第 33 卷 第 19 期 计 算 机 工 程 2007 年 10 月
Vol.33 No.19 Computer Engineering October 2007
·安全技术· 文章编号：1000—3428(2007)19—0138—02 文献标识码：A 中图分类号：TP309

阶数为 2 的 *pq* 周期广义割圆序列的自相关值

白恩健[1,2]，刘晓娟[3]
（1. 东华大学信息科学与技术学院，上海 201620；2. 信息安全国家重点实验室，中国科学院研究生院，北京 100039；
3. 上海电力学院数理系，上海 200090）

摘 要：给出了关于阶数为 2 的*pq*周期广义割圆序列自相关值的几个猜想，这类序列是由Ding和Helleseth构造的，大量的实验结果验证了猜想的正确性，但没有找到理论证明的方法。结果表明这类序列的自相关值为 5-, 4-或 3-值，序列具有“好”的自相关性质，而且这类序列也具有大的线性复杂度，可以作为流密码中的密钥流序列或作为随机数发生器。
关键词：序列；广义割圆类；自相关值

Autocorrelation Values of New Generalized Cyclotomic Sequences of Order Two of Length *pq*

BAI En-jian[1,2], LIU Xiao-juan[3]
(1. College of Information Science & Technology, Donghua University, Shanghai 201620;
2. State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Beijing 100039;
3. Department of Mathematics and Physics, Shanghai University of Electric Power, Shanghai 200090)

【Abstract】 This paper gives some conjectures on the autocorrelation values of new generalized cyclotomic sequences of order 2 of length *pq* defined by Ding and Helleseth. The results show that the autocorrelation functions of these sequences are 5-, 4- or 3-valued. These sequences have good autocorrelation property. The conjectures come from a computer programm which compute the autocorrelation values. All tested examples confirme to these conjectured values and so these assumptions appear to be well founded. However, a theoretical confirmation is not yet forthcoming. These sequences also have large linear complexity, which make it possible as key stream in stream ciphers or as random number generators.
【Key words】 sequence; generalized cyclotomic classes; autocorrelation values

1 概述

设 p,q 为两个相异素数，满足

$$\gcd(p-1,q-1)=2$$

定义 $N=pq$，$e=(p-1)(q-1)/2$。根据中国剩余定理存在模 p 和模 q 的公共本原元 g。设 x 是满足下式的一个整数

$$x\equiv g(\bmod p), x\equiv 1(\bmod q)$$

由于 g 是公共本原元，则再由中国剩余定理

$$ord_N(g)=lcm(ord_p(g),ord_q(g))$$
$$=lcm(p-1,q-1)=e$$

其中，$ord_N(g)$ 表示 $g \bmod N$ 的乘法阶。

阶数为 2 的Ding和Helleseth广义割圆类[1]定义为

$$D_0^{(N)}=\{g^{2s}:s=0,1,\cdots,(e-2)/2\}\cup$$
$$\{g^{2s}x:s=0,1,\cdots,(e-2)/2\}$$
$$D_1^{(N)}=\{g^{2s+1}:s=0,1,\cdots,(e-2)/2\}\cup$$
$$\{g^{2s+1}x:s=0,1,\cdots,(e-2)/2\}$$

这里乘法是 Z_N 中的乘法。文献[1]证明了

$$Z_N^*=D_0^{(N)}\cup D_1^N, D_0^{(N)}\cap D_1^{(N)}=\Phi$$

其中，Φ 代表空集。

定义

$$D_0^{(p)}=\{g^{2s}:s=0,1,\cdots,(p-3)/2\},$$
$$D_0^{(q)}=\{g^{2s}:s=0,1,\cdots,(q-3)/2\},$$
$$D_1^{(p)}=gD_0^{(p)}, D_1^{(q)}=gD_0^{(q)}, R=\{0\}$$
$$C_0=R\cup qD_0^{(p)}\cup pD_0^{(q)}\cup D_0^{(N)}$$
$$C_1=qD_1^{(p)}\cup pD_1^{(q)}\cup D_1^{(N)}$$

