正形阵与线性正形置换

李瑞虎，　赵全习，　郭罗斌
（空军工程大学 导弹学院，陕西 三原　713800）

摘　要：利用矩阵的有理标准型理论，给出正形阵和线性正形置换的判定定理，构造性地解决了线性正形置换的结构问题。利用本原多项式理论解决了谷大武和肖国镇提出的最大线性正形置换的计数问题。

关键词：有理标准型；正形置换；正形阵；本原多项式
中图分类号：O157.4 TN911.22　　**文献标识码**：A　　**文章编号**：1009－3516(2001)04－82－85

正形置换是一类完全映射。早在1955年，M、HALL和J、PAIGE[1]对完全映射进行了研究。近年来，人们证明正形置换具有很好的密码特性[2~3]，于是正形置换成为数学工作者和密码工作者研究的热点问题。但到目前为止人们还没有搞清楚正形置换的结构及计数问题，于是人们退而求其次，先考虑线性正形置换[4~5]，文献[4]得到了线性正形置换的一些结果及计数下界，并提出有待解决的四个问题。本文用抽象代数的方法得到线性正形置换的系统且完整结果，并解决文献[4]提出的一个问题。

设 $\boldsymbol{F}_2$ 是二元域，$\boldsymbol{F}_2^n$ 是 $\boldsymbol{F}_2$ 上 $\boldsymbol{n}$ 维行向量空间，$\boldsymbol{I}$ 是 F_2^n 的恒等置换，同时不加区别地用 I 表示 n 阶单位阵。

定义1　设 $R:F_2^n\to F_2^n$ 为置换(即双射)，若 $\boldsymbol{R}+\boldsymbol{I}$ 仍为置换，就称 $\boldsymbol{R}$ 为 $\boldsymbol{F}_2^n$ 上的正形置换，记其全体为 OP_n(有些文献记之为 $S^0(n)$，见文献[3])。并称 $\overline{\boldsymbol{R}}=\boldsymbol{R}+\boldsymbol{I}$ 为 $\boldsymbol{R}$ 的补。

定义2　设 $\boldsymbol{R}\in OP_n$，若 $\boldsymbol{R}$ 为线性的，则称 $\boldsymbol{R}$ 为线形置换，其全体记为 LOP_n。特别地若 $\boldsymbol{R}\in LOP_n$，且有

$$\overline{\boldsymbol{R}}=\begin{pmatrix}0 & X_1 & X_2 & \cdots & X_{2^n-1} & X_{2^n-1}\\ 0 & X_2 & X_3 & \cdots & X_{2^n-1} & X_1\end{pmatrix}=$$

$$(0)(X_1\quad X_2\quad \cdots\quad X_{2^n-1})$$

其中 $X_i\in\boldsymbol{F}_2^n;1\leqslant i\leqslant 2^n-1$；则称 $\boldsymbol{R}$ 为最大线性正形置换，其全体记为 $MLOP_n$。

定义3　设 $\boldsymbol{A}$ 是 F_2 上 n 阶方阵，若 $|\boldsymbol{A}|=|\boldsymbol{A}+\boldsymbol{I}|=1$，则称 $\boldsymbol{A}$ 为 F_2 上 n 阶正形阵；其全体记为 OM_n。

由文献[2][3][4]可知下面的定理成立。

定理1　设 R 为线性变换，则 $R\in LOP_n$ 当且仅当 R 在 $\boldsymbol{F}_2^n$ 的任意一组基下的矩阵是正形阵。

推论1　$\boldsymbol{A}$ 为正形阵当仅当对任意可逆阵 $\boldsymbol{P}$ 有 $\boldsymbol{PAP}^{-1}$ 仍为正形阵。

于是我们可得到 $|LOP_n|=|OM_n|$，并且可固定 $\boldsymbol{F}_2^n$ 的基 $e_1,e_2,\cdots,e_n$，其中 e_i 是第 i 个分量为1，其余分量0为 n 维列向量；设线性正形置换 R 在这组基下的矩阵记为 $\boldsymbol{A}$(在易混淆时可记之为 $\boldsymbol{A}_R$)，于是可将对 R 的研究转化为对 $\boldsymbol{A}$ 的研究。

