云南大学学报（自然科学版），2004，26（1）：11~14　　CN 53-1045/N　ISSN 0258-7971
Journal of Yunnan University

一般有限域 $GF(p^m)$ 上线性码的自同构群*

王国栋，叶　锐，陆正福
（云南大学 数学系，云南 昆明　650091）

摘要：对单式阵群作一个较详细的研究，并将 $GF(2^m)$ 上线性码的自同构群的一些结论推广到最一般的有限域 $GF(p^m)$ 上去，这里的 p 是任意的素数.

关键词：线性码；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)01-0011-04

设 C 是一个线性编码. C 的自同构群 $\mathrm{Aut}C$ 在码论研究中，尤其是译码中很有用，然而寻求 $\mathrm{Aut}C$ 一般十分困难. 在文献[1]及我们所给的其它论文中，我们曾用矩阵广义逆理论对 $\mathrm{Aut}C$ 进行了研究，得出一些颇有价值的理论及一些很有效的计算方法，将 $\mathrm{Aut}C$ 的研究推进了一步. 但文献[1]的结果还仅限于 $GF(2^m)$ 上，为了使这些结果可用于更多的码类，需将它们推广到最一般的有限域 $GF(p^m)$ 上去. 这种推广要涉及单式阵群问题（在 $GF(2^m)$ 上仅涉及置换阵群），因而更为困难和复杂.

下面，先对单式阵群作一个较为详尽的研究，找出它的一些规律.

1　单式阵群

定义 1　设 $\boldsymbol{H}$ 是有限域 F 上的 $(n-k)\times n$ 阶的行满秩矩阵，齐次线性方程组

$$\boldsymbol{H}x = 0$$

的解空间 $N(\boldsymbol{H})$ 称为 F 上的一个 $[n, k]$ 线性码，其中 k 是 $N(\boldsymbol{H})$ 的维.

对置换 $\sigma \in S_n$（n 次对称群）及有限域 $GF(q)(q = p^m)$ 上的 n 维向量 $\boldsymbol{a} = (a_1, a_2, \cdots, a_n)$，$\boldsymbol{a}\sigma = (a_{\sigma(1)}, a_{\sigma(2)}, \cdots, a_{\sigma(n)})$. 设 $\delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$（kronecker 符号），则可用置换阵 $\boldsymbol{A} = (\delta_{i,\sigma(j)})$ 来代替 σ 的作用.

令 $\mathscr{P}$ 代表 n 阶置换阵全体所构成的置换阵群，则 $\mathscr{P}$ 与 S_n 同构. 其同构对应是

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \longleftrightarrow \boldsymbol{A} = (\delta_{i,\sigma(j)}).$$

令 $i_t = \sigma(t)$，则矩阵 $\boldsymbol{A} = (e_{i_1} e_{i_2} \cdots e_{i_n})$，其中 $e_{i_t} = (0 \cdots 0\ 1\ 0 \cdots 0)^{\mathrm{T}}$ 是第 i_t 位为 1 的单位向量（下同），$t = 1, 2, \cdots, n$.

例 **1**　$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$，则 $\boldsymbol{A} = (e_2\ e_3\ e_1\ e_4)$（4 阶置换阵）.

定义 **2**[2]　称有限域 $GF(q)(q = p^m)$ 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.

例 **2**　有限域 $GF(3^2) = \{0, 1, \alpha^1, \alpha^2, \cdots, \alpha^7\}$（$\alpha^8 = 1$）上的矩阵 $\tilde{\boldsymbol{A}} = \begin{bmatrix} 0 & \alpha^2 & 0 \\ 0 & 0 & 1 \\ \alpha^5 & 0 & 0 \end{bmatrix}$ 就是一个单式阵.

由此定义，可表 $\tilde{\boldsymbol{A}} = \boldsymbol{AD}$，其中 $\boldsymbol{A} \in \mathscr{P}$，$\boldsymbol{D} \in \mathscr{D}$（$n$ 阶非异对角阵全体所成群）.

令 $\mathscr{R} = \mathscr{PD} = \{\boldsymbol{AD} \mid \boldsymbol{A} \in \mathscr{P}, \boldsymbol{D} \in \mathscr{D}\}$，则 $\mathscr{R}$ 便是 $GF(q)$ 上所有 n 阶单式阵所成集合. 当 $q = 2$ 时，$\mathscr{R} = \mathscr{P}$.

为简便计，将对角阵记为 $\boldsymbol{D} = \langle \lambda_1\ \lambda_2 \cdots \lambda_n \rangle$.

* 收稿日期：2003-09-08
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）；云南省省校合作项目（19-7）：（北京大学—云南大学）.
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问题方面的研究.

引理 **1** 对 $\boldsymbol{D}=\langle\lambda_1\ \lambda_2\cdots\lambda_n\rangle\in\mathscr{D}$, $\lambda_i\in GF(q)$, $\boldsymbol{A}=(e_{i_1}\ e_{i_2}\cdots e_{i_n})\in\mathscr{P}$ 有 $\boldsymbol{DA}=\boldsymbol{A}\overline{\boldsymbol{D}}$, 其中 $\overline{\boldsymbol{D}}=\langle\lambda_{i_1}\ \lambda_{i_2}\cdots\lambda_{i_n}\rangle$.

