变换矩阵(mod n)的阶及两种推广 Arnold 变换矩阵*

杨礼珍 陈克非**

(上海交通大学计算机科学与工程系, 上海 200030)

摘要 分析了矩阵(mod n)的阶的结构, 然后给出有限域上的矩阵的阶与其Jordan标准形的关系. 接着给出两种2维Arnold变换矩阵的n维推广: A型Arnold变换矩阵和B型Arnold变换矩阵, 并在给出的关于矩阵阶的结果的基础上给出它们的阶的分析结果和其他性质.

关键词 矩阵 Jordan标准形 有限域 信息隐藏

随着网络技术的快速发展, 越来越多的私有信息和公众信息通过网络传播. 如何通过网络安全地传递信息成为一个迫切需要解决的问题, 现已发展了不少技术来保证信息的安全, 信息隐藏是其中一项重要技术. 信息隐藏[1]包含数字水印(watermark)、数字指纹(fingerprint) 和信息伪装(steganography). 置乱技术是图像信息隐藏的一项技术[2], 本文将对置乱技术的两个方面进行研究: 变换矩阵(或矩阵(mod n))的阶的理论分析, 以及提出新的置乱变换并对之进行分析.

确定变换矩阵的阶是置乱变换的重要方面, 但现有文献中缺少这方面的理论分析结果, 仅有文献[2]研究了矩阵变换(模运算)具有周期(即阶)的充要条件; 因此, 在本文中我们对矩阵的阶进行了理论分析: 在第二部分, 给出了矩阵的阶的结构, 在第三部分, 给出了矩阵的阶与其Jordan标准形的关系.

文中的另一方面是提出两种新的n维Arnold变换[3]矩阵: A型和B型Arnold变换矩阵. Arnold 变换由于对图像的置乱处理具有良好的效果而受到重视[2]: 文献[4]把平面 Arnold 变换推广到三维空间, 文献[2]推广到任意 n 维空间. 本文中, 不仅给出了两种新的 Arnold 变换的推广, 且在矩阵的阶的理论结果上给出它们

2003-02-26 收稿, 2003-05-27 收修改稿
* 国家自然科学基金重大研究计划资助项目(批准号: 90104005)及国家"八六三"计划资助项目(2001AA144060)
** E-mail: chen-kf@cs.sjtu.edu.cn

的性质及阶的分析结果; 这些将在第四部分给出.

1 基本定义及已有结论

记号: gcd(•)表示最大公约数, lcm(•)表示最小公倍数, min(•)表示取最小的数, $[x]$表示 x 的整数部分, $\lfloor x \rfloor$表示地板函数, det(A)记为矩阵 A 的行列式, I 记为单位矩阵, R 表示环, F 表示域, $GF(q)$表示阶为 q 的有限域; $a \mid b$ 表示 a 整除 b.

定义 1 对于一给定的素数 p, 设 $p^m \| n$, 即 $p^m \mid n$, $p^{m+1} \nmid n$, 则记 $pot_p n = m$.

定义 2 环 R 上的 n 维矩阵构成的环记为 $M_n(R)$, $M_n(R)$上的可逆元的全体记为 $GL_n(R)$.

定理 A[5] 环 R 上的 $GL_n(R)$对矩阵乘法构成一个群.

定理 B[5] 如果 R 是一个交换环, 那么矩阵 $A \in M_n(R)$ 是可逆的当且仅当它的行列式在 R 中是可逆的.

定义 3 域 F 上的元素 α 的阶定义为 $\min\{n : \alpha^n = 1, n \in \mathbb{Z}^+\}$, 记为 $ord_F(\alpha)$, $F = GF(q)$ (q 为素数 p 的乘幂)时, 简记为 $ord_q(\alpha)$.

定义 4 环 R 上的可逆矩阵 A 的阶定义为 $\min\{n : A^n = 1, n \in \mathbb{Z}^+\}$, 记为 $ord_R(A)$, 当 $R = Z_N$ 时简记为 $ord_N(A)$.

定义 5[2] 对给定的 N 阶数字图像 P, 我们说变换

$$\begin{pmatrix} x_1' \\ x_2' \\ \vdots \\ x_n' \end{pmatrix} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} (\mathrm{mod}\, N) \tag{1}$$

(a_{ij} 为整数, $x_1, \cdots, x_n \in \{0,1,\cdots,N-1\}$)关于 P 的周期为 m_N, 指 m_N 是使得图像 P 经一系列变换后回复到 P 的最少次数.

变换矩阵不是对所有的向量都具有周期, 如所有矩阵对 0 向量都具有周期, 不可逆矩阵可能对非零向量不具有周期, 这里只讨论对所有的向量都具有周期的矩阵. 以下定理说明了矩阵变换对所有向量都具有周期的充分必要条件.

