代数几何码译码算法纵览

李 宝,冯登国,卿斯汉
(中国科学院软件研究所,信息安全国家重点实验室,北京 100080)

摘 要: 本文重点考察了代数几何码译码算法的两个典型代表——Ehrhard 译码算法和大数表决方案. 描述了译码算法从 Reed-Solomon 码、Goppa 码到代数几何码译码算法的两条不同发展途径.

关键词: 代数几何码; 译码; 算法; 大数表决
中图分类号: TN911.22 **文献标识码**: A **文章编号**: 0372-2112 (2001) 01-0110-08

A Survey on Decoding Algorithms of Algebraic-Geometric Codes

LI Bao, FENG Deng-guo, QING Si-han
(Institute of Software, State Key Lab. of Information Security, Chinese Academy of Sciences, Beijing 100080, China)

Abstract: Two representatives are discussed primarily of decoding algorithms of algebraic-geometric codes. Two different approaches to decoding algorithms of algebraic-geometric codes are presented here evolving from decoding algorithms of Reed-Solomon codes and Goppa codes.

Key words: algebraic-geometric code; decoding; algorithm; majority voting

1 引言

编码理论主要研究三个问题: (1) 最佳编码能有多好; (2) 如何构造好码; (3) 如何译码. 关于问题 (1) 已经给出了各种上下界,其中一个重要的界是 Gilbert-Varshamov 界. 构造达到或超过 Gilbert-Varshamov 界的纠错码就成为问题 (2) 的重要课题. 70 年代, Goppa[1] 首先使用有限域上的代数曲线来构造码. 80 年代初, Tsfasman、Vlădut 和 Zink[2] 将 Goppa 的思想与代数几何中的深刻结果相结合,构造出一系列纠错码,使其信息率超过 Gilbert-Varshamov 界. 代数几何码即指这些利用有限域上的代数曲线构造的线性分组码. 问题 (3) 就是针对构造出的码,给出有效的译码算法. 这也是本文关心的问题. 1989 年, Justesen、Larsen、Elbrønd Jensen、Havemose 及 Høholdt 首先将 Arimoto 和 Peterson 对 RS 码的译码算法进行推广,对平面曲线上的代数几何码给出了一个译码算法[3]. 1990 年, Skorobogatov 和 Vlădut[4] 又将其推广到任意代数曲线上. 这样就有了所谓基本译码算法和改进译码算法[4,5].

1992 年, Porter、Shen 和 Pellikaan[6] 以及 Ehrhard[7] 给出一个运用子结式序列的译码算法,这个算法与改进译码算法等价.

突破始于 1993 年,在这一年 Ehrhard[8]、Feng 和 Rao[9] 都给出了纠错能力达到 $\lfloor (d-1)/2 \rfloor$ 个错误的译码算法.

还有相当多的文献讨论代数几何码译码算法的各种改进和推广. 我们认为 Ehrhard 的译码算法和 Feng、Rao 的大数表决方案是代数几何码译码算法的典型代表,纠错能力的突破始于它们,最具本质意义. 从历史的角度看,这两个算法解决问题的不同方式还代表了代数编码译码算法的两条主要发展途径: 一条是从校验矩阵的角度出发,将校验矩阵进行适当的扩充(添加新行),使其中的某些行能组成一可逆阵,并确定足够多的错误向量的伴随式,从而纠正错误,得到正确的码字; 另一条是首先试图确定错误向量的错误位置多项式(函数),从而确定错误向量的值.

我们认为这两种途径代表了代数编码译码算法成长、发展、推广的历程. 本文描述了译码算法的这两条发展途径,提供了一种平行的对比,希望能在众多的译码算法中给出参照系,对理清思路有所帮助.

2 预备知识

代数几何码的研究涉及到代数曲线中一些较深入的知识,在此只能罗列出本文中涉及的代数几何以及与线性分组码的译码有关的一些基本概念. 有兴趣的读者可参看文[11~17,22].

2.1 代数几何基本概念

设 q 是 p 的素数幂, F_q 是有 q 个元素的域, $\bar{F}_q$ 是 F_q 的代数闭包, P_n 是 F_q 上 n 维射影空间. 一条定义在 F_q 上的光滑射影曲线 χ 是指一组齐次多项式 $f_1, \cdots, f_r \in F_q[X_0, \cdots, X_n]$ 的公共零点集且满足对所有 $P \in \chi$, 矩阵

$$D_P := \left(\frac{\partial f_\rho}{\partial X_\upsilon}(P) \right)_{\substack{0 \le \upsilon \le n \\ 1 \le \rho \le r}}$$

的秩为 $n-1$. 以后我们简称光滑曲线为曲线. 我们总假设曲

收稿日期: 1999-10-28; 修回日期: 2000-07-02
基金项目: 国家 973 项目基金 (No. G1999035802); 甘肃省中青年科技基金 (No. YS981-A25-001)

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

线 χ 是不可约的,即 χ 不是两条不同曲线的并.

具有相同次数的齐次多项式 $f, g \in \overline{F}_q[X_0, \cdots, X_n]$ 的商 f/g 称为 χ 上的有理函数,如果 g 在 χ 上不恒等于零. 用 $F_q(\chi)$ 表示系数在 F_q 中的有理函数域. 定义 χ 上的微分形式集合 $\Omega(\chi)$ 为由符号 $\{dg\}_{g \in \overline{F}_q(\chi)}$ 关于关系

$$d(fg) = fdg + gdf,\ d(f+g) = df + dg,\ da = 0,\ \forall a \in \overline{F}_q$$

生成的 $\overline{F}_q(\chi)$ ——线性空间.

设 $P \in \chi$,考虑有理函数 $f = g/h$, $h(P) \neq 0$ 组成的环 R_P. 极大理想 $\{f \in R_p \mid f(P) = 0\} \subset R_P$ 的生成元称为 χ 在 P 的局部参量. 若 t_P 为 χ 在 p 的局部参量对任有理函数 $f \neq 0$,使得 $f/t_P^n \in R_P$ 的最大整数 n 为 f 在 P 的阶,记为 $v_P(f)$. 对微分形式 $0 \neq \omega = fdt_P$,定义 $v_P(\omega) = v_P(f)$. 对任意 $v_P(f) \geq m$ 的有理函数 $f \in F_q(\chi)$,都存在序列 $a_i \in F_q$, $i \geq m$,使得

$$v_P\left(f - \sum_{i=m}^{n} a_i t_P^i\right) \geq n+1.$$

$f = \sum_{i=m}^{\infty} a_i t_P^i$ 称为 f 在 P 的局部幂级数. $\eta = \sum_{i=m}^{\infty} a_i t_P^i dt_P$ 称为 $\eta = fdt_P$ 的局部幂级数, $\mathrm{Re}s_P\eta := a_{-1}$ 称为 η 在 P 的留数. 如果 $v_P(\eta) \geq -1$, $v_P(f) \geq 0$,则

$$\mathrm{Re}s_P(f\eta) = f(P)\,\mathrm{Re}s_P\eta$$

除子 D 定义为形式和 $D = \sum n_P P$,其中 $n_P \in Z$ 且 n_P 只对有限多个 $P \in \chi$ 不为零. 集 $\mathrm{sup}\,p(D) = \{P \in \chi \mid n_P \neq 0\}$ 称为除子 D 的支集. D 的次数定义为 $\deg D = \sum n_P$.

对 $f \in F_q(\chi)$, $(f) := \sum v_P(f)\,P$ 称为主除子. 对 $\omega \in \Omega(\chi)$, $(\omega) := \sum v_P(\omega)\,P$ 称为典范除子.

除子 $D = \sum n_P P$ 称为正的,记为 $D \geq 0$,如果对每个 $P \in \chi$, $n_P \geq 0$.