1　有理标准形

设 $\boldsymbol{A}$ 是 $\boldsymbol{F}_2$ 上 n 阶方阵，λ 是 $\boldsymbol{F}_2$ 上未定元，矩阵 $\boldsymbol{\lambda J}-\boldsymbol{A}$ 叫 $\boldsymbol{A}$ 的特征矩阵；由文献[6、7]可知 $\boldsymbol{\lambda J}-\boldsymbol{A}$ 经过一系列初等变换可变成对角形 $\boldsymbol{D}=\mathrm{diag}\{1,1,\cdots,1,d_1(\lambda),d_2(\lambda),\cdots,d_k(\lambda)\}$，其中 $\partial d_1(\lambda)\geqslant 1$ 且 $d_i(\lambda)\mid d_{i+1}(\lambda),1\leqslant i\leqslant k$。

收稿日期：2000－08－17
作者简介：李瑞虎(1966－)，男，安徽亳州人，副教授，硕士，主要从事代数编码与密码学研究.

下文叙述中总是对 $d_i(\lambda)$ 作如上假设。

定义 4　设 $\lambda I - A$ 经初等变换变成对角形 $D = \mathrm{diag}\{1,1,\cdots,1,d_1(\lambda),d_2(\lambda),\cdots,d_k(\lambda)\}$,则 $1,1,\cdots,1,d_1(\lambda),d_2(\lambda),\cdots,d_k(\lambda)$ 为 A 的不变因子。

由文献[6~7]易知 $d_k(\lambda)$ 是 A 的最小多项,$\prod_{i=1}^{k} d_i(\lambda) = f(\lambda)$ 是 A 的特征多项式。

定义 5　设 $g(\lambda) = \lambda^m \pm a_1\lambda^{m-1} + \cdots + a_{m-1}\lambda + a_m$ 为 F_2 上多项式,m 阶方阵

$$N_0 = C(g(\lambda)) = \begin{pmatrix} 0 & & & 0 & a_m \\ 1 & 0 & & 0 & a_{m-1} \\ & 1 & \ddots & & \vdots \\ & & & & \vdots \\ & & & 0 & a_2 \\ & & & 1 & a_1 \end{pmatrix}$$

叫做 $g(\lambda)$ 的友矩阵。在一定条件下 N_0 为正形阵,并叫做 m 阶典型正形阵。

引理 1　N_0 为正形阵$\Leftrightarrow a_m = 1$ 且 $\sum_{i=1}^{m} a_i = 0 \Leftrightarrow g(\lambda)$ 没有一次因式。

证明　因 $|N_0| = a_m$,$|N_0 + I| = 1 + \sum_{i=1}^{m} a_i$,

故 N_0 为正形阵$\Leftrightarrow a_m = 1$ 且 $\sum_{i=1}^{m} a_i = 1$。

又因 $g(0) = a_m$,$g(1) = 1 + \sum_{i=1}^{m} a_i$,

故 N_0 为正形阵$\Leftrightarrow g(\lambda)$ 没有一次因式。

引理 2 文献[6~7]设 A 的不变因子为 $1,1,\cdots,1,d_1(\lambda),\cdots,d_k(\lambda)$,$N_i$ 为 $d_i(\lambda)$ 的友矩阵,则 A 相似于

$$N = \begin{pmatrix} N_1 & & & \\ & N_2 & & \\ & & & \\ & & & N_k \end{pmatrix} = diag\{N_1, N_2, \cdots, N_k\}$$

引理 2 中的 N 叫 A 的有理标准型。

定理 2　设 A 的不变因子为 $1,1,\cdots,1,d_1(\lambda),d_2(\lambda),\cdots,d_k(\lambda)$,$N_i$ 为 $d_i(\lambda)$ 的友阵,则 A 为正形阵$\Leftrightarrow$ N_i 为正形阵,$1 \leqslant i \leqslant k \Leftrightarrow d_i(\lambda)$ 没有一次因式,$1 \leqslant i \leqslant k \Leftrightarrow d_k(\lambda)$ 没有一次因式$\Leftrightarrow A$ 的特征多项式 $f(\lambda)$ 没有一次因式。

