一类新的周期为$2pq$的二元广义分圆序列的线性复杂度

李瑞芳 柯品惠*
(福建师范大学网络安全与密码技术福建省重点实验室 福州 350007)

摘 要：该文提出一类新的周期为$2pq$，p和q为不同奇素数的广义分圆序列，并给出了该序列线性复杂度的计算公式。在已知序列支撑集的情况下，利用该公式可以得到该序列线性复杂度的精确值。

关键词：密码学；有限域；广义分圆序列；线性复杂度
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2014)03-0650-05
DOI: 10.3724/SP.J.1146.2013.00751

The Linear Complexity of a New Class of Generalized Cyclotomic Sequence with Period $2pq$

Li Rui-fang Ke Pin-hui*
(*Key Laboratory of Network Security and Cryptology*, *Fujian Normal University*, *Fuzhou* 350007, *China*)

Abstract: A new class of generalized cyclotomic sequence with period $2pq$ is proposed in this paper, where p and q are distinct primes. A formula for computing the linear complexity of the proposed sequence is also given. With the knowledge of the support set of the generalized cyclotomic sequence, its linear complexity can be easily determined using the formula.

Key words: Crpytography; Finite fields; Generalized cyclotomic sequence; Linear complexity

1 引言

一条序列的线性复杂度定义为生成该序列的最短的线性移位寄存器的长度。在密码学等相关领域的应用中，伪随机序列必须具有高的线性复杂度[1,2]。从安全的角度讲，一条好的序列往往要求它的线性复杂度必须不小于其周期长度的一半。

由于具有较好的代数结构，分圆序列近年来得到深入研究，并取得了一系列的研究成果[3–15]。文献[9]研究周期为p^{n+1}的二元广义分圆序列，并给出了计算该序列线性复杂度的有效方法。文献[10]给出了两类周期为$2p^n$的二元广义分圆序列，并分析了该序列的线性复杂度。文献[11]对其做了进一步的推广，给出了具有高线性复杂度的周期为$2p^n$的二元广义分圆序列的一般构造，并分析了该序列的自相关性质。文献[13]定义了周期为$p^{m+1}q^{n+1}$的二元广义分圆序列，并计算了该序列的线性复杂度。文献[14]定义了模p^m上的六阶广义分圆序列，计算了该序列的线性复杂度，并给出了p^2情形下的序列的迹表示。文献[15]构造了周期为$2pq$的广义分圆序列，并计算了其线性复杂度，结果表明该序列具有较高的线性复杂度。

文献[15]仅考虑了$\gcd(p-1,q-1)=2$及序列支撑集为模p，q和pq的相同分圆类这一特殊情形。本文将在文献[15]基础上，考虑$\gcd(p-1,q-1)=e$，$e\geq 2$的周期为$2pq$的广义分圆序列的一般构造。新构造的序列的支撑集可以灵活定义。同时，本文也给出了这类序列线性复杂度的计算公式。在已知序列的支撑集的情况下，利用该公式可以容易得到该序列线性复杂度的精确值。本文结构安排如下：第2节给出模$2pq$的广义分圆的定义，由此给出了周期为$2pq$的二元广义分圆序列的一般构造；第3节，利用文献[9]的方法，给出了新构造序列的线性复杂度的计算公式；第4节给出结论。

2 周期为$2pq$的二元广义分圆序列的新构造

设$N=2pq$，p，q为不同奇素数，g是模$2p,2q,p$和q的公共本原根，而y是Z_{2pq}中满足式(1)所示同余方程的解。

$$\left.\begin{aligned} y&\equiv g \pmod{2p}\\ y&\equiv 1 \pmod{2q}\end{aligned}\right\} \tag{1}$$

