云南大学学报（自然科学版） 2001，24（2）：85~87 CN 53-1045/N ISSN 0258-7971
Journal of Yunnan University

$GF(2^m)$ 上线性码的自同构群的进一步研究*

王国栋，罗裕梅
（云南大学 数学系，云南 昆明 650091）

摘要：对已有的一个置换属于线性码 C 的自同构群的若干行之有效的判别准则及计算方法作进一步研究．并在此基础上进行简化，提出了一种寻求一个线性码的自同构群的颇为有效的方法．

关键词：线性码；置换群；自同构群；广义逆；简化运算
中图分类号：O 157 文献标识码：A 文章编号：0258-7971(2002)02-0085-03

我们知道线性码的自同构群在码的研究中，尤其是在译码中是很有用的，然而一般说来，寻求一个线性码的自同构群很困难．在文献[1]中，我们使用矩阵广义逆理论所给出的若干结论是颇为有效的．尽管如此，由于在码论中，一般计算量都非常大，因此很有必要对我们的结论作进一步研究和简化以减少计算工作量，有时这种减少的程度还相当可观．

对 $\sigma \in S_n$（n 次对称群）及有限域 $GF(2^m)$ 上的 n 维向量 $a=(a_1, a_2, \cdots, a_n)$，$a\sigma=(a_{\sigma(1)}, a_{\sigma(2)}, \cdots, a_{\sigma(n)})$．设 C 是一个 $[n, k]$ 线性码，C 的自同构群用 $\mathrm{Aut}\,C$ 记之，即 $\mathrm{Aut}\,C=\{\sigma \in S_n \mid C\sigma=C\}$，$\mathrm{Aut}\,C$ 是 S_n 的子群．

在文献[1]中，我们曾得出如下2个定理：

定理1[1] 设 C 是 $[n, k]$ 线性码，行满秩阵 $M_{k\times n}$ 是 C 的生成阵，则对 $\sigma \in S_n$，$\sigma \in \mathrm{Aut}\,C \Leftrightarrow$ 矩阵方程 $XM=MA$（X 可逆）有解 $\Leftrightarrow MAM^{(1)}M=MA$（$M^{(1)}$ 是 M 的 $\{1\}-$ 逆），其中矩阵 $A=a_{ij}=(\delta_{i,\sigma(j)})$，$\delta_{i,k}=\begin{cases}1 & i=k\\ 0 & i\neq k\end{cases}$ Kronecker 符号．在有解时，只有唯一解 $X_0=MAM^{(1)}$（可逆）$\Leftrightarrow$ 核 $N(M)$ 是 A 的不变子空间 $\Leftrightarrow MAH^T=0$（其中 H 是 C 的校验阵，且设 H 行满秩）．此式将生成阵和一致校验阵有趣地联系起来．

在定理1的基础上又得出

定理2[1] 设 C 是 $[n, k]$ 线性码，令 $G=\mathrm{Aut}\,C$．$A \in G$ 则 $\Phi: A \to MAM^{(1)}=K \in GL(k, F)$（一般线性群）是 G 到 $\Phi(G)$ 的满同态射．$\Phi(G)$ 是 $GL(k, f)$ 的子群，且商群

$G/\mathrm{Ker}\,\Phi \cong \Phi(G)$，核 $\mathrm{Ker}\,\Phi=\{A \in G \mid \Phi(A)=MAM^{(1)}=I_K\}$．

若 Φ 是单射且 $\Phi(G)=GL(k, F)$ 则 $G \cong GL(k, F)$．

由于 $\mathrm{Aut}\,C \cong \mathrm{Aut}\,C^{\perp}$（$C$ 的对偶码），所以若校验阵 $H_{(n-k)\times n}$ 是行满秩的，则也可用 H 代替上面的 M 来进行讨论，得出完全相同的结果．

注意 有时 M，H 不一定行满秩，则可这样处理：因存在可逆阵 E 使 $EM=\begin{pmatrix}\widetilde{M}\\ 0\end{pmatrix}$，$\widetilde{M}$ 行满秩，所以可用 $\widetilde{M}$ 代替 M 进行讨论．又存在可逆阵 T 使 $TH=\begin{pmatrix}\overline{H}\\ 0\end{pmatrix}$，$\overline{H}$ 行满秩，而 $Hx=0$ 与 $\overline{Hx}=0$ 同解，因此可用 $\overline{H}$ 代替 H 来进行讨论．故不失一般性，可设 M，H 行满秩．