令　　$L(D) := \{f \in F_q(\chi) \mid (f) + D \geq 0\} \cup \{0\}$

$$\Omega(D) := \{\omega \in \Omega(\chi) \mid (\omega) \geq D\} \cup \{0\}.$$

则 $L(D)$ 和 $\Omega(D)$ 都是有限维 F_q ——向量空间,其维数分别记为 $l(D)$ 和 $i(D)$.

定理 2.1　(Riemann-Roch) 设 χ 为非奇异曲线. 则存在一个整数 $\gamma \geq 0$,称为 χ 的亏格,使得

$$l(D) = 1 + \deg D - \gamma + i(D).$$

定理 2.2　(留数公式) 对任 $\omega \in \Omega(\chi)$,

$$\sum_{P \in \chi} \mathrm{Re}s_P(\omega) = 0$$

2.2　译码问题

设 C 是 F_q^n 中一线性分组码,即 $C \subseteq F_q^n$ 是一个 F_q-线性空间. 称 F_q^n 中的元素为字,码 C 中的元素为码字. 两个字 $\mathrm{a} = (a_1, \cdots, a_n)$ 和 $\mathrm{b} = (b_1, \cdots, b_n)$ 的 Hamming 距离定义为

$$d(\mathrm{a}, \mathrm{b}) = |\{i \mid a_i \neq b_i\}|.$$

字 a 的 Hamming 重量定义为

$$wt(a) = |\{i \mid \mathrm{a}_i \neq 0\}|.$$

码 C 的最小距离定义为

$$d = d(C) = \min\{d(\mathrm{a}, \mathrm{b}) \mid \mathrm{a} \neq \mathrm{b}, \mathrm{a}, \mathrm{b} \in C\}$$

字 y 到码 C 的距离定义为

$$d(y, C) = \min\{d(y, c) \mid c \in C\}$$

若 c 是传送字,而 $y = c + e$ 是接收字,则称 e 为错误向量. 若 $d(y, C) = t'$,则存在码字 c 和错误向量 e 使得 $y = c' + e$ 且 $wt(e') = t'$. 若错误的个数不超过 $(d-1)/2$,即 $wt(e') \leq (d-1)/2$,则可断定 $c = c'$, $e = e'$. 即当 y 到码 C 的距离最多为 $(d-1)/2$ 时,离 y 最近的码字是唯一的.

若 A 是一个算法,它以一个对 (C, y) 作为输入,以 $A(C, y)$ 作为输出,其中 C 是一线性码, y 是一个长度与 C 的长度相同的字,则 A_C 是算法 A 在码 C 上的限制,即 A_C 以字 y 作为输入,而以 $A(C, y)$ 作为输出. 因此,译码过程可分为两部分:第一部分是预处理部分. 这是对一个适当的码 C,构作一个译码器 A_C. 这部分可以是耗时的. 第二部分是对每个接收到的字 y 进行译码,这一部分需要速度很快.

矩阵 H 称为码 C 的校验阵,如果 $C = \{c \in F_q^n \mid Hc^T = 0\}$,其中 c^T 为 c 的转置. 码 C 的对偶码定义为 $C^T = \{b \in F_q^n \mid bc^T = 0,\ \forall c \in C\}$

命题 2.3　设 H 是码 C 的校验阵. 假设有接收字 $y = c + e$,并已知一包含 y 的所有错误位置的集合 J,且 $|J| \leq d-1$. 则错误向量是下列方程的唯一解:

$$Hx^T = Hy^T \text{ 且 } x_j = 0,\ \forall j \notin J.$$

3　从 RS 码、Goppa 码到代数几何码

代数几何码是 Goppa 首先将 Goppa 码推广,利用有限域上的代数曲线构造的. 随后,从数学概念出发,代数几何码的定义方式可进一步扩展,从而得到几种不同的代数几何码. 利用 Riemann-Roch 定理和留数公式等揭示的概念间的深刻联系,可以得到这些代数几何码间的相互关系. 这使我们能用更统一的观点看待线性分组码理论. 从概念上可将 RS 码和 Goppa 码看作代数几何码的特例,从而将代数几何码看成 RS 码和 Goppa 码的推广.

3.1　代数几何码

给出一种代数几何码(广义 Reed-Solomon 码)的定义.

设 χ 为有限域 F_q 上亏格为 γ 的曲线, $P_1, \cdots, P_n$ 是 χ 上 n 个不同的有理点,用 D 记除子 $P_1 + \cdots + P_n$. 设 G 为一除子,其支集与 D 的支集无交. 作映射

$$Ev_D : L(G) \to F_q^n,\ f \mid \to (f(P_1), \cdots, f(P_n)).$$

这个映射是 F_q-线性的,且当 $\deg G < n$ 时为单射. 用 $C_L(D, G)$ 记这个映射的像.

定义 3.1　$C_L(D, G)$ 称为代数几何码或广义 Reed-Solomon 码. 它们的基本性质如下:

定理 3.1　$C_L(D, G)$ 是 $[n, k, d]$-码. 当 $\deg G < n$ 时,有

$$k \geq \deg G - \gamma + 1,\ d \geq n - \deg G.$$

此外,若 $\deg G > 2\gamma - 2$,则 $k = \deg G - \gamma + 1$

$C_L(D, G)$ 的 Goppa 设计距离定义为 $n - \deg G$,记为 d_γ.

下面给出另一种代数几何码(几何 Goppa 码)的定义.

作映射

$$\mathrm{Re}s_D : \Omega(G - D) \to F_q^n,\ \eta \mid \to (\mathrm{Re}s_{P_1}(\eta), \cdots, \mathrm{Re}s_{P_n}(\eta)).$$

这个映射是 F_q-线性的,且当 $\deg G > 2\gamma - 2$ 时为单射. 用 $C_\Omega(D, G)$ 记这个映射的像.

定义 3.2　$C_\Omega(D, G)$ 称为代数几何码或几何 Goppa 码.

它们有下面的基本性质:

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

定理 3.2 $C_\Omega(D, G)$ 是 $[n, k, d]$-码. 当 $\deg G > 2g - 2$ 时,有 $k \geq n - \deg G + g - 1$, $d \geq \deg G - 2g + 2$

此外,若 $\deg G < n$,则

$$k = n - \deg G + g - 1$$

$C_\Omega(D, G)$ 的 Goppa 设计距离定义为 $\deg G - 2g + 2$,也记为 d_T. 因 $\mathrm{Re}s_{P_i}(f\eta) = f(P_i)\mathrm{Re}s_{P_i}(\eta)$,留数公式就揭示出这两种代数几何码之间的联系.

定理 3.3 $C_L(D, G)$ 与 $C_\Omega(D, G)$ 互为对偶码.

对有理点 $P_1, \cdots, P_n$,总存在微分 ω 使得 $\mathrm{Re}s_{P_i}(\omega) = 1$, $i = 1, \cdots, n$,再加上事实 $L(G)$ 同构于 $\Omega((\omega) - G)$,就有

定理 3.4 $C_L(D, G) = C_\Omega(D, (\omega) + D - G)$.

这个事实表明仅考虑 $C_\Omega(D, G)$ 的译码算法不会失去一般性.

定义 3.3 形如 $C_L(D, mQ)$ 或 $C_\Omega(D, mQ)$ 码称为一点代数几何码,其中 Q 是不同于 $P_1, \cdots, P_n$ 的 χ 上的 F_q-有理点.

3.2 Reed-Solomon 码

Reed-Solomon 码可以看成最简单的代数曲线-直线上定义的代数几何码.