证明　因 A 与它的有理标准形 $N = diag\{N_1, N_2, \cdots, N_k\}$ 相似,故 A 为正形阵$\Leftrightarrow N$ 为正形阵。

因 $|N| = |N_1||N_2|\cdots|N_k|$,$|N + I| = |N_1 + I_{n_1}||N_2 + I_{n_2}|\cdots|N_k + I_{n_k}|$ 其中 $n_i = \partial(d_i(\lambda))$,$1 \leqslant i \leqslant 2^n - 1$。

由于 $d_i(\lambda) | d_k(\lambda)$,$f(\lambda) = \prod_{i=1}^{k} d_i(\lambda)$;故据引理 1 可知 A 为正形阵$\Leftrightarrow N$ 为正形阵$\Leftrightarrow N_i$ 为正形阵,$1 \leqslant i \leqslant k$ $\Leftrightarrow d_i(\lambda)$ 没有一次因式$\Leftrightarrow d_k(\lambda)$ 没有一次因式$\Leftrightarrow f(\lambda)$ 没有一次因式。

定理 3　F_2^n 的线性变换 R 为正形置换$\Leftrightarrow R$ 在基 $e_1, e_2, \cdots, e_n$ 下的矩阵 A 的特征多项式没有一次因式。

2　最大线性正形置换的判定与计数

文献[8]给出用最大线性正形置换构造非线性正形置换的算法,用文献[8]的方法只要找出一个最大线性正形置换就能得到一批非线性正形置换。下面我们给出最大线性正形置换的判定定理与最大线性正形置换的计数公式。

引理 3　设线性正形置换 R 在基 $e_1, e_2, \cdots, e_n$ 下的矩阵为 A,若 A 的不变因子为 $1,1,\cdots,1,d_(\lambda)$, $d_2(\lambda),\cdots,d_k(\lambda)$,$N = diag\{N_1, N_2, \cdots, N_k\}$ 是 A 的有理标准型;若 $k \geqslant 2$,则 R 不是最大线性正形置换。

证明　令 $\partial(d_i(\lambda)) = n_i$,$1 \leqslant i \leqslant k$,则 $n_1 + n_2 + \cdots + n_k = n$,且每个 $n_i > 2$。

由于 A 相似于 N,故存在 F_2^n 的一组基 $\beta_1, \beta_2, \cdots, \beta_{n_1}, \beta_{n_1+1}, \cdots, \beta_{n_1+n_2}, \cdots, \beta_n$,使得 R 在该组基下的矩阵为 $N = diag\{N_1, N_2, \cdots, N_k\}$。

设 $L_{n_1}^* = <\beta_1,\cdots,\beta_{n_1}>\backslash\{0\}$, $L_{n_2}^* = <\beta_{n_1+1},\cdots,\beta_{n_1+n_2}>\backslash\{0\}$, $L_{n_k}^* = <\beta_{\sum_{i=1}^{k-1}n_i},\cdots,\beta_n>\backslash\{0\}$,

则 $R(L_{n_i}^*)\subset L_{n_i}^*$, $1\leqslant i\leqslant k$;从而 $\boldsymbol{R}$ 的不相交轮换的个数 $\geqslant k+1$ 个;由于 $k\geqslant 2$ 故 $\boldsymbol{R}$ 不是最大线性正形置换。

定义 6[7] 设 $g(\lambda)$ 是 F_2 上常数项为 1 的非常数多项式,使得 $g(\lambda)\mid(\lambda^l-1)$ 的最小自然数 l 叫做 $g(\lambda)$ 的周期,记为 $p(g(\lambda))=l$。

定理 4 设线性正形置换 $\boldsymbol{R}$ 在基 $e_1,e_2,\cdots,e_n$ 上的矩阵为 A, A 的特征多项式为 $f(\lambda)$ 则 $\boldsymbol{R}$ 为最大线正形置换$\Leftrightarrow p(f(\lambda))=2^n-1\Leftrightarrow f(\lambda)$ 为 n 次本原多项式。

