# Arnold 变换的周期及其应用*

李 兵[1,2], 徐家伟[2]
(1. 中南大学数学与计算机科学学院, 湖南 长沙 410008;
2. 长沙理工大学数学与计算机科学学院, 湖南 长沙 410077)

摘 要: 探讨了 Arnold 变换的周期性, 主要结果包括: ①通过构造一个整数序列 $\{G_n\}$ 并研究 Arnold 变换的周期与该整数序列 $\{G_n\}$ 的联系, 获得了一些关于 Arnold 变换周期的新的性质, 特别是文中得到的素数阶数字图像周期的上界比已有的结果更精确; ②给出了计算 Arnold 变换最小周期的一种算法, 实验结果说明该算法优于已有的一些算法。

关键词: 图像信息保密; 数字图像; 置乱变换; Arnold 变换; 周期
中图分类号: O241.6; TN919.31 文献标识码: A 文章编号: 0529-6579(2004)S2-0139-04

保护数字图像的安全已经成为普遍关注的问题。图像置乱技术作为对数字图像加密的一种基本方法已被广泛地研究。近年来, 许多基于几何变换的置乱技术被提出来或被应用, Arnold 变换就是其中的一种。20 世纪 90 年代末, 齐东旭等人对 Arnold 变换及其在图像信息隐蔽和图像置乱技术中的应用作了大量的工作[1-7]。例如齐东旭、邹建成等人给出了矩阵变换模周期存在的条件, 研究了 Fibonacci-$Q$ 矩阵变换的模周期和 Arnold 变换模周期之间的关系等[1], 而文献 [3, 4, 6] 中则讨论了 Arnold 变换在图像信息隐蔽中应用, 文 [7, 8] 研究了 Arnold 变换的周期性及 Arnold 变换的最小模周期的算法。但是到目前为止, 人们仍然没有很好地解决快速、有效地计算 Arnold 的模周期等问题。

1992 年 Dyson 和 Falk 得到了 Arnold 变换的最小模周期 $P(N)$ 的上界, 即 $P(N) \leqslant N^2/2$, 并对部分的最小周期证明了 $P(N) \leqslant 12N/7$。

本文进一步讨论了 Arnold 变换的模周期的性质。主要内容包括: ①通过构造一个整数序列 $\{G_n\}$ 并研究 Arnold 变换的模周期与该整数序列 $\{G_n\}$ 的联系, 我们获得了一些关于 Arnold 变换模周期的新性质, 特别是, 我们得到的素数阶数字图像模周期的上界比上述已有的结果更精确 (见文中推论 4); ②给出了计算 Arnold 变换最小模周期的算法, 实验结果说明该算法优于已有的一些算法。

## 1 整数序列 $\{G_n\}$ 与 Arnold 变换周期

本文中未说明定义的概念请参见文献 [1] 或 [2], 代数符号可参见文 [11]。对于给定的 $N$ 阶图像 $P$, 说一个整数 $T$ 是 Arnold 变换关于该图像的模 $N$ 周期是指经过 $T$ 次变换后图像 $P$ 又回到 $P$, 而最小的模 $N$ 周期是图像 $P$ 经过变换回复到 $P$ 的最少次数。用 $P(N)$ 表示 2 维 Arnold 变换关于 $N$ 阶图像的最小模周期。在需要而且不会出现误解的时候, 也用 $p(N)$ 表示 2 维 Arnold 变换关于 $N$ 阶图像的任一个模 $N$ 周期。下列命题是显然的。

命题 1 设自然数 $N > 1$, 则对于任一 $p(N)$ 有: $P(N) = p(N)$

为了研究 2 维 Arnold 变换的周期及其性质, 构造一个整数序列 $\{G_n\}$ 如下:

$$G_1 = 1,\ G_2 = 3;\ G_{n+2} = 3G_{n+1} - G_n \quad n \geqslant 1 \tag{1}$$

由 (1) 式有

$$G_n = 3G_{n+1} - G_{n+2} \quad n \geqslant 1 \tag{2}$$

当时, 式 (2) 的右端是有意义的, 以此定义 $G_0$。依次类推, 可定义一切 $G_{-n}$ ($n > 0$)。容易证明下列引理。

引理 1 设整数 $n \geqslant 0$, 则 $G_n = -G_{-n}$。

以后我们用 $\lambda_1, \lambda_2$ 分别表示 $\frac{3+\sqrt{5}}{2}, \frac{3-\sqrt{5}}{2}$。

引理 2 设整数 $n \geqslant 0$, 则 $G_n = \frac{1}{\sqrt{5}}(\lambda_1^n - \lambda_2^n)$。