由广义中国剩余定理[2]，这样的g和y总是存在的。

令$\gcd(p-1,q-1)=e$，记$d=\dfrac{(p-1)(q-1)}{e}$。

定义1 对$0\leq i\leq e-1$，

2013-05-27收到，2013-08-12改回
国家自然科学基金(61102093)资助课题
*通信作者：柯品惠 keph@fjnu.edu.cn

$$D_i^{(2pq)}=\left\{g^s y^i \pmod{2pq}: s=0,1,\cdots,d-1\right\}$$
$$D_i^{(pq)}=\left\{g^s y^i \pmod{pq}: s=0,1,\cdots,d-1\right\}$$
$$D_i^{(2p)}=\left\{g^{es+i} \pmod{2p}: s=0,1,\cdots,R_p-1\right\}$$
$$D_i^{(p)}=\left\{g^{es+i} \pmod{p}: s=0,1,\cdots,R_p-1\right\}$$
$$D_i^{(2q)}=\left\{g^{es+i} \pmod{2q}: s=0,1,\cdots,R_q-1\right\}$$
$$D_i^{(q)}=\left\{g^{es+i} \pmod{q}: s=0,1,\cdots,R_q-1\right\}$$
$$D_0^{(1)}=\{0\},\ D_1^{(1)}=\{pq\}$$

其中 $R_p=(p-1)/e,\ R_q=(q-1)/e$。

易验证，

$$\begin{aligned}Z_N &= Z_{2pq}^*\bigcup 2Z_{pq}^*\bigcup pZ_{2q}^*\bigcup 2pZ_q^*\bigcup qZ_{2p}^*\\ &\quad\bigcup 2qZ_p^*\cup\{0\}\cup\{pq\}\\ &=\bigcup_{i=0}^{e-1}D_i^{(2pq)}\bigcup_{i=0}^{e-1}2D_i^{(pq)}\bigcup_{i=0}^{e-1}qD_i^{(2p)}\bigcup_{i=0}^{e-1}2qD_i^{(p)}\\ &\quad\bigcup_{i=0}^{e-1}pD_i^{(2q)}\bigcup_{i=0}^{e-1}2pD_i^{(q)}\bigcup_{i=0}^{e-1}D_i^{(1)}\end{aligned}$$

设 $I^{(2pq)},I^{(pq)},I^{(2p)},I^{(p)},I^{(2q)},I^{(q)}$ 均为 $\{0,1,\cdots,e-1\}$ 的子集，且 $\varnothing\neq I^{(1)}\subseteq\{0,1\}$，定义

$$\begin{aligned}C_1 &= \bigcup_{k\in I^{(2pq)}}D_k^{(2pq)}\bigcup_{k\in I^{(pq)}}2D_k^{(pq)}\bigcup_{k\in I^{(2p)}}qD_k^{(2p)}\\ &\quad\bigcup_{k\in I^{(p)}}2qD_k^{(p)}\bigcup_{k\in I^{(2q)}}pD_k^{(2q)}\bigcup_{k\in I^{(q)}}2pD_k^{(q)}\bigcup_{k\in I^{(1)}}D_k^{(1)}\end{aligned}$$

而 $C_0=Z_N\setminus\{C_1\}$。按照式(2)构造一条 N 长二元序列 $S=\{s_i\}$：

$$s_i=\begin{cases}1, & i\pmod N\in C_1\\ 0, & i\pmod N\in C_0\end{cases}\tag{2}$$