有限域上矩阵的 $\{1\}-$ 逆的计算问题．

据文献[1]，对有限域上的任何一个矩阵，它的 $\{1\}-$ 逆是存在的[2]，实际上我们仍可仿照文献[3]的方法求取之：设 B 是一个秩为 r 的 $k\times n$ 阵，

* 收稿日期：2001-09-08
基金项目：云南省自然科学基金资助项目（96F020Q）；云南省省校合作项目：“金融数学学科建设”．
作者简介：王国栋（1938- ），男，云南人，教授，主要从事代数编码理论与矩阵论的研究．

存在可逆阵 E 与置换阵 P 使 $EB = \begin{pmatrix} R \\ 0 \end{pmatrix}$ 是 Hermite 型的, 又 $EBP = \begin{pmatrix} I_r & Q \\ 0 & 0 \end{pmatrix}$, 于是 $P\begin{pmatrix} I_r & \\ & L \end{pmatrix}E$ 是 B 的 $\{1\}$ - 逆, L 是适当阶的任何矩阵, 令 $L = 0$, 则它是 B 的 $\{1, 2\}$ - 逆.

定理**3** 设 C 是一个 $[n, k]$ 线性码, 而行满秩阵 $M_{k\times n}$ 是 C 的生成阵, 则存在可逆阵 E 使 $_kE_nM_n = R$ (Hermite 型), 又存在置换阵 P 使 $EMP = [I_k\ Q]$. 于是

$$\sigma \in \mathrm{Aut}\,C \Leftrightarrow MAP_1R = MA, \text{ 其中}$$

$$A = (\delta_{i,\sigma(j)}) \leftarrow\sigma, \tag{1}$$

P_1 是 P 的前 k 列所构成的子阵, R 与 P_1 可由行初等变化与列交换得出.

证明 据定理 1 及 $MAM^{(1)}M = MA\left(P\begin{pmatrix} I_k \\ 0 \end{pmatrix}E\right)M = MAP\begin{pmatrix} R \\ 0 \end{pmatrix} = MAP_1R$ 知.

定理**4** 若 C 的生成阵为 $M = [M_1\ M_2]_{k\times n}$, 其中 M_1 是 k 阶可逆阵, 则令 $A = (\delta_{i,\sigma(j)}) \leftarrow\sigma$ 将 A 分块成 $A = [A_1\ A_2]$, 其中 A_1 是 $n \times k$ 阵, 则

$$\sigma \in \mathrm{Aut}\,C \Leftrightarrow MA_1M_1^{-1}M_2 = MA_2, \tag{2}$$

证明 令 $E = M_1^{-1}$, 则 $EM = M_1^{-1}[M_1\ M_2] = [I_k\ M_1^{-1}M_2] \Rightarrow M$ 的 $\{1\}$ - 逆 $M^{(1)} = \begin{pmatrix} I_k \\ 0 \end{pmatrix}M_1^{-1} = \begin{pmatrix} M_1^{-1} \\ 0 \end{pmatrix}$, 因此

$$MAM^{(1)}M = M[A_1\ A_2]\begin{pmatrix} M_1^{-1}M \\ 0 \end{pmatrix} =$$

$$MA_1M_1^{-1}M = MA_1M_1^{-1}[M_1\ M_2] =$$

$$[MA_1\ MA_1M_1^{-1}M_2].$$

由定理 1 知 (2) 成立.

特别, 若 C 是系统码, 即 C 的生成阵是 $M = [I_k\ M_2]$ 的线性码, 则

$$\sigma \in \mathrm{Aut}\,\xi \Leftrightarrow MA_1M_2 = MA_2. \tag{3}$$

注意 若 C 的校验阵是 $H = [H_1\ H_2]$ 且 H_1 可逆, 则对 $\sigma \in S_n$, $A = (\delta_{i,\sigma(j)}) \leftarrow\sigma$, 则

$$\sigma \in \mathrm{Aut}\,C \Leftrightarrow HA_1H_1^{-1}H_2 = HA_2. \tag{4}$$

特别若 $H = [I\ H_2]$, 则 $\sigma \in \mathrm{Aut}\,\xi \Leftrightarrow HA_1H_2 = HA_2$. 倘若 $H = [H_1\ I]$, 则 C 的生成阵是 $M = [I\ -H_1^T]$, 即 C 是系统码, 可由 (3) 进行判断. 因此有时用校验阵处理反而方便.

