云南大学学报（自然科学版），2004，26（2）：93~97　　CN 53-1045/N　ISSN 0258-7971
Journal of Yunnan University

二次剩余码的自同构群*

王国栋，杨　洋，陆正福
（云南大学 数学系，云南 昆明　650091）

摘要：针对二次剩余码的自同构置换建立了判定定理，利用矩阵的广义逆理论研究了二次剩余码的扩展码的自同构群，并用实例验证了相关结论.

关键词：二次剩余(QR)码；单式阵群；自同构群；广义逆
中图分类号：O 157　　文献标识码：A　　文章编号：0258-7971(2004)02-0093-05

线性码的自同构群研究是代数编码中的一项基础研究，它对于译码算法的设计，密码体制的设计和分析都具有重要的基础意义. 将自同构置换表示为置换矩阵，并将矩阵的广义逆理论引入到线性码的自同构群的研究中，可以见之于文献[1,2]. 文献[1]研究了二元有限域 $GF(2)$ 上线性码的自同构群，文献[2]进一步研究了一般有限域 $GF(p^m)$ 上线性码的自同构群，所得结果具有可推广的理论价值，其中的计算方法属于有效方法. 本文利用文献[1,2]的结果研究二次剩余码的自同构群. 为此首先将文献[2]的一些主要结论开列于下.

设 $\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}\in S_n$（$n$ 次对称群）. σ 对应于一个置换阵 $\boldsymbol{A}=(\delta_i,\sigma(j))=(e_{i_1}\ e_{i_2}\ \cdots\ e_{i_n})$，$e_{i_t}$ 是单位列向量（$t=1,2,\cdots,n$），则 $S_n\cong\mathscr{P}$（置换阵群）.

称 $GF(p^m)$ 上的 $n\times n$ 阵 $\tilde{\boldsymbol{A}}$ 为单式阵，若 $\tilde{\boldsymbol{A}}$ 的每行每列正好有一个非零元. 于是可表 $\tilde{\boldsymbol{A}}=\boldsymbol{AD}$，其中 $\boldsymbol{A}\in\mathscr{P},\boldsymbol{D}\in\mathscr{D}$（$n$ 阶非异对角阵群）.

在本文中，将置换阵 $\boldsymbol{A}=(e_{i_1}\ e_{i_2}\ \cdots\ e_{i_n})$ 简记成 $(e_{i_1 i_2\cdots i_n})$，对角阵 $\boldsymbol{D}$ 简记成 $\boldsymbol{D}=\langle\lambda_1\ \lambda_2\ \cdots\ \lambda_n\rangle$.

在文献[2]中，我们曾证明了如下命题，在本文二次剩余码的讨论中需要用到它们.

命题 **1**[2]　对置换阵 $\boldsymbol{A}=(e_{i_1 i_2\cdots i_n})$，对角阵 $\boldsymbol{D}=\langle\lambda_1\ \lambda_2\ \cdots\ \lambda_n\rangle$，有等式 $\boldsymbol{DA}=\boldsymbol{A}\overline{\boldsymbol{D}}$，其中 $\overline{\boldsymbol{D}}=\langle\lambda_{i_1}\ \lambda_{i_2}\ \cdots\ \lambda_{i_n}\rangle$.

命题 **2**[2]　对 $\boldsymbol{A}=(e_{i_1 i_2\cdots i_n})$，$\boldsymbol{D}=\langle\lambda_1\ \lambda_2\ \cdots\ \lambda_n\rangle$. 将 $\boldsymbol{D}$ 写成 $\boldsymbol{D}_0=\langle\lambda_1^{(0)}\ \lambda_2^{(0)}\ \cdots\ \lambda_n^{(0)}\rangle$ 并令

$$\boldsymbol{D}_t=\langle\lambda_1^{(t)}\ \lambda_2^{(t)}\ \cdots\ \lambda_n^{(t)}\rangle=\langle\lambda_{i_1}^{(t-1)}\ \lambda_{i_2}^{(t-1)}\ \cdots\ \lambda_{i_n}^{(t-1)}\rangle\qquad(t=0,1,2,\cdots,k-1),$$

则单式阵 $\tilde{\boldsymbol{A}}=\boldsymbol{AD}=\boldsymbol{AD}_0$ 的 k 次幂

$$\tilde{\boldsymbol{A}}^k=(\boldsymbol{AD})^k=\boldsymbol{A}^k\boldsymbol{D}_{k-1}\boldsymbol{D}_{k-2}\cdots\boldsymbol{D}_1\boldsymbol{D}_0.\qquad(1)$$

此式对计算 $\tilde{\boldsymbol{A}}$ 的阶很方便.