证明 因 $\boldsymbol{A}^{-1}=\boldsymbol{A}^{\mathrm{T}}$,

所以 $\boldsymbol{A}\langle\lambda_{i_1}\ \lambda_{i_2}\cdots\lambda_{i_n}\rangle\boldsymbol{A}^{\mathrm{T}}=\lambda_{i_1}e_{i_1}e_{i_1}^{\mathrm{T}}+\cdots+\lambda_{i_n}e_{i_n}e_{i_n}^{\mathrm{T}}=\lambda_1e_1e_1^{\mathrm{T}}+\cdots+\lambda_ne_ne_n^{\mathrm{T}}=\langle\lambda_1\ \lambda_2\cdots\lambda_n\rangle=\boldsymbol{D}$.

因而 $\boldsymbol{DA}=\boldsymbol{A}\overline{\boldsymbol{D}}$.

定理 **1** 对 n 阶的一般线性群 $GL(n,F)(F=GF(q))$ 上的 2 个子群 $\mathscr{P}$ 及 $\mathscr{D}$ 作它们的乘积

$$\mathscr{R}=\mathscr{P}\mathscr{D}=\{\boldsymbol{AD}\mid\boldsymbol{A}\in\mathscr{P},\boldsymbol{D}\in\mathscr{D}\},$$

则 $\mathscr{R}$ 也是 $GL(n,F)$ 的子群, 称为单式阵群, 且 $\mathscr{R}$ 的阶 $|\mathscr{R}|=(q-1)^n n!$.

证明 令 $\boldsymbol{A}_1\boldsymbol{D}_1,\boldsymbol{A}_2\boldsymbol{D}_2\in\mathscr{R}$ 由引理 1

$$(\boldsymbol{A}_1\boldsymbol{D}_1)(\boldsymbol{A}_2\boldsymbol{D}_2)=\boldsymbol{A}_1(\boldsymbol{D}_1\boldsymbol{A}_2)\boldsymbol{D}_2=(\boldsymbol{A}_1\boldsymbol{A}_2)(\overline{\boldsymbol{D}_1}\boldsymbol{D}_2)\in\mathscr{R}$$

所以 $\mathscr{R}$ 成群, $\boldsymbol{I}_n$ 是 $\mathscr{R}$ 的单位元. 已知有如下阶的关系: $|\mathscr{R}|=|\mathscr{P}||\mathscr{D}|/|\mathscr{P}\cap\mathscr{D}|$. 令 $\boldsymbol{B}\in\mathscr{P}\cap\mathscr{D}$ 则 $\boldsymbol{B}$ 是置换阵且 $\boldsymbol{B}$ 的对角元均非 0, 推出 $\boldsymbol{B}=\boldsymbol{I}_n$. 所以 $|\mathscr{R}|=|\mathscr{P}||\mathscr{D}|$. 对 $\boldsymbol{D}=\langle\lambda_1\ \lambda_2\cdots\lambda_n\rangle\in\mathscr{D}$, $\lambda_i\in GF^*(q)$, $|GF^*(q)|=q-1$. 因而 $|\mathscr{D}|=(q-1)^n$, 但 $|\mathscr{P}|=n!$, 最终 $|\mathscr{R}|=(q-1)^n n!$.

下面给出单式阵的一些运算规律.

引理 **2** 设置换阵 $\boldsymbol{A}=(e_{i_1}\ e_{i_2}\cdots e_{i_n})$, 其中 $i_1i_2\cdots i_n$ 是 $12\ \cdots\ n$ 的一个排列. 倘若排列中的自然数 t 在第 k_t 位置上($t=1,2,\cdots,n$), 则

(1) $\boldsymbol{A}=(e_{i_1}\ e_{i_2}\cdots e_{i_n})=\begin{bmatrix}\widetilde{e}_{k_1}\\ \widetilde{e}_{k_2}\\ \vdots\\ \widetilde{e}_{k_n}\end{bmatrix}$, 其中 $\widetilde{e}_{k_t}=(0\ \cdots0\ 1\ 0\ \cdots0)$ 是单位行向量(而 $e_{i_1},e_{i_2},\cdots,e_{i_n}$ 是单位列向量).

(2) $\boldsymbol{A}^{-1}=\boldsymbol{A}^{\mathrm{T}}=(e_{k_1}e_{k_2}\cdots e_{k_n})=\begin{bmatrix}\widetilde{e}_{i_1}\\ \widetilde{e}_{i_2}\\ \vdots\\ \widetilde{e}_{i_n}\end{bmatrix}$, $\widetilde{e}_{i_t}=(0\ \cdots0\ 1\ 0\ \cdots0)$ 是单位行向量.

证明 (1) 容易得出.

(2) 因 $\widetilde{e}_{k_i}e_{k_j}=\begin{cases}1 & i=j\\ 0 & i\neq j\end{cases}$, 所以由(1), $\boldsymbol{A}(e_{k_1}\ e_{k_2}\cdots e_{k_n})=\boldsymbol{I}_n$, 推出 $\boldsymbol{A}^{-1}=(e_{k_1}\ e_{k_2}\cdots e_{k_n})$.