下面给出的定理 5 对寻求 $\mathrm{Aut}\,C$ 很有帮助.

令置换 $\sigma = \begin{pmatrix} 1 & \cdots & k & \cdots & n \\ i_1 & \cdots & i_k & \cdots & i_n \end{pmatrix}$ $\leftrightarrow$置换阵 $A = (\delta_{i,\sigma(j)}) = (e_{i_1}\ \cdots\ e_{i_k}\ \cdots\ e_{i_n})$, 其中 $e_{i_t}^T = (0\cdots\overset{i_t}{1}\cdots 0)$ 是单位列向量, $t = 1, 2, \cdots, n$.

事实上, 因 $\delta_{i_t,\sigma(s)} = \begin{cases} 1 & s = t, \\ 0 & s \neq t. \end{cases}$ 所以 $\delta_{i_t,\sigma(t)} = \delta_{i_t,i_t} = 1$, 即 A 中位置 (i_t, i_t) 上的元为 1, 其余为 0, 所以 $A = (e_{i_1}\ \cdots\ e_{i_k}\ \cdots\ e_{i_n})$.

令 $N = \{1, 2, \cdots n\}$, 任意取定 k 个互异的正整数 $i_1, i_2, \cdots, i_k \in N$, 令 $N - \{i_1, i_2, \cdots, i_k\} = \{i_{k+1}, i_{k+2}, \cdots, i_n\}$, 设 $x_{k+1}x_{k+2}\cdots x_n$ 是 $i_{k+1}, i_{k+2}, \cdots, i_n$ 的任意排列, 则 $\sigma = \begin{pmatrix} 1 & \cdots & k & k+1 & \cdots & n \\ i_1 & \cdots & i_k & x_{k+1} & \cdots & x_n \end{pmatrix} \in S_n$ (n 次对称群), 这样的 σ 共有 $(n-k)!$ 个.

定理**5** 设 C 是 $[n, k]$ 线性码, $k \times n$ 阶行满秩阵 $M = [M_1\ M_2] = [T_1\ T_2\ \cdots\ T_n]$ 是 C 的生成阵, 其中 T_i 是 M 的第 i 列 (T_i 可能等于 T_j). 任意取定 k 个互异的正整数 $i_1, i_2, \cdots, i_k \in N$, 构造 $n \times k$ 阶阵 $A_1 = (e_{i_1}\ e_{i_2}\ \cdots e_{i_k})$, 则 $MA_1 = [T_{i_1}\ T_{i_2}\ \cdots\ T_{i_k}]$, 又设 $x_{k+1}x_{k+2}\cdots x_n$ 是前面所说的 $i_{k+1}, i_{k+2}, \cdots, i_n$ 的任意排列. 作 $A = [A_1\ A_2] = (e_{i_1}\ \cdots e_{i_k}\ e_{x_{k+1}}\ \cdots e_{x_n}) \leftarrow\sigma = \begin{pmatrix} 1 & \cdots & k & k+1 & \cdots & n \\ i_1 & \cdots & i_k & x_{k+1} & \cdots & x_n \end{pmatrix} \in S_n$, 若 M_1^{-1} 存在, 则

$$\sigma \in \mathrm{Aut}\,C \Leftrightarrow MA_1M_1^{-1}M_2 =$$

$$[T_{x_{k+1}}\ T_{x_{k+2}}\ \cdots T_{x_n}]_{k\times(n-k)}. \tag{5}$$

证明 因上面所作出的 A 是一个置换阵, 因此由 $MA_1 = [T_{i_1}\ T_{i_2}\ \cdots\ T_{i_k}] \Rightarrow MA_2 = [T_{x_{k+1}}\ T_{x_{k+2}}\ \cdots\ T_{x_n}]$, 再由定理 4 便得出所要的结论.