设 C 是 $GF(p^m)$ 上的一个 $[n,k]$ 线性码，C 的自同构群

$$\mathrm{Aut}C=\{\tilde{\boldsymbol{A}}=\boldsymbol{AD}\in\mathscr{PD}\mid\forall c\in C,c\tilde{\boldsymbol{A}}\in C\}.$$

命题 **3**[2]　设 C 是 $GF(p^m)$ 上的 $[n,k]$ 线性码，行满秩的 $k\times n$ 矩阵 $\boldsymbol{M}$ 是 C 的生成阵，则对

* 收稿日期：2003-08-10
基金项目：云南省自然科学基金资助项目(2002F0012M)；云南省教育厅科研基金项目(0111155)；云南大学理(工)科校级科研重点项目(2003Z010C).
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方面的研究.

$$\tilde{A} = AD \in \mathscr{P}, \tilde{A} \in \mathrm{Aut}\, C \Leftrightarrow MADM^{(1)}M = MAD, \quad (2)$$

其中 $M^{(1)}$ 是 M 的任何一个{1}-逆.

对某些特殊情况(常用), 命题 3, 还可作如下简化(从而大大减少计算量). 即有:

定理 1 设[n, k]线性码 C 的生成阵被分块成 $M = [M_1\ M_2]$ 后, M_1 是 k 阶的可逆阵, 对单式阵 $\tilde{A} = AD$, 将 A, D 作如下分块:

$A = [A_1\ A_2]$ $D = \begin{bmatrix} D_1 & 0 \\ 0 & D_2 \end{bmatrix}$ (D_1, D_2 亦可逆), 则对

$$\tilde{A} = AD \in \mathscr{P}, \tilde{A} \in \mathrm{Aut}\, C \Leftrightarrow MA_1D_1M_1^{-1}M_2 = MA_2D_2, \quad (3)$$

证明 因此时 $M^{(1)} = \begin{bmatrix} M_1^{-1} \\ 0 \end{bmatrix}$, $M^{(1)}M = \begin{bmatrix} I_k & M_1^{-1}M_2 \\ 0 & 0 \end{bmatrix}$, 因此 $MADM^{(1)}M = [MA_1\ MA_2]\begin{bmatrix} D_1 & 0 \\ 0 & D_2 \end{bmatrix}\begin{bmatrix} I_k & M_1^{-1}M_2 \\ 0 & 0 \end{bmatrix} = [MA_1D_1\ MA_2D_2]\begin{bmatrix} I_k & M_1^{-1}M_2 \\ 0 & 0 \end{bmatrix} = [MA_1D_1\ MA_1D_1M_1^{-1}M_2]$. 所以由命题 3, $AD \in \mathrm{Aut}\, C \Leftrightarrow MADM^{(1)}M = MAD \Leftrightarrow MA_1D_1M_1^{(-1)}M_2 = MA_2D_2$, 证毕.

推论 1 若 C 是系统码, 即 $M_1 = I_k$, 则

$$AD \in \mathrm{Aut}\, C \Leftrightarrow MA_1D_1M_2 = MA_2D_2. \quad (4)$$

在二次剩余码的自同构群研究中, 除了遇上形如 AD 的单式阵外还会遇上 DA 类型的单式阵(见下例), 此时为了能应用定理, 需将 DA 作如下处理:

设 $D = \langle \lambda_1\ \lambda_2\ \cdots\ \lambda_n \rangle$, $A = (e_{i_1 i_2 \cdots i_n})$. 据命题 1, $DA = A\bar{D}$, $\bar{D} = \langle \lambda_{i_1}\ \lambda_{i_2}\ \cdots\ \lambda_{i_n} \rangle = \begin{bmatrix} \bar{D}_1 & 0 \\ 0 & \bar{D}_2 \end{bmatrix}$, 其中 $\bar{D}_1 = \langle \lambda_{i_1}\ \cdots\ \lambda_{i_k} \rangle$, 而 $\bar{D}_2 = \langle \lambda_{i_{k+1}}\ \cdots\ \lambda_{i_n} \rangle$. 于是由定理得出

$$DA \in \mathrm{Aut}\, C \Leftrightarrow A\bar{D} \in \mathrm{Aut}\, C \Leftrightarrow MA_1\bar{D}_1M_1^{-1}M_2 = MA_2\bar{D}_2 \quad (5)$$

现在用上面所建立的定理来讨论二次剩余码的自同构群问题.

设 p, l 是 2 个不相同的素数且 l 是 mod$p$ 的二次剩余, 用 Γ_1 及 Γ_2 代表 mod$p$ 的二次剩余及二次非剩余集合.

设商环 $$R = GF(l)[x]/(x^p - 1).$$

定义 1[3] 二次剩余码 Q, $\bar{Q}$, N, $\bar{N}$ 是商环 R 上的循环码(理想), 它们分别以 $q(x)$, $(x-1)q(x)$, $n(x)$, $(x-1)n(x)$ 为生成多项式, 其中

$$q(x) = \prod_{r \in \Gamma_1}(x - \alpha^r), \qquad n(x) = \prod_{n \in \Gamma_2}(x - \alpha^n).$$

它们的系数在有限域 $GF(l)$ 中, 其中 α 是 p 次原根, 它在 $GF(l)$ 的某个扩域中, 而且 $\bar{Q} \subset Q$, $\bar{N} \subset N$, $\dim Q = \dim N = \frac{1}{2}(p+1)$, 而 $\dim \bar{Q} = \dim \bar{N} = \frac{1}{2}(p-1)$.

下面我们来探讨二次剩余码 Q 的扩展码 $\hat{Q}$ 的自同构群问题, $\hat{Q}$ 是一个自对偶码, 即 $(\hat{Q})^{\perp} = \hat{Q}$. 它具有良好的性质.

我们以 $l = 3$, $p = 11$ 作为范例(其它二次剩余码的自同构群可类似地处理). 此时 $\Gamma_1 = \{1, 3, 4, 5, 9\}$, $\Gamma_2 = \{2, 6, 7, 8, 10\}$. 已知 $\hat{Q}$ 的生成阵是

$$G = \begin{bmatrix} \bar{G} & 0 \\ 1\ 1\ \cdots\ 1 & 1 \end{bmatrix}_{12 \times 12} \quad (GF(3)\text{ 上的矩阵})$$

其中 $\bar{G}$ 可由 $\bar{Q}$ 的幂等多项式 $F_q(x) = 1 + x^2 + x^6 + x^7 + x^8 + x^{10}$ 作出. 而 $\begin{bmatrix} \bar{G} \\ 1\ 1\ \cdots\ 1 \end{bmatrix}$ 便是 Q 的生成阵. Q 是[11, 6, 5]的 Golay 码, $\hat{Q}$ 是此 Golay 码的扩展码.

因 $l = 3 > 2$, 所以 Aut($\hat{Q}$) 由保持 $\hat{Q}$ 不变的所有单式阵 $\tilde{A} = AD$ 构成(单式阵群, 我们已在文献[1]

中作了较详细的研究). 由于 Q 是线性的, 因此若 $\tilde{A} \in \mathrm{Aut}(Q)$, 则 $\forall t \in GF(l)$, 有 $t(\boldsymbol{AD}) \in \mathrm{Aut}(Q)$. 为方便计算, 只考虑 $t = 1$ 的情况, 并把这样得到的 $\mathrm{Aut}(Q)$ 的元集记为 $\mathrm{Aut}(Q)^+$ (见文献[3]).