* 收稿日期: 2004-09-11
基金项目: 国家自然科学基金资助项目 (10171008); 湖南省自然科学基金资助项目 (04JJ6028); 湖南省教育厅重点科研基金资助项目 (03A002)
作者简介: 李 兵 (1957 年生), 男, 博士, 教授; E-mail: libcs@263.net 或 lib@csust.cn

证明 考虑方程组

$$\begin{cases} G_{n+1} = 3G_n - G_{n-1} \\ G_n = G_n \end{cases}, n > 0,$$

设 $M = \begin{bmatrix} 0 & 1 \\ -1 & 3 \end{bmatrix}$，则

$$[G_n, G_{n+1}]^{\mathrm{T}} = M[G_{n-1}, G_n]^{\mathrm{T}}$$

故

$$[G_{n-1}, G_n]^{\mathrm{T}} = M^{n-1}[G_1, G_2]^{\mathrm{T}}$$

易知 $\lambda^1, \lambda^2$ 是矩阵 $M$ 的特征值，对应的特征向量分别是 $[a, \lambda_1, a]^{\mathrm{T}}$ 和 $[b, \lambda_2, b]^{\mathrm{T}}$，$a, b$ 是实数。现在考虑方程组 $\begin{cases} a + b = 1 \\ \lambda^1 a + \lambda^2 b = 3 \end{cases}$，它有一个非零解 $a = \frac{5+3\sqrt{5}}{10}$，$b = \frac{5-3\sqrt{5}}{10}$，所以由

$$\begin{bmatrix} a \\ \lambda_1 \alpha \end{bmatrix} + \begin{bmatrix} b \\ \lambda_2 b \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \end{bmatrix}$$

即知

$$\begin{bmatrix} \frac{5+3\sqrt{5}}{10} \\ \frac{15+7\sqrt{5}}{10} \end{bmatrix} + \begin{bmatrix} \frac{5-3\sqrt{5}}{10} \\ \frac{15-7\sqrt{5}}{10} \end{bmatrix} \begin{bmatrix} 1 \\ 3 \end{bmatrix}$$

因此

$$[G_n, G_{n+1}]^{\mathrm{T}} = M^{n-1}[1, 3]^{\mathrm{T}} =$$

$$M^{n-1}\begin{bmatrix} \frac{5+3\sqrt{5}}{10} \\ \frac{15+7\sqrt{5}}{10} \end{bmatrix} + M^{n-1}\begin{bmatrix} \frac{5-3\sqrt{5}}{10} \\ \frac{15-7\sqrt{5}}{10} \end{bmatrix} =$$

$$\lambda_1^{n-1}\begin{bmatrix} \frac{5+3\sqrt{5}}{10} \\ \frac{15+7\sqrt{5}}{10} \end{bmatrix} + \lambda_2^{n-1}\begin{bmatrix} \frac{5-3\sqrt{5}}{10} \\ \frac{15-7\sqrt{5}}{10} \end{bmatrix}$$

这样当 $n > 0$ 时

$$G_n = \lambda_1^{n-1} \cdot \frac{5+3\sqrt{5}}{10} + \lambda_2^{n-1} \cdot \frac{5-3\sqrt{5}}{10} =$$

$$\frac{1}{\sqrt{5}}(\lambda_1^n - \lambda_2^n)$$

最后，当 $n = 0$ 时，结论显然亦成立。

引理 3 设 $n$ 是自然数，则

$$A^n = \begin{bmatrix} G_{n+1} - 2G_n & G_n \\ G_n & G_{n+1} - G_n \end{bmatrix}$$