证明 (1)设 $l=p(f(\lambda))<2^n-1$,任取 $\beta_1\in F_2^n\backslash\{0\}$,令 $R^{i-1}(\beta_1)=\beta_i$, $1\leqslant i\leqslant l=1$ 则 $(\beta_1,\beta_2,\cdots,\beta_l)=(\beta_1,R(\beta_1),R^2(\beta_1),\cdots,R^{l-1}(\beta_1))$ 构成 R 的一个轮换,且它和 R 的轮换分解的其他部分不相交,故 R 不是最大线性正形置换,故当 R 为最大线性正形置换时必有 $p(f(\lambda))=2^n-1$。

(2)设 $p(f(\lambda))=2^n-1$ 则由文献[7]可知 $f(\lambda)$ 是不可约的且为本原的。故 $\boldsymbol{A}$ 的有理标准型必为

$$\boldsymbol{N}=\begin{pmatrix}0 & & & 0 & a_m\\ 1 & 0 & & 0 & a_{m-1}\\ & 1 & \ddots & \vdots & \vdots\\ & & \ddots & & \\ & & & 0 & a_2\\ & & & 1 & a_1\end{pmatrix},\text{其中 } \lambda^n+a_1\lambda^{n-1}+\cdots+a_{n-1}\lambda+a_n=f(\lambda)$$

故存在 $\boldsymbol{F}_2^n$ 的一组基 $\boldsymbol{X}_1,\boldsymbol{X}_2,\cdots,\boldsymbol{X}_n$ 使 $\boldsymbol{R}$ 在该组基下的矩阵为 $\boldsymbol{N}$,且此时有 $R^{j-1}(X_1)=X_j$, $1\leqslant j\leqslant n$,令 $R^k(X_1)=X_k$, $0\leqslant k\leqslant 2^n-2$。下面证明若 $0\leqslant s<t\leqslant 2^n-1$,则必有 $X_s\neq X_t$。否则由 $X_s=X_t$ 得 $R^t(X_1)=R^s(X_1)$,即 $R^{t-s}(X_1)=X_1$,从而有 $\boldsymbol{R}^{t-s}(X_2)=\boldsymbol{R}^{t-s+1}(X_1)=\boldsymbol{R}(X_1)=X_2$

$$\boldsymbol{R}^{t-s}(X_3)=R^{t-s+1}(X_2)=R(X_2)=X_3$$

$$\boldsymbol{R}^{t-s}(X_n)=\boldsymbol{R}^{t-s+1}(X_{n-1})=R(X_{n-1})=X_n$$

$$\therefore \boldsymbol{R}^{t-s}=I \qquad \therefore f(\lambda)\mid(\lambda^{t-s}-1)$$

这与 $p(f)=2^n-1$ 矛盾。

从而 $(X_1,X_2,\cdots,X_n,\cdots,X_{2^n-2},X_{2^n-1})$ 构成 R 的一个轮换,又由于 R 是线性的,所以 $R(0)=0$,故

$$\boldsymbol{R}=\begin{pmatrix}0 & X_1 & X_2 & \cdots & X_{2^n-2} & X_{2^2-1}\\ 0 & X_2 & X_3 & \cdots & X_{2^n-1} & X_1\end{pmatrix}=(0)(X_1\quad X_2\quad\cdots\quad X_{2^n-1})$$

即 R 是最大线性正形置换。

总结(1)(2)可知定理得证。

引理 4 若 N 是 n 阶典型正形阵, N 的特征多项式为 $f(\lambda)$ 不可约,则与 N 可交换的可逆阵的个数为 2^n-1。

证明 因 N 是循环矩阵,由文献[6]定理 3.16 的推论可知与 N 可交换的矩阵只有 N 的多项式。

令 $\varphi(N)$ 是 N 的多项式,由于 $f(N)=0$,故 $\varphi(N)$ 可写成一个次数小于等于 $n-1$ 的多项式 $\varphi_1(N)$,其中 $\varphi(\lambda)=\varphi_1(\lambda)(\mathrm{mod}f(\lambda))$。若 $\varphi_1(N)\neq 0$,则 $\varphi_1(N)$ 必可逆。否则令 $h(N)\varphi_1(N)=0$,其中 $\partial(h(\lambda))\leqslant n-1$ 且 $h(\lambda)\neq 0$ 则 $f(\lambda)\mid\varphi_1(\lambda)h(\lambda)$,由于 $f(\lambda)$ 不可约可知 $f(\lambda)\mid\varphi_1(\lambda)$ 或 $f(\lambda)\mid h(\lambda)$,矛盾。