定义 **2**[3, 4]　设 p 是形如 $8m \pm 1$ 的素数, 则 $\{0, 1, \cdots, p-1, \infty\}$ (即一维射影空间) 的一切形如

$$y \to \frac{ay + b}{cy + d}, \qquad a, b, c, d \in GF(p) \text{ 且 } ad - bc = 1$$

的置换称为特殊射影线性群, 记为 $PSL_2(p)$, 且 $|PSL_2(p)| = \frac{1}{2}(p^2 - 1)p$. $PSL_2(p)$ 可由 3 个置换

$$S: y \to y + 1, \quad V: y \to \rho^2 y, \quad T: y \to -1/y$$

生成(其中 ρ 是 $GF(p)$ 中的本原元).

据 Gleanson-Prange 定理[3]: $\mathrm{Aut}(Q)^+$ 包含一个与 $PSL_2(p)$ 同构的群, 此群可由 $\boldsymbol{S}$, $\boldsymbol{V}$ 及 $\boldsymbol{T}'$ 生成, 其中 $\boldsymbol{T}'$ 是 $\boldsymbol{T}$ 的如下单式推广, 即对向量 $\boldsymbol{C} = (C_0, C_1, \cdots, C_{p-1}, C_\infty)$, 若 $\boldsymbol{C}$ 的分量的脚标 $i = \infty$ 及 $i \in \Gamma_1$, 则将 C_i 乘以 1 后, 再作用置换 $\boldsymbol{T}: i \to -1/i$; 若 C 的分量的脚标 $i = 0$ 及 $i \in \Gamma_2$, 则将 C_i 乘以 (-1) 后, 再作用置换 $\boldsymbol{T}: i \to -1/i$. 准上, 对于 $l = 3$, $p = 11$ 时, 因 $\Gamma_1 = \{1, 3, 4, 5, 9\}$, $\Gamma_2 = \{2, 6, 7, 8, 10\}$. 于是

(i) $S = (0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10)(\infty)$.

(ii) 因 2 是 $GF(11)$ 的本原元, 所以令 $V: y \to 4y$, 则得出

$$\boldsymbol{V} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \infty \\ 0 & 4 & 8 & 1 & 5 & 9 & 2 & 6 & 10 & 3 & 7 & \infty \end{pmatrix}.$$

(iii) 由于 $\boldsymbol{T} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \infty \\ \infty & 10 & 5 & 7 & 8 & 2 & 9 & 3 & 4 & 6 & 1 & 0 \end{pmatrix}$. 所以据 $\boldsymbol{T}'$ 的定义

$$\boldsymbol{CT}' = (2C_0, C_1, 2C_2, C_3, C_4, C_5, 2C_6, 2C_7, 2C_8, C_9, 2C_{10}, C_\infty)\boldsymbol{T} = (2C_\infty, C_{10}, 2C_5, C_7, C_8, C_2, 2C_9, 2C_3, 2C_4, C_6, 2C_1, C_0).$$

兹用本文的推论来验证 $\boldsymbol{S}$, $\boldsymbol{V}$, $\boldsymbol{T}' \in \mathrm{Aut}(Q)^+$, 经计算 6×12 阶的行满秩阵 ($GF(3)$ 上的)

$$\boldsymbol{M} = [\boldsymbol{M}_1\ \boldsymbol{M}_2] = \left[\begin{array}{cccccc|cccccc} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right],$$

其中 $\boldsymbol{M}_1^{-1} = \begin{bmatrix} 1 & 0 & 2 & 2 & 0 & 1 \\ 0 & 1 & 0 & 2 & 2 & 1 \\ 0 & 0 & 1 & 1 & 0 & 2 \\ 2 & 0 & 1 & 2 & 1 & 1 \\ 0 & 2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 2 & 2 & 2 & 2 \end{bmatrix}$, $\boldsymbol{M}_1^{-1}\boldsymbol{M}_2 = \begin{bmatrix} 2 & 2 & 1 & 2 & 0 & 1 \\ 0 & 2 & 2 & 1 & 2 & 1 \\ 2 & 2 & 0 & 1 & 1 & 2 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 2 & 2 & 2 & 1 & 0 \\ 1 & 2 & 1 & 0 & 2 & 2 \end{bmatrix}$