定理 C[2] 矩阵变换 A 对所有向量都具有周期的充分必要条件是 det(A)与 N 互素. 此处 A 是变换的矩阵.

注 1 由定理 B 可知 det (A)与 N 互素, 即 $A \in GL_n(Z_N)$.

可逆矩阵 A 对不同向量的周期是不同的, 如所有可逆矩阵对零向量的周期都是 1, 但对非零向量的周期就比较复杂, 因为矩阵 A 可逆, 所以必存在正整数 m 使得 $A^m = I$, 这时对所有 $y \in (Z_n)^n$ 恒有 $y = A^m y$, 所以我们只讨论矩阵 A 的阶 $ord_N(A)$.

2　矩阵的阶的结构

下面我们给出 $GL_n(Z_N)$上的矩阵的阶的结构分析.

定理 1　N 为正整数, 且 $N = uv$, u 和 v 互素, 对任意 Z 上的矩阵 A 满足 $A\bmod(N)\in GL_n(Z_N)$, 有

$$ord_N(A\bmod(N)) = lcm(ord_u(A\bmod(u)), ord_v(A\bmod(v))).$$

证　因为 $A\bmod(N)\in GL_n(Z_N)$, 由定理 B 得到 $\det(A)(\bmod N)$和 N 互素, 所以 $\det(A)(\bmod u) = \det(A)(\bmod N)(\bmod u)$与 u 互素, 由定理 B 得到 $A\bmod(u)$是 $M_n(Z_u)$的可逆元. 同理 $A\bmod(v)$是 $M_n(Z_v)$上的可逆元. 因此 $A\bmod(u)$和 $A\bmod(v)$分别在 $M_n(Z_u)$和 $M_n(Z_v)$上存在阶.

记 $u' = ord_u(A(\bmod u))$, $v' = ord_v(A(\bmod v))$, 因为

$$A^{u'} \equiv I(\bmod u), \tag{2}$$

其中, u' 是满足等式(2)的最小正整数, 所以存在 $B\in M_n(Z_u)$, $B\not\equiv 0(\bmod u)$, 以及整数 $k>0$, 使得 $A^{u'} = I + u^k B$. 设 $m = \mathrm{lcm}(u', v')$, $s = m/u'$. 考察以下二项展开式:

$$A^m = (I + u^k B)^s = I + C_s^1 u^k B + \cdots + C_s^{s-1} u^{k(s-1)} B^{s-1} + u^{ks} B^s, \tag{3}$$

由上式得到 $A^m \equiv I(\bmod u)$. 同理可证 $A^m \equiv I(\bmod v)$. 因为 u 和 v 互素, 所以 $A^m \equiv I(\bmod m)$, 因此 $ord_N(A(\bmod N)) \mid \mathrm{lcm}(ord_u(A(\bmod u)), ord(A\bmod(v)))$. 另一方面, 设 $N' = ord_N(A(\bmod N))$, 必存在 $C\in M_n(Z_N)$, $C\not\equiv 0(\bmod N)$, 以及整数 $h>0$, 使得 $A^{N'} = I + N^h C$, 所以 $A^{N'} \equiv I(\bmod u)$, 因此 $ord_u(A(\bmod u)) \mid N'$. 同理 $ord_v(A(\bmod v)) \mid N'$, 所以 $\mathrm{lcm}(ord_u(A(\bmod u)), ord_v(A(\bmod v))) \mid N'$. 综上所述, 即可得到 $ord_N(A\bmod(N)) = \mathrm{lcm}(ord_u(A\bmod(u)), ord_v(A\bmod(v)))$.

由定理 1 立即得到以下结论:

定理 2　N 为正整数, 且 N 的因式分解为 $N = p_1^{r_1}\cdots p_m^{r_m}$, 其中 p_i 和 p_j $(i \neq j)$ 是互不相同的素数, $r_i \geqslant 1$ $(1\leqslant i\leqslant m)$, 那么对任意 Z 上的矩阵 A 满足 $A\bmod(N)\in GL_n(Z_N)$ 有 $ord_N(A\bmod(N)) = \mathrm{lcm}(ord_{p^{r_i}}(A\bmod(p^{r_i})), i = 1,\cdots,m)$.

所以只要确定了模为素数幂的矩阵的阶, 即可求出模为合数的阶.

下面对文献[6]的两个定理进行推广, 这两个定理是关于模为素数的乘幂时, 关于矩阵的阶的结论. 虽然文献[6]的结论只针对 2 阶矩阵, 但其证明是和矩阵的阶数无关的, 所以我们不加证明直接引用推广后的定理.

定义 6　设 p 是素数, 令 k_j 记为 $A \bmod p^j$ 的阶.