称 $S(x)=\sum_{i\in C_1}x^i\in Z_2[x]$ 为序列 S 的生成多项式，则序列 S 的极小多项式为

$$m(x)=\left(x^N-1\right)\Big/\gcd\left(x^N-1,S(x)\right)\tag{3}$$

进而，序列 S 的线性复杂度为

$$L_s=N-\deg\left(\gcd\left(x^N-1,S(x)\right)\right)\tag{4}$$

本文仅考虑 $I^{(2pq)}=I^{(pq)},\ I^{(2p)}=I^{(p)},\ I^{(2q)}=I^{(q)}$ 的情形。

3　线性复杂度

本节将计算第 2 节定义的广义分圆序列的线性复杂度，为此，需要如下引理。

引理 1 记号同上，$0\le i\le e-1$，有

(1) $D_i^{(2pq)}=\{x+\delta_{pq}:x\in D_i^{(pq)}\}$，其中

$$\delta_{pq}=\begin{cases}0, & x\pmod 2=1\\ pq, & x\pmod 2=0\end{cases}$$

(2) $D_i^{(2p)}=\{x+\delta_p:x\in D_i^{(p)}\}$，其中

$$\delta_p=\begin{cases}0, & x\pmod 2=1\\ p, & x\pmod 2=0\end{cases}$$

(3) $D_i^{(2q)}=\{x+\delta_q:x\in D_i^{(q)}\}$，其中

$$\delta_q=\begin{cases}0, & x\pmod 2=1;\\ q, & x\pmod 2=0.\end{cases}$$

证明　由于(2), (3)类似可证，这里只证明(1)。

对任意的 $x\in D_i^{(pq)}$，显然，$\gcd(x,pq)=1$。又由 δ_{pq} 的定义，$x+\delta_{pq}$ 为奇数。从而，$x+\delta_{pq}\in Z_{2pq}^*$。又 $x+\delta_{pq}\equiv x\pmod{pq}$，$x+\delta_{pq}\in D_i^{(2pq)}$。因此，$\{x+\delta_{pq}:x\in D_i^{(pq)}\}\subseteq D_i^{(2pq)}$。再由 $|D_i^{(2pq)}|=|D_i^{(pq)}|$，可知结论成立。　　证毕

注： 由引理 1 易知，$D_i^{(2pq)}\equiv D_i^{(pq)}\pmod{pq}$，$D_i^{(2p)}\equiv D_i^{(p)}\pmod p$，$D_i^{(2q)}\equiv D_i^{(q)}\pmod q$，进而，$2D_i^{(2pq)}\equiv 2D_i^{(pq)}\pmod{2pq}$，$2qD_i^{(2p)}\equiv 2qD_i^{(p)}\pmod{2pq}$，$2pD_i^{(2q)}\equiv 2pD_i^{(q)}\pmod{2pq}$。

定义如式(5)辅助多项式：

$$\begin{aligned}&S_{(2pq)}(x)=\sum_{t\in D_0^{(2pq)}}x^t,\quad S_{(pq)}(x)=\sum_{t\in D_0^{(pq)}}x^{2t}\\ &S_{(2p)}(x)=\sum_{t\in D_0^{(2p)}}x^{qt},\quad S_{(p)}(x)=\sum_{t\in D_0^{(p)}}x^{2qt}\\ &S_{(2q)}(x)=\sum_{t\in D_0^{(2q)}}x^{pt},\quad S_{(q)}(x)=\sum_{t\in D_0^{(q)}}x^{2pt}\end{aligned}\tag{5}$$

由于序列的周期为 N，所以式(5)多项式的指数均模 N 计算。由引理 1 的注记，

$$\begin{aligned}&S_{(2pq)}^2(x)=S_{(pq)}(x),\ S_{(2p)}^2(x)=S_{(p)}(x),\\ &S_{(2q)}^2(x)=S_{(q)}(x)\end{aligned}\tag{6}$$

因此，第 2 节式(2)定义的序列 S 的生成多项式为

$$\begin{aligned}S(x) &= \sum_{k\in I^{(2pq)}}S_{(2pq)}\left(x^{y^k}\right)+\sum_{k\in I^{(2p)}}S_{(2p)}\left(x^{g^k}\right)\\ &\quad+\sum_{k\in I^{(2q)}}S_{(2q)}\left(x^{g^k}\right)+\sum_{k\in I^{(pq)}}S_{(pq)}\left(x^{g^k}\right)\\ &\quad+\sum_{k\in I^{(p)}}S_{(p)}\left(x^{g^k}\right)+\sum_{k\in I^{(q)}}S_{(q)}\left(x^{g^k}\right)+x^{\delta}\end{aligned}\tag{7}$$

其中 $\delta=0$ 或 pq。记

$$\left.\begin{aligned}S_1(x) &= \sum_{k\in I^{(2pq)}}S_{(2pq)}\left(x^{y^k}\right)+\sum_{k\in I^{(2p)}}S_{(2p)}\left(x^{g^k}\right)\\ &\quad+\sum_{k\in I^{(2q)}}S_{(2q)}\left(x^{g^k}\right)\\ S_2(x) &= \sum_{k\in I^{(pq)}}S_{(pq)}\left(x^{g^k}\right)+\sum_{k\in I^{(p)}}S_{(p)}\left(x^{g^k}\right)\\ &\quad+\sum_{k\in I^{(q)}}S_{(q)}\left(x^{g^k}\right)\end{aligned}\right\}\tag{8}$$