的行是 Q 的生成阵 $\boldsymbol{G}$ 的行向量组的极大无关组, 所以 $Q = \mathrm{Span}\,\boldsymbol{G} = \mathrm{Span}(\boldsymbol{M})$ (行生成空间). 于是由推论知:

对 $\tilde{A} = \boldsymbol{AD} \in \mathscr{R}$, $\tilde{A} \in \mathrm{Aut}Q^+ \Leftrightarrow \boldsymbol{MA}_1\boldsymbol{D}_1\boldsymbol{M}_1^{-1}\boldsymbol{M}_2 = \boldsymbol{MA}_2\boldsymbol{D}_2$,

其中 $\boldsymbol{D} = \begin{bmatrix} \boldsymbol{D}_1 & 0 \\ 0 & \boldsymbol{D}_2 \end{bmatrix}$.

为了方便起见, 将上面得出的 $\boldsymbol{S}$, $\boldsymbol{V}$, $\boldsymbol{T}$ 及 $\boldsymbol{T}'$ 作改写: 以 $i+1$ 代替 i, $i \in GF(11)$, 且以 12 代替 ∞ (即射影直线上的无穷远点), 并写出上面置换对应的矩阵, 则

$$\boldsymbol{S} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 1 & 12 \end{pmatrix} \leftrightarrow \text{置换阵 } \boldsymbol{A}_S = (e_{2\,3\,4\,5\,6\,7\,8\,9\,10\,11\,1\,12}),$$

$$\boldsymbol{V}=\begin{pmatrix}1&2&3&4&5&6&7&8&9&10&11&12\\1&5&9&2&6&10&3&7&11&4&8&12\end{pmatrix}\leftrightarrow\text{置换阵 }\boldsymbol{A}_V=(e_{1\,5\,9\,2\,6\,10\,3\,7\,11\,4\,8\,12}),$$

$$\boldsymbol{T}=\begin{pmatrix}1&2&3&4&5&6&7&8&9&10&11&12\\12&11&6&8&9&3&10&4&5&7&2&1\end{pmatrix}\leftrightarrow\text{置换阵 }\boldsymbol{A}_T=(e_{12\,11\,6\,8\,9\,3\,10\,4\,5\,7\,2\,1}).$$

由 $\boldsymbol{T}'$ 的定义知, 它所对应的矩阵是一个单式阵 $\tilde{\boldsymbol{A}}=\boldsymbol{D}\boldsymbol{A}_T$, 其中 $\boldsymbol{D}=\langle 2\ 1\ 2\ 1\ 1\ 1\ 2\ 2\ 2\ 1\ 2\ 1\rangle$. 为了利用(5) 式来判断 $\boldsymbol{T}'$ 是否属于 $\mathrm{Aut}(Q)^+$. 利用命题 1, 将 $\tilde{\boldsymbol{A}}$ 写成

$$\tilde{\boldsymbol{A}}=\boldsymbol{D}\boldsymbol{A}_T=\boldsymbol{A}_T\bar{\boldsymbol{D}},\ \text{其中 }\bar{\boldsymbol{D}}=\langle 1\ 2\ 1\ 2\ 2\ 2\ 1\ 1\ 1\ 2\ 1\ 2\rangle,$$

并将 $\boldsymbol{A}_T$ 及 $\bar{\boldsymbol{D}}$ 作如下分块: $\boldsymbol{A}_{T_1}=(e_{12\,11\,6\,8\,9\,3})$, $\boldsymbol{A}_{T_2}=(e_{10\,4\,5\,7\,2\,1})$, $\bar{\boldsymbol{D}}_1=\langle 1\ 2\ 1\ 2\ 2\ 2\rangle$, $\bar{\boldsymbol{D}}_2=\langle 1\ 1\ 1\ 2\ 1\ 2\rangle$, 则经计算有

$$\boldsymbol{M}\boldsymbol{A}_{T_1}\bar{\boldsymbol{D}}_1\boldsymbol{M}_1^{-1}\boldsymbol{M}_2=\begin{bmatrix}0&0&0&2&0&2\\1&1&0&0&1&2\\1&0&1&0&1&0\\1&1&0&0&0&2\\0&1&1&2&1&2\\1&1&1&2&1&2\end{bmatrix}=\boldsymbol{M}\boldsymbol{A}_{T_2}\bar{\boldsymbol{D}}_2\Rightarrow\boldsymbol{T}'\in\mathrm{Aut}(\boldsymbol{A})^+\ (\text{由(5) 式}).$$

类似地可推断 $\boldsymbol{S}$, $\boldsymbol{V}\in\mathrm{Aut}Q^+$ (作 mod 3 运算), 此时只要令 $\boldsymbol{D}=\boldsymbol{I}_p$ 即可.

