第16卷 第4期　　电 子 科 学 学 刊　　Vol. 16, No. 4
1994 年 7 月　　JOURNAL OF ELECTRONICS　　July, 1994

循环码研究中的一种几何方法

钱 霖 君
(苏州丝绸工学院　苏州 215005)

摘要　本文采用几何的方法对循环码进行了研究. 证明了 BCH 码的校验矩阵是用循环变换的特征向量作基底时的一种表示形式，从而把循环码的研究纳入到线性系统理论研究的框架之中.

关键词　循环码，几何方法，特征向量

1 引言

差错控制的编码理论目前主要有两种研究方法：现代代数法[1]和有限正交展开法[2]. 本文则采用几何的方法对循环码进行研究，证明 BCH 码的校验矩阵是用循环变换的特征向量作基底时的一种表示形式. 从而提供了一种将一般循环码和有限几何循环码进行统一研究的可能性.

2 主要结果

设 F_2 为二元域，$V_n(F_2)$ 是定义在 F_2 上的 n 维向量空间. 令 Σ 是 $V_n(F_2)\to V_n(F_2)$ 的循环变换，即 $\forall v^{\tau}\in V_n(F_2)$，$v=(v_0v_1\cdots v_{n-1})$，有

$$\Sigma_1 v^{\tau}=(v_{n-1}v_0\cdots v_{n-2})^{\tau} \text{ 或 } \Sigma_2 v^{\tau}=(v_1v_2\cdots v_0)^{\tau}.$$

这里，Σ_1 为右循环移位算子；Σ_2 为左循环移位算子. 显然，Σ 是线性变换.

引理 1　对循环变换 Σ 而言，n 维线性空间 $V_n(F_2)$ 的最小多项式

$$\varphi(x)=x^n-1. \tag{1}$$

引理 2　循环变换 Σ_1 和 Σ_2 在基底 $e_0^{\tau}=(10\cdots0)^{\tau}$，$e_1^{\tau}=(010\cdots0)^{\tau},\cdots,e_{n-1}^{\tau}=(00\cdots01)^{\tau}$ 中的表示分别为

$$\sigma_1=\begin{bmatrix}0&1&0\cdots0\\0&0&1\cdots0\\\vdots&&\\1&0&0\cdots0\end{bmatrix} \text{ 和 } \sigma_2=\begin{bmatrix}0&0\cdots0&1\\1&0\cdots0&0\\\vdots&\vdots&\\0&0\cdots1&0\end{bmatrix}, \tag{2}$$

且 $\sigma_1=\sigma_2^{-1}$，$\sigma_1=\sigma_2^{\tau}$.

引理 3　循环变换 Σ 的特征多项式就是 $V_n(F_2)$ 的最小多项式，即

$$|xI-\sigma_{1,2}|=x^n-1. \tag{3}$$

定理 1　对任意大于 1 的正整数 n，设

$$\varphi(x)=h(x)g(x), \tag{4}$$

1993-04-20 收到，1993-10-08 定稿
钱霖君　男，1936 年生，副教授，现从事现代控制理论的教学和科研工作.

其中 $\partial^0 h(x)=k$，$\partial^0 g(x)=n-k$，则

$$\mathrm{Ker}[h(\sigma_1)]=\{v^r\mid h(\sigma_1)v^r=0,\forall v^r\in V_n(F_2)\};\tag{5}$$

$$\mathrm{Ker}[g(\sigma_1)]=\{v^r\mid g(\sigma_1)v^r=0,\forall v^r\in V_n(F_2)\}\tag{6}$$

都是 $V_n(F_2)$ 的 σ_1——不变子空间：$\mathrm{Ker}[h(\sigma_1)]$ 就是 k 维循环码的码空间，而 $\mathrm{Ker}[g(\sigma_1)]$ 就是相应的 $n-k$ 维的对偶循环码的码空间。而且，$h(x)$ 和 $g(x)$ 分则是 $\mathrm{Ker}[h(\sigma_1)]$ 和 $\mathrm{Ker}[g(\sigma_1)]$ 的最小多项式。