则

$$S(x)=S_1(x)+S_2(x)+x^{\delta}\tag{9}$$

由于本文仅考虑 $I^{(2pq)}=I^{(pq)}$, $I^{(2p)}=I^{(p)}$, $I^{(2q)}=I^{(q)}$ 的情形。 因此，

$$S(x)=S_1(x)+S_1^2(x)+x^{\delta} \tag{10}$$

由式(4)，序列 S 的线性复杂度为

$$\begin{aligned} L_s &= N-\deg\left(\gcd\left(x^N-1,S(x)\right)\right) \\ &= N-\deg\left(\gcd\left(\left(x^{pq}-1\right)^2,S(x)\right)\right) \end{aligned} \tag{11}$$

由于 $\gcd(2,pq)=1$，因此在 Z_2 的扩域上存在 pq 次单位根，记为 θ。

引理 2 设 θ 的定义同上， 对于 $0\le i\le pq-1$，则 θ 不可能是 $S(x)$ 的重根。

证明 为了证明结论，只需证明对任意的 $0\le i\le pq-1$，若 θ 是 $S(x)$ 的根，则 θ 不可能是 $S'(x)$ 的根，这里 $S'(x)$ 表示 $S(x)$ 的导数多项式。

事实上，若 θ 既是 $S(x)$ 的根又是 $S'(x)$ 的根，由 $S(\theta^i)=S_1(\theta^i)+S_1^2(\theta^i)+1=0$， 则 $S_1(\theta^i)+S_1^2(\theta^i)=1$。易知，当 $\delta=0$ 时， $S'(x)=S_1'(x)$，而当 $\delta=pq$ 时，$S'(x)=S_1'(x)+x^{pq-1}$。当 $\delta=0$ 时，若 θ 也是 $S'(x)$ 的根，则 $S_1(\theta^i)=\theta^i S_1'(\theta^i)=\theta^i S'(\theta^i)=0$。当 $\delta=pq$ 时，类似可证， $S_1(\theta^i)=1$。 均与 $S_1(\theta^i)+S_1^2(\theta^i)=1$ 矛盾。 证毕

记

$$T_{(pq)}(x)=\sum_{t\in D_0^{(pq)}}x^t,\ T_{(p)}(x)=\sum_{t\in D_0^{(p)}}x^t,\ T_{(q)}(x)=\sum_{t\in D_0^{(q)}}x^t$$

引理 3 设 θ 是 Z_2 的扩域上的 pq 次单位根，则对 $0\le i\le pq-1$，

$$S_{(2pq)}(\theta^t)=\begin{cases} T_{(pq)}\left(\theta^{y^j}\right), & t\in D_j^{(pq)},\ 0\le j\le e-1 \\ \dfrac{q-1}{e}(\bmod 2), & t\in qD_j^{(p)},0\le j\le e-1 \\ \dfrac{p-1}{e}(\bmod 2), & t\in pD_j^{(q)},0\le j\le e-1 \\ 0, & t=0 \end{cases} \tag{12}$$

证明 由定义， $S_{(2pq)}(\theta^t)=\sum_{i\in D_0^{(2pq)}}\theta^{it}$。易知，当 $t=0$ 时，

$$S_{(2pq)}(\theta^t)=\mid D_0^{(2pq)}\mid=d\equiv 0(\bmod 2) \tag{13}$$

当 $t\in D_j^{(pq)}$ 时，不妨设 $t=g^s y^j$， 由 $D_0^{(2pq)}$ 的定义及 $D_0^{(2pq)}\equiv D_0^{(pq)}(\bmod pq)$ 知

$$S_{(2pq)}(\theta^t)=\sum_{i\in D_0^{(2pq)}}\theta^{g^s y^j i}=\sum_{i\in D_0^{(pq)}}\theta^{y^j i}=T_{(pq)}(\theta^{y^j}) \tag{14}$$

当 $t\in qD_j^{(p)}$ 时， 不妨设 $t=qu,u\in D_j^{(p)}$， 则

$$S_{(2pq)}(\theta^t)=\sum_{i\in D_0^{(2pq)}}\theta^{qui}=\sum_{i\in D_0^{(pq)}}\theta^{qui} \tag{15}$$

当 i 取遍 $D_0^{(pq)}$ 中的元素时， $i(\bmod p)$ 恰好取遍 Z_p^* 中每个元素 $(q-1)/e$ 次。 因此，

$$S_{(2pq)}(\theta^t)=\sum_{i\in D_0^{(pq)}}(\theta^q)^{ui}=\frac{q-1}{e}(\bmod 2) \tag{16}$$