下面来算由 $\boldsymbol{S}$, $\boldsymbol{V}$, $\boldsymbol{T}'$ 所生成的群的阶, 为此先求 $\boldsymbol{T}'$ 的阶, 即 $\tilde{\boldsymbol{A}}=\boldsymbol{A}_T\boldsymbol{D}$ 的阶. 因 $|\boldsymbol{T}|=2$, 知 $|\boldsymbol{A}_T|=2$, 由命题 2, 令

$$\bar{\boldsymbol{D}}=\bar{\boldsymbol{D}}_0=\langle 1\ 2\ 1\ 2\ 2\ 2\ 1\ 1\ 1\ 2\ 1\ 2\rangle,$$

因 $\boldsymbol{A}_T=(e_{12\,11\,6\,8\,9\,3\,10\,4\,5\,7\,2\,1})$, 所以

$\bar{\boldsymbol{D}}_1=\langle 2\ 1\ 2\ 1\ 1\ 1\ 2\ 2\ 2\ 1\ 2\ 1\rangle$, 显然 $\bar{\boldsymbol{D}}_1\bar{\boldsymbol{D}}_0=2\boldsymbol{I}$.

从而 $\tilde{\boldsymbol{A}}^2=(\boldsymbol{A}_T\bar{\boldsymbol{D}})^2=\boldsymbol{A}_T^2\bar{\boldsymbol{D}}_1\bar{\boldsymbol{D}}_0=2\boldsymbol{I}$, $\tilde{\boldsymbol{A}}^3=2\tilde{\boldsymbol{A}}$, $\tilde{\boldsymbol{A}}^4=\boldsymbol{I}$. 所以 $|\tilde{\boldsymbol{A}}|=4$. 因此

$\boldsymbol{V}^i\boldsymbol{S}^j(\boldsymbol{T}')^k\boldsymbol{S}^l\in\mathrm{Aut}(Q)^+$, 其中 $0\leqslant i<5$, $0\leqslant j, l<11$, $0\leqslant k<4$.

一个更有启发的例子是 $l=11$, $p=7$ 的二次剩余码, 此时 $\Gamma_1=\{1,2,4\}$, $\Gamma_2=\{3,6,5\}$, Q 的幂等多项式是 $F_q(x)=2+4(x+x^2+x^4)+10(x^3+x^6+x^5)$. Q 的扩展码 $\bar{Q}$ 的生成矩阵是

$$\begin{bmatrix}\bar{\boldsymbol{G}}&0\\1\cdots1&2\end{bmatrix},\ (\bar{Q})^{\perp}=\bar{Q},$$

且行满秩矩阵 $\boldsymbol{M}=[\boldsymbol{M}_1\ \boldsymbol{M}_2]=\begin{bmatrix}2&4&4&10&\cdot&4&10&10&0\\10&2&4&4&\cdot&10&4&10&0\\10&10&2&4&\cdot&4&10&4&0\\1&1&1&1&\cdot&1&1&1&2\end{bmatrix}$ 可作为 $\bar{Q}$ 的生成阵($GF(11)$ 上的矩阵),

$$\boldsymbol{M}_1^{-1}=\begin{bmatrix}1&10&8&6\\3&2&2&9\\1&3&2&3\\6&7&10&5\end{bmatrix},\ \boldsymbol{M}_1^{-1}\boldsymbol{M}_2=\begin{bmatrix}10&4&5&1\\5&1&1&7\\1&1&7&6\\7&6&10&10\end{bmatrix}(\text{作 mod 11 运算}),$$