记 $A^{k_1} = I + p^s B$, $B\not\equiv 0(\bmod p)$, 其中整数 $s>0$.

定理 D[6]　如果素数 p 是奇数, 或者 $s>1$, 那么 $k_1 = k_2 = \cdots = k_s$, 并且对所有的 $i = 1, 2, \cdots$, 有 $k_{s+i} = p^i k_1$.

定理 E[6] 设 $p=2$, $s=1$, 那么 $k_2=2k_1$, 设 $A^{k_2}=I+2^tD$, 其中 $D\not\equiv 0(\mathrm{mod}\,2)$, 那么当 $2\leqslant i\leqslant t$ 时, $k_i=k_2$, 当 $i>t$ 时, $k_i=2^{i-t}k_2$.

注 2 定理 E 在表达形式上与文献[6]稍有差别.

3 有限域上的矩阵的阶

这一部分我们将给出有限域上的矩阵的阶与其 Jordan 标准形的关系.

定义 7 矩阵 A 和 B 相似, 如果存在可逆矩阵 P 使得 $A=P^{-1}BP$.

接下来我们有关于相似矩阵的阶的结论, 结论是显而易见的.

定理 3 设 R 是环, n 为任意正整数, 那么 $GL_n(R)$上的相似矩阵的阶相同.

定理 4 设 F 是域, F' 是 F 的扩域, n 为任意正整数, $A\in GL_n(F)$, 那么 A 在 F 上的阶等于 A 在 F' 上的阶.

定义 8 Jordan 子块 $J_\alpha(n)$为$n\times n$矩阵$\begin{bmatrix}\alpha & 0 & \cdots & 0\\ 1 & \alpha & \cdots & 0\\ \vdots & \vdots & & \vdots\\ 0 & 0 & \cdots & \alpha\end{bmatrix}$.

引理 1[7]

$$J_\alpha(n)^m=\begin{bmatrix}\alpha^m & 0 & \cdots & 0 & 0\\ C_m^1\alpha^{m-1} & \alpha^m & \cdots & 0 & 0\\ \vdots & C_m^1\alpha^{m-1} & \cdots & 0 & 0\\ C_m^{\min\{m,n-1\}}\alpha^{m-\min(m,n-1)} & \vdots & \cdots & 0 & 0\\ 0 & C_m^{\min\{m,n-1\}}\alpha^{m-\min(m,n-1)} & \cdots & \cdots & 0\\ \vdots & 0 & \cdots & \cdots & \cdots\\ & \vdots & \cdots & C_m^1\alpha^{m-1} & \alpha^m\end{bmatrix}.$$

定理 F(Lucas 相似定理)[8] 令 p 为素数及

$$r=r_mp^m+\cdots+r_1p+r_0\ (0\leqslant r_i<p),$$
$$k=k_mp^m+\cdots+k_1p+k_0\ (0\leqslant k_i<p),$$

那么 $C_r^k=\prod_{i=0}^{m}C_{r_i}^{k_i}(\mathrm{mod}\,p)$.

引理 2 设 p 为素数, 整数 $n>1$, $r=a_fp^f+\cdots+a_1p+a_0$, 这里, $1\leqslant a_f<p$, $0\leqslant a_i<p$, $i=0,1,\cdots,f-1$, $1\leqslant r<n$; 那么 $C_n^1\equiv C_n^2\equiv\cdots\equiv C_n^r\equiv 0(\mathrm{mod}\,p)$ 当且仅当 $p^{f+1}\mid n$.

证 设 $n=b_gp^g+\cdots b_1p+b_0$, 其中, $1\leqslant b_g<p$, $0\leqslant b_j<p$, $j=0,1,\cdots,g-1$. 显然 $g\geqslant f$.

1) 充分性. 因为 $p^{f+1}\mid n$, 所以 $b_0=b_1=\cdots=b_f=0$. 对任意 $1\leqslant m\leqslant r$, 设

$m=c_hp^h+\cdots+c_1p+c_0$, 其中, $1\leqslant c_h<p$, $0\leqslant c_j<p$, $j=0,1,\cdots,h-1$; 根据定理 F, 有 $C_n^m\equiv\prod_{i=0}^{h}C_{b_i}^{c_i}\equiv 0(\mathrm{mod}\ p)$.

2) 必要性. 对任意 $m=p^h\leqslant r$, 其中 $0\leqslant h\leqslant f$, 由题意及定理 F 知, $C_n^m\equiv C_{b_h}^1\equiv b_h\equiv 0(\mathrm{mod}\ p)$, 故 $b_h=0$, $0\leqslant h\leqslant f$, 因此 $p^{f+1}\mid n$.

