 $i_1,i_2,\cdots,i_w$，错值分别为 $Y_1,Y_2,\cdots,Y_w$。记 $X_j=\alpha_{i_j}, j=1,2,\cdots,w.$。因为 $Ha^T=0$，故校验子 S_j 为

$$S_j=\sum_{i=1}^{n}\frac{v_i\alpha_i^j}{G(\alpha_i)}=\sum_{i=1}^{w}\frac{Y_iX_i^j}{G(X_i)},\qquad j=0,1,\cdots,r-1. \tag{3}$$

[1] 1995-03-13 收到，1995-06-30 定稿
国家自然科学基金和国家杰出青年基金资助课题

显然，若 $w \le t = \lfloor (d-1)/2 \rfloor$，则校验子 S_j 是唯一确定的。

2 译 Goppa 码的新方法

定义位置多项式 $L(z)$ 如下：

$$L(z) = \prod_{i=1}^{w}(z - X_i) = z^w + \sum_{i=1}^{w} \sigma_i z^{w-i}. \tag{4}$$

再定义幂和函数 S_i 为

$$S_i = \sum_{j=1}^{w} \frac{Y_j X_j^i}{G(X_j)}, \qquad i = 0, 1, \cdots, q^m - 2. \tag{5}$$

定理 1　$S_i + \sum_{j=1}^{w} \sigma_j S_{i-j} = 0,\ w \le i < q^m - 1.$

证明　在 (4) 式中以 X_j 代替 z，则有

$$X_j^w + \sum_{b=1}^{w} \sigma_b X_j^{w-b} = 0. \tag{6}$$

对 (6) 式两边乘上 $\frac{Y_j X_j^{i-w}}{G(X_j)}$，再对 $j = 1, 2, \cdots, w$ 取和，则有

$$\sum_{j=1}^{w} \frac{Y_j X_j^i}{G(X_j)} + \sum_{b=1}^{w} \sigma_b \sum_{j=1}^{w} \frac{Y_j X_j^{i-b}}{G(X_j)} = 0, \tag{7}$$

即 $S_i + \sum_{j=1}^{w} \sigma_j S_{i-j} = 0,\ w \le i < q^m - 1$ 成立。　　证毕

设 Goppa 的维数为 k，则 $d \le n - k + 1$。故若 $w \le t$，便有 $2w \le n - k$ 成立。那么此时由文献 [5] 中讨论可知只由下面 (8) 式便可唯一确定位置多项式 $L(z)$。这样做可以减少译码的复杂度 [2]。

$$S_i + \sum_{j=1}^{w} \sigma_j S_{i-j} = 0, \qquad w \le i < n - k. \tag{8}$$

令 A 表示 K 的分圆陪集首集，即分圆陪集代表集，再令 $R = \{r, r+1, \cdots, n-k\} \bigcap A = \{r_1, r_2, \cdots, r_l\}$。关于分圆陪集首集 A 的特性和求法参见文献 [6,7]，关于 $n-k$ 上限求法可参见文献 [7]，这里不一一叙述。下面我们定义校验多项式 F，F 由如下几个多项式组成：

$$f_i = S_i + \sum_{j=1}^{w} \sigma_j S_{i-j}, \qquad w \le i < n - k; \tag{9}$$

$$h_j = \sigma_j^{q^m} - \sigma_j, \qquad 1 \le j \le w; \tag{10}$$

$$l_{r_j} = S_{r_j}^{q^m} - S_{r_j}, \qquad 1 \le j \le l. \tag{11}$$

用 $K[\sigma_1, \sigma_2, \cdots, \sigma_w; S_{r_1}, S_{r_2}, \cdots, S_{r_l}]$ 表示定义在 K 上的多变量多项式环。显然，$F \subset K[\sigma_1, \sigma_2, \cdots, \sigma_w; S_{r_1}, S_{r_2}, \cdots, S_{r_l}]$。令 $V(F)$ 表示 F 在代数闭包 $\overline{K}$ 上的公共根集合。如果以 $I(F)$ 表示由 F 产生的理想，那么显然有 $V(I(F)) = V(F)$ 成立。如果 $w \le t$，则 $0 < |V(F)| < \infty$。