下面给出 Arnold 变换的模 $N$ 周期的一个重要性质。

定理 1 设 $n$ 为自然数，$N > 1$，则 $P(N) \mid n$ 的充要条件是：$N \mid (G_n, G_{n+1} - 1)$

证明 充分性。据引理 3，有 $A^n \equiv E(\mathrm{mod}\ N)$，从而由命题 1 有 $P(N) \mid n$。

必要性。因为 $P(N) \mid n$，所以 $A^n \equiv E(\mathrm{mod}\ N)$ 再用引理 3，可以推出

$$G_n = 0(\mathrm{mod}\ N),\ G_{n+1} = 1(\mathrm{mod}\ N)$$

从而 $N \mid (G_n, G_{n+1} - 1)$。

下面的定理 2 是我们改进算法的理论基础。

引理 4 设整数 $a, b, c \neq 0, n \geqslant 0$，$c \mid 2a$，$c \mid (3a + 5b)$，

则 $\frac{a + b\sqrt{5}}{c}\lambda_1^n + \frac{a - b\sqrt{5}}{c}\lambda_2^n$ 是整数。

引理 5 设 $n$ 是整数，则

$$G_{2n} = G_n(G_{n+1} - G_{n-1});$$

$$G_{2n-1} = (G_n - G_{n-1})(G_n + G_{n-1})$$

引理 6 设 $n$ 是整数，则

$$G_{2n+1} - 1 = G_n(G_{n+2} - G_n);$$

$$G_{2n} - 1 = (G_{n+1} - G_n)(G_n + G_{n-1})$$

引理 7 设 $n$ 是整数。

(1) 如果 $n$ 是偶数，则 $(G_n, G_{n+1} - 1) = G_{\frac{n}{2}}$

(2) 如果 $n$ 是奇数，则

$$(G_n, G_{n+1} - 1) = G_{\frac{n-1}{2}} + G_{\frac{n+1}{2}}$$

证明

(1) 由引理 5 和引理 6 可得

$$G_n = G_{n/2}\left(G_{n/2+1} - G_{n/2-1}\right),$$

$$G_{n+1} - 1 = G_{n/2}\left(G_{n/2+2} - G_{n/2}\right)$$

令 $u = \frac{-5-\sqrt{5}}{10}\lambda_1^{n/2} + \frac{-5+\sqrt{5}}{10}\lambda_2^{n/2}$，

$v = \frac{5-\sqrt{5}}{10}\lambda_1^{\frac{n}{2}} + \frac{5+\sqrt{5}}{10}\lambda_2^{n/2}$，由引理 4 知 $u, v$ 是整数。通过计算可得

$$u(G_{n/2+1} - G_{n/2-1}) + v(G_{n/2+2} - G_{n/2}) = 1$$

所以 $(G_{n/2+1} - G_{n/2-1}, G_{n/2+2} - G_{n/2}) = 1$，从而

$$(G_n, G_{n+1} - 1) = G_{n/2}$$

(2) 与 (1) 同理可得

$$G_n = (G_{(n+1)/2} - G_{(n-1)/2})(G_{(n+1)/2} - G_{(n-1)/2}),$$

$$G_{n+1} - 1 = (G_{(n+3)/2} - G_{(n+1)/2})(G_{(n+1)/2} + G_{(n-1)/2})$$

令 $u = \frac{1}{\sqrt{5}}(\lambda_1^{(n+1)/2} - \lambda_2^{(n+1)/2})$，

$$v = \frac{5-3\sqrt{5}}{10}\lambda_1^{(n+1)/2} + \frac{5+3\sqrt{5}}{10}\lambda_2^{(n+1)/2}$$

再由引理 4 知 $u$，$v$ 是整数。而且

$$u(G_{(n+1)/2} - G_{(n-1)/2}) + v(G_{(n+3)/2} - G_{(n+1)/2}) = 1$$

所以

$$(G_{(n+1)/2} - G_{(n-1)/2}, G_{(n+3)/2} - G_{(n+1)/2}) = 1$$

从而

$$(G_n, G_{n+1} - 1) = G_{(n-1)/2} + G_{(n+1)/2}$$

定理 2 设 $n$ 是正整数，则

(1) 如果 $n$ 是偶数, $P(N) \mid n$ 的充要条件是 $N \mid G_{\frac{n}{2}}$;

(2) 如果 $n$ 是奇数, $P(N) \mid n$ 的充要条件是 $N \mid (G_{(n-1)/2} + G_{(n+1)/2})$。

证明　用定理 1 和引理 7 可以证明, 细节略。

## 3　Arnold 变换的模 $p$ 周期

引理 8　设素数 $p > 2$, $m$ 是自然数 $1 < m < p$, 则 $p \mid C_{p+1}^{m}$。

引理 9　设 $n$ 是自然数, $p$ 是素数且 $0 < m < p$, 则 $p \mid C_{p}^{m}$。

引理 10　设 $n$ 是自然数, 则有:

(1) 当 $n$ 是偶数时,

$$2^{n-1} G_n = C_n^1 3^{n-1} + C_n^3 3^{n-3} \cdot 5 + \cdots + C_n^{n-3} 3^3 \cdot 5^{(n-4)/2} + C_n^{n-1} 3 \cdot 5^{\frac{n-2}{2}};$$