例 **3** 设 $\boldsymbol{A}=(e_4e_2e_1e_3)$, 排列 4213 中 1, 2, 3, 4 分别在 $k_1=3$, $k_2=2$, $k_3=4$, $k_4=1$ 位置上, 所以

$$\boldsymbol{A}=\begin{bmatrix}\widetilde{e}_3\\ \widetilde{e}_2\\ \widetilde{e}_4\\ \widetilde{e}_1\end{bmatrix}=\begin{bmatrix}0&0&1&0\\ 0&1&0&0\\ 0&0&0&1\\ 1&0&0&0\end{bmatrix},$$

$$\boldsymbol{A}^{-1}=(e_{k_1}\ e_{k_2}\ e_{k_3}\ e_{k_4})=(e_3e_2e_4e_1)=\begin{bmatrix}\widetilde{e}_4\\ \widetilde{e}_2\\ \widetilde{e}_1\\ \widetilde{e}_3\end{bmatrix}=\begin{bmatrix}0&0&0&1\\ 0&1&0&0\\ 1&0&0&0\\ 0&0&1&0\end{bmatrix}.$$

在实际中我们常要计算单式阵的逆及它的阶, 因而不可回避地要计算它的幂, 为此给出下面方便而有效的方法.

定理 **2** 设单式阵 $\tilde{\boldsymbol{A}}=\boldsymbol{AD}=(e_{i_1}\ e_{i_2}\cdots e_{i_n})\langle\lambda_1\lambda_2\cdots\lambda_n\rangle$, 则

(1) $\tilde{\boldsymbol{A}}$ 的逆 $\tilde{\boldsymbol{A}}^{-1}=(\boldsymbol{AD})^{-1}=(e_{k_1}\ e_{k_2}\cdots e_{k_n})\langle\lambda_{k_1}^{-1}\ \lambda_{k_2}^{-1}\cdots\lambda_{k_n}^{-1}\rangle$, 其中 k_t 的定义见引理 2.

(2) 将 $\boldsymbol{D}=\langle\lambda_1\ \lambda_2\cdots\lambda_n\rangle$ 记为 $\boldsymbol{D}_0=\langle\lambda_1^{(0)}\ \lambda_2^{(0)}\cdots\lambda_n^{(0)}\rangle$. 由排列 $i_1i_2\cdots i_n$(由 $\boldsymbol{A}$ 知)及 $\boldsymbol{D}_0$ 可作出一个 $\boldsymbol{D}_1=\langle\lambda_{i_1}^{(0)}\ \lambda_{i_2}^{(0)}\cdots\lambda_{i_n}^{(0)}\rangle$. 将 $\boldsymbol{D}_1$ 又记为 $\boldsymbol{D}_1=\langle\lambda_1^{(1)}\ \lambda_2^{(1)}\cdots\lambda_n^{(1)}\rangle$, 由 $\boldsymbol{D}_1$ 又可作出 $\boldsymbol{D}_2=\langle\lambda_{i_1}^{(1)}\ \lambda_{i_2}^{(1)}\cdots\lambda_{i_n}^{(1)}\rangle$, 记为 $\boldsymbol{D}_2=\langle\lambda_1^{(2)}\ \lambda_2^{(2)}\cdots\lambda_n^{(2)}\rangle$. 仿此不断往下做, 得出一个对角阵序列

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

则 $\tilde{\boldsymbol{A}}=\boldsymbol{AD}$ 的 k 次幂

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

(此公式提供了一个规范且简易的计算幂的方法).

(3) 设还另有一个单式阵 $\tilde{\boldsymbol{B}}=\boldsymbol{BD}_1=(e_{j_1}\ e_{j_2}\cdots e_{j_n})\langle\mu_1\ \mu_2\cdots\mu_n\rangle$, 则乘积

$$\tilde{\boldsymbol{A}}\ \tilde{\boldsymbol{B}}=\boldsymbol{AB}\langle\lambda_{j_1}\mu_1\ \lambda_{j_2}\mu_2\cdots\lambda_{j_n}\mu_n\rangle.$$

证明 (1) 因

$$\tilde{\boldsymbol{A}}^{-1}=(\boldsymbol{AD})^{-1}=\boldsymbol{D}^{-1}\boldsymbol{A}^{-1}=$$

$$\langle \lambda_1^{-1}\ \lambda_2^{-1}\cdots\lambda_n^{-1}\rangle(e_{k_1}\ e_{k_2}\cdots e_{k_n}) =$$

$$(e_{k_1}\ e_{k_2}\cdots e_{k_n})\langle \lambda_{k_1}^{-1}\ \lambda_{k_2}^{-1}\cdots\lambda_{k_n}^{-1}\rangle(\text{由引理 2}).$$

(2) 用数学归纳法证之. 当 $k=1$ 时, (1) 式显然成立.

