周期为 pq 的四元广义分圆序列的线性复杂度

魏万银 杜小妮 李芝霞 万辊琦

(西北师范大学数学与统计学院 兰州 730070)

摘 要 基于Gray映射和Ding-广义分圆理论,在 Z_4 上构造了一类周期为 pq 的四元广义分圆序列。在有限域 F_r($r\geqslant 5$ 为奇素数)上研究了新序列对应的傅里叶谱序列,并依据傅里叶谱序列的重量确定了新序列的线性复杂度。结果表明,新序列具有良好的线性复杂度性质,能够抗击B-M算法的攻击,是密码学意义上性质良好的伪随机序列。

关键词 密码学,有限域,傅里叶谱序列,四元序列,线性复杂度,B-M算法

中图法分类号 TN918.4 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.06.029

Linear Complexity of Quaternary Generalized Cyclotomic Sequences with Period pq

WEI Wan-yin DU Xiao-ni LI Zhi-xia WAN Yun-qi

(College of Mathematics and Statistics, Northwest Normal University, Lanzhou 730070, China)

Abstract Based on the theory of Gray mapping and Ding-generalized cyclotomic, a new class of quaternary sequence over Z_4 with period pq was constructed firstly. Then we determined the corresponding Fourier spectral sequence of the new sequence over the finite field F_r($r\geqslant 5$, prime). Finally, we obtained the linear complexity of the new sequence from the weights of its Fourier spectral sequence. Results show that the sequence has large linear complexity and can resist the attack by B-M algorithm. It's a good pseudorandom sequence from the viewpoint of cryptography.

Keywords Cryptography, Finite field, Fourier spectral sequence, Quaternary sequence, Linear complexity, B-M algorithm

1 引言

伪随机序列可广泛地应用于扩频通信系统、码分多址系统、全球定位系统和软件测试等[1-2]。作为一种信号形式,具有良好相关特性的伪随机序列可用做雷达测距、同步和线性系统测量的信号。具有高线性复杂度的伪随机序列也有多方面的应用,如用于加密系统等。根据Berlekamp-Msassey算法,若一个周期为 N 的序列的线性复杂度大于 $\frac{N}{2}$,则可称其为一个好的序列或具有高线性复杂度[3]。

分圆序列由于具有良好的代数结构得到了人们的广泛研究。近年来,利用分圆构造四元序列亦有一些研究结果,这些成果主要集中于 Z_4 上四元序列的构造及其相关性分析[4-11],而很少讨论四元序列的线性复杂度。有关 F_{r^m} 上四元序列的结果较少,主要见文献[12-14]。文献[15-16]基于Whiteman-广义分圆在 Z_4 上分别构造了一类周期为 pq 的四元序列并讨论了其线性复杂度。受此启发,本文基于Ding-广义分圆,在 Z_4 上构造了周期为 pq 的一类新的平衡四元序列,并研究了其在有限域 F_r($r\geqslant 5$ 为奇素数)上的线性复杂度。

2 相关概念

定义1 设 u 为一个素数,θ 是 F_{u^m} 中一个 N 阶元素,则定义 F_u 上周期为 N 的序列 $\{s(t)\}$ 的离散傅里叶变换为:

$$A_k=\sum_{t=0}^{N-1}s(t)\theta^{tk},0\leqslant k\leqslant N-1$$

其中,A_k 称作 $\{s(t)\}$ 的傅里叶谱,记 $A=\{A_k\}$ 为傅里叶谱序列,有:

$$s(t)=\frac{1}{N}\sum_{k=0}^{N-1}A_k\theta^{-tk},0\leqslant t\leqslant N-1$$

引理1[3] 符号含义同上,则:

$$\sum_{i=0}^{N-1}\theta^{di}=\begin{cases}0, & d\neq 0(\mathrm{mod}\ N)\\ N, & d=0(\mathrm{mod}\ N)\end{cases}$$

引理2[3] 设 $A=\{A_k\}$ 是 $\{s(t)\}$ 的傅里叶谱序列,则序列 $\{s(t)\}$ 的线性复杂度为:

$$LC(s)=|\{k|A_k\neq 0,0\leqslant k<N\}|$$

由引理2知,

到稿日期:2016-05-03 返修日期:2016-07-02 本文受国家自然科学基金资助项目(61202395,61462077,61562077),教育部"新世纪优秀人才计划"基金资助项目(NCET-12-0620)资助。