引理 3　设 q 是素数 p 的乘幂, α是有限域 $GF(q)$上的可逆元, $n>1$, $n-1=a_fp^f+\cdots+a_1p+a_0$, 这里, $1\leqslant a_f<p$, $0\leqslant a_i<p$, $i=0,1,\cdots,f-1$, 那么 $ord_{GF(q)}(J_\alpha(n))=p^{f+1}\cdot ord_{GF(q)}(\alpha)$.

证　由引理 1 容易得到 $J_\alpha(n)^m=I$, 当且仅当$\alpha^m=1$, $C_m^i\alpha^{m-i}=0$, $i=1,\cdots,\min(m,n-1)$. 而$\alpha^m=1$ 当且仅当 $ord_{GF(q)}(\alpha)\mid m$. 因为$\alpha$为可逆元, 所以 $C_m^i\alpha^{m-i}=0$ 当且仅当 $C_m^i\equiv 0(\mathrm{mod}\ p)$. 若 $C_m^{\min(m,n-1)}\equiv 0(\mathrm{mod}\ p)$, 则 $\min(m,n-1)\neq m$, 即 $m>n-1$, 那么由引理 2 得到 $C_m^i\equiv 0(\mathrm{mod}\ p)$ ($i=0,\cdots,n-1$)当且仅当 $p^{f+1}\mid m$, 其中f为引理所定义.

综上所述, $J_\alpha(n)^m=I$ 当且仅当 $\mathrm{lcm}(ord_{GF(q)}(\alpha),p^{f+1})\mid m$, 因为 $ord_{GF(q)}(\alpha)$ 和 p 互素, 故 $ord_{GF(q)}(J_\alpha(n))=p^{f+1}\cdot ord_{GF(q)}(\alpha)$.

定理 5　设 p 是素数, F 是特征为 p 的有限域, $A\in GL_n(F)$, A 的特征多项式为 $f(\lambda)$, $f(\lambda)$的分裂域为 F', 其所有特征根为 $\lambda_1,\cdots,\lambda_m$, λ_i 所对应的 Jordan 块的维数为 $k_{i,j}$, $j=1,\cdots,s_i$, 设 $k=\max\{k_{i,j},\ i=1,\cdots,m,\ j=1,\cdots,s_i\}$. 若 $k=1$, 则 $ord_F(A)=\mathrm{lcm}(ord_{F'}(\lambda_1),\cdots,ord_{F'}(\lambda_m))$; 若 $k>1$, 设 $k-1=a_fp^f+\cdots+a_1p+a_0$, 其中, $1\leqslant a_f<p$, $0\leqslant a_u<p$, $u=0,1,\cdots,f-1$; 那么, $ord_F(A)=p^{f+1}\mathrm{lcm}(ord_{F'}(\lambda_1),\cdots,ord_{F'}(\lambda_m))$.

证　A 和以下形式的 Jordan 标准形相似[9]:

$$\begin{bmatrix} J_{\lambda_1}(k_{1,1}) & 0 & & \cdots & & 0 \\ 0 & \ddots & \ddots & & & \\ & \ddots & J_{\lambda_1}(k_{1,s_1}) & 0 & & \vdots \\ \vdots & & 0 & J_{\lambda_2}(k_{2,1}) & \ddots & \\ & & & \ddots & \ddots & 0 \\ 0 & & \cdots & & 0 & J_{\lambda_m}(k_{m,s_m}) \end{bmatrix}.$$

因此矩阵A的阶等于其Jordan形的各个Jordan子矩阵的阶的最小公倍数, 由引理 3 容易得到结论.

注 3　求 $\mathrm{ord}_F(A)$的关键在于计算 $d=\mathrm{lcm}(ord_{F'}(\lambda_1),\cdots,ord_{F'}(\lambda_m))$, 其中$\lambda_1,\cdots,\lambda_m$ 为矩阵的所有特征根. 若 F 的特征为 p, A 的维数为 n, 则 $\mathrm{ord}_F(A)=$

$\min\{p^f d \mid A^{p^f d} = I,\ 0 \leqslant f \leqslant \lfloor \log_p(n-1) \rfloor + 1\}$. 因此已知 d 计算 $\mathrm{ord}_F(A)$的复杂度最多为 $O(\log_p(n-1)\log_2 pn^3 + \log_2^d n^3)$.

4 两种新的推广 n 维 Arnold 变换

4.1 基本 Arnold 变换

定义 9[2] 设有单位正方形上的点(x, y), 将点(x, y)变成另一点 (x', y') 的变换为

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\mathrm{mod}\, N). \tag{4}$$

此变换称作二维 Arnold 变换, 简称 Arnold 变换.