设 $k=m$ 成立, 即 $\tilde{\boldsymbol{A}}^m=\boldsymbol{A}^m\boldsymbol{D}_{m-1}\boldsymbol{D}_{m-2}\cdots\boldsymbol{D}_1\boldsymbol{D}_0$ 成立, 来证 $k=m+1$ 成立. 令 $\boldsymbol{W}=\boldsymbol{D}_{m-1}\boldsymbol{D}_{m-2}\cdots\boldsymbol{D}_1\boldsymbol{D}_0$, 则

$$\tilde{\boldsymbol{A}}^{m+1}=\tilde{\boldsymbol{A}}\,\tilde{\boldsymbol{A}}^m=(\boldsymbol{A}\boldsymbol{D}_0)\boldsymbol{A}^m\boldsymbol{W}=$$

$$\boldsymbol{A}(\boldsymbol{D}_0\boldsymbol{A})\boldsymbol{A}^{m-1}\boldsymbol{W}=$$

$$\boldsymbol{A}\boldsymbol{A}\langle\lambda_1^{(0)}\ \lambda_2^{(0)}\cdots\lambda_n^{(0)}\rangle\boldsymbol{A}^{m-1}\boldsymbol{W}(\text{由引理 1})=$$

$$\boldsymbol{A}^2\langle\lambda_1^{(1)}\ \lambda_2^{(1)}\cdots\lambda_n^{(1)}\rangle\boldsymbol{A}^{m-1}\boldsymbol{W}=$$

$$\boldsymbol{A}^3\langle\lambda_{i_1}^{(1)}\ \lambda_{i_2}^{(1)}\cdots\lambda_{i_n}^{(1)}\rangle\boldsymbol{A}^{m-2}\boldsymbol{W}=$$

$$\boldsymbol{A}^3\langle\lambda_1^{(2)}\ \lambda_2^{(2)}\cdots\lambda_n^{(2)}\rangle\boldsymbol{A}^{m-2}\boldsymbol{W}=\cdots=$$

$$\boldsymbol{A}^{m+1}\langle\lambda_1^{(m)}\ \lambda_2^{(m)}\cdots\lambda_n^{(m)}\rangle\boldsymbol{A}^0\boldsymbol{W}=$$

$$\boldsymbol{A}^{m+1}\boldsymbol{D}_m\boldsymbol{W}=\boldsymbol{A}^{m+1}\boldsymbol{D}_m\boldsymbol{D}_{m-1}\cdots\boldsymbol{D}_1\boldsymbol{D}_0.$$

(3) 因 $\tilde{\boldsymbol{A}}\ \tilde{\boldsymbol{B}}=\boldsymbol{A}\boldsymbol{D}\boldsymbol{B}\boldsymbol{D}_1=\boldsymbol{A}(\boldsymbol{D}\boldsymbol{B})\boldsymbol{D}_1=\boldsymbol{A}\boldsymbol{B}(\bar{\boldsymbol{D}}\boldsymbol{D}_1)$(由引理 1) $=\boldsymbol{A}\boldsymbol{B}\langle\lambda_{i_1}\ \lambda_{i_2}\cdots\lambda_{i_n}\rangle\cdot\langle\mu_1\ \mu_2\cdots\mu_n\rangle$.

例 **4**　求有限域 $GF(2^3)=\{0,1,\alpha,\cdots,\alpha^6\}$ ($\alpha^7=1$) 上的单式阵 $\tilde{\boldsymbol{A}}=\begin{bmatrix}0&\alpha^5&0&0\\0&0&0&1\\\alpha^2&0&0&0\\0&0&\alpha&0\end{bmatrix}$ 的阶.

将看到 $\tilde{\boldsymbol{A}}$ 的阶 $|\tilde{\boldsymbol{A}}|=28$. 如果用矩阵的乘法去求 $|\tilde{\boldsymbol{A}}|$, 计算量太大, 也容易出错. 用上定理中的公式 (1) 来做, 工作量大为减少, 且它的计算格式很规范.

易见 $\tilde{\boldsymbol{A}}=\boldsymbol{A}\boldsymbol{D}=\boldsymbol{A}\boldsymbol{D}_0$, 其中 $\boldsymbol{A}=(e_{i_1}e_{i_2}e_{i_3}e_{i_4})=(e_3\ e_1e_4\ e_2)$, 而 $\boldsymbol{D}_0=\langle\lambda_1^{(0)}\ \lambda_2^{(0)}\ \lambda_3^{(0)}\ \lambda_4^{(0)}\rangle=\langle\alpha^2\ \alpha^5\ \alpha\ 1\rangle$, 其中排列 $i_1i_2i_3i_4$ 是 3142, 因此计算格式如下:

$\boldsymbol{D}_0=\langle\alpha^2\ \alpha^5\ \alpha\ 1\rangle$, 由排列 3142 知,

$\boldsymbol{D}_1=\langle\alpha\ \alpha^2\ 1\ \alpha^5\rangle$, $\boldsymbol{D}_1\boldsymbol{D}_0=\langle\alpha^3\ 1\ \alpha\ \alpha^5\rangle$,

$\boldsymbol{D}_2=\langle1\ \alpha\ \alpha^5\ \alpha^2\rangle$, $\boldsymbol{D}_2\boldsymbol{D}_1\boldsymbol{D}_0=\langle\alpha^3\ \alpha\ \alpha^6\ 1\rangle$,