证明　我们只给出定理最后部分的证明，其余部分的证明见文献[3]。设 $e_0^r=(10\cdots0)^r$，$e_1^r=(010\cdots0)^r,\cdots,e_{k-1}^r=(0\cdots010\cdots0)^r$。显然，它们的最小多项式都是(1)式中的 $\varphi(x)$。因此，消息空间 $\mathrm{Span}\{e_0^r,e_1^r,\cdots,e_{k-1}^r\}$ 的最小多项式也是 $\varphi(x)$[3]。而空间 $\mathrm{Span}\{g(\sigma_1)e_0^r,g(\sigma_1)e_1^r,\cdots,g(\sigma_1)e_{k-1}^r\}$ 就是循环码的码空间 $\mathrm{Ker}[h(\sigma_1)]$。但因 $\varphi(\sigma_1)e_i^r=h(\sigma_1)g(\sigma_1)e_i^r=0$，$i=0,1,\cdots,k-1$，所以 $h(x)$ 是 $g(\sigma_1)e_i^r$，$0\leqslant i\leqslant k-1$ 的最小多项式。因此，$h(x)$ 是 $\mathrm{Ker}[h(\sigma_1)]=\mathrm{Span}\{g(\sigma_1)e_0^r,\cdots,g(\sigma_1)e_{k-1}^r\}$ 的最小多项式。同理可证 $g(x)$ 是 $\mathrm{Ker}[g(\sigma_1)]$ 的最小多项式。

关于循环码编码器与循环变换特征多项式的关系有以下定理。

定理 2　设循环变换的特征多项式 $\varphi(x)=h(x)g(x)$，那么以 $g(x)$ 为特征多项式的、单输入单输出的、无零点的能观标准形实现的离散系统就是 (n,k) 系统循环码的编码器。

证明　若设 $g(x)=g_0+g_1x+\cdots+g_{n-k}x^{n-k}$，那么定理 2 所述的能观标准形实现的动态方程为

$$\begin{bmatrix}x_0(j+1)\\x_1(j+1)\\\vdots\\x_{n-k-1}(j+1)\end{bmatrix}=\begin{bmatrix}0&0\cdots0&-g_0\\1&0\cdots0&-g_1\\\vdots&&\vdots\\0&0\cdots1&-g_{n-k-1}\end{bmatrix}\begin{bmatrix}x_0(j)\\x_1(j)\\\vdots\\x_{n-k-1}(j)\end{bmatrix}+\begin{bmatrix}1\\0\\\vdots\\0\end{bmatrix}u(j),\tag{7}$$

$$y(j)=[00\cdots1]\begin{bmatrix}x_0(j)\\x_1(j)\\\vdots\\x_{n-k-1}(j)\end{bmatrix}.\tag{8}$$

显然，这个离散系统就是文献[4]中的一种 (n,k) 系统循环码编码器。

定理 3　当 $n>1$ 为奇数时，设 $\varphi(x)=h(x)g(x)$，则

$$V_n(F_2)=\mathrm{Ker}[h(\sigma_1)]\oplus\mathrm{Ker}[g(\sigma_1)].\tag{9}$$

进一步，若设 $\partial^0 h(x)=k$，$\partial^0 g(x)=n-k$，且 $g(x)=g_0+g_1x+\cdots+g_{n-k}x^{n-k}$，$g=(g_0g_1\cdots g_{n-k}0\cdots0)$，则

$$\mathrm{Ker}[h(\sigma_1)]=\mathrm{Span}\{g^r,\sigma_1g^r,\cdots\sigma_1^{k-1}g^r\}.\tag{10}$$

证明　由于 $n>1$ 为奇数，因此 $\varphi(x)=x^n-1$ 无重因式。如果 $\varphi(x)=h(x)g(x)$，则 $h(x)$ 与 $g(x)$ 必互素。根据文献[3]的空间第一分解定理，就有

$$V_n(F_2)=\mathrm{Ker}[h(\sigma_1)]\oplus\mathrm{Ker}[g(\sigma_1)].\tag{11}$$

定理的其余部分则不难根据多项式 $h(x)g(x)=x^n-1$ 的乘法的系数与 $h(\sigma_1)\sigma_1^ig^r$ 的乘法关系加以证实的。其实

$$\boldsymbol{G}=\begin{bmatrix}\boldsymbol{g}\\ \boldsymbol{g}\sigma_1\\ \vdots\\ \boldsymbol{g}\sigma_1^{k-1}\end{bmatrix} \tag{12}$$

就是一般循环码的生成矩阵.