4.2 文献[2]所推广的 n 维 Arnold 变换

文献[2]把基本的 Arnold 变换推广到了以下形式的 n 维 Arnold 变换:

$$\begin{pmatrix} x_1' \\ x_2' \\ \vdots \\ x_n' \end{pmatrix} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 2 & 2 & \cdots & 2 & 2 \\ 1 & 2 & 3 & \cdots & 3 & 3 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 1 & 2 & 3 & \cdots & n-1 & n-1 \\ 1 & 2 & 3 & \cdots & n-1 & n \end{bmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} (\mathrm{mod}\, N). \tag{5}$$

4.3 两种新的 n 维 Arnold 变换矩阵

下面我们对 2 维 Arnold 变换矩阵做两种类型的推广, 分别称为 A 型 n 维 Arnold 变换矩阵和 B 型 n 维 Arnold 变换矩阵. 文献[2]中的推广是 B 型 Arnold 变换矩阵的一种类型.

4.3.1 A 型 Arnold 变换矩阵

Massey[10]在其设计的 SAFER 类型分组密码中使用了一种"伪随机 Hadamard 变换(pseduo-Hadamard transform)", 简称 PHT, 其中 2-PHT 定义为

$$H_2 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix},$$

并在文献[10]中把 2 维 PHT 推广到 n 维, 记为 n-PHT, 定义如下:

$$H_n = \begin{bmatrix} 2 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 2 & 1 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 1 & 1 & 1 & \cdots & 2 & 1 \\ 1 & 1 & 1 & \cdots & 1 & 1 \end{bmatrix}, \tag{6}$$

为了和 2 维 Arnold 变换矩阵相一致, 同时受 n-PHT 启发, 我们定义了如下的

n 维 Arnold 变换矩阵.

定义 10　Z_N 上的 A 型 n 维 Arnold 变换矩阵为以下 $n\times n$ 矩阵:

$$Ra_n=\begin{bmatrix}1&1&1&\cdots&1&1\\1&2&1&\cdots&1&1\\\vdots&\vdots&\vdots&&\vdots&\vdots\\1&1&1&\cdots&2&1\\1&1&1&\cdots&1&2\end{bmatrix}. \tag{7}$$

定理 6　Ra_n 和 H_n 相似.

证　$n=2$ 时, 令 $P=\begin{bmatrix}0&1\\1&0\end{bmatrix}$, $n>2$ 时, 令 $P=\begin{bmatrix}0&0&1\\0&I_{n-2}&0\\1&0&0\end{bmatrix}$, 其中 I_{n-2} 是 $(n-2)\times(n-2)$ 单位矩阵, 有 $P^{-1}=P$, 而且 $H_n=P^{-1}Ra_nP$.

由定理 3 得到, H_n 和 Ra_n 有相同的阶, 所以只需要讨论 Ra_n 的阶, 就可以得到 H_n 的阶.

容易证明以下性质:

性质 1　环 Z_N 上的 A 型 Arnold 变换矩阵的行列式恒为 1.

性质 2　环 Z_N 上的 A 型 n 维 Arnold 变换矩阵的可逆矩阵为

$$\begin{bmatrix}n&-1&-1&\cdots&-1&0\\-1&1&0&\cdots&0&0\\-1&0&1&\cdots&0&0\\\vdots&\vdots&\vdots&&\vdots&\vdots\\-1&0&0&\cdots&1&0\\-1&0&0&\cdots&0&1\end{bmatrix}.$$

定理 7　n 为大于 1 的整数, N 为 2 的乘幂时, A 型 Arnold 变换矩阵 Ra_n 的阶为

1) n 为偶数时, 令 $t=\begin{cases}2+pot_2(k+1), & n=4k+2,\\3+pot_2k, & n=4k;\end{cases}$ $s=\begin{cases}3, & n=4k+2,\\6, & n=4k.\end{cases}$ 那么

$$ord_{2^i}(Ra_n)=\begin{cases}3, & i=1,\\s, & i=2,\cdots,t,\\s\cdot 2^{i-t}, & i>t.\end{cases}$$

2) n 为奇数时, 令 $t=\begin{cases}2+pot_2(k+1), & n=4k+3,\\1, & n=4k+1,\end{cases}$ 那么 $ord_{2^i}(Ra_n)$

$$=\begin{cases}4, & i=1,\cdots,t,\\2^{i-t+2}, & i>t.\end{cases}$$

证　对 Ra_n 进行分块:

$$Ra_n=\begin{bmatrix}1 & \alpha\\ \alpha^{\mathrm{T}} & X+I_{n-1}\end{bmatrix},$$

其中$\alpha=(1,\cdots,1)$为 $n-1$ 维向量，I_{n-1}是$(n-1)\times(n-1)$单位矩阵，X是所有元素均为 1 的$(n-1)\times(n-1)$矩阵. 那么

$$Ra_n{}^2=\begin{bmatrix}n & (n+1)\alpha\\ (n+1)\alpha^{\mathrm{T}} & (n+2)X+I_{n-1}\end{bmatrix},\ Ra_n{}^3=\begin{bmatrix}a & b\alpha\\ b\alpha^{\mathrm{T}} & cX+I_{n-1}\end{bmatrix},$$

$$Ra_n{}^4=\begin{bmatrix}d & e\alpha\\ e\alpha^{\mathrm{T}} & fX+I_{n-1}\end{bmatrix}.$$

其中，$a=n^2+n-1$，$b=n(n+2)$，$c=(n+1)(n+2)$，$d=n^3+2n^2-n-1$，$e=(n+1)(n^2+2n-1)$，$f=(n+1)(n^2+3n+1)$.