$$\boldsymbol{S}=\begin{pmatrix}1&2&3&4&5&6&7&8\\2&3&4&5&6&7&1&8\end{pmatrix}\leftrightarrow\boldsymbol{A}_S=(e_{2\,3\,4\,5\,6\,7\,1\,8}),$$

$$\boldsymbol{V}=\begin{pmatrix}1&2&3&4&5&6&7&8\\1&3&5&7&2&4&6&8\end{pmatrix}\leftrightarrow\boldsymbol{A}_V=(e_{1\,3\,5\,7\,2\,4\,6\,8})\quad(\text{取 }\rho=3),$$

$$\boldsymbol{T}=\begin{pmatrix}1&2&3&4&5&6&7&8\\8&7&4&3&6&5&2&1\end{pmatrix}\leftrightarrow\boldsymbol{A}_T=(e_{8\,7\,4\,3\,6\,5\,2\,1}).$$

T' ←→单式阵 $DA_T = A_T\overline{D}$, D = 〈10 1 1 10 1 10 10 1〉, $\overline{D}$ = 〈1 10 10 1 10 1 1 10〉则 $T' \in \mathrm{Aut}(Q)^+$. 事实上, 将 A_T 及 $\overline{D}$ 分块为

$A_{T_1} = (e_{8743})$, $A_{T_2} = (e_{6521})$, $\overline{D}_1$ = 〈1 10 10 1〉, $\overline{D}_2$ = 〈10 1 1 10〉, 则

$$MA_{T_1}\overline{D}_1M_1^{-1}M_2 = \begin{bmatrix} 0 & 10 & 10 & 4 \\ 0 & 10 & 4 & 4 \\ 0 & 4 & 4 & 2 \\ 2 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & & & \\ & 10 & & \\ & & 10 & \\ & & & 1 \end{bmatrix} \begin{bmatrix} 10 & 4 & 5 & 1 \\ 5 & 1 & 1 & 7 \\ 1 & 1 & 7 & 6 \\ 7 & 6 & 10 & 10 \end{bmatrix} = \begin{bmatrix} 1 & 4 & 4 & 9 \\ 7 & 10 & 2 & 1 \\ 1 & 4 & 10 & 1 \\ 10 & 1 & 1 & 10 \end{bmatrix}$$

$$MA_{T_2}\overline{D}_2 = \begin{bmatrix} 10 & 4 & 4 & 2 \\ 4 & 10 & 2 & 10 \\ 4 & 4 & 10 & 10 \\ 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 10 & & & \\ & 1 & & \\ & & 1 & \\ & & & 10 \end{bmatrix} = \begin{bmatrix} 1 & 4 & 4 & 9 \\ 7 & 10 & 2 & 1 \\ 1 & 4 & 10 & 1 \\ 10 & 1 & 1 & 10 \end{bmatrix} \quad (\text{作 mod 11 运算}),$$

两式相等 $\Rightarrow T' \in \mathrm{Aut}(Q)^+$ (同理验证 S, $V \in \mathrm{Aut}(Q)^+$).

上面两例证实了本文诸结论的正确性, 且给出的是一种很有效的、有自己特色的方法. 这不仅能验证 Gleanson– Prange 定理的结论, 而且能求出 $\mathrm{Aut}(Q)^+$ 中更多的置换甚至整个 $\mathrm{Aut}(Q)^+$ (如果需要的话).

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] 王国栋, 叶　锐, 陆正福. 一般有限域 $GF(p^m)$ 上线性码的自同构群[J]. 云南大学学报(自然科学版), 2004, 26(1): 11—14.

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

[4] 华罗庚, 万哲先. 典型群[M]. 上海: 上海科学技术出版社, 1963.

The automorphism group of quadratic-residue codes

WANG Guo-dong, YANG Yang, LU Zheng-fu

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

Abstract: The theorems on the automorphism permutation of the quadratic-residue codes are established. The theory of the generalized inverse is used to study the automorphism group of the extended quadratic-residue codes. The results are verified by some examples.

Key words: quadric-residue code; monomial matrix group; automorphism group; generalized inverse

MSC(2000): 20B25