魏万银(1989—),女,硕士生,主要研究方向为密码学;**杜小妮**(1972—),女,博士,教授,博士生导师,主要研究方向为密码学,E-mail:ymLdxn@126.com(通信作者)。

$$LC(s)=N-|\{k|A_k=0,0\leqslant k<N\}| \tag{1}$$

定义 2　定义示性函数 $I_\omega(t)$ 和二次特征 $\eta_\omega(t)(\omega=p$ 或 $q)$ 分别为：

$$I_\omega(t)=\begin{cases}1, & t=0(\bmod\omega)\\ 0, & t\neq 0(\bmod\omega)\end{cases}$$

$$\eta_\omega(t)=\begin{cases}0, & t=0(\bmod\omega)\\ 1, & t\in QR_\omega,\\ -1, & t\in NQR_\omega\end{cases}$$

其中，QR_ω 和 NQR_ω 分别是模素数 ω 的二次剩余和二次非剩余的集合。

令 p 和 q 为两个奇素数，$N=pq$，$d=gcd(p-1,q-1)$，$e=(p-1)(q-1)/d$。设 g 为 p 和 q 公共的本原元。整数 x 满足 $x\equiv g \bmod p$ 和 $x\equiv 1 \bmod q$。则 $D_k^{(N)}=\{g^{dt+i}x^j:t=0,1,\cdots,\frac{e}{d}-1\}(i=0,1,\cdots,d-1)$，称 $D_i^{(N)}$ 为关于 p 和 q 的 d 阶的 Ding-广义分圆类，显然有：

$$Z_N^*=\bigcup_{i=0}^{d-1}D_i^{(N)},\ D_i^{(N)}\cap D_j^{(N)}=\Phi,i\neq j$$

3　四元序列的线性复杂度

下文总假设 p 和 q 是两个不同的奇素数，$N=pq$，定义：

$P=\{p,2p,3p,\cdots,(q-1)p\}$

$Q=\{q,2q,3q,\cdots,(p-1)q\}$

则模 N 的剩余类环 $Z_N=\{0\}\cup P\cup Q\cup Z_N^*$，其中 Z_N^* 是 Z_N 中所有可逆元的集合。由中国剩余定理可知 $Z_N\cong Z_p\times Z_q$，即对任意 $t\in Z_N$，有 $t=(t_1,t_2)$，其中 $t\equiv t_1(\bmod p)$，$t\equiv t_2(\bmod q)$，即

$$t=qq_p^{-1}t_1+pp_q^{-1}t_2(\bmod pq)$$

周期为 pq 的二元 Ding-广义分圆序列为：

$$s_1(t)=\begin{cases}1, & t\in P\\ 0, & t\in\{0\}\cup Q\\ \dfrac{1-\eta_q(t)}{2}, & t\in Z_{pq}^*\end{cases}$$

$$s_2(t)=\begin{cases}0, & t\in P\\ 1, & t\in\{0\}\cup Q\\ \dfrac{1-\eta_q(t)}{2}, & t\in Z_{pq}^*\end{cases}$$

定义四元广义分圆序列 $\{s(t)\}=\varphi[s_1(t),s_2(t)]$，其中 $\varphi[s_1(t),s_2(t)]$ 为 Gray 映射。

$$\varphi[s_1,s_2]=\begin{cases}0, & (s_1,s_2)=(0,0)\\ 1, & (s_1,s_2)=(0,1)\\ 2, & (s_1,s_2)=(1,1)\\ 3, & (s_1,s_2)=(1,0)\end{cases}$$

由式(1)知，通过计算 $\{s(t)\}$ 的傅里叶谱序列中非零元的个数可确定序列的线性复杂度。

然而，傅里叶变换是在有限域上定义的，因此首先对四元序列找一个合适的有限域。设奇素数 $r\geqslant 5$，且不等于 p 和 q，F_{r^m} 是 $x^{pq}-1$ 的分裂域，$m>1$。设 $\theta,\alpha=\theta^q,\beta=\theta^p$ 分别是 F_{r^m} 上的 pq 次、p 次、q 次单位根。由定义 2 可知：

$$s_1(t)=\frac{1}{2}(1-[1-I_p(t_1)][1-I_q(t_2)]\eta_q(t_2)+I_p(t_1)-I_q(t_2)-I_p(t_1)I_q(t_2))$$

$$s_2(t)=\frac{1}{2}(1-[1-I_p(t_1)][1-I_q(t_2)]\eta_q(t_2)-I_p(t_1)+I_q(t_2)+I_p(t_1)I_q(t_2))$$