设 $\alpha = (\alpha_1, \cdots, \alpha_n)$ 为 F_q 的 n 个不同元素组成的有序组. k 维 Reed-Solomon 码定义为

$$RS_k(\alpha) = \{(f(\alpha_1), \cdots, f(\alpha_n)) \mid f \in F_q[\chi], \deg f < k\}.$$

设 $x = (x_1, \cdots, x_n)$ 为 F_q 的 n 个非零元素组成的有序组. 广义 k 维 Reed-Solomon 码定义为

$$GRS_k(\alpha, x) = \{(f(\alpha_1)x_1, \cdots, f(\alpha_n)x_n) \mid f \in F_{q^m}[\chi], \deg f < k\}$$

设 $g \in F_q[\chi]$使得 $g(\alpha_i) = x_i$, $i = 1, \cdots, n$. 设 $P_i = [\alpha_i, 1]$, $Q = [1, 0]$为射影直线的无穷远点. 设 $D = P_1 + \cdots + P_n$. 定义射影直线上的除子 $G = (k - 1)Q - (g)$. 则 $GRS_k(\alpha, x) = C_L(D, G)$. 所有广义 RS 码组成的集合恰是射影直线上的所有形如 $C_L(D, G)$ 的码组成的集合. 这也就是称曲线上形如 $C_L(D, G)$ 的码为广义 RS 码的原因.

3.3 Goppa 码

设 $L = \{\alpha_1, \cdots, \alpha_n\}$ 为 F_{q^m} 的 n 个不同元素组成的集合. 设 $g \in F_{q^m}[\chi]$使得 $g(\alpha_i) \neq 0$, $i = 1, \cdots, n$. 古典 Goppa 码 $\Gamma(L, g)$ 定义为

$$\Gamma(L, g) = \{c \in F_q^n \mid \sum \frac{c_i}{X - \alpha_i} \equiv 0 \bmod g(X)\}$$

设 P_i, Q, D 与上述 RS 码中的相同. 若取 E 为 g 的零点形成的除子,则 $\Gamma(L, g) = C_\Omega(D, E-Q)$,且

$$c \in \Gamma(L, g) \text{ 当且仅当 } \sum \frac{c_i}{X - \alpha_i} dX \in \Omega(E - Q - D).$$

这就是为什么有些作者将几何 Goppa 码的定义扩大到形如 $C_\Omega(D, E - Q)$ 的码的子域子码的原因.

$C_L(D, G)$ 与 $C_\Omega(D, G)$ 的对偶性可由这样的事实看出: Goppa 码 $\Gamma(L, g)$ 的校验阵等于广义 RS 码的生成阵

$$\begin{pmatrix} g(\alpha_1)^{-1} & \cdots & g(\alpha_1)^{-1} \\ \alpha_1 g(\alpha_1)^{-1} & \cdots & \alpha_n g(\alpha_1)^{-1} \\ \cdots & \cdots & \cdots \\ \alpha_1^{r-1} g(\alpha_1)^{-1} & \cdots & \alpha_n^{r-1} g(\alpha_1)^{-1} \end{pmatrix}$$

其中 r 是 Goppa 多项式 g 的次数.

4 从 Arimoto-Peterson 译码算法到 Ehrhard 译码算法

本节考察从 Arimoto-Peterson 译码算法到 Ehrhard 译码算法的发展途径:从 RS 码的 Arimoto-Peterson 译码算法、Goppa 码的译码算法到基本译码算法、Ehrhard 译码算法. 贯穿于这些算法中的基本思路是首先利用接收字的信息,得到错误位置函数(多项式),再利用这些信息得到错误值. 在这里,重点是找出错误位置函数(多项式).

假设 C 是码, d 是其设计距离. 设 $c = (c_1, \cdots, c_n)$ 是被传送的码字, $y = c + e$ 是接收到的字,其中 $e = (e_1, \cdots, e_n)$ 是错误向量.

4.1 Arimoto-Peterson 译码算法

因 Arimoto-Peterson 译码算法已推广到 BCH 码上,我们直接考察 BCH 码的译码算法.

设 C 是 BCH 码,译码过程可分为三步:

(1) 计算伴随式

设校验阵为

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \alpha^{d-1} & \alpha^{2(d-1)} & \cdots & \alpha^{(d-1)(n-1)} \end{pmatrix},$$

则 y 的伴随式为

$$S = (s_1, \cdots, s_n)^T = Hy^T = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \alpha^{d-1} & \alpha^{2(d-1)} & \cdots & \alpha^{(d-1)(n-1)} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \cdots \\ y_n \end{pmatrix}$$

(2) 找出错误位置多项式

设 e 的非零分量为 $e_{i_1}, \cdots, e_{i_w}$, $i_1, \cdots, i_w$ 即为 y 的错误位置. 令 $X_r = \alpha^{i_r}$, $r = 1, \cdots, w$. 错误位置多项式即为

$$\sigma(z) = \prod_{i=1}^{w}(1 - X_i z) = \sum_{i=0}^{w} \sigma_i z^i$$

因 σ_i 与伴随式 s_i 间可由 Newton 恒等式连接,所以由伴随式可计算出错误位置多项式.

(3) 确定错误值

首先找出错误位置多项式的零点. 然后令 $\omega(z) = \sigma(z) + \sum_{i=1}^{w} z X_i Y_i \prod_{\substack{j=1 \\ j \neq i}}^{w}(1 - X_j z)$,其中 $Y_r = e_{i_r}$,则 Y_i 可由 $\omega(z)$ 算出

$$Y_i = \omega(X_i^{-1}) / \prod_{j \neq i}(1 - X_j X_i^{-1}) = -X_i \omega(X_i^{-1}) / \sigma'(X_i^{-1}).$$

因 $\frac{\omega(z)}{\sigma(z)} = 1 + \sum_{i=1}^{w} \frac{z X_i Y_i}{1 - z X_i} = 1 + \sum_{i=1}^{w} Y_i \sum_{j=1}^{\infty} (z X_i)^j$

$= 1 + S(z)$,

故 $\omega(z) = (1 + S(z))\sigma(z)$,其中 $S(z) = \sum_{i=1}^{\infty} s_i z^i$,由于 $\deg \omega(z) \leq \deg \sigma(z)$,只须 $s_1, \cdots, s_n$,即可确定 $\omega(z)$.

4.2 Goppa 码的译码

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

Goppa 码的译码过程大致与 BCH 码的一致. 设 C 是 Goppa 码. 设错误向量 e 的 Hamming 重量 $wt(e) < t/2$, t 为 $g(x)$ 的次数. 将伴随式定义为多项式 $S(x) \equiv \sum_{i=1}^{n} \frac{e_i}{x - \gamma_i} \bmod g(x)$. 定义错误位置多项式为 $\sigma(z) := \prod_{r=1}^{w}(z - \gamma_{i_r})$ 及伴随多项式 $\omega(z) := \sum_{r=1}^{w} e_{i_r} \prod_{k \neq r}(z - \gamma_{i_k})$. 由于 $S(z)\sigma(z) = \omega(z) \bmod (g(z))$, 利用 Berlekamp-Massey 算法或基于 Euclid 算法的方法就可找到满足上述方程的最低次数解 $\sigma(z)$ 和 $\omega(z)$, 从而确定错误值.

4.3　基本译码算法

设 $C_\Omega(D, G)$ 是设计距离为 $d = \deg G - 2g + 2$ 的代数几何码. 设 $y = c + e$ 是接收到的字, 其中错误向量 e 的 Hamming 重量 $wt(e) = t$. 设 $I = \{i \mid e_i \neq 0\}$ 为错误位置集, $Q = \sum_{i \in I} P_i$ 为错误位置除子. 设 F 是任一其支集与 D 的支集无交的除子. 则 $L(F)$ 中的错误位置函数集合为 $L(F - Q)$. 令

$$K(y, F) = \{f \in L(F) \mid \sum y_i f(P_i) g(P_i) = 0, \ \forall g \in L(G - F)\}$$

则当 F 满足条件

$$\deg F \geq t + g \tag{1}$$

$$\deg(G - F) > t + 2g - 2 \tag{2}$$

时, $L(F - Q) = K(y, F)$. 对给定的 $L(F)$ 和 $L(G - F)$ 的基底, 通过解含 $l(F)$ 个未知量、$l(G - F)$ 个方程的线性方程组可确定 $K(y, F)$. 对 F 的次数的限制导致 $K(y, F)$ 中的非零元素最多有 $d - 1$ 个零点, 利用命题 2.3, 就可得到错误值. 由于满足条件(1)、(2)的最大的 t 为 $\lfloor (d - 1 - \gamma)/2 \rfloor$, 所以基本译码算法只能纠 $\lfloor (d - 1 - \gamma)/2 \rfloor$ 个错.