引理 4 设 $n=2^r-1$, r 为大于 1 的正整数,则 σ_1 和 σ_2 的模态矩阵分别为

$$\boldsymbol{T}_1=\begin{bmatrix}1 & 1 & \cdots & 1\\ 1 & \alpha & \cdots & \alpha^{n-1}\\ \vdots & & & \\ 1 & \alpha^{n-1} & \cdots & (\alpha^{n-1})^{n-1}\end{bmatrix} \text{ 和 } \boldsymbol{T}_2=\begin{bmatrix}1 & \alpha^{n-1} & \cdots & (\alpha^{n-1})^{n-1}\\ 1 & \alpha^{n-2} & \cdots & (\alpha^{n-2})^{n-1}\\ \vdots & & & \\ 1 & 1 & \cdots & 1\end{bmatrix}, \tag{13}$$

且

$$\boldsymbol{T}_1\Lambda=\sigma_1\boldsymbol{T}_1, \tag{14}$$

$$\Lambda=\begin{bmatrix}1 & & & \\ & \alpha & & 0\\ & & \ddots & \\ 0 & & & \alpha^{n-1}\end{bmatrix}, \tag{15}$$

其中,α 是域 F_{2^r} 的本原元,$1,\alpha,\cdots,\alpha^{n-1}$ 是域 F_{2^r} 中的 2^r-1 个非零元,它们必两两互异.

有了上面这个引理,我们就可着手证明有关 BCH 码奇偶校验矩阵的一个结果.

定理 4 设 $n=2^r-1$, r 为大于 1 的正整数. 则 BCH 码的奇偶校验矩阵可表示为

$$\boldsymbol{H}=\begin{bmatrix}1 & \alpha_1 & \cdots & \alpha_1^{n-1}\\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1}\\ \vdots & & & \\ 1 & \alpha_{n-k} & \cdots & \alpha_{n-k}^{n-1}\end{bmatrix}, \tag{16}$$

其中 $\alpha_i(1\leqslant i\leqslant n-k)$是定理 2 中特征多项式 $g(x)$的 $n-k$ 个不同的根,且 $\alpha_i\in\{\alpha^j\mid 1\leqslant j\leqslant 2^r-1\}$. $\boldsymbol{H}$是一个 $(n-k)\times n$ 矩阵.

证明 考虑到 $h(\sigma_2)g(\sigma_2)\boldsymbol{u}^{\mathrm{T}}=0$,这里 $\boldsymbol{u}^{\mathrm{T}}\in\mathrm{Span}\{\boldsymbol{e}_0^{\mathrm{T}},\boldsymbol{e}_1^{\mathrm{T}},\cdots,\boldsymbol{e}_{k-1}^{\mathrm{T}}\}$, 即消息空间中的任一消息. 取前式转置,得 $\boldsymbol{u}g(\sigma_2)^{\mathrm{T}}h(\sigma_2)^{\mathrm{T}}=0$. 显然,$\boldsymbol{u}g(\sigma_2)^{\mathrm{T}}=\boldsymbol{u}g(\sigma_1)=(c_0c_1\cdots c_{n-1})$ 是 $\mathrm{Ker}[h(\sigma_1)]$ 中的任一码向量. 而由引理 2 知 $h(\sigma_2)^{\mathrm{T}}=h(\sigma_1)$.再根据引理 4,将(14),(15)式代入,得 $(c_0c_1\cdots c_{n-1})h(\boldsymbol{T}_1\Lambda\boldsymbol{T}_1^{-1})=0$, 即 $(c_0c_1\cdots c_{n-1})\boldsymbol{T}_1h(\Lambda)=0$. 因此,有

$$\begin{aligned}&(c_0+c_1+\cdots+c_{n-1}\quad c_0+c_1\alpha+\cdots+c_{n-1}\alpha^{n-1}\quad\cdots\\ &c_0+c_1\alpha^{n-1}+\cdots+c_{n-1}(\alpha^{n-1})^{n-1})\\ &\times\begin{bmatrix}h_0+h_1+\cdots+h_k & & & \\ & h_0+h_1\alpha+\cdots+h_k\alpha^k & & 0\\ & & \ddots & \\ 0 & & & h_0+h_1\alpha^{n-1}+\cdots+h_k(\alpha^{n-1})^k\end{bmatrix}\\ &=0.\end{aligned} \tag{17}$$