当 $t\in pD_j^{(q)}$ 时， 类似可证。 证毕

定义 2 对 $0\le i,j\le e-1$, $d=((p-1)(q-1))/e$，

$$D_{i,j}^{(pq)}=\{g^{es+j}y^i\mid s=0,\cdots,\frac{d}{e}-1\} \tag{17}$$

易知， $D_i^{(pq)}=\bigcup_{j=0}^{e-1}D_{i,j}^{(pq)}$, $0\le i\le e-1$。

引理 4 设 θ 是 Z_2 的扩域上的 pq 次单位根，对 $0\le t\le pq-1$，

$$S_{(2p)}\left(\theta^t\right)=\begin{cases} T_{(p)}\left(\theta_p^{g^{i+j}}\right), & t\in D_{i,j}^{(pq)},0\le i,j\le e-1 \\ T_{(p)}\left(\theta_p^{qg^j}\right), & t\in qD_j^{(p)},0\le j\le e-1 \\ \dfrac{p-1}{e}(\bmod 2), & t\in pD_j^{(q)}\cup\{0\},0\le j\le e-1 \end{cases} \tag{18}$$

其中 $\theta_p=\theta^p$。

证明 由定义， $S_{(2p)}(\theta^t)=\sum_{h\in D_0^{(2p)}}\theta^{qht}$。从而，当 $t\in pD_j^{(q)}\cup\{0\}$ 时， 显然有

$$S_{(2p)}(\theta^t)=\mid D_0^{(2p)}\mid=\frac{p-1}{e}(\bmod 2) \tag{19}$$

当 $t\in D_{i,j}^{(pq)}$ 时，不妨设 $t=g^{es_0+j}y^i$， 由 $qD_0^{(2p)}=qD_0^{(p)}(\bmod pq)$ 得

$$S_{(2p)}\left(\theta^t\right)=\sum_{h\in D_0^{(2p)}}\theta^{hqg^{es_0+j}y^i}=\sum_{h\in D_0^{(p)}}\theta_p^{hg^{i+j}}=T_{(p)}\left(\theta_p^{g^{i+j}}\right) \tag{20}$$

当 $t\in qD_j^{(p)}$ 时， 不妨设 $t=qg^{es_0+j}$，类似地，

$$S_{(2p)}\left(\theta^t\right)=\sum_{h\in D_0^{(2p)}}\theta_p^{q^2hg^{es_0+j}}=\sum_{h\in D_0^{(p)}}\theta_p^{qg^j}=T_{(p)}\left(\theta_p^{qg^j}\right) \tag{21}$$

综上， 可知结论成立。 证毕

类似于引理 4，容易证明引理 5。

引理 5 设 θ 是 Z_2 的扩域上的 pq 次单位根，对 $0\le t\le pq-1$，有

$$S_{(2q)}(\theta^t)=\begin{cases} T_{(q)}(\theta_q^{g^j}), & t\in D_{i,j}^{(pq)},0\le i,j\le e-1 \\ T_{(q)}(\theta_q^{pg^j}), & t\in pD_j^{(q)},0\le j\le e-1 \\ \dfrac{q-1}{e}(\bmod 2), & t\in qD_j^{(p)}\cup\{0\},0\le j\le e-1 \end{cases} \tag{22}$$

其中 $\theta_q=\theta^q$。

对 $0\le i,j\le e-1$，定义

$$\left.\begin{aligned} A_{i,j} &= \sum_{k\in I^{(2pq)}}T_{(pq)}\left(\theta^{y^{i+k}}\right)+\sum_{k\in I^{(2p)}}T_{(p)}\left(\theta_p^{g^{i+j+k}}\right) \\ &\quad +\sum_{k\in I^{(2q)}}T_{(q)}\left(\theta_q^{g^{j+k}}\right) \\ B_i &= \sum_{k\in I^{(2p)}}T_{(p)}\left(\theta_p^{g^{i+k}}\right),\quad C_j=\sum_{k\in I^{(2q)}}T_{(q)}\left(\theta_q^{g^{j+k}}\right) \end{aligned}\right\} \tag{23}$$