4.4　Ehrhard 译码算法

Ehrhard 译码算法可视为基本译码算法和改进译码算法的发展, 通过让算法找出依赖于接收字的那些除子而避开了改进译码算法中需预先找出除子 $F_1, \cdots, F_s$ 的困难, 从而使纠错能力达到码的最小设计距离的一半.

码 $C_\Omega(D, G)$ 是留数映射 Res_D 的像

$$\mathrm{Res}_D : \Omega(G - D) \to F_q^n.$$

当 $\deg(G) > 2g - 2$ 时, Res_D 是单射. 可以证明, 存在除子 $G' \leq G$ 和线性映射

$$F_q^n \to \Omega(G' - D), \ y \mid \to \eta_y$$

使得

(1) $\mathrm{Res}_D(\eta_y) = y, \ \forall y \in F_q^n$,

(2) $c \in C_\Omega(D, G) \Leftrightarrow \eta_c \in \Omega(G - D)$.

设 F 是除子, 使得 $\deg(G - F) > 2g - 2$. 则

$$\Omega(G - D - F) \cap \Omega(G' - F) = \Omega(G - F) = \{0\}.$$

因此 $\Omega(G - D - F) + \Omega(G' - F)$ 是直和. 令

$$\pi : \Omega(G - D - F) \oplus \Omega(G' - F) \to \Omega(G' - F)$$

是沿着 $\Omega(G - D - F)$ 的投影. 对每个 $y \in F_q^n$, 定义

$$S(F) := \{f \in L(F) \mid \eta_y \in \Omega(G - D - F) \oplus \Omega(G' - F)\}$$

$S(F)$ 仅依赖于陪集 $y + C$, 本质上与基本译码算法中 $K(y, F)$ 是一样的.

命题 4.1　设 $L(F - Q) \neq 0$, $\deg(F) \leq d - g - 1$. 则下面的陈述仅有一个成立:

(a) $S(F) = L(F - Q)$; (b) 存在有理点 $P \in \mathrm{supp}(D)$ 使得 $s(F - P) \leq s(F) - 2$, 其中 $s(F)$ 是 $S(F)$ 的维数.

命题 4.2　存在正和列

$$0 \to L(F - Q) \xrightarrow{l} S(F) \xrightarrow{\Phi} \Omega(G - F - Q),$$

其中 l 是 $L(F - Q) \to L(F)$ 的包含映射, $\Phi(f) = \eta_e - \pi(\eta_y)$.

推论 1　$l(F - Q) \leq s(F) \leq l(F - Q) + i(G - F - Q)$.

推论 2　$e = \mathrm{Res}_D \pi(\eta_y)/f, \ \forall f \in L(F - Q) \setminus \{0\}$.

由命题 4.2 及其推论可以这样来构造一个译码算法: 只要 $\Omega(G - F - Q) = \{0\}$, 由推论 1 有 $S(F) = L(F - Q)$, 由接收字 y 可计算出 $S(F)$, 然后任取非零 $f \in S(F)$, 用推论 2 确定 e. 这与基本算法几乎是一样的. 但是, 只有当 $\deg(Q) \leq (d - 1 - g)/2$ 时, 才能保证

$$L(F - Q) = S(F) \tag{3}$$

$$L(F - Q) \neq \{0\} \tag{4}$$

由命题 4.1, 当 $L(F - Q) \neq S(F)$ 时, 总能找到点 $P \in \mathrm{supp}D$ 使得 $s(F - P) \leq s(F) - 2$, 而 $l(F - P - Q) \leq l(F - Q) + 1$. 在算法开始时取除子 F 使得 $s(F) - l(F - Q) \leq g$, 这样不断的从除子 F 中去掉点, 经过有限步后, 必能使条件(3)、(4)得到满足.

算法 $A(F)$. (1) 输入 y. (2) 令 $j := 1$ 和 $F_1 = F$. (3) 找点 $P \in \{P_1, \cdots, P_n\}$ 使得 $s(F_j - P) \leq s(F_j) - 2$. 如果存在这样的点, 则令 $F_{j+1} := F_j - P$, j 递增 1, 继续步骤(3). 否则, (4) 取 $f \in S(F_j) \setminus \{0\}$, 计算 $e = Res_D \pi(\eta_y)/f$. (5) 输出 e. 于是, 有下面的定理.

定理 4.3　设 χ 是亏格为 g 的曲线, $C_\Omega(D, G)$ 是 χ 上的代数几何码, 其设计距离为 $d \geq 6g + t^*$, $t^* = \lfloor (d - 1)/2 \rfloor$. 则 $A(F)$ 可纠 $t \leq t^*$ 个错误.

5　从 BCH 码、Goppa 码的译码算法到 Feng-Rao 大数表决法

从码的校验矩阵的角度考察译码算法, 容易将 BCH 码和 Goppa 码的译码算法转化为考察错误向量的伴随式序列的线性递推关系, 并用 Berlekamp-Massey 算法计算出更多的伴随式的问题. 这种想法甚至可以推广到交错码上去.

李、周、肖[18~21]从校验矩阵的角度考虑了 BCH 码和 Goppa 码的译码算法, 将上述想法加以改造, 推广到一点代数几何码的译码中去. 李、周、肖[18~21]首先在序列上引入了一类新型递推关系 ——A-型递推关系, 引入了 A-型递推关系的极小多项式集的概念以及刻划 A-型递推关系长度的 d-集的概念, 对满足一定条件的 A-型递推关系建立了一致预言定理等基础性定理. 然后推广了 Berlekamp-Massey 算法, 对满足一定条件的 A-型递推关系建立了广义 Berlekamp-Massey 算法. 并对序列上的 A-型递推关系建立了大数表决方案. 对于一点代数几何码, 研究了错误向量的伴随式序列, 在其上引入了一种 A-型递推关系, 并用代数曲线的知识证明这种 A-型递推关系的 d-集的大小受到错误个数的限制, 利用文[18~21]建立的

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

广义 Berlekamp-Massey 算法和大数表决方案,将 BCH 码和 Goppa 码的译码算法推广,建立了一点代数几何码的一个有效译码算法.

5.1 BCH码与 Goppa 码的译码

我们从码的校验矩阵的角度重新考察 BCH 码与 Goppa 码的译码. BCH 码的译码　设 α 是 F_q 的扩域中的一个 n 次本原单位根. 则矩阵

$$H=\begin{pmatrix}1 & \alpha^{r} & \alpha^{2r} & \cdots & \alpha^{(n-1)r}\\ 1 & \alpha^{r+1} & \alpha^{2(r+1)} & \cdots & \alpha^{(n-1)(r+1)}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ 1 & \alpha^{r+d-2} & \alpha^{2(r+d-2)} & \cdots & \alpha^{(n-1)(r+d-2)}\end{pmatrix}$$

就是一个最小设计距离为 d 的 BCH 码的校验阵. 对任意接收字 $y=c+e\in F_q^n$,假设 e 的 Hamming 重量 $wt(e)\leq\lfloor(d-1)/2\rfloor$. 知道 e 的前 $d-1$ 个伴随式为 $s_i(e)=s_i(y)=\sum_{l=1}^{n}\alpha^{(l-1)(r+i-1)}y_l$, $i=1,\cdots,d-1$.