容易验证，对所有 $n>1$，$Ra_n{}^2\not\equiv I_n(\mathrm{mod}\,2)$.

1) 当 n 为偶数时:

1.1) 容易验证，$Ra_n{}^3\equiv I_n(\mathrm{mod}\,2)$，所以$ord_2(Ra_n)=3$.

1.2) 令$B=Ra_n{}^3-I_n=\begin{bmatrix}a-1 & b\alpha\\ b\alpha^{\mathrm{T}} & cX\end{bmatrix}$. 考察$\gcd(a-1,b,c)=n+2$，所以当$n=4k+2$时，有$2^{-1}B\equiv 0(\mathrm{mod}\,2)$，根据定理 D，若$t=pot_2\gcd(a-1,b,c)=2+pot_2(k+1)$，则当$2\leqslant i\leqslant t$时，$ord_{2^i}(Ra_n)=3$，当$i>t$时，$ord_{2^i}(Ra_n)=3\cdot 2^{i-t}$.

1.3) 若 $n=4k$，有$2^{-1}B\not\equiv 0(\mathrm{mod}\,2)$，根据定理 E，$ord_4(Ra_n)=2ord_2(Ra_n)=6$.

$$Ra_n^6=\begin{bmatrix}a^2+(n-1)b^2 & b(a+(n-1)c+1)\alpha\\ b(a+(n-1)c+1)\alpha^{\mathrm{T}} & (b^2+(n-1)c^2+2c)X+I_{n-1}\end{bmatrix}.$$

因为

$$a^2+(n-1)b^2-1=n(n-1)(n+2)(n^2+3n+1),$$

$$b(a+(n-1)c+1)=n(n+1)(n+2)(n^2+2n-2),$$

$$b^2+(n-1)c^2+2c=n(n+2)(n^3+4n^2+3n-1);$$

且n^3+4n^2+3n-1为奇数，所以

$$\begin{aligned}t&=pot_2\gcd(a^2+(n-1)b^2-1,\ b(a+(n-1)c+1),\ b^2+(n-1)c^2+2c)\\&=pot_2[n(n+2)]=3+pot_2k.\end{aligned}$$

由定理 E 得到，当 $2\leqslant i\leqslant t$ 时，$ord_{2^i}(Ra_n)=ord_4(Ra_n)=6$，当 $i>t$ 时，$ord_{2^i}(Ra_n)=6\cdot 2^{i-t}$.

2) 当 n 为奇数时:

2.1) 容易验证，$Ra_n{}^3\not\equiv I_n(\mathrm{mod}\,2)$，$Ra_n{}^4\equiv I_n(\mathrm{mod}\,2)$，所以$ord_2(Ra_n)=4$.

2.2) 设 $g=d-1=(n+1)(n^2+n-2)$, 令 $g'=n^2+n-2$, $e'=n^2+2n-1$, $f'=n^2+3n+1$; 那么 $g=(n+1)g'$, $e=(n+1)e'$, $f=(n+1)f'$. 因为 $g'+f'-2e'=1$, 所以 $\gcd(g',e',f')=1$, 因此 $\gcd(g,e,f)=n+1$.

当 $n=4k+3$ 时, 令 $t=pot_2\gcd(g,e,f)=2+pot_2(k+1)$., 由定理D得到, 当 $2\leqslant i\leqslant t$ 时, $ord_{2^i}(Ra_n)=4$, 当 $i>t$ 时, $ord_{2^i}(Ra_n)=2^{i-t+2}$.

2.3) 当 $n=4k+1$ 时, 有 $pot_2\gcd(g,e,f)=1$, 由定理 E 得到

$$ord_4(Ra_n)=2ord_2(Ra_n)=8.$$

考察 $Ra_n^{\,8}-I_n=\begin{bmatrix} x & y\alpha \\ y\alpha & zX+I_{n-1}\end{bmatrix}$, 其中 $x=d^2+(n-1)e^2-1$, $y=e(d+(n-1)f+1)$, $z=e^2+(n-1)f^2+2f=(n+1)z'$, 其中, $z'=(n+1)e'^2+(n^2-1)f'^2+2f'$. 容易验证 $x\equiv 0(\mathrm{mod}\,4)$, $y\equiv 0(\mathrm{mod}\,4)$, $z\equiv 0(\mathrm{mod}\,4)$, $z'\equiv 2(\mathrm{mod}\,4)$, $n+1\equiv 2(\mathrm{mod}\,4)$, 所以 $pot_2 z=2$, $pot_2\gcd(x,y,z)=2$; 由定理 E 得到, 当 $i\geqslant 2$ 时, $ord_{2^i}(Ra_n)=2^{i+1}$.