则

$$\begin{aligned}s(t)&=\varphi[s_1(t),s_2(t)]\\&=3s_1(t)+s_2(t)-2s_1(t)s_2(t)\\&=\frac{1}{2}[3-2\eta_q(t_2)+2I_q(t_2)\eta_q(t_2)+3I_p(t_1)+2I_p(t_1)\eta_q(t_2)-2I_p(t_1)I_q(t_2)\eta_q(t_2)-3I_p(t_1)I_q(t_2)-I_q(t_2)+I_p(t_1)\eta_q^2(t_2)+I_q(t_2)\eta_q^2(t_2)-I_p(t_1)I_q(t_2)\eta_q^2(t_2)-\eta_q^2(t_2)]\end{aligned}$$

根据示性函数和二次特征的定义，序列 $\{s(t)\}$ 的傅里叶谱序列 $A=\{A_k\}(0\leqslant k\leqslant N-1)$ 中的项可化简整理为：

$$\begin{aligned}A_k&=\sum_{t=0}^{N-1}s(t)\theta^{tk}\\&=\frac{1}{2}[3\sum_{t=0}^{N-1}\theta^{tk}-2\sum_{t=0}^{N-1}\eta_q(t_2)\theta^{tk}+3\sum_{t=0}^{N-1}I_p(t_1)\theta^{tk}+2\sum_{t=0}^{N-1}I_p(t_1)\eta_q(t_2)\theta^{tk}+\sum_{t=0}^{N-1}I_p(t_1)\eta_q^2(t_2)\theta^{tk}-\sum_{t=0}^{N-1}I_q(t_2)\theta^{tk}-\sum_{t=0}^{N-1}\eta_q^2(t_2)\theta^{tk}-3]\end{aligned}$$

引理 3[17]　设 θ 是 F_{r^m} 上的 pq 次本原单位根，则 $\sum_{i\in Z_{pq}}\theta^i=0$，$\sum_{i\in pZ_q^*}\theta^i=-1$，$\sum_{i\in qZ_p^*}\theta^i=-1$。

下文中总假定 $S_q=\sum_{j\in QR_q}\beta^j$，$S_p=\sum_{i\in QR_p}\alpha^i$。

引理 4　符号含义同上，对于 $0\leqslant k<N$ 有：

(1) $\sum_{t=0}^{N-1}I_p(t_1)\eta_q(t_2)\theta^{tk}$

$$=\begin{cases}0, & k\in\{0\}\cup qZ_p^*\\ (2S_q+1), & k\in Z_{pq}^*\cup pZ_q^*\ \text{且}\ k\in QR_q\\ -(2S_q+1), & k\in Z_{pq}^*\cup pZ_q^*\ \text{且}\ k\in NQR_q\end{cases}$$

(2) $\sum_{t=0}^{N-1}\eta_q(t_2)\theta^{tk}=\begin{cases}0, & k\in\{0\}\cup qZ_p^*\cup Z_{pq}^*\\ p(2S_q+1), & k\in pZ_q^*,k\in QR_q\\ -p(2S_q+1), & k\in pZ_q^*,k\in NQR_q\end{cases}$

(3) $\sum_{t=0}^{N-1}\eta_q^2(t_2)\theta^{tk}=\begin{cases}p(q-1), & k=0\\ -p, & k\in pZ_q^*\\ 0, & k\in qZ_p^*\cup Z_{pq}^*\end{cases}$

(4) $\sum_{t=0}^{N-1}I_p(t_1)\eta_q^2(t_2)\theta^{tk}=\begin{cases}q-1, & k\in\{0\}\cup qZ_p^*\\ -1, & k\in Z_{pq}^*\cup pZ_q^*\end{cases}$

(5)[15] $\sum_{t=0}^{N-1}I_p(t_1)\theta^{tk}=\begin{cases}q(\bmod r) & k\in\{0\}\cup qZ_p^*\\ 0, & \text{其他}\end{cases}$

(6)[15] $\sum_{t=0}^{N-1}I_q(t_2)\theta^{tk}=\begin{cases}p(\bmod r), & k\in\{0\}\cup pZ_q^*\\ 0, & \text{其他}\end{cases}$