(17)式中的矩阵显然是个对角矩阵. 考虑到在 F_{2^r} 的 2^r-1 个互异的非零元中有 k 个元是 $h(x)$ 的根,因此,在上述的对角矩阵中有 k 个元为 0, $n-k$ 个元为非零元. 已设 $\alpha_i,(1\leqslant i\leqslant n-k)$为 $g(x)$ 的根,因此有 $c_0+c_1\alpha_1+\cdots+c_{n-1}\alpha_1^{n-1}=0$, $c_0+c_1\alpha_2+$

$\cdots + c_{n-1}\alpha_2^{n-1} = 0, \cdots, c_0 + c_1\alpha_{n-k} + \cdots + c_{n-1}\alpha_{n-k}^{n-1} = 0$。把它写成矩阵的形式，即

$$\begin{bmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1} \\ \vdots & & & \\ 1 & \alpha_{n-k} & \cdots & \alpha_{n-k}^{n-1} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix} = 0, \tag{18}$$

式中的矩阵显然为一个 $(n-k)\times n$ 矩阵 $\boldsymbol{H}$，它就是一般 BCH 码的奇偶校验矩阵。

这样，我们就证明了定理 4.这个定理说明了循环码的校验矩阵 $h(\sigma_1)$ 在 $n = 2^r - 1$ 的条件下，确可以通过适当的坐标变换(从 $\boldsymbol{e}_0^r, \boldsymbol{e}_1^r, \cdots, \boldsymbol{e}_{n-1}^r$ 变换到以特征向量 $(11\cdots1)^r$, $(1\alpha\cdots\alpha^{n-1})^r, \cdots, (1\alpha^{n-1}\cdots(\alpha^{n-1})^{n-1})$ 为基底的坐标系）表示成 BCH 码常用的校验矩阵的形式[4]。从而证明了 BCH 码的校验矩阵确是用循环变换的特征向量作基底时的一种表示形式。

推论　设 $r = 11$，那么由域 $F_{2^{11}}$ 中的 23 次本原单位根 β 的最小多项式 $g(x) = 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11}$[5] 是生成的 Golay 码的校验矩阵

$$\boldsymbol{H} = \begin{bmatrix} 1 & \beta & \cdots & \beta^{22} \\ 1 & \beta^2 & \cdots & (\beta^2)^{22} \\ & & \vdots & \end{bmatrix}, \tag{19}$$

其中 $\beta, \beta^2, \cdots$ 都是 $g(x)$ 的根。

不难看出，本节的结论都可以直接推广到定义在域 $F_q(q \neq 2)$ 上的循环码的情形，特别是 RS 码的情形。显然，本节的结果也可以推广到伪随机码的讨论。

3　结束语

本文仅采用坐标变换的几何方法导出了 BCH 码的校验矩阵的通用形式，从而给出了研究循环码理论的又一种方法，并把此种研究方法纳入到线性系统理论一般研究方法的框架之中。

参　考　文　献

[1] 万哲先. 代数和编码，北京：科学出版社，1968，第四章，§ 3和 § 5.

[2] 肖国镇. 科学通报，1980，25(17)：779—782.

[3] 韩京清，等. 线性系统理论代数基础. 沈阳：辽宁科学技术出版社，1985，180—224。

[4] 吴伯修，等. 信息论与编码. 南京：东南大学出版社，1991，170—172.

[5] McEliece R J. The Theory of Information and Coding. Massachusetts, USA: Addison-Wesley Publishing Company, 1977, 186—190.

A GEOMETRIC APPROACH TO CYCLIC CODES

Qian Linjun

(Suzhou Institute of Silk Textile Technology, Suzhou 215005)

Abstract　The cyclic codes are studied by using the geometric method. It is proved that the parity check matrix for BCH code is a representation form in the eigenvector basis. Thus the study on cyclic codes may be brought into the framework of linear system theory.

Key words　Cyclic codes, BCH code, Geometric approach