定理 8　环 Z_N 上的 A 型 n 维 Arnold 变换矩阵 Ra_n 的特征多项式

$$f(\lambda)=\begin{cases}\lambda^2-3\lambda+1, & n=2,\\ (\lambda-1)^{n-2}(\lambda^2-\lambda(n+1)+1), & n>2.\end{cases}\tag{8}$$

证　$n=2$ 时容易证之.

$n>2$ 时, 对 $\lambda E-Ra$ 按顺序实行以下初等变换: 1)第 i 行 $-$ 第$(i-1)$行, $i=n, n-1, \cdots, 2$; 2) 第 i 行$=$ 第 i 行$/(\lambda-1)$, $i=3, \cdots, n$; 3) 第 i 列 $=$ 第 i 列 $+$ 第$(i+1)$列, $i=n-1, \cdots, 2$; 得到

$$T=\begin{bmatrix} \lambda-1 & -(n-1) & -(n-2) & \cdots & -2 & -1\\ -\lambda & \lambda-1 & 0 & \cdots & 0 & 0\\ 0 & 0 & 1 & \cdots & 0 & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & \cdots & 0 & 1 & 0\\ 0 & 0 & \cdots & 0 & 0 & 1\end{bmatrix},$$

所以 $f(\lambda)=(\lambda-1)^{n-2}|T|=(\lambda-1)^{n-2}(\lambda^2-\lambda(n+1)+1)$.

由注 3 知道, 计算 Ra_n 的阶关键在于计算其特征根. 而由定理 8 可知, Ra_n 有 $n-2$ 个根为 1, 其余两个根为 $\lambda^2-\lambda(n+1)+1$ 的根. 以下命题讨论了 $\lambda^2-\lambda(n+1)+1$ 的根.

命题 1　设 p 为奇素数, $n\geqslant 2$, 设 $GF(p)$ 上的多项式 $g(\lambda)=\lambda^2-\lambda(n+1)+1$ 的两个根为 λ_1,λ_2, 那么

$$\begin{cases}\lambda_1=\lambda_2=1, & n\equiv 1(\bmod p),\\ \lambda_1=\lambda_2=-1, & n\equiv -3(\bmod p),\\ \lambda_1\neq\lambda_2, & \text{其他.}\end{cases}$$

证 如果 $g(\lambda)$有重根，必有 $g'(\lambda)=2\lambda-(n+1)=0$，即 $\lambda=2^{-1}\times(n+1)$，代入 $g(\lambda)=0$ 并解之得到 $n\equiv 1(\bmod p)$或$n\equiv -3(\bmod p)$. 容易验证：当 $n\equiv 1(\bmod p)$ 时，$\lambda_1=\lambda_2=1$，当 $n\equiv -3(\bmod p)$ 时，$\lambda_1=\lambda_2=-1$；否则，二根互异.

4.3.2 *B* 型 Arnold 变换矩阵

定义 11 对任意正整数 N, Z_N 上的 B 型 n 维 Arnold 变换矩阵为以下 $n\times n$ 矩阵:

$$R(b)_n=\begin{bmatrix} b & b & b & \cdots & b & b\\ b & b+1 & b+1 & \cdots & b+1 & b+1\\ b & b+1 & b+2 & \cdots & b+2 & b+2\\ \vdots & \vdots & \vdots & & \vdots & \vdots\\ b & b+1 & b+2 & \cdots & b+(n-2) & b+(n-2)\\ b & b+1 & b+2 & \cdots & b+(n-2) & b+(n-1)\end{bmatrix}, \tag{9}$$

其中 b 为 Z_N 上的可逆元.

从我们的定义可看出，(5)式中定义的 n 维 Arnold 变换矩阵(即文献 [9] 所定义的 n 维 Arnold 变换矩阵)是 $b=1$ 时的 B 型 n 维 Arnold 变换矩阵.

容易证明以下性质:

性质 3 Z_N 上的 B 型 n 维 Arnold 变换矩阵 $R(b)_n$ 的行列式为 b.

因此 B 型 n 维 Arnold 变换矩阵为 R_N 上的可逆矩阵.