证明：(1) 因为

$$\sum_{t=0}^{N-1}I_p(t_1)\eta_q(t_2)\theta^{tk}=\sum_{t\in Z_q^*}\eta_q(t_2)\theta^{ptk}=\sum_{t\in QR_q}\beta^{tk}-\sum_{t\in NQR_q}\beta^{tk}$$

且$|QR_q|=|NQR_q|$，所以当$k\in\{0\}\cup qZ_p^*$时，$\beta^{tk}=1$，则

$$\sum_{t\in QR_q}\beta^{tk}-\sum_{t\in NQR_q}\beta^{tk}=0$$

当$k\in Z_{pq}^*\cup pZ_q^*$时，

$$\sum_{t=0}^{N-1}I_p(t_1)\eta_q(t_2)\theta^{tk}=\begin{cases}2S_q+1, & k\in QR_q\\ -(2S_q+1), & k\in NQR_q\end{cases}$$

(2)因为

$$\begin{aligned}\sum_{t=0}^{N-1}\eta_q(t_2)\theta^{tk}&=\sum_{t_1=0}^{p-1}\sum_{t_2=1}^{q-1}\eta_q(t_2)\theta^{qq_p^{-1}t_1k+pp_q^{-1}t_2k}\\&=\sum_{t_1=0}^{p-1}\theta^{qq_p^{-1}t_1k}\sum_{t_2=1}^{q-1}\eta_q(t_2)\theta^{pp_q^{-1}t_2k}\\&=\sum_{t_1=0}^{p-1}\alpha^{kt_1}\Big(\sum_{t_2\in QR_q}\beta^{kt_2}-\sum_{t_2\in NQR_q}\beta^{kt_2}\Big)\end{aligned}$$

所以，当$k\in\{0\}\cup qZ_p^*\cup Z_{pq}^*$时，

$$\sum_{t=0}^{N-1}\eta_q(t_2)\theta^{tk}=0$$

当$k\in pZ_q^*$时，$\sum_{t_1=0}^{p-1}\alpha^{kt_1}=p$，则

$$\sum_{t=0}^{N-1}\eta_q(t_2)\theta^{tk}=\begin{cases}p(2S_q+1), & k\in QR_q\\ -p(2S_q+1), & k\in NQR_q\end{cases}$$

(3)、(4)的证明与(1)、(2)类似，此处不再赘述。

引理5 设符号含义同上，

$$A_k=\begin{cases}pq+2q-2, & k=0\\ 2(q-1), & k\in qZ_p^*\\ 2S_q-1, & k\in Z_{pq}^*,k\in QR_q\\ -2S_q-3, & k\in Z_{pq}^*,k\in NQR_q\\ (2-2p)S_q-p-1, & k\in pZ_q^*,k\in QR_q\\ (2p-2)S_q+p-3, & k\in pZ_q^*,k\in NQR_q\end{cases}$$

证明：由引理3—引理4直接可证。

引理6[15] 设符号含义同上，则$S_p\in F_r\Leftrightarrow r\in QR_p$；$S_q\in F_r\Leftrightarrow r\in QR_q$。

定理1 设$r\geqslant 5$，则周期为pq的四元广义分圆序列$\{s(t)\}$的线性复杂度如下：

(1) 当$r\in NQR_q$时，

$$LC(s)=\begin{cases}pq, & r\nmid(pq+2q-2),r\nmid(q-1)\\ pq-p+1, & r\nmid(pq+2q-2),r\mid(q-1)\\ pq-1, & r\mid(pq+2q-2),r\nmid(q-1)\end{cases}$$

(2)当$r\in QR_q$时，若$(2S_q-1)(-2S_q-3)\equiv 0(\bmod r)$，则

$$LC(s)\geqslant\frac{(p-1)(q-1)}{2}$$

若$(2S_q-1)(-2S_q-3)\not\equiv 0(\bmod r)$，则

$$LC(s)\geqslant(p-1)(q-1)$$

证明：(1)当$r\in NQR_q$时，$S_q\in F_r{}^m\backslash F_r$，$2S_q-1\neq 0$，$(2-2p)S_q-p-1\neq 0$，$-2S_q-3\neq 0$，$(2p-2)S_q+p-3\neq 0$，则结果显然。