$\boldsymbol{D}_3=\langle\alpha^5\ 1\ \alpha^2\ \alpha\rangle$,

$\boldsymbol{D}_3\boldsymbol{D}_2\boldsymbol{D}_1\boldsymbol{D}_0=\langle\alpha\ \alpha\ \alpha\ \alpha\rangle=\alpha\boldsymbol{I}_4$,

故 $\tilde{\boldsymbol{A}}^4=\boldsymbol{A}^4\boldsymbol{D}_3\boldsymbol{D}_2\boldsymbol{D}_1\boldsymbol{D}_0=\boldsymbol{I}_4(\alpha\boldsymbol{I}_4)=\alpha\boldsymbol{I}_4$($\boldsymbol{A}$ 的阶由置换性质很易求出), 所以 $(\tilde{\boldsymbol{A}}^4)^7=\tilde{\boldsymbol{A}}^{28}=\alpha^7\boldsymbol{I}_4=\boldsymbol{I}_4$. 因此, $|\tilde{\boldsymbol{A}}|=28$.

2　$GF(q)$ 上线性码的自同构群问题

下面总设 C 是有限域 $GF(q)$ ($q=p^m$) 上的一个 $[n,k]$ 线性码, 且设 $k\times n$ 阵 $\boldsymbol{M}$ 是 C 的生成阵, 不失一般性, 还假定 $\boldsymbol{M}$ 行满秩.

定义 **3**[2]　设 C 是 $GF(q)$ 上的 $[n,k]$ 线性码, C 的自同构群

$$\mathrm{Aut}\,C=\{\tilde{\boldsymbol{A}}=\boldsymbol{A}\boldsymbol{D}\in\mathscr{P}\mathscr{D}\mid\text{对任何 } c\in C,\ c\boldsymbol{A}\boldsymbol{D}\in C\}.$$

对 $GF(q)$ 上的任何 $k\times k$ 可逆阵 $\boldsymbol{Y}$, 令 $\tilde{\boldsymbol{M}}=\boldsymbol{Y}\boldsymbol{M}$, 则行生成空间 $\mathrm{span}(\tilde{\boldsymbol{M}})=\mathrm{span}(\boldsymbol{M})$. 因此不难得出, 对单式阵 $\boldsymbol{A}\boldsymbol{D}\in\mathscr{R}$ 有

$\boldsymbol{A}\boldsymbol{D}\in\mathrm{Aut}\,C\Leftrightarrow$存在 $GF(q)$ 上的 $k\times k$ 阵 $\boldsymbol{X}$, 使

$$\boldsymbol{X}\boldsymbol{M}=\boldsymbol{M}\boldsymbol{A}\boldsymbol{D},\qquad(2)$$

这等价于, $\boldsymbol{A}\boldsymbol{D}\in\mathrm{Aut}\,C\Leftrightarrow$ 矩阵方程 $\boldsymbol{X}\boldsymbol{M}=\boldsymbol{M}\boldsymbol{A}\boldsymbol{D}$ ($\boldsymbol{X}$ 可逆) 有解.

下面给出本文的另一个重要定理.

定理 **3**　设 C 是 $GF(q)$ 上的 $[n,k]$ 线性码, 且行满秩阵 $\boldsymbol{M}$ 是 C 的生成阵, 则对单式阵 $\tilde{\boldsymbol{A}}=\boldsymbol{A}\boldsymbol{D}\in\mathscr{R}$

$\tilde{\boldsymbol{A}}\in\mathrm{Aut}\,C\Leftrightarrow$矩阵方程 $\boldsymbol{X}\boldsymbol{M}=\boldsymbol{M}\tilde{\boldsymbol{A}}$ 有解($\boldsymbol{X}$ 非异) $\Leftrightarrow\boldsymbol{M}\tilde{\boldsymbol{A}}\ \boldsymbol{M}^{(1)}\boldsymbol{M}=\boldsymbol{M}\tilde{\boldsymbol{A}}$,

$$(3)$$

其中 $\boldsymbol{M}^{(1)}$ 是 $\boldsymbol{M}$ 的任何一个 $\{1\}-$ 逆. 若有解, 则 $k\times k$ 可逆阵 $\boldsymbol{X}_0=\boldsymbol{M}\tilde{\boldsymbol{A}}\ \boldsymbol{M}^{(1)}$ 是方程的唯一解.

证明　据文献[3], 复数域上的矩阵方程

$$\boldsymbol{X}\boldsymbol{M}=\boldsymbol{M}\tilde{\boldsymbol{A}}$$

有解的充要条件是 $\boldsymbol{M}\tilde{\boldsymbol{A}}\ \boldsymbol{M}^{(1)}\boldsymbol{M}=\boldsymbol{M}\tilde{\boldsymbol{A}}$. 若有解, 则解集是

$$S=\{\boldsymbol{M}\tilde{\boldsymbol{A}}\ \boldsymbol{M}^{(1)}+\boldsymbol{Y}(\boldsymbol{I}_k-\boldsymbol{M}\boldsymbol{M}^{(1)})\mid\boldsymbol{Y}\text{是}C\text{上的任何 }k\times k\text{阵}\}=\{\boldsymbol{M}\tilde{\boldsymbol{A}}\ \boldsymbol{M}^{(1)}\}(\text{因}\boldsymbol{M}\text{行满秩, 所以 }\boldsymbol{M}\boldsymbol{M}^{(1)}=\boldsymbol{I}_k).$$