由于次数小于 n 且非零的多项式的个数为 2^n-1,故与 N 可交换的可逆阵的个数为 2^n-1。

定理 5 n 阶最大线性正形置换的个数为 $\mid MLOP_n\mid=\dfrac{\varphi(2^n-1)}{n}\cdot\mid GL_n(F_2)\mid/2^n-1$,其中 φ 为欧拉函数, $GL_n(F_2)$ 为 F_2 上 n 阶一般线性群。

证明 设 R 为最大线性正形置换,它在基 $e_1,e_2,\cdots,e_n$ 下的矩阵为 $\boldsymbol{A}$, $\boldsymbol{A}$ 的特征多项式为 $f(\lambda)$,则 $f(\lambda)$ 为本原多项式。由于 F_2 上 n 次本原多项式的个数为 $\dfrac{\varphi(2^n-1)}{n}$,故互不相似的 $\boldsymbol{A}$ 的类数为 $\dfrac{\varphi(2^n-1)}{n}$ 个。

记与 $\boldsymbol{A}$ 相似的矩阵的集合为 $S(\boldsymbol{A})$,让 $GL_n(F_2)$ 按照 $PXP^{-1}(X\in S(\boldsymbol{A}))$ 作用在 $S(\boldsymbol{A})$ 上,则此作用是可迁的,且在 $\boldsymbol{A}$ 点处的稳定子群 $\mathrm{stab}(\boldsymbol{A})$ 是一个 2^n-1 阶子群,故 $\mid S(\boldsymbol{A})\mid=\lfloor GL_n(F_2);\mathrm{stab}(\boldsymbol{A})\rfloor=\mid GL_n(F_2)$

$|/2^n-1$。

总结以上就证得 $|MLOP_n| = \frac{\varphi(2^n-1)}{n} \cdot |GL_n(F_2)|/2^n-1$。

至此我们已完全地回答了文献[4]提出的关于 $MLOP_n$ 的问题。

参考文献:

[1] Hall M, Paige L J. Complete mapping of finite groups[J]. Pacific J Math, 1955, (5): 541 - 549.

[2] 刘振华,舒　畅. 正形置换的研究与应用[A]. 龚奇敏. 第五届通信保密论文集[C]. 北京:科学出版社,1995,39 - 43.

[3] 冯登国,刘振华. 关于正形置换的构造[J]. 通信保密,1996,18(2):61 - 64.

[4] 谷大武,肖国镇. 关于正形置换的构造与计数[J]. 西安电子科技大学学报,1997,24(3):381 - 385.

[5] 亢保元,田建波,王育民. 线性置换与正形置换[J]. 西安电子科技大学学报,1998,25(2):254 - 255.

[6] Jackbson N. Basic Algebra(I)[M]. New York: W. H. Freeman and Commpany, 1985.

[7] 万哲先. 代数与编码[M]. 北京:科学出版社,1985.

[8] Mittcnthal L. Block Substitutions using orthomorphic mapping[J]. Advance in Applied Mathematice, 1995, 16(1): 59 - 71.

Orthomorphic Matrix and Linear Orthomorphic Permutation

LI Rui-hu,　ZHAO Quan-xi,　GUO Luo-bin

(The Missile Institute of the Air Force Engineering University, Sanyuan 713800, China)

Abstract: A criterion theorem of orthomorphic matrix and linear orthomorphic permutation is obtained by using rational standard theory of matrix and the structure of Linear orthomorphic permutation is also solved by a constructive approach. The enumeration problem of MLOP put forward by Gu Dawu and Xiao guozhen is answered by using primitive polynomial.

Key words: rational canonical form; orthomorphic matrix; orthomorphic permutation; primitive polynomial.