(2)当$r\in QR_q$时，由引理6知，$S_q\in F_r$。

若$(2S_q-1)(-2S_q-3)\equiv 0(\bmod r)$，则

$$LC(s)\geqslant\frac{(p-1)(q-1)}{2}$$

若$(2S_q-1)(-2S_q-3)\not\equiv 0(\bmod r)$，则

$$LC(s)\geqslant(p-1)(q-1)$$

结束语 本文推广了文献[15]的结果，在Z_4上构造了一类新的平衡四元广义分圆序列，并利用对应的傅里叶谱序列的重量和序列之间的关系确定了序列的线性复杂度。结果表明，当$r\in QR_q$且$(2S_q-1)(-2S_q-3)\equiv 0(\bmod r)$时，序列的线性复杂度较低，而在其他情形中，序列的线性复杂度均大于$\frac{pq}{2}$，能满足保密通信的要求，是密码学意义上性质良好的序列。

参 考 文 献

[1] LIU Y L, QIN X L, ZHAO X J, et al. Lightweight RFID Authentication Protocol Based on Digital Signature [J]. Computer Science, 2015, 42(2): 95-100. (in Chinese)
刘亚丽，秦小麟，赵向军，等. 基于数字签名的轻量级RFID认证协议[J]. 计算机科学，2015，42(2)：95-100.

[2] XU L P, HU B. Distribution of a family of Five-valued Cross Correlation Function[J]. Computer Science, 2015, 42(9): 144-149. (in Chinese)
徐立平，胡斌. 一类五值互相关函数分布[J]. 计算机科学，2015，42(9)：144-149.

[3] GOLOMB S W, GUANG G. Signal Design for Good Correlation For Wireless Communication[M]. Cambridge, U. K.: Cambridge Univ. Press., 2005.

[4] KIM Y S, JANG J W, KIM S H. New quaternary sequences with ideal autocorrelation constructed from binary sequences with ideal autocorrelation[J]. IEEE Transactions on Information Theory, 2009, E96. A(9): 278-281.

[5] KIM Y S, CHUNG J S, NO J S. On the autocorrelation distribution of Sidel'nikov sequence[J]. IEEE Trans. Inf. Theory, 2005, 51(9): 3303-3307.

[6] KIM Y S, JANG J W, KIM S H. New construction of quaternary sequences with ideal autocorrelation constructed from Legendre sequences[J]. IEEE Transactions on Information Theory, 2009, 1(9): 282-285.

[7] TANG X H, DING C S. New classes of balanced quaternary sequences and almost balanced binary sequences with optimal autocorrelation value[J]. IEEE Trans. Inf. Theory, 2010, 56(12): 6398-6405.

[8] CHUNG J H, HAN Y K, YANG K. New quaternary sequences with even period and three valued autocorrelation[J]. IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences, 2010, E93-A(1): 309-315.

[9] LIM T, NO J S, CHUNG H. New construction of quaternary sequences with good correlation using binary with good correlation [J]. IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences, 2011, E94-A(8): 1701-1705.

(下转第188页)

Fault Tree Analysis into AADL Models[C]// IEEE High Assurance Systems Engineering Symposium. IEEE Computer Society, 2007: 15-22.

[9] SINGHOFF F, LEGRAND J, NANA L, et al. Cheddar: a flexible real time scheduling framework[J]. Abstr, 2004, xxiv(4): 1-8.

[10] JEAN-PAUL B, RAPHAËL C, DAVID C, et al. A mapping from AADL to Java-RTSJ[C]// International Workshop on Java Technologies for Real-Time and Embedded Systems, Jtres 2007. Institute of Computer Engineering, Vienna University of Technology, September 2007, Vienna, Austria. 2007: 165-174.

[11] GAO J L, ZHANG G, JING X C, et al. Reliability modeling and evaluation method of software system based on AADL [J]. Frontiers of Computer Science and Technology, 2011, 5(10): 942-952. (in Chinese)
高金梁, 张刚, 经小川, 等. 采用 AADL 的软件系统可靠性建模与评估方法[J]. 计算机科学与探索, 2011, 5(10): 942-952.

[12] DONG Y W, WANG G R, ZHANG F, et al. AADL model reliability analysis and evaluation tool[J]. Journal of Software, 2011, 22(6): 1252-1266. (in Chinese)
董云卫, 王广仁, 张凡, 等. AADL 模型可靠性分析评估工具[J]. 软件学报, 2011, 22(6): 1252-1266.