此结论可推广到有限域 $GF(q)$ 上[4], 且上述结论不依赖于 $\boldsymbol{M}^{(1)}$ 的选择(见下面定理 4 的证明过程). 因此若上述矩阵方程有解, 则 $k=$ 秩$(\boldsymbol{M})=$ 秩$(\boldsymbol{M}\tilde{\boldsymbol{A}})=$ 秩$(\boldsymbol{M}\tilde{\boldsymbol{A}}\ \boldsymbol{M}^{(1)}\boldsymbol{M})\leqslant$秩$(\boldsymbol{M}\tilde{\boldsymbol{A}}\ \boldsymbol{M}^{(1)})$, 推出 k 阶方阵是可逆阵, 且它是唯一解.

进一步, 令 $G=\mathrm{Aut}\,C$. 由定理 3, 对 $\tilde{\boldsymbol{A}}=\boldsymbol{A}\boldsymbol{D}\in G$, 由于此时 $\boldsymbol{M}\tilde{\boldsymbol{A}}\ \boldsymbol{M}^{(1)}$ 可逆, 可定义映射

$$\varphi:\tilde{\boldsymbol{A}}\mid\rightarrow\boldsymbol{M}\tilde{\boldsymbol{A}}\ \boldsymbol{M}^{(1)}=\boldsymbol{K}\in GL(k,F)(\text{一般线性群}),\qquad(4)$$

其中 $\boldsymbol{M}^{(1)}$ 是 $\boldsymbol{M}$ 的任何一个 $\{1\}-$ 逆. 可证 φ 是 G 到 $\varphi(G)$ 的同态满射. 事实上, 由文献[3], $\{1\}-$ 逆

集合可表征为

$$M\{1\}=\{\boldsymbol{M}^{(1)}+\boldsymbol{Z}-\boldsymbol{M}^{(1)}\boldsymbol{M}\boldsymbol{Z}\mid \boldsymbol{Z}\text{ 是}GF(q)\text{上的任何 }n\times k\text{ 阵}\}$$

任取 $\boldsymbol{B}\in M\{1\}$, 设 $\boldsymbol{B}=\boldsymbol{M}^{(1)}+\boldsymbol{Z}-\boldsymbol{M}^{(1)}\boldsymbol{M}\boldsymbol{Z}$, 某个 $\boldsymbol{Z}$, 则

$$\boldsymbol{M}\tilde{\boldsymbol{A}}\ \boldsymbol{B}=\boldsymbol{M}\tilde{\boldsymbol{A}}\ \boldsymbol{M}^{(1)}+\boldsymbol{M}\tilde{\boldsymbol{A}}\ \boldsymbol{Z}-\boldsymbol{M}\tilde{\boldsymbol{A}}\ \boldsymbol{M}^{(1)}\boldsymbol{M}\boldsymbol{Z}=\boldsymbol{M}\tilde{\boldsymbol{A}}\ \boldsymbol{M}^{(1)}$$

(因 $\tilde{\boldsymbol{A}}\in G$, 所以据上定理 $\boldsymbol{M}\tilde{\boldsymbol{A}}\ \boldsymbol{M}^{(1)}\boldsymbol{M}=\boldsymbol{M}\tilde{\boldsymbol{A}}$), 所以表达式 $\boldsymbol{M}\tilde{\boldsymbol{A}}\ \boldsymbol{M}^{(1)}$ 不依赖于 $\boldsymbol{M}^{(1)}$ 的选择. 因此 φ 是映射.

设 $\tilde{\boldsymbol{A}}_1=\boldsymbol{A}_1\boldsymbol{D}_1$ 及 $\tilde{\boldsymbol{A}}_2=\boldsymbol{A}_2\boldsymbol{D}_2\in G$, 则由(2)式知, 存在 $\boldsymbol{K}_1,\boldsymbol{K}_2\in GL(k,F)$, 使

$$\boldsymbol{K}_1\boldsymbol{M}=\boldsymbol{M}\boldsymbol{A}_1\boldsymbol{D}_1,\ \boldsymbol{K}_2\boldsymbol{M}=\boldsymbol{M}\boldsymbol{A}_2\boldsymbol{D}_2\Rightarrow$$

$$\boldsymbol{K}_1\boldsymbol{K}_2\boldsymbol{M}=\boldsymbol{K}_1\boldsymbol{M}\boldsymbol{A}_2\boldsymbol{D}_2=\boldsymbol{M}\boldsymbol{A}_1\boldsymbol{D}_1\boldsymbol{A}_2\boldsymbol{D}_2=\boldsymbol{M}\tilde{\boldsymbol{A}}_1\tilde{\boldsymbol{A}}_2,$$

因此 $\varphi(\tilde{\boldsymbol{A}}_1\tilde{\boldsymbol{A}}_2)=\boldsymbol{M}\tilde{\boldsymbol{A}}_1\tilde{\boldsymbol{A}}_2\boldsymbol{M}^{(1)}=\boldsymbol{K}_1\boldsymbol{K}_2\boldsymbol{M}\boldsymbol{M}^{(1)}=\boldsymbol{K}_1\boldsymbol{K}_2\boldsymbol{I}_k=\boldsymbol{K}_1\boldsymbol{K}_2=\varphi(\tilde{\boldsymbol{A}}_1)\varphi(\tilde{\boldsymbol{A}}_2)$. 所以 φ 是 G 到 $\varphi(G)$ 的同态满射.