为了求出位置多项式 $L(z)$，我们还需要定义 Σ_j ， $j=1,2,\cdots,w$, 作为 F 根的第 j 个分量全体组成的集合。令 $z=(\sigma_1^*,\cdots,\sigma_w^*;S_{r_1}^*,\cdots,S_{r_l}^*)\in V(F)$，则对于 j 有 $(1\le j\le w)$

$$\Sigma_j=\{\sigma_j^*|(\sigma_1^*,\cdots,\sigma_w^*;S_{r_1}^*,\cdots,S_{r_l}^*)\in V(F)\}. \tag{12}$$

引理 1 [8] 令 E 是 $K[\sigma_1,\sigma_2,\cdots,\sigma_w;S_{r_1},S_{r_2},\cdots,S_{r_l}]$ 的一个理想，f 是 $K[\sigma_1,\cdots,\sigma_w;S_{r_1},\cdots,S_{r_l}]$ 一个多项式。如果对任意 $z=(\sigma_1^*,\cdots,\sigma_w^*;S_{r_1}^*,\cdots,S_{r_l}^*)\in V(E)$ (E 在 $\overline{K}$ 上的公共根集合)，均有 $f(z)=0$ 成立，那么存在一个正整数 h 使得 $f^h\in E$ 。

运用引理 1 和定理 1，用类似于文献 [3] 中定理 4 证明方法可得如下译码定理。

定理 2 令 $K[\sigma_j]$ 表示 K 上关于变量 σ_j 的多项式环，那么 $I(F)\bigcap K[\sigma_j]$ 是 $K[\sigma_j]$ 中一个主理想。设 $g_j(\sigma_j)$ 表示 $I(F)\bigcap K[\sigma_j]$ 生成首一多项式，则

$$g_j(\sigma_j)=\sigma_j-\sigma_j^*, \tag{13}$$

其中 σ_j^* 是位置多项式 $L(z)=z^w+\sum_{j=1}^{w}\sigma_j z^{w-j}$ 的系数，这里要求 $w\le t=\lfloor(d-1)/2\rfloor$ 。

定理 2 告诉我们， $L(z)$ 可通过求得主理想 $I(F)\bigcap K[\sigma_j]$, $j=1,2,\cdots,w$ 的生成多项式而得到。而由文献 [2,9] 可知：对于多项式环 $K[\sigma_j]$ 上一个多项式理想的首一生成多项式可通过生成其 Gröbner 基来产生。Gröbner 基理论是计算代数中重要内容，有广泛的应用范围. 关于 Gröbner 基详细讨论参见文献 [10] 。

下面给出译 Goppa 码的新算法。

第一步 计算校验子 S_i, $i=0,1,2,\cdots,r-1$ 。如果 S_i 全为 0，则终止运行。此时是 $e=0$ 情况。否则，令 $w_b=1$，进行第二步。

第二步 令 $h=1$，再令校验多项式集 F 为 $F=\{S_i+\sum_{j=1}^{w_b}\sigma_j S_{i-j}|w_b\le i<n-k\}\bigcup\{\sigma_j^{q^m}-\sigma_j|1\le j\le w_b\}\bigcup\{S_{r_j}^{q^m}-S_{r_j}|r_j\in R\}$

第三步 定义变量 $\sigma_1,\cdots,\sigma_{w_b};S_{r_1},\cdots,S_{r_l}$ 次序为 $\sigma_h<\sigma_1<\cdots<\sigma_{h-1}<\sigma_{h+1}<\cdots<\sigma_{w_b}<S_{r_1}<\cdots<S_{r_l}$ 。求出此次序下的标准 Gröbner 基 G_h 。如果 $1\in G_h$，令 $w_b=w_b+1$ 并退回到第二步。否则，继续进行第四步。

第四步 求出 $G_h\bigcap K[\sigma_h]$ 公共根集合 V_h 。如果 $|V_h|>1$，则终止运行。否则，进行第五步。

第五步 令 $h=h+1$ 。如果 $h\le w_b$，退回到第三步。否则继续进行第六步。

第六步 令 $V_j=\{\sigma_j^*\}$, $j=1,2,\cdots,w_b$ 。求出位置多项式 $L(z)=z^{w_b}+\sum_{j=1}^{w_b}\sigma_j z^{w_b-j}$ 非零根。这可通过 Chien 搜索来完成。再用文献 [4] 第 386 页公式求出错值 Y_j, $j=1,2,\cdots,w_b$ 。