[13] LIU J J, MENG H N. Reliability analysis tool of avionics system based on AADL[J]. Modern Electronic Technology, 2014, 37(8): 65-68. (in Chinese)
刘建军, 孟海宁. 基于 AADL 的航电系统可靠性分析工具[J]. 现代电子技术, 2014, 37(8): 65-68.

[14] CHENG Y H, HUANG Z Q, KAN S L. System reliability modeling method combining AADL and IMC[J]. Computer Engineering and Science, 2015, 37(8): 1517-1524. (in Chinese)
程亦涵, 黄志球, 阚双龙. 一种结合 AADL 和 IMC 的系统可靠性建模方法[J]. 计算机工程与科学, 2015, 37(8): 1517-1524.

[15] TANG Y, SU W, LI S Y. AADL model to the generalized stochastic Petri net conversion tool[J]. Modern Electronic Technology, 2015, 38(12): 62-65. (in Chinese)
汤玥, 苏威, 李蜀瑜. AADL 模型到广义随机 Petri 网的转换工具[J]. 现代电子技术, 2015, 38(12): 62-65.

[16] SHEN N M, LI J, BAI H Y. Transformation and verification of AADL data flow model of real time system based on Uppaal[J]. Computer Science, 2016(1): 211-217.

[17] SHARVIA S, PAPADOPOOULOS Y. Integrating Model Checking with HiP-HOPS in Model-Based Safety Analysis[J]. Reliability Engineering System Safety, 2015, 135: 64-80.

[18] SU W. Research on verification technology of embedded software system based on AADL[D]. Xi'an: Shanxi Normal University, 2015. (in Chinese)
苏威. 基于 AADL 的嵌入式软件系统验证技术研究[D]. 西安: 陕西师范大学, 2015.

[19] GAO L, DONG Y W, ZHANG F. AADL system reliability model conversion method [J]. Computer Engineering, 2011, 37(14): 21-26.

[20] BOZZANO M, CIMATI A, KATOEN J P, et al. Safety, Dependability and Performance Analysis of Extended AADL Models [J]. Computer Journal, 2011, 54(5): 754-775.

[21] YANG Z B, PI L, HU K, et al. Architecture design and analysis of complex embedded real time systems: AADL[J]. Journal of Software, 2010, 21(5): 899-915. (in Chinese)
杨志斌, 皮磊, 胡凯, 等. 复杂嵌入式实时系统体系结构设计与分析语言: AADL[J]. 软件学报, 2010, 21(5): 899-915.

(上接第 176 页)

[10] JANG J W, KIM S H. Quaternary sequences with good autocorrelation constructed by Gray mapping[J]. IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences, 2009, E92-A(8): 2139-2140.

[11] YANG Z, KE P H. Construction of quaternary sequences of length pq with low correlation[J]. Cryptography and Communications, 2011, 3(2): 55-64.

[12] DU X N, CHEN Z X. Linear complexity of quaternary sequence generated using generalized cyclotomic classes modulo 2p[J]. IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences, 2011, 94(5): 1214-1217.

[13] KE P H. New classes of quaternary cyclotomic sequence of length $2p^m$ with high linear complexity[J]. Inf. Process. Lett., 2012, 112(16): 646-650.

[14] CHANG Z L, LI D D. On the linear complexity of quaternary cyclotomic sequences with the period $2pq$[J]. IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences, 2014, 97(2): 679-684.

[15] LI D D, WEN Q Y, ZHANG J, et al. Linear complexity of generalized cyclotomic quaternary sequences with period pq[J]. IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences, 2014, E97-A(5): 1153-1158.

[16] WANG G H, DU X N, WAN Y Q, et al. Linear complexity of balanced quaternary generalized cyclotomic sequences with period pq[J]. Journal of Shandong University (Natural Science), 2016, 51(9): 145-150. (in Chinese)
王国辉, 杜小妮, 万韫琦, 等. 周期为 pq 的平衡四元广义分圆序列的线性复杂度[J]. 山东大学学报(理学版), 2016, 51(9): 145-150.

[17] CHANG Z L, LI D D. On the linear complexity of generalized cyclotomic binary sequence of length $2pq$[J]. Applicable Algebra in Engineering, Communication and Computing, 2010: 21(2): 93-108.