及

$$\delta_{i,j}=\begin{cases}1, & A_{i,j}+A_{i,j}^2\equiv 1(\bmod 2)\\ 0, & A_{i,j}+A_{i,j}^2\neq 1(\bmod 2)\end{cases} \tag{24}$$

$$\eta_i=\begin{cases}1, & B_i+B_i^2\equiv 1(\bmod 2)\\ 0, & B_i+B_i^2\neq 1(\bmod 2)\end{cases} \tag{25}$$

$$\lambda_i=\begin{cases}1, & C_i+C_i^2\equiv 1(\bmod 2)\\ 0, & C_i+C_i^2\neq 1(\bmod 2)\end{cases} \tag{26}$$

定理 1　记号同上，则序列 S 的线性复杂度为

$$L_s=N-\sum_{i=0}^{e-1}\sum_{j=0}^{e-1}\delta_{i,j}\frac{d}{e}-\sum_{i=0}^{e-1}\eta_i R_q-\sum_{i=0}^{e-1}\lambda_i R_p \tag{27}$$

证明　由序列 S 的生成多项式 $S(x)=S_1(x)+S_1^2(x)+x^\delta$，其中

$$S_1(x)=\sum_{k\in I^{(2pq)}}S_{(2pq)}\left(x^{y^k}\right)+\sum_{k\in I^{(2p)}}S_{(2p)}\left(x^{g^k}\right)+\sum_{k\in I^{(2q)}}S_{(2q)}\left(x^{g^k}\right) \tag{28}$$

由引理 2 得，

$$\begin{aligned}L_s&=N-\deg\left(\gcd\left(x^N-1,S(x)\right)\right)\\&=N-\deg\left(\gcd\left(x^{pq}-1,S(x)\right)\right)\end{aligned} \tag{29}$$

对 $t=0$，由引理3，引理4及引理5，$S_1(\theta^0)=S_1(1)=0+\frac{p-1}{e}+\frac{q-1}{e}(\bmod 2)$。从而，$S(1)=S_1(1)+S_1^2(1)+1=1$。

对 $t\in D_{i,j}^{(pq)},\ 0\le i,j\le e-1$，由引理 3，引理 4 及引理 5 得

$$S_1(\theta^t)=\sum_{k\in I^{(2pq)}}T_{(pq)}\left(\theta^{y^{i+k}}\right)+\sum_{k\in I^{(2p)}}T_{(p)}\left(\theta_p^{g^{i+j+k}}\right)+\sum_{k\in I^{(2q)}}T_{(q)}\left(\theta_q^{g^{i+k}}\right)=A_{i,j} \tag{30}$$

从而，$S(\theta^t)=A_{i,j}+A_{i,j}^2+1=0$ 当且仅当 $A_{i,j}+A_{i,j}^2\equiv 1(\bmod 2)$。

对 $t\in pD_j^{(q)},\ 0\le j\le e-1$，由引理 3，引理 4 及引理 5 得

$$\begin{aligned}S_1(\theta^t)&=\frac{p-1}{e}\left(\left|I^{(2pq)}\right|+\left|I^{(2q)}\right|\right)+\sum_{k\in I^{(2p)}}T_{(p)}\left(\theta_p^{qg^{i+k}}\right)\\&=\frac{p-1}{e}\left(\left|I^{(2pq)}\right|+\left|I^{(2q)}\right|\right)+B_i\end{aligned} \tag{31}$$

从而，$S(\theta^t)=S_1(\theta^t)+S_1^2(\theta^t)+1=B_i+B_i^2+1=0$ 当且仅当 $B_i+B_i^2\equiv 1(\bmod 2)$。

对 $t\in qD_j^{(p)},0\le j\le e-1$，类似可证，$S(\theta^t)=S_1(\theta^t)+S_1^2(\theta^t)+1=C_i+C_i^2+1=0$ 当且仅当 $C_i+C_i^2\equiv 1(\bmod 2)$。

由 $\left|D_{i,j}^{(2pq)}\right|=\frac{d}{e},\ \left|D_j^{(q)}\right|=R_q,\ \left|D_j^{(p)}\right|=R_p,\ 0\le i,j\le e-1$，知

$$\begin{aligned}L_s&=N-\left|\left\{t\mid S\left(\theta^t\right)=0,0\le t\le pq-1\right\}\right|\\&=N-\left(\sum_{i=0}^{e-1}\sum_{j=0}^{e-1}\delta_{i,j}\frac{d}{e}+\sum_{i=0}^{e-1}\eta_i R_q+\sum_{i=0}^{e-1}\lambda_i R_p\right)\end{aligned} \tag{32}$$