注意： (1) 如果 $1\in G_h$，则 $V(F)=\phi$ [2] 。

(2) 如果 $|V_h|>1$，则 $w_b>t=\lfloor(d-1)/2\rfloor$ 。

(3) 记 $I(G_h)$ 表示 G_h 生成的理想，则有 $I(G_h)=I(F)$ 。

很明显，上述译码算法纠错能力非常好，可以达到 $t=\lfloor(d-1)/2\rfloor$ 。而且对于某些 $w>t$ 个错误也可能正确纠正。此外，本文所给出的译码方法容易推广到 Alternant 码上去，也可以推广到广义 Goppa 码上去 [11] 。

篇幅所限，下面只简述一个例子来说明译码的新方法。

例 1　取 L=GF$(2^3)=\{0,1,\alpha,\cdots,\alpha^6\}$，$\alpha$ 是 GF(2^3) 的本原元。再取 $G(z)=z^2+z+1$，这是一个 [8,2,5] Goppa 码 [4]，其校验矩阵为

$$H=\begin{bmatrix} 1 & 1 & \alpha^2 & \alpha^4 & \alpha^2 & \alpha & \alpha & \alpha^4 \\ 0 & 1 & \alpha^3 & \alpha^6 & \alpha^5 & \alpha^5 & \alpha^6 & \alpha^3 \end{bmatrix} \tag{14}$$

设发射码字为 $a=(0,0,0,0,0,0,0,0)$，接收码字为 $v=(0,0,0,0,0,1,1,0)$。译码过程是：计算校验子 $S_0=0, S_1=\alpha^5+\alpha^6\neq 0$。取 $w_b=1$，则此时，$S_1+\sigma_1 S_0=S_1\neq 0$，故 $1\in G_N$。令 $w_b=2$，则此时，$V_1=\{\alpha^5+\alpha^4\}, V_2=\{\alpha^2\}$，求 $L(z)=z^2+(\alpha^5+\alpha^4)z+\alpha^2$ 根得 $X_1=\alpha^4, X_2=\alpha^5$。因此 $a=(0,0,0,0,0,1,1,0)+(0,0,0,0,0,1,1,0)=(0,0,0,0,0,0,0,0)$。

参 考 文 献

[1] Brinton Cooper III A. Direct solution of BCH decoding equations, Communication, Control and Signal Processing. Amsterdam, The Netherland: Elsevier Science Publishers, 1990, 281–286.

[2] Chen X, *et al.* Use of Gröbner bases to decode binary cyclic codes up to the true minimum distance. IEEE Trans. on IT., 1994, IT-40(5): 1654–1660.

[3] Chen X, *et al.* General principles for the algebraic decoding of cyclic codes. IEEE Trans. on IT , 1994, IT-40(5): 1661–1663.

[4] MacWilliams F J, Sloane N J A. The theory of error-correcting codes, Amsterdam: North Holland Pubishers, 1977.

[5] Massey J L. Shift-register synthesis and BCH decoding. IEEE Trans. on IT., 1969, IT-15(1): 122–127.

[6] 岳殿武. 求分圆陪集首元的新算法. 通信保密, 1995, 16(1): 28–32.

[7] 岳殿武. 循环陪集结构及其应用. 系统科学与数学, 1992, 12(1): 15–20.

[8] Lang S. Algebra, 2nd ed. Menlo Park, CA: Addison-Wesley, 1984, 375.

[9] Buchberger B. Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory, Multidimensional Systems Theory. Dordrecht: Reidel, 1985, 185–232.

[10] Becker T. Gröbner Bases. NewYork: Springer-Verlag, 1993.

[11] 冯贵良，曾开明. 广义 Goppa 码最小距离下限的扩张及其译码，中国科学, 1983, 12(8): 745–755.

ALGEBRAIC DECODING OF GOPPA CODES FROM A POLYNOMIAL IDEAL POINT OF VIEW

Yue Dianwu　　Hu Zhengming*

(*Nanjing University of Posts and Telecommunications, Nanjing* 210003)

*(*Beijing University of Posts and Telecommunications, Beijing* 100088)

Abstract　From a polynomial ideal point of view, a general algebraic method for decoding Goppa codes is presented. It is shown that such a method can correct $t=\lfloor (d-1)/2 \rfloor$ errors, where d is the true minimum distance of the given Goppa code.

Key words　Goppa code, Decoding, Ideal theory, Gröbner base

岳殿武：　男，1965 年生，博士，从事编码与密码研究工作.

胡正名：　男，1931 年生，教授，博士生导师，从事应用数学与信息科学的教学与科研工作.