现在将校验阵 H 扩充为

$$\bar{H}=\begin{pmatrix}1 & \alpha^{r} & \alpha^{2r} & \cdots & \alpha^{(n-1)r}\\ 1 & \alpha^{r+1} & \alpha^{2(r+1)} & \cdots & \alpha^{(n-1)(r+1)}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ 1 & \alpha^{r+d-2} & \alpha^{2(r+d-2)} & \cdots & \alpha^{(n-1)(r+d-2)}\\ 1 & \alpha^{r+d-1} & \alpha^{2(r+d-1)} & \cdots & \alpha^{(n-1)(r+d-1)}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ 1 & \alpha^{r+d-2} & \alpha^{2(r+d-2)} & \cdots & \alpha^{(n-1)(r+d-2)}\end{pmatrix}$$

$\bar{H}$ 当然是可逆的. 由于 $wt(e)\leq\lfloor(d-1)/2\rfloor$,所以当计算 e 的伴随式时,只涉及到 $\bar{H}$ 的 $\lfloor(d-1)/2\rfloor$ 列. 对 $\bar{H}$ 的任意 $\lfloor(d-1)/2\rfloor$ 列,其第 $\lfloor(d-1)/2\rfloor+1$ 行一定被其前 $\lfloor(d-1)/2\rfloor$ 行线性表出,并且由 Vandermonde 矩阵的性质易知,其第 $\lfloor(d-1)/2\rfloor+2$ 行也被位于它前面的 $\lfloor(d-1)/2\rfloor$ 行同样线性表出. 依此类推,一直到其第 n 行都可被位于它前面的 $\lfloor(d-1)/2\rfloor$ 行同样线性表出. 由于 $s_i(e)=\sum_{l=1}^{n}\alpha^{(l-1)(r+i-1)}e_l$, $i=1,\cdots,n$,上述事实就意味着 e 的伴随式序列 $s_i(e)$, $i=1,\cdots,n$ 满足一个长度不超过 $\lfloor(d-1)/2\rfloor+1$ 的线性递推关系. 在用 Berlekamp-Massey 算法求这个线性递推关系的极小多项式时,由于极小多项式的次数不超过 $\lfloor(d-1)/2\rfloor$,只需用 Berlekamp-Massey 算法处理前 $d-1$ 个元素,就可得到这个唯一的极小多项式. 用这个极小多项式或者说用这个线性递推关系就可算出剩下的 $n-d+1$ 个伴随式 $s_i(e)$, $i=d,\cdots,n$ 的值. 然后由 $\bar{H}e^T=(s_1(e),\cdots,s_n(e))^T$ 就可算出 $e^T=\bar{H}^{-1}(s_1(e),\cdots,s_n(e))^T$.

Goppa 码的译码　Goppa 码是狭义 BCH 码的推广. 对 Goppa 码也可以进行类似的讨论.

Goppa 码的校验阵为

$$H=\begin{pmatrix}g(\alpha_1)^{-1} & \cdots & g(\alpha_1)^{-1}\\ \alpha_1 g(\alpha_1)^{-1} & \cdots & \alpha_n g(\alpha_n)^{-1}\\ \cdots & \cdots & \cdots\\ \alpha_1^{r-1} g(\alpha_1)^{-1} & \cdots & \alpha_n^{r-1} g(\alpha_n)^{-1}\end{pmatrix}$$

其最小设计距离为 $r+1$. 将 H 扩充为

$$\bar{H}=\begin{pmatrix}g(\alpha_1)^{-1} & \cdots & g(\alpha_1)^{-1}\\ \alpha_1 g(\alpha_1)^{-1} & \cdots & \alpha_n g(\alpha_n)^{-1}\\ \cdots & \cdots & \cdots\\ \alpha_1^{r-1} g(\alpha_1)^{-1} & \cdots & \alpha_n^{r-1} g(\alpha_n)^{-1}\\ \alpha_1^{r} g(\alpha_1)^{-1} & \cdots & \alpha_n^{r} g(\alpha_n)^{-1}\\ \cdots & \cdots & \cdots\\ \alpha_1^{n-1} g(\alpha_1)^{-1} & \cdots & \alpha_n^{n-1} g(\alpha_n)^{-1}\end{pmatrix}$$

这个矩阵当然也是可逆的.

对任意接收字 $y=c+e$,假设 e 的 Hamming 重量 $wt(e)\leq\lfloor r/2\rfloor$. 我们知道 e 的前 r 个伴随式为 $s_i(e)=s_i(y)=\sum_{l=1}^{n}\alpha_l^{i-1}g(\alpha_l)y_l$, $i=1,\cdots,r$. 由于 $wt(e)\leq\lfloor r/2\rfloor$,所以当计算 e 的伴随式时,最多涉及到 $\bar{H}$ 的 $\lfloor r/2\rfloor$ 列. 对 $\bar{H}$ 的任意 $\lfloor r/2\rfloor$ 列,若其前 $\lfloor r/2\rfloor+1$ 行之间有一个线性关系,对第 j 列乘以 α_j^r,则易知其第 2 行到第 $\lfloor r/2\rfloor+2$ 行之间也保持这个线性关系. 依此类推,这几个列任意连续的 $\lfloor r/2\rfloor+1$ 行之间都保持这个线性关系. 由伴随式的定义,这就导致伴随式序列 $s_i(e)$, $i=1,\cdots,n$ 满足一个长度不超过 $\lfloor r/2\rfloor+1$ 的线性递推关系. 同前面的讨论一样,在用 Berlekamp-Massey 算法求这个线性递推关系的极小多项式时,由于极小多项式的次数不超过 $\lfloor r/2\rfloor$,只需用 Berlekamp-Massey 算法处理前 r 个元素,就可得到这个唯一的极小多项式. 用这个极小多项式或者说用这个线性递推关系就可算出剩下的 $n-r$ 个伴随式 $s_i(e)$, $i=r+1,\cdots,n$ 的值. 然后由 $\bar{H}e^T=(s_1(e),\cdots,s_n(e))^T$ 就可算出 $e^T=\bar{H}^{-1}(s_1(e),\cdots,s_n(e))^T$.

我们试图把上述作法推广到代数几何码的译码中去. 首先在序列上引入一类新型递推关系 ——A-刑递推关系并建立了一致预言定理等基础性定理.

5.2 序列上的 A-型递推关系

从多项式零化序列的角度,李、周、肖[18~21]给出了 A-型递推关系的概念.

设 $(N_0,\perp)$ 为可消交换半群,其中 $\perp$ 为保持自然序的可换二元运算,即 $i<j\Rightarrow i+k<j+k$, $\forall k\in N_0$

0 为恒等元. 用 $\preceq$ 表示与 $\perp$ 相应的偏序:

$$i\preceq j \text{ 如果存在 } j\in N_0 \text{ 使得 } i\perp j=k.$$

定义 5.1　集 $\Delta\subseteq N_0$ 称为 d-集,如果

$$t\in\Delta\wedge s\preceq t\Rightarrow s\in\Delta$$

定义 5.2　设 Δ 为 d-集. $r\in N_0\setminus\Delta$ 称为 Δ 的一个外界,如果 r 在偏序 $\preceq$ 下是 $N_0\setminus\Delta$ 中的极小元. Δ 的所有外界组成的集记为 $Ext\Delta$.

d-集可完全由其外界来确定

$$\Delta=\{t\mid r\not\preceq t,\ \forall r\in Ext\Delta\}$$

定义 5.3　设 $V\subseteq F_q[X]$ 为多项式集. 称集

$$\Delta(V)=\{t\in N_0\mid \deg f\not\preceq t,\ \forall f\in V\}$$

为 V 的 d-集. 易知 V 的 d-集是一个 d-集.

用 S 来表示一个序列 $s_0,s_1,s_2,\cdots$.