定理 **4** 令 $[n,k]$ 线性码 C 的自同构群 $\mathrm{Aut}C=G(\mathscr{A}$的子群). 对 $\tilde{\boldsymbol{A}}=\boldsymbol{A}\boldsymbol{D}\in G$, 则映射

$$\varphi:\tilde{\boldsymbol{A}}\mid\rightarrow\boldsymbol{M}\tilde{\boldsymbol{A}}\ \boldsymbol{M}^{(1)}=\boldsymbol{K}\in GL(k,F)\text{(一般线性群)}$$

是 G 到 $\varphi(G)$ 的同态满射. 从而商群

$$G/\ker\varphi\cong\varphi(G),$$

其中核 $\ker\varphi=\{\tilde{\boldsymbol{A}}\in G\mid\varphi(\tilde{\boldsymbol{A}})=\boldsymbol{K}=\boldsymbol{M}\tilde{\boldsymbol{A}}\ \boldsymbol{M}^{(1)}=\boldsymbol{I}_k\}$, $\boldsymbol{I}_k$ 是 $GL(k,F)$ 中的单位元. 特别若 $\ker\varphi=\boldsymbol{I}_n$, 则 φ 是单射, 此时 $G\cong\varphi(G)$. 若还有 $\varphi(G)=GL(k,F)$, 则

$$G=\mathrm{Aut}C\cong GL(k,F),\ F=GF(q).$$

在这种情况下, $\mathrm{Aut}C$ 的计算可归结为 $GL(k,F)$ 的计算. 文献[5]中所给定的2个命题的证明过程提供了计算 $GL(k,F)$ 的方法. 此二命题是:

①[5] 在有限域 $GF(q)$ 上的 n 维向量空间中, 一共有

$$(q^n-1)(q^n-2)\cdots(q^n-q^{t-2})$$

个线性无关的向量组, 每组含 t 个向量.

②[5] n 级一般线性群 $GL(n,F)(F=GF(q))$ 含有

$$(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$$

个元素.

下面通过一个具体例子来阐明怎样利用本文的结果来求取一个线性码的自同构群. 考 $GF(3)$ 上的 $[4,2]$ 线性码, 其生成阵是 $\boldsymbol{M}=\begin{bmatrix}1&0&2&2\\0&1&2&1\end{bmatrix}$. 其码字是0000, 0212, 1110, 2011, 2220, 0121, 1022, 1201, 2102.

兹证 $\mathrm{Aut}C\cong GL(2,F)$, $F=GF(3)$(共含 $(3^2-1)(3^2-3)=48$ 个元).

为简便计, 将4阶单式阵 $\tilde{\boldsymbol{A}}$ 分块成 $\tilde{\boldsymbol{A}}=[\tilde{\boldsymbol{A}}_1,\tilde{\boldsymbol{A}}_2]$. 算出 $\boldsymbol{M}^{(1)}=\begin{bmatrix}\boldsymbol{I}_2\\0\end{bmatrix}$, $\boldsymbol{M}^{(1)}\boldsymbol{M}=\begin{bmatrix}\boldsymbol{I}_2&\boldsymbol{U}\\0&0\end{bmatrix}$, $\boldsymbol{U}=\begin{bmatrix}2&2\\2&1\end{bmatrix}$, 据定理3知

$$\tilde{\boldsymbol{A}}\in\mathrm{Aut}C\Leftrightarrow\boldsymbol{M}\tilde{\boldsymbol{A}}\ \boldsymbol{M}^{(1)}\boldsymbol{M}=\boldsymbol{M}[\tilde{\boldsymbol{A}}_1\tilde{\boldsymbol{A}}_2]\begin{bmatrix}\boldsymbol{I}_2&\boldsymbol{U}\\0&0\end{bmatrix}=\boldsymbol{M}[\tilde{\boldsymbol{A}}_1\tilde{\boldsymbol{A}}_2]\Leftrightarrow\boldsymbol{M}\tilde{\boldsymbol{A}}_1\boldsymbol{U}=\boldsymbol{M}\tilde{\boldsymbol{A}}_2.\qquad(5)$$

对任何 $\boldsymbol{K}\in GL(2,F)$, 则由 $\boldsymbol{K}=\boldsymbol{M}\tilde{\boldsymbol{A}}\ \boldsymbol{M}^{(1)}=\boldsymbol{M}[\tilde{\boldsymbol{A}}_1\tilde{\boldsymbol{A}}_2]\begin{bmatrix}\boldsymbol{I}_2\\0\end{bmatrix}=\boldsymbol{M}\tilde{\boldsymbol{A}}_1$. 据 $\boldsymbol{M}$ 的结构, 由 $\boldsymbol{K}=\boldsymbol{M}\tilde{\boldsymbol{A}}_1$ 容易得出 $\tilde{\boldsymbol{A}}_1$. 再由 $\boldsymbol{K}\boldsymbol{U}=\boldsymbol{M}\tilde{\boldsymbol{A}}_2$, 即可定出 $\tilde{\boldsymbol{A}}_2$, 于是 $\tilde{\boldsymbol{A}}=[\tilde{\boldsymbol{A}}_1\tilde{\boldsymbol{A}}_2]$ 便是 $\boldsymbol{K}$ 的原像, 即 φ 是 G 到 $GL(2,F)$ 上的映射.