则 $C_0\cup C_1=Z_N, C_0\cap C_1=\Phi$。

文献[1]定义了一种阶数为 2 的 *pq* 周期广义割圆序列 $\{s_i\}$。

$$s_i=\begin{cases}0,(i \bmod N)\in C_0\\1,(i \bmod N)\in C_1\end{cases}, i\geq 0$$

显然，序列的最小周期为 N，在一个周期段中有 $(N-1)/2$ 个 1，$(N+1)/2$ 个 0。该类序列满足平衡性。

笔者在文献[2]中研究了该类序列的线性复杂度：该类序列的线性复杂度最大值为 N，最小值为 $(N-1)/2$。该类序列具有大的线性复杂度。

借助于计算机程序，本文给出了关于该类序列自相关值的几个猜想。

2 主要结果

序列 $\{s_i\}$ 的周期自相关函数定义为

基金项目：国家自然科学基金资助项目(60503009)
作者简介：白恩健(1977－)，男，讲师、博士，主研方向：密码学与信息安全；刘晓娟，讲师、硕士
收稿日期：2006-11-13 **E-mail：**baiej@dhu.edu.cn

$$AC_s(\omega)=\sum_{i\in Z_N}(-1)^{s_{i+\omega}-s_i}\quad 0\le\omega\le N-1$$

通过一个计算机程序计算了一些序列的自相关值，并由此得到了关于自相关值的几个猜想。实验的结果肯定了笔者猜想结果的正确性。

设 $p<q$，$\left(\frac{p}{q}\right)$表示 Legendre 符号。

猜想 1

(1)若 $p\equiv 1(\mathrm{mod}\,8)$，并且$\left(\frac{p}{q}\right)$=1 或 $p\equiv 5(\mathrm{mod}\,8)$，并且$\left(\frac{p}{q}\right)$=1，则

$$AC_s(\omega)=\begin{cases}N,\omega=0\\N-p+1,\omega\in qD_0^{(p)}\\N-p-3,\omega\in qD_1^{(p)}\\-p,others\end{cases}$$

(2)若 $p\equiv 1(\mathrm{mod}\,8)$，并且$\left(\frac{p}{q}\right)$=-1 或 $p\equiv 5(\mathrm{mod}\,8)$，并且$\left(\frac{p}{q}\right)$=-1，则

$$AC_s(\omega)=\begin{cases}N,\omega=0\\(p-4)(q-1)+1,\omega\in qD_0^{(p)}\\(p-4)(q-1)-3,\omega\in qD_1^{(p)}\\-p+4,\omega\in Z_N^*\\-p,\omega\in pZ_q^*\end{cases}$$

猜想 2

(1)若 $p\equiv 3(\mathrm{mod}\,8)$，$\left(\frac{p}{q}\right)$=1 且$\left(\frac{q}{p}\right)$=1 或 $p\equiv 7(\mathrm{mod}\,8)$，$\left(\frac{p}{q}\right)$=1 且$\left(\frac{q}{p}\right)$=1，则

$$AC_s(\omega)=\begin{cases}N,\omega=0\\N-p+1,\omega\in qZ_p^*\\-p+2,\omega\in pD_0^{(q)}\cup D_0^{(N)}\\-p-2,\omega\in pD_1^{(q)}\cup D^{(N)}{}_1\end{cases}$$

(2)若 $p\equiv 3(\mathrm{mod}\,8)$，$\left(\frac{p}{q}\right)$=1 且$\left(\frac{q}{p}\right)$=-1 或 $p\equiv 7(\mathrm{mod}\,8)$，$\left(\frac{p}{q}\right)$=1 且$\left(\frac{q}{p}\right)$=-1，则

$$AC_s(\omega)=\begin{cases}N,\omega=0\\N-p-1,\omega\in qZ_p^*\\-p,others\end{cases}$$