定义 5.4　称多项式 $\sigma=\sum_i\sigma_iX^i\in F_q[X]$ 零化序列 S,记为

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

$\sigma(S)=0$,如果 $\sum_i \sigma_i s_i = 0$

下面给出 A-型递推关系的定义.

定义 5.5　对任意 $i,j\in N_0$,取定 $\phi_{i,j}=\sum_{u=0}^{i\perp j} c_{i,j}^u X^u \in F_q[X]$ 为 $i\perp j$ 次多项式. 称序列 S 在 $p\in N_0$ 满足以多项式 $\sigma=\sum_{i=0}^{k}\sigma_i X^i$ 为特征多项式的 A-型递推关系,如果 (a) $p\succeq k$;或 (b) $p\succeq k$ 并且多项式 $\sigma=\sum_i \sigma_i \phi_{i,p\neg k}$ 零化 S($\neg$ 表示 $\perp$ 的逆运算). 此时,也称多项式 σ 对序列 S 在 p 有效.

定义 5.6　设 $r\in N_0$. 称序列 S 直到 r 满足以 σ 为特征多项式的 A-型递推关系,如果对所有 $p\prec r$, S 在 p 都满足定义 5.5. 此时,也称多项式 σ 对序列 S 直到 r 有效. 这样的多项式全体记为 V_r. 用 Δ_r 记 $\Delta(V_r)$.

注　若令 $\perp=+$ 为通常的整数加法,且取 $\phi_{i,j}=X^{i+j}$,则 A-型递推关系就是线性递推关系.

定义 5.7　设 $\sigma\in V_r$,且 $\deg\sigma=k\preceq r$. 则称值

$$P_r(\sigma)=\frac{-1}{lc(\sigma)\,lc(\phi_{k,r\neg k})}\left[\sigma_k\sum_{u=0}^{r-1}c_{k,r\neg k}^u s_u+\sum_{i=0}^{k-1}\sigma_i\phi_{i,r\neg k}(S)\right]$$

对 σ 对 s_r 的预言,其中 $lc(\sigma)$ 表示 σ 的首项系数.

定义 5.8　集 $F_r\subseteq V_r$ 称为 S 直到 r 的极小多项式集,如果 F_r 的次数集 $T_r=\{t=\deg\sigma\mid \sigma\in F_r\}$ 与 $Ext\Delta_r$ 相同.

假设 A-型递推关系满足条件

$$(a)\quad \phi_{i,j}=\phi_{j,i},\ \forall i,j\in N_0 \tag{5}$$

$$(b)\quad \sum_{u=0}^{j\perp k}c_{j,k}^u\phi_{i,u}=\sum_{v=0}^{i\perp j}c_{i,j}^v\phi_{k,v},\ \forall i,j,k\in N_0 \tag{6}$$

则有下面的一致预言定理. 这个定理对建立 Berlekamp-Massey 算法起着关键的作用.

定理 5.1　(一致预言定理) 设 S 为序列. 设 $\sigma_1,\sigma_2\in V_r$,且 $\deg\sigma_1\perp\deg\sigma_2\preceq r$. 则 σ_1 和 σ_2 对 s_r 的预言一致,即

$$P_r(\sigma_1)=P_r(\sigma_2)$$

下面的定理描述了随着 r 的增大, d-集是如何扩大的.

定理 5.2　若 $\sigma\in V_r$ 且 $\sigma\notin V_{r+1}$,则 $r\neg\sigma\in\Delta_{r+1}$.

取定一族满足条件 (5)、(6) 的多项式 $\phi_{i,j}$,则 A-型递推关系随之确立. 李、周、肖[18~21]推广 Berlekamp-Massey 算法,给出了一个算法,使得对给定序列 S,可求出对序列 S 直到 $r+1$ 成立的 A-型递推关系的极小多项式集,这个算法被称为广义 Berlekamp-Massey 算法.

在广义 Berlekamp-Massey 算法的基础上,李、周、肖[18~21]对文[9]中大数表决方案进行了提炼,给出了 A-型递推关系的大数表决方案,这是大数表决方案的另一种表述方式.

5.3　大数表决方案

如果已知一个序列 S 的前 n 个元素,第 $n+1$ 个以后的元素是未知的,又知道生成它的线性递推关系的 d-集的大小不能超过 $n/2$,即极小多项式的次数不能超过 $n/2$,那么一旦用 Berlekamp-Massey 算法和序列 S 的前 n 个元素求出了极小多项式,序列 S 的第 $n+1$ 个以后的未知元素都可由这个极小多项式计算出来. 事实上,BCH 码的译码算法正是利用了这一事实. 对错误向量重量的限制 ($wt(e)\preceq(d-1)/2$, d 为最小设计距离) 导致接收字的伴随式序列所满足的线性递推关系的 d-集的大小不能超过 $(d-1)/2$. 这样,如果已经知道了伴随式序列的前 $d-1$ 个值(在译 BCH 码时,这恰好是知道的),用 Berlekamp-Massey 算法就可求出次数不超过 $(d-1)/2$ 的极小多项式. 用这个极小多项式就能算出 n(码的长度) 个伴随式的值,从而确定错误向量的值.

在用广义 Berlekamp-Massey 算法对代数几何码进行译码的研究中,也想利用类似的相法. 但由于 A-型递推关系是非线性的,且一般说来序列的加标集是个偏序集,即极小多项式集所含极小多项式不止一个,这就导致所谓大数表决方案的产生:通过对序列所满足的 A-型递推关系的 d-集的大小的限制,使得利用极小多项式集中的极小多项式对序列中的未知元素进行预言时,导致 d-集变化最大的预言一定是正确的.

下面详细表述大数表决方案.

设 A-型递推关系已给定,即已取定一族满足条件 (5)、(6) 的多项式 $\phi_{i,j}$. 设 $S=s_0,\cdots,s_{r-1},s_r$ 为序列,其中 $s_0,\cdots,s_{r-1}$ 是已知的, s_r 是未知的.

由广义 Berlekamp-Massey 算法,可求得直到 r 有效的 A-型递推关系的极小多项式集 $F_r=\{\sigma^{(1)},\cdots,\sigma^{(k)}\}$. 对每个 $\sigma^{(i)}$,若 $\deg\sigma^{(i)}\preceq r$,则可计算出 $\sigma^{(i)}$ 对 s_r 的预言 $P_r(\sigma^{(i)})$. 令

$$K_i=\{j\in N_0\mid j\preceq r\neg\deg\sigma^{(i)}\}$$

若 $P_r(\sigma^{(i)})$ 是错误的预言,即 $\sigma^{(i)}\notin V_{r+1}$,由定理 5.2,有 $K_i\subseteq\Delta_{r+1}$. 若令　　$K_i'=K_i\setminus\Delta_r$

则 Δ_{r+1} 至少比 Δ_r 多出 K_i'.

令 $w_1,\cdots,w_p$ 表示所有如上这样得到的对 s_r 的不同的预言. 令

$$L_j=\bigcup_{i\in W_j}K_i',\ W_j=\{i\mid P_r(\sigma^{(i)})=w_j\}$$

即对 s_r 的预言相同的那些极小多项式所对应的比 Δ_r 多出的那一部分.

类似线性递推关系的极小多项式的次数的增大规律,可给出 A-型递推关系的 d-集的增大规律.

设 $K'=\bigcup_{j=1}^{p}L_j$,即 Δ_{r+1} 比 Δ_r 多出的那一部分, $N_r=\{j\in N_0\mid j\preceq r\}$. 令 $d_r=|N_r|$ 为 N_r 所含元素的个数.

引理 5.3　$|K'|\geq d_r-2|\Delta_r|$.

大数表决方案的主要内容包括在下面的定理中.