倘若 M_1^{-1} 不存在, 则有置换阵 P, 使 $MP = [\widetilde{M}_1, \widetilde{M}_2]$ 且 $\widetilde{M}_1$ 可逆.

定理 4 的优点在于: 只需由 $A_n^k = \frac{n!}{(n-k)!}$ 个排列 $i_1\ i_2\ \cdots\ i_k$ 便能借助 (5) 式找出整个的 $\mathrm{Aut}\,C$, 在很多情况下, $A_n^k \ll |S_n| = n! = (n-k)!A_n^k$.

下面再通过 $GF(2)$ 上长为 p 的二次剩余码 C 的延长码 $\hat{C}$ 来说明我们所给出的方法的实施过

程. C 的生成阵是

$$G=\left(\begin{array}{ccccccc|c}1&0&0&1&0&1&1&0\\1&1&0&0&1&0&1&0\\1&1&1&0&0&1&0&0\\0&1&1&1&0&0&1&0\\1&0&1&1&1&0&0&0\\0&1&0&1&1&1&0&0\\0&0&1&0&1&1&1&0\\1&1&1&1&1&1&1&1\end{array}\right),$$

令 $M=[M_1\ M_2]=$

$$\left(\begin{array}{cccc|cccc}1&0&0&1&0&1&1&0\\1&1&0&0&1&0&1&0\\1&1&1&0&0&1&0&0\\1&1&1&1&1&1&1&1\end{array}\right),$$

则 M 的行向量组是 G 的行向量组的极大无关组, 且

$$M_1^{-1}=\begin{pmatrix}1&0&1&1\\1&1&1&1\\0&1&1&0\\0&0&1&1\end{pmatrix},$$

$$M_1^{-1}M_2=\begin{pmatrix}1&1&0&1\\0&1&1&1\\1&1&1&0\\1&0&1&1\end{pmatrix}.$$

于是可用定理 5 的方法求 $\mathrm{Aut}C$. 例如取置换阵

$$A=[A_1\mid A_2]=[e_1e_2e_3e_5\mid e_4e_6e_8e_7],$$

则

$$MA_1M_1^{-1}M=\begin{pmatrix}1&1&0&1\\0&0&0&1\\0&1&0&0\\1&1&1&1\end{pmatrix}=MA_2\Rightarrow A\in\mathrm{Aut}C.$$

由定理 4, 原则上可对 S_8 中的 $8!$ 个置换逐个进行检验来找出整个 $\mathrm{Aut}C$, 但这样做计算量太大. 采用定理 5 的方法, 仅需对 $A_8^4=8\cdot7\cdot6\cdot5$ 个排列 $i_1i_2i_3i_4$ 进行处理, 由于 $|S_8|=24\cdot A_8^4$, 因此计算量可减少近 24 倍(相当可观). 我们用此法编制了通用计算程序不仅证实了特殊线性群 PSL(7) 中的 168 个元属于 $\mathrm{Aut}C$, 而且还准确地求出了整个的 $\mathrm{Aut}C$, 它包含 1 344 个 8 元置换[4], 效果很好, 可见定理 5 的方法是很有效的.

[参　考　文　献]

[1] 王国栋, 石剑平. 线性码的自同构群[J]. 高等学校计算数学学报, 2000, 11(增刊): 65—67.

[2] PEARL M H. Generalized inverses of matrices with entries taken from an arbitrary field[J]. Linear Algebra and Applications, 1968, 1(5): 571—587.

[3] Ben-Isreal A, GREVILLE T N E. Generalized inverses: Theory and applications[M]. New York: John Wiley & Sons, 1974.

[4] MACWILLIAMS F J, SLOANE N J A. The theory of error-correcting codes[M]. New York: Orth-holland Publishing Company, 1977.

The Further Research about the Automorphism Group of a Linear Code over $GF(2^m)$

WANG Guo-dong, LUO Yu-mei

(Department of Mathematics, Yunnan University, Kunming 650091, China)

Abstract: On basis of several effective methods to judge a permutation whether belong to the Automorphism group of Linear code a more effective method for the Automorphism group of Linear code is given.

Key words: linear code; automorphism group; permutation group; generalized inverse; simplified operation