证毕

文献[15]构造的二元广义分圆序列是上述构造的特殊情形，此时 $\gcd(p-1,\ q-1)=2$，且 $I^{(2pq)}=I^{(2p)}=I^{(2q)}=\{1\}$。此时，

$$A_{i,j}=T_{(pq)}\left(\theta^{y^{i+1}}\right)+T_{(p)}\left(\theta_p^{g^{i+j+1}}\right)+T_{(q)}\left(\theta_q^{g^{j+1}}\right),\quad B_i=T_{(p)}\left(\theta_p^{g^{i+1}}\right),\ C_j=T_{(q)}\left(\theta_q^{g^{j+1}}\right) \tag{33}$$

由于，$2\in D_0^{(p)}$ 当且仅当 $p\equiv\pm1(\bmod 8)$，$2\in D_0^{(q)}$ 当且仅当 $q\equiv\pm1(\bmod 8)$，及 $2\in D_0^{(pq)}$ 当且仅当 $p\equiv\pm1(\bmod 8)$ 和 $q\equiv\pm1(\bmod 8)$，或 $p\equiv\pm3(\bmod 8)$ 和 $q\equiv\pm3(\bmod 8)$[2]。由 θ 是 pq 次单位根。容易知道，

$$\left(\sum_{t\in D_0^{(p)}}+\sum_{t\in D_1^{(p)}}\right)\theta_p^t=1,\ \left(\sum_{t\in D_0^{(q)}}+\sum_{t\in D_1^{(q)}}\right)\theta_q^t=1$$

$$\left(\sum_{t\in D_0^{(pq)}}+\sum_{t\in D_1^{(pq)}}\right)\theta^t=1$$

从而，对任意的 $0\le i,j\le 1$，若 $p\equiv\pm1(\bmod 8)$，$B_i+B_i^2=0$。若 $p\equiv\pm3(\bmod 8)$，$B_i+B_i^2=1$。若 $q\equiv\pm1(\bmod 8)$，$C_j+C_j^2=0$。若 $q\equiv\pm3(\bmod 8)$，$C_j+C_j^2=1$。若 $p\equiv\pm1(\bmod 8)$ 和 $q\equiv\pm1(\bmod 8)$，或 $p\equiv\pm3(\bmod 8)$ 和 $q\equiv\pm3(\bmod 8)$，或 $p\equiv\pm1(\bmod 8)$ 和 $q\equiv\pm3(\bmod 8)$，或 $p\equiv\pm3(\bmod 8)$ 和 $q\equiv\pm1(\bmod 8)$，均有 $A_{i,j}+A_{i,j}^2=0$。根据上述分析及定理 1，容易得到文献[15]的主要结论。

4　结论

本文推广了文献[15]的结果，考虑了一般的周期为 $2pq$，其中 $\gcd(p-1,q-1)=e,\ e\ge 2$ 的二元广义分圆序列的构造，此时序列的支撑集取值灵活。特别地，当 $|I^{(2pq)}|=|I^{(2p)}|=|I^{(2q)}|=e/2$ 时，新构造的序列一定是平衡的。

参 考 文 献

[1] Golomb S W and Gong G. Signal Design for Good Correlation: For Wireless Communications, Cryptography and Radar Applications[M]. Cambridge: UK, Cambridge University Press, 2005: 174–175.

[2] Cusick T, Ding C, and Renvall A. Stream Ciphers and Number Theory[M]. Amsterdam: The Netherlands, North-Holland Mathematical Library 55, 1998: 198–212.

[3] Ding C and Helleseth T. Generalized cyclotomy and its applications[J]. *Finite Fields and Their Applications*, 1999, (4): 467–474.

[4] Ding C, Hellseth T, and Shan W. On the linear complexity of Legendre sequences[J]. *IEEE Transactions on Information Theory*, 1998, 44(3): 1276–1278.

[5] Kim Y J, Jin S Y, and Song H Y. Linear complexity and autocorrelation of prime cube sequences[J]. *LNCS*, 2007, 4851: 188–197.

[6] Kim Y J and Song H Y. Linear complexity of prime n-square sequences[C]. IEEE International Symposium on Information Theory, Toronto, Canada, 2008: 2405–2408.

[7] Yan T, Sun R, and Xiao G. Autocorrelation and linear complexity of the new