(2) 当 $n$ 是奇数时,

$$2^{n-1} G_n = C_n^1 3^{n-1} + C_n^3 3^{n-3} \cdot 5 + \cdots + C_n^{n-2} 3^2 \cdot 5^{(n-3)/2} + 5^{(n-1)/2}。$$

限于篇幅, 我们略去上述几个引理的证明。

定理 3　设 $p \neq 5$ 为大于 2 的素数, 那么:

(1) 当 $(5/p) = -1$ 时, $P(p) \mid (p+1)$;

(2) 当 $(5/p) = 1$ 时, $P(p) \mid (p-1)$。

证明　根据引理 10,

$$2^p G_{p+1} = C_{p+1}^1 3^p + C_{p+1}^3 3^{p-2} \cdot 5 + \cdots + C_{p+1}^{p-2} 3^3 \cdot 5^{(p-3)/2} + C_{p+1}^{p} 3 \cdot 5^{(p-1)/2} =$$

$$3 \cdot (p+1)(3^{p-1} + 5^{(p-1)/2}) + C_{p+1}^3 3^{p-2} \cdot 5 + \cdots + C_{p+1}^{p-2} 3^3 \cdot 5^{(p-3)/2} \quad (3)$$

$$2^{p-1} G_p = C_p^1 3^{p-1} + C_p^3 3^{p-3} \cdot 5 + \cdots + C_p^{p-2} 3^2 \cdot 5^{(p-3)/2} + 5^{(p-1)/2}$$

所以

$$2^{p-1}(G_p + 1) = C_p^1 3^{p-1} + C_p^3 3^{p-3} \cdot 5 + \cdots + C_p^{p-2} 3^2 \cdot 5^{(p-3)/2} + 5^{(p-1)/2} \quad (4)$$

$$2^p (G_{p+1} - 3) = 3 \cdot (p+1)(3^{p-1} + 5^{(p-1)/2}) + C_{p+1}^3 3^{p-2} \cdot 5 + \cdots + C_{p+1}^{p-2} 3^3 \cdot 5^{(p-3)/2} - 6 \cdot 2^{p-1} \quad (5)$$

$$2^{p-1}(G_p - 1) = C_p^1 3^{p-1} + C_p^3 3^{p-3} \cdot 5 + \cdots + C_p^{p-2} 3^2 \cdot 5^{(p-3)/2} + 5^{(p-1)/2} - 2^{p-1} \quad (6)$$

由 Fermat 小定理可得:

$3^{p-1} \equiv 1 \pmod p$, $p > 3$; $2^{p-1} \equiv 1 \pmod p$。

(1) 显然, 当 $p = 3$ 时, (1) 成立, 当 $p > 3$ 时, 因为 $(5/p) = -1$, 由 Euler 判别法可得 $5^{(p-1)/2} \equiv -1 \pmod p$, 所以

$$3^{p-1} + 5^{(p-1)/2} \equiv 0 \pmod p,$$

$$2^{p-1} 5^{(p-1)/2} \equiv 0 \pmod p。$$

再利用引理 8 和引理 9 可得:

$$p \mid C_{p+1}^3, p \mid C_{p+1}^5, \cdots, p \mid C_{p+1}^{p-2};$$

$$p \mid C_p^1, p \mid C_p^3, \cdots, p \mid C_p^{p-2}.$$

从而由式 (3)、(4) 可得 $p \mid G_{p+1}$, $p \mid (G_p + 1)$。

于是 $G_{p+2} - 1 \equiv 3G_{p+1} - (G_p + 1) \equiv 0 \pmod p$, 故

$$p \mid (G_{p+1}, G_{p+2} - 1)$$

从而由定理 1, $P(p) \mid (p+1)$。故当 $(5/p) = -1$ 时, $P(p) \mid (p+1)$。

(2) 因为 $(5/p) = 1$, 所以由 Euler 判别法可得

$$5^{(p-1)/2} \equiv 1 \pmod p$$

故

$$3^{p-1} + 5^{(p-1)/2} \equiv 2 \pmod p,$$

$$2^{p-1} - 5^{(p-1)/2} \equiv 0 \pmod p$$

所以

$$3 \cdot (p+1)(3^{p-1} + 5^{(p-1)/2}) - 6 \cdot 2^{p-1} \equiv 0 \pmod p$$

由引理 8 和引理 9 有:

$$p \mid C_{p+1}^3, p \mid C_{p+1}^5, \cdots, p \mid C_{p+1}^{p-2};$$

$$p \mid C_p^1, p \mid C_p^3, \cdots, p \mid C_p^{p-2}$$

所以由式 (5)、(6) 得

$$p \mid (G_{p+1} - 3), p \mid (G_p - 1)。$$

从而

$$G_{p-1} \equiv 3(G_p - 1) - (G_{p+1} - 3) \equiv 0 \pmod p$$

所以

$$p \mid (G_{p-1}, G_p - 1)$$

由定理 1 知 $P(p) \mid (p-1)$, 故当 $(5/p) = 1$ 时, $P(p) \mid (p-1)$。

推论 4　设 $p \neq 5$ 为大于 2 的素数, 那么 $P(p)$ 必小于或等于 $(p+1)$。

证明　利用定理 3 可以证明。

## 4　最小模周期的算法

本文的算法的主要思想就是利用定理 2 进行计算。首先可以证明 $(G_n, G_{n+1}) = 1$ (略)。算法如下 (程序 A 略):

(1) 初始化 $n = 1$;

(2) 如果 $N \mid G$ 成立, 返回 $2n$; 如果 $N \mid (G_n + G_{n+1})$ 成立, 返回 $2n+1$; 跳到 (4);

(3) $n = n + 1$, 计算 $G_n$, $G_{n+1}$, 跳到 (2);

(4) 输出结果, 退出程序。

与文献 [8] 给出的算法 (程序 B) 相比较, 由表 1 可见本文的算法要优于其算法。

表 1 两种算法运行时间的比较

Tab. 1 The comparison between the runtime of the two algorithems

| $N$ | $P(N)$ | 程序 A 的运行时间 s | 程序 B 的运行时间 s |
|---|---|---|---|
| $10^6$ | 750000 | 1.00 | 2.00 |
| $10^7$ | 7500000 | 9.00 | 17.00 |
| $10^8$ | 75000000 | 86.00 | 164.00 |
| $97^4$ | 89441954 | 117.00 | 231.00 |
| $103^4$ | 113643608 | 133.00 | 251.00 |

参考文献:


[1] QI D X, ZOU J C, HAN X Y. A new class of scrambling transformation and its application in the image information covering[J]. Science in China (Series E), 2000, 43(3): 304—312.

[2] 齐东旭, 邹建成, 韩效宥. 一类新的置乱变换及其在图像信息隐藏中的应用[J]. 中国科学(E), 2000, 30(5): 440—447.

[3] DING W, QI D X. A new kind of digital image transformation in information disguising[M]. Information Sciences and Mieroeleetronic Technology(in Chinese), Beijing: Academic Press, 1998: 309—311.

[4] DING W, QI D X. Digital image transformation and information hiding and disguising technology [J]. J Computers, 1998, 21(9): 838.

[5] ZOU J C, TIE X Y. The Arnold transformation of image transformation and its periodicity[C]. 中国计算机图形学学术会议文集, 2000.

[6] QI D X. Matrix transformation and its application to image hiding[J]. J North China Univ Tech, 1999, 11(1): 24—28.

[7] SUN W. The periodicity of arnold transformation[J]. J North China Univ Tech(in Chinese), 1999, 11(1): 29.

[8] ZOU J C, TIE X Y. Arnold transformation of digital image with two dimension and its periodicity[J]. J North China Univ Tech, 2000, 12(1): 10—14.

[9] DYSON F J, FALK H. Period of a discrete cat Mapping[J]. The Amer Math Monthly, 1992, 99: 603—614.

[10] CHENG T L, XIA L Z. Digital process[M]. Beijing: The People Post Press, 1990.

[11] 潘承洞, 潘承彪. 简明数论[M]. 北京: 北京大学出版社, 1998.

[12] 周持中. 斐波那契—卢卡斯序列[M]. 长沙: 湖南科技出版社, 1993.


# On the Periods of Arnold Transformations and Some Applications


*LI Bing*[1], *XU Jia wei*[2]

(1. School of Mathematics Science & Computing Science, Changsha University of Science & Technology, Changsha 410077, China;
2. School of Mathematics Science & Computing Technology, Central South University, Changsha 410008, China)



**Abstract**: The properties of the period of Arnold transformation are studied. The main results include: ① A new integer sequence is introduced, then by making use of the properties of this sequence some new properties of the periods of Arnold transformation are obtained, especially in the prime situation, a more accurate upper bound of the periods is given; ② A new algorithm is proposed which is better than that proposed by some other papers.



**Key words**: cryptoguard of image information; digital image; scrambling transformation; Arnold transformation; periodicity