定理 9 Z_N 上的 B 型 n 维 Arnold 变换矩阵 $R(b)_n$ 的特征多项式 $f(\lambda)$满足

$$\begin{pmatrix} f(\lambda)\\ g(\lambda)\end{pmatrix}=\begin{bmatrix}\lambda-1 & \lambda\\ -1 & \lambda\end{bmatrix}^{n-1}\begin{pmatrix}\lambda-b\\ -b\end{pmatrix}.$$

证 对 $\lambda E-R(b)_n$ 实行以下初等变换：第 i 行 = 第 i 行 − 第$(i-1)$行，$i=n, \cdots, 2$, 得到

$$x_n=\begin{bmatrix}\lambda-b & -b & -b & \cdots & -b & -b\\ -\lambda & \lambda-1 & -1 & \cdots & -1 & -1\\ 0 & -\lambda & \lambda-1 & \cdots & -1 & -1\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & 0 & \cdots & \lambda-1 & -1\\ 0 & 0 & 0 & \cdots & -\lambda & \lambda-1\end{bmatrix}.$$

设

$$y_n=\begin{vmatrix} \lambda-b & -b & -b & \cdots & -b & -b \\ -\lambda & \lambda-1 & -1 & \cdots & -1 & -1 \\ 0 & -\lambda & \lambda-1 & \cdots & -1 & -1 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & \lambda-1 & -1 \\ 0 & 0 & 0 & \cdots & -\lambda & -1 \end{vmatrix}_{n\times n}.$$

分别对 x_n 和 y_n 的最后一行进行 Laplace 展开得到

$$\begin{cases} \det(x_n)=(\lambda-1)\det(x_{n-1})+\lambda\det(y_{n-1}), \\ \det(y_n)=-\det(x_{n-1})+\lambda\det(y_{n-1}). \end{cases} \tag{10}$$

定理结论由(10)式易得.

由于 $R(b)_n$ 的特征多项式的表达式比较复杂, 使得特征根的分析较为困难, 所以我们不对 $R(b)_n$ 的阶进行一般性讨论; 但根据文献[2]的计算机计算结果, 可知道当模为 2 和 4 时, $R(1)_3$ 和 $R(1)_4$ 的阶都为 7, 模为 8 时, 阶都为 14, 根据定理 D 和 E 得到以下结论:

定理 10　当 $N=2, 4$ 时, $R(1)_3$ 和 $R(1)_4$ 的阶均为 7; 当 $N=2^i$, $i>2$ 时, $R(1)_3$ 和 $R(1)_4$ 的阶为 $7\cdot 2^{i-2}$.

4.3.3　优点和应用

A 型 n 维 Arnold 变换矩阵和 n-PHT 变换矩阵是相似的, 所以我们也给出了 n-PHT 的相应结果. 同时, A 型 n 维 Arnold 变换也具有 n-PHT 变换的优点: 矩阵元素由 1 和 2 组成, 使得计算快速简单. 由于 n-PHT 变换矩阵可用在分组密码设计中, A 型 n 维 Arnold 变换矩阵也可应用到分组密码设计中. 我们期望, A 型 n 维 Arnold 变换矩阵也可应用到图像置乱变换中.

B 型 n 维 Arnold 变换矩阵进一步推广了齐东旭等人提出的推广 n 维 Arnold 变换矩阵, 进一步扩大了图像隐藏的加密容量.

参　考　文　献

1 Pfitzmann A, et al. Information Hiding: Third International Workshop, LNCS, Vol 1768. Springer, 2000

2 齐东旭, 邹建成, 韩效成. 一种新的置乱变换及其在图像信息隐藏中的应用. 中国科学, E 辑, 2000, 30(5): 440~447

3 Arnold V I, Arez A. Ergodic problems of classical mechanics. In: Benjamin W A, ed. Mathematical Physics Monograph Series. New York, 1968

4 邹建成, 铁小匀. 数字图像的 Arnold 变换及其周期性. 中国计算机图形学学术会议论文集. 杭州: 2000

5 Jacobson N. Basic Algebra I. 2nd ed. New York: W H Freeman and Company, 1985, 92~96

6 Brown E, Vaughan T P. Cycles of directed graphs defined by matrix multiplication (mod n). Discrete Mathematics, 2001, 239: 109~120

7 Jacoboson N. Lectures in abstract algebra, Vol 2. Linear Algebra. New York: Van Nostrand, 1953

8 Fine N J. Binomial coefficients modulo a prime. Amer Math Monthly, 1947, 54: 589~592

9 Bell A D. Math 731/732: Modern Algebra. University of Wisconsin-Milwaukee, 2000

10 Massey L J. On the optimality of SAFER+ diffusion. Submit to AES Round1 Conf2. http://csrc.nist.gov/encryption/aes/round1/conf2/papers/massey.pdf