令 $\boldsymbol{I}_2=\boldsymbol{K}=\boldsymbol{M}\tilde{\boldsymbol{A}}_1\Rightarrow\tilde{\boldsymbol{A}}_1=(e_1,e_2)$, 再由

$$\boldsymbol{K}\boldsymbol{U}=\boldsymbol{I}_2\boldsymbol{U}=\boldsymbol{U}=\boldsymbol{M}\tilde{\boldsymbol{A}}_2\Rightarrow$$

$$\tilde{\boldsymbol{A}}_2=(e_3,e_4)\Rightarrow\ker\varphi=\boldsymbol{I}_4.$$

所以

$$G=\mathrm{Aut}C\cong GL(2,F)\text{(阶为 48)}.$$

借助定理2的公式(1)及两子群的乘积(又称部积), 可将 G 中的48个元具体求出: 事实上, 分别令 $\boldsymbol{K}=\begin{bmatrix}0&2\\2&1\end{bmatrix}$ 及 $\begin{bmatrix}0&2\\1&2\end{bmatrix}$, 分别求出了 G 中的2个元

$$\tilde{\boldsymbol{A}}=(2e_2\ e_4\ e_1\ e_3),$$

$$\tilde{\boldsymbol{B}}=(e_2\ e_3\ e_1\ e_4),$$

由公式(1), 可很快算出 $\tilde{\boldsymbol{A}},\tilde{\boldsymbol{B}}$ 的阶 $|\tilde{\boldsymbol{A}}|=8$, $|\tilde{\boldsymbol{B}}|=3$. 于是 $\tilde{\boldsymbol{A}},\tilde{\boldsymbol{B}}$ 分别生成8阶及3阶的循环群 $(\tilde{\boldsymbol{A}})$ 与 $(\tilde{\boldsymbol{B}})$. 考它们的乘积 $W=(\tilde{\boldsymbol{A}})(\tilde{\boldsymbol{B}})\subseteq G$. 由于 $(\tilde{\boldsymbol{A}})\cap(\tilde{\boldsymbol{B}})=\boldsymbol{I}_4$, 所以

$$|W|=|(\tilde{\boldsymbol{A}})||(\tilde{\boldsymbol{B}})|=8\times3=24.$$

由此

$$W\cup2W=G=\mathrm{Aut}C.$$

这样一来, $\mathrm{Aut}C$ 的全部元就具体求出了.

(下转第 19 页)

[8] SHANG Ya-dong, GUO Bo-ling. The global attraction for the periodic initial value problem for dissipative generalized symmetric regularized long wave equations[J]. J Math Engi, preprint.
[9] BABIN A V, VISHIK M I. Regular attractors of semi-groups and evolution equations[J]. J Math Pures Appl, 1983, 62: 441—491.
[10] DAI Zheng-de, GUO Bo-ling. Inertial fractal sets for dissipative zakharov system[J]. Acta Math Appl Sinica, 1997, 13(3): 279—288.

Exponential attractor for dissipative generalized symmetric regularized long wave equation

CHENG Jie, DAI Zheng-de
(Department of Mathematics, Yunnan University, Kunming 650091, China)

Abstract: The dissipative generalized symmetric regularized long wave equation is considered. The existence of exponetially attractor is showed by using spectral decomposition method. The upper bounds of it's fractal dimension is obtained.

Key words: symmetric regularized long wave equation; exponential attractor; fractal dimension
MSC(2000): 35Q55; 35K57

* *

(上接第 14 页)

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] MACWILLIAMS F J, SLOANE N J A. The theory of error-correcting codes[M]. New York: Ortl-holland Publishing Company, 1977.
[3] BEN-ISREAL A, GREVILLE T N E. Generalized inverses: Theory and applications[M]. New York: John Wiley & Sons, 1974.
[4] PEARL M H. Generalized inverses of matrices with entries taken from an arbitrary field[J]. Linear Algebra and Applications, 1968, 1(5): 571—587.
[5] 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 a linear code over the general finite field $GF(p^m)$

WANG Guo-dong, YE Rui, LU Zheng-fu
(Department of Mathematics, Yunnan University, Kunming 650091, China)

Abstract: On the basis of studying the monomial matrix it is extended the result of the finite field $GF(2^m)$ to the most general finite field $GF(p^m)$, where p is any prime number.

Key words: linear code; monomial matrix; automorphism group; generalized inverse
MSC(2000): 20B25