定理 5.4　假设序列 S 满足的 A-型递推关系的 d-集的大小都不超过 $(d_r-1)/2$,即 $|\Delta_{r+1}|\preceq(d_r-1)/2$,那么,令 $l\in\{1,\cdots,p\}$ 为使 $|L_l|$ 最大的数. 则必有　　$s_r=w_l$

5.4　伴随式序列与 A-型递推关系

设 $C=C_Q(D,G)$ 为曲线 χ 上一点代数几何码,其中 $D=\sum_{l=1}^{n}P_l$, $G=mQ$. 设 $O=\{o_i\mid i\in N_0\}$ 是以递增顺序排列的 Q 的所有非空隙组成的集, $o_0=0$. 由 Riemann-Roch 定理,有

$$0=o_0<o_1<\cdots<o_{\gamma-2}<o_{\gamma-1}=2\gamma-1,$$

$$o_i=i+\gamma,\ i\geq\gamma.$$

设 $E=\{f_i\mid i\in N_0\}$ 为基函数集,即对每个 $i\in N_0$, f_i 是曲线 χ 上仅以 Q 为极点的有理函数,且极的阶为 $\mathrm{ord}_Q(f_i)=o_i$. 当 $m>2\gamma-2$ 时,矩阵

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

$$H=\begin{pmatrix} f_0(P_1) & \cdots & f_0(P_n) \\ \cdots & \cdots & \cdots \\ f_{m-\gamma}(P_1) & \cdots & f_{m-\gamma}(P_n) \end{pmatrix}$$

为码 C 的校验阵. 以后,总假设 $m>2\gamma-2$. 这时,码 C 的最小设计距离为 $d=m-2\gamma+2$.

对 $y=(y_1,\cdots,y_n)\in F_q^n$,定义

$$s_i(y)=\sum_{l=1}^{n} f_i(P_l)\,y_l,\ 0\le i\le m-\gamma \qquad (7)$$

为 γ 的伴随式. 易知

$$y\in C\Leftrightarrow s_i(y)=0,\ i=0,\cdots,m-\gamma$$

译码时,当接收到字 $y=c+e$ 后,其中 $c\in C$ 为码字,e 是错误向量. 有 $s_i(y)=s_i(e)$, $\forall i\le m-\gamma$

首先,要将矩阵 H 通过添加新的行扩大为新的矩阵 $\overline{H}$. 将 $f_{m-\gamma+1}(P_1),\cdots,f_{m-\gamma+1}(P_n)$ 作为新的一行添加给矩阵 H,然后是 $f_{m-\gamma+2}(P_1),\cdots,f_{m-\gamma+2}(P_n)$,一直添加到行 $f_{n+\gamma-1}(P_1),\cdots,f_{n+\gamma-1}(P_n)$,就得到的一个矩阵 $\overline{H}$. 由于这个矩阵是码 $C_\Omega(D,(n+2\gamma-1)Q)$ 的校验阵,由定理 3.2 知,码 $C_\Omega(D,(n+2\gamma-1)Q)$ 的最小距离大于 n. 因此,$\overline{H}$ 的 n 列必线性无关,即 $\overline{H}$ 的秩为 n. 于是可找到这个矩阵的一个 n 阶可逆子阵

$$\overline{H}(i_1,\cdots,i_n)=\begin{pmatrix} f_{i_1}(P_1) & \cdots & f_{i_1}(P_n) \\ \cdots & \cdots & \cdots \\ f_{i_n}(P_1) & \cdots & f_{i_n}(P_n) \end{pmatrix},\ i_n\le n+\gamma-1$$

这时,有

$$\overline{H}(i_1\cdots i_n)\,e^T=(s_{i_1}(e),\cdots,s_{i_n}(e))^T$$

如果能知道所有的 $s_{i_1}(e),\cdots,s_{i_n}(e)$,就能求出

$$e^T=\overline{H}(i_1\cdots i_n)^{-1}(s_{i_1}(e),\cdots,s_{i_n}(e))^T.$$

现在的问题是如何由已知的 $s_i(e)$, $i\le m-\gamma$,求出未知的 $s_i(e)$, $m-\gamma<i\le n+\gamma-1$.

遵循 BCH 码和 Goppa 码的译码思路,假设对错误向量的 Hamming 重量加以限制,比如说,小于码 C 的最小设计距离 d 的一半,那么,在计算 e 的伴随式 $s_i(e)$ 时将只涉及到矩阵 $\overline{H}$ 的 $\lfloor(d-1)/2\rfloor$ 个列. 但是,在这里没有像在 BCH 码译码或 Goppa 码译码时那么走运,矩阵 $\overline{H}$ 比 BCH 码和 Goppa 码的校验阵要复杂得多,没有那么好的性质. 当 $\overline{H}$ 前 k 行之间有一个线性关系时,无法推出从第二行到第 k 行之间也有这个线性关系. 我们只能推出行向量 $(f_0(P_1)f_1(P_1),\cdots,f_0(P_n)f_1(P_n)),\cdots,(f_{k-1}(P_1)f_1(P_1),\cdots,f_{k-1}(P_n)f_1(P_n))$ 之间有这个线性关系. 这 k 个行向量与 $\overline{H}$ 的第二行到第 k 行的关系是复杂的,一般说来,不是互相线性表出的关系. 能直接看出的,只是对应行向量相应的有理函数的极的阶数是一样的. 如果能利用这个关系导出伴随式序列上的一个 A-型递推关系,那么就有可能利用广义 Berlekamp-Massey 算法和大数表决方案来确定未知伴随式的值,最终给出一个译码算法.

定义 5.9 设 $e=(e_1,\cdots,e_n)\in F_q^n$, $f_i\in E$. 称

$$s_i=\sum_{l=1}^{n} f_i(P_l)\,e_l$$

为 e 的伴随式. 称序列 $S=\{s_i\mid i\in N_0\}$ 为 e 的伴随式序列.

下面,利用刚才所提到的在 Q 点具有阶数相同的极的有理函数之间的关系来导出伴随式序列所满足的递推关系.

定义 N_0 上的二元运算"$\perp$"如下

$$i\perp j=k \quad \text{如果 } o_i+o_j=o_k,\ o_i,o_j,o_k\in O$$

易验 $(N_0,\perp)$ 为可消交换半群,且 $\perp$ 为保持自然序的可换二元运算,0 为恒等元.

任取 $f_i,f_j\in E$,则 f_if_j 也仅以 Q 为极点,且

$$\mathrm{ord}_Q(f_if_j)=\mathrm{ord}_Q(f_i)+\mathrm{ord}_Q(f_j)=o_i+o_j=o_{i\perp j}$$

所以,$f_if_j\in L(o_{i\perp j}Q)$ 且 f_if_j 的极的阶数与 $f_{i\perp j}$ 的相同. 因 $f_0,\cdots,f_{i\perp j}$ 是 F_q 向量空间 $L(O_{i\perp j}Q)$ 的一个基,所以 f_if_j 可被其线性表出,即

$$f_if_j=\sum_{u=0}^{i\perp j} c_{i,j}^{u}f_u,\ c_{i,j}^{u}\in F_q,\ c_{i,j}^{i\perp j}\neq 0$$

这就是我们要利用的关系.

令

$$\Phi_{i,j}=\sum_{u=0}^{i\perp j} c_{i,j}^{u}X^u,\ i,j\in N_0$$

将上述多项式取为定义 A-型递推关系所需要的那族多项式. 因 $f_if_j=f_jf_i$, $(f_if_j)f_k=f_i(f_jf_k)$, $i,j,k\in N_0$. 易验 $\Phi_{i,j}$ 一定满足条件(5)、(6).

定义 5.10 称多项式 σ 对伴随式序列 S 在 $p\in N_0$ 有效,如果对如上取定的 $\Phi_{i,j}$,伴随式序列 S 在 p 满足以多项式 σ 为特征多项式的 A-型递推关系. 类似地,称多项式 σ 对伴随式序列 S 直到 $r\in N_0$ 有效,如果对如上取定的 $\Phi_{i,j}$,伴随式序列 S 直到 r 满足以多项式 σ 为特征多项式的 A-型递推关系.