(3)若 $p\equiv 3(\mathrm{mod}\,8)$，$\left(\frac{p}{q}\right)$=-1 且$\left(\frac{q}{p}\right)$=1 或 $p\equiv 7(\mathrm{mod}\,8)$，$\left(\frac{p}{q}\right)$=-1 且$\left(\frac{q}{p}\right)$=1，则

$$AC_s(\omega)=\begin{cases}N,\omega=0\\-p+8,\omega\in\frac{1}{2}Z_N^*\\-p,\omega\in pZ_q^*\cup\frac{1}{2}Z_N^*\\(p-4)(q-1)-1,\omega\in qZ_p^*\end{cases}$$

(4)若 $p\equiv 3(\mathrm{mod}\,8)$，$\left(\frac{p}{q}\right)$=-1 且$\left(\frac{q}{p}\right)$=-1 或 $p\equiv 7(\mathrm{mod}\,8)$，$\left(\frac{p}{q}\right)$=-1 且$\left(\frac{q}{p}\right)$=-1，则

$$AC_s(\omega)=\begin{cases}N,\omega=0\\-p+6,\omega\in D_0^{(N)}\\-p-2,\omega\in pD_1^{(q)}\\-p+2,\omega\in pD_0^{(q)}\cup D_1^{(N)}\\(p-4)(q-1)-1,\omega\in qZ_p^*\end{cases}$$

3 结束语

从以上的猜想结论可以看到这类序列的自相关值为 5-值，4-值或 3-值，具有低的自相关性。高线性复杂度和低相关性是评价一个伪随机序列随机性的最基本的两个指标，该类序列有可能作为流密码中的密钥流序列或作为随机数生成器。

当然，如何从理论上来证明上述猜想的正确性，将是进一步需要探索和研究的。

参考文献

1 Ding C, Helleseth T. New Generalized Cyclotomy and Its Applications[J]. Finite Fields and Their Applications, 1998, 4(2): 140-166.

2 Bai E, Liu X, Xiao G. Linear Complexity of New Generalized Cyclotomic Sequences of Order Two of Length *pq*[J]. IEEE Transactions on Information Theory, 2005, 51(5): 1849-1853.

（上接第 129 页）

基于 RSA 的同态密钥协商。本文所提出的密钥协商协议适合在大规模和恶意的环境下进行会话密钥的建立，该协议的安全性是基于大整数的因式分解。该协议在会话密钥的建立的过程中只有加法同态，而没有指数运算，所以和传统的密钥协商协议相比，该协议具有更快的运算速度。

参考文献

1 Diffie W, Hellman M. New Directions in Cryptography[J]. IEEE Trans. on Inform. Theory, 1976, 22(6): 644-654.

2 Steiner M, Tsudik G, Waidner M. Key Agreement in Dynamic Peer Groups[J]. IEEE Trans. on Parallel and Distributed Systems, 2000, 11(8): 769-780.

3 Du W, Deng J, Han Y, et al. A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge[C]//Proc. of IEEE INFOCOM'04. 2004.

4 Rivest R L, Shamir A, Adleman L. A Method for Obtaining Digital Signatures and Public-key Cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.

5 Xiang Guangli, CHEN Xinmeng, ZHU Ping, et al. A Method of Homomorphic Encryption[J]. Wuhan University Journal of Natural Sciences, 2006, 11(1): 181-184.

6 Rivest R L, Adlem L, Dertouzos M L. On Data Banks and Privacy Homomorphism[M]//Demillo R A. Foundations of Secure Computation. New York: Academic Press, 1978: 169-179.

7 Domingo-Ferrer J, Herrera-Joancomart I J. A New Privacy Homomorphism and Applications[J]. Information Processing Letters, 1996, 60(5): 277-282.

8 Sander T, Tschudin C. Towards Mobile Cryptography[C]//Proceedings of the IEEE Symposium on Security and Privacy. Oakland, CA: IEEE Computer Society Press, 1998.

9 Burrows M, Abadi M, Needham R. A Logic of Authentication[R]. Digital Systems Research Center, Technical Report: 39, 1989.