这样,就在伴随式序列上引进了一种 A-型递推关系.

如所期望的,对向量 e 的伴随式序列来说,它所满足的这种 A-型递推关系的 d-集的大小要受到 e 的 Hamming 重量 $wt(e)$ 的限制.

定理 5.5 设 S 是 e 的伴随式序列. 则 $|\Delta_r|\le wt(e)$

其中 $|\Delta_r|$ 表示集 Δ_r 所含元素的个数.

在 5.4 中曾定义了量 d_r,现在定义码 $C=C_\Omega(D,mQ)$ 的 Feng-Rao 距离如下.

定义 5.11 称

$$d_{FR}=\min\{d_r\mid r>m-\gamma\}=\min\{\,|\{j\in N_0\mid j\le r\}|\ \mid r>m-\gamma\}$$

为码 $C=C_\Omega(D,mQ)$ 的 Feng-Rao 距离.

由文[9]知,$d_{FR}\ge d$.

定理 5.6 假设 e 的 Hamming 重量 $wt(e)$ 满足

$$wt(e)\le\lfloor(d_{FR}-1)/2\rfloor$$

那么可以用大数表决方案即定理 5.4 来确定 e 的未知伴随式 s_i, $m-\gamma<i\le n+\gamma-1$ 的值.

5.5 一个有效译码算法

现在可以将整个译码算法描述如下.

对给定码 $C=C_\Omega(D,mQ)$,首先对矩阵

$$\overline{H}=\begin{pmatrix} f_0(P_1) & \cdots & f_0(P_n) \\ \cdots & \cdots & \cdots \\ f_{n+\gamma-1}(P_1) & \cdots & f_{n+\gamma-1}(P_n) \end{pmatrix}$$

进行预处理,找到它的一个可逆子阵 $\overline{H}(i_1,\cdots,i_n)$,并计算出它的逆矩阵 $\overline{H}(i_1\cdots i_n)^{-1}$.

当接收到一个字 $y=c+e\in F_q^n$ 后,假设 $wt(e)\le\lfloor(d_{FR}-$

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

1)/2」. (1)用式(7)计算伴随式 $s_i(e) = s_i(y)$, $i \le m - \gamma$. (2)用广义 Berlekamp-Massey 算法计算出对已知伴随式序列 $s_0, \cdots, s_{m-\gamma+1}$直到 $m - \gamma + j + 1$ 成立的 A-型递推关系的一个极小多项式集, $j \ge 0$. (3)运用大数表决方案,即定理 5.4,找出未知伴随式 $s_{m-\gamma+j+1}$的正确值.重复执行(2)、(3),直到所有 s_r, $r \le i_n$,的值都得到. (4)计算 $e^T = \bar{H}(i_1 \cdots i_n)^{-1}(s_{i_1}, \cdots, s_{i_n})^T$

6　结束语

比较译码算法发展的两条途径,在代数几何码以前的译码算法两条途径中的相应译码算法都是等价的,在概念上是相互对应的.代数几何码虽然在概念上可看作 RS 码和 Goppa 码的推广,然而译码算法的发展却产生了分歧:从错误位置多项式的角度考虑问题,得到 Ehrhard 译码算法;从校验矩阵的角度出发,得到大数表决法. Ehrhard 译码算法和大数表决法的关系仍然没搞清楚.当然大数表决法似乎是针对一点代数几何码来说的,而 Ehrhard 译码算法似乎对码的距离有所要求,但是否能提炼出两者共同的本质,得到一种统一的表达,仍然是饶有兴味的问题.这一点对译码算法以及代数几何码本身的理解都极有意义.

参考文献:

[1] V. D. Goppa. Codes associated with divisors [J]. Probl. Inform. Transm. 1977,13:22 - 26.

[2] M. A. Tsfasman, S. G. Vlădut, and T. Zink. Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound. Math [J]. Nachrichten, 1982, 109:21 - 28.

[3] J. Justesen, et al. Construction and decoding of a class of algebraic geometric codes [J]. IEEE Trans. Inform. Theory, July 1989, 35:811 - 821.

[4] A. N. Skorobogatov and S. G. Vlădut. On the decoding of algebraic-gecometric codes [J]. IEEE Trans. Inform. Theory, Nov. 1990, 36: 1051 - 1060.

[5] M. A. Tsfasman and S. G. Vlădut. Algebraic-geometric codes [J]. Mathematics and its Applications, Dordrecht, The Netherlands: Kluwer, 1991:58.

[6] S. C. Porter, B.-Z. Shen, and R. Pellikaan. On decoding geometric Goppa codes using and extra place [J]. IEEE Trans. Inform. Theory, Nov. 1992, 38:1663 - 1676.

[7] D. Ehrhard. Decoding algebraic-geometric codes by solving a key equation [A]. Proc. AGCT-3, Luminy 1991, Lect. Notes Math. [C], 1992, 1518:18 - 25.

[8] D. Ehrhard. Achieving the designed error capacity in decoding algebraic-geometric codes [J]. IEEE Trans. Inform. Theory, May 1993, 39:743 - 751.

[9] G.-L. Feng and T. R. N. Rao. Decoding of algebraic-geometric codes up to the designed minimum distance [J]. IEEE Trans. Inform. Theory, Juan. 1993, 39:37 - 45.

[10] 李宝.一类代数几何码的译码算法 [D].博士论文:西安电子科技大学,1998.

[11] W. Fulton. Algebraic Curves. An Introduction to Algebraic Geometry [M]. New York, Amsterdam: W. A. Benjamin, 1969.

[12] R. Hartshorne. Algebraic geometry [M]. Graduate Texts in Mathermatics, vol. 52. Berlin, Heidelberg, New York: Springer-Verlag, 1972.

[13] C. Moreno. Algebraic Curves Over Finite Fields. Cambridge Tracts in Math [M]. Cambridge, U. K.: Cambridge Univ. Press, 1991, 97.

[14] J. H. van Lint. Introduction to Coding Theory [M]. New York: Springer-Verlag, 1982.

[15] F. J. McWilliams and N. J. A. Sloane. The Theory of Error-Correcting Codes North-Holland Math. Library [M]. Amsterdam, The Netherlands: North-Holland, 1977, 16.

[16] W. W. Peterson and E. J. Weldon. Error-Correcting Codes [M]. MIT Press, 1972.

[17] T. HØholdt, R. Pellikaan. On the decoding of algebraic-geometric codes [J]. IEEE Trans Inform Theory, vol IT-41, 1995:1589 - 1614.

[18] B. Li, L. F. Zhou and G. Z. Xiao. A type of recurring relation on sequences and efficient decoding of a class of algebraic-geometric codes (I) [J]. Science in China (Series E), 1998, 41(6):631 - 640.

[19] B. .Li, L. F. Zhou and G. Z. Xiao. A type of recurring relation on sequences and efficient decoding of a class of algebraic-geometric codes (II) [J]. Science in China (Series E), 1999, 42(1):28 - 35.

[20] 李宝,周林芳,肖国镇.序列递推关系与一类代数几何码的有效译码(1) [J].中国科学 E 辑,1998,28(5).

[21] 李宝,周林芳,肖国镇.序列递推关系与一类代数几何码的有效译码(2) [J].中国科学 E 辑,1998,28(6).

[22] I. Blake, C. Heegard, T. HØholdt and V. Wei, Algebraic-geometry codes [J]. IEEE Trans. Inform. Theory, Oct. 1995, IT-44: 2596 - 2618.

作者简介:

李　宝　1962 年出生,1998 年获工学博士学位.现在中科院软件所做博士后研究工作.主要研究方向为编码学、密码学.

冯登国　1965 年生,1995 年获工学博士学位.现为信息安全国家重点实验室副主任.主要研究方向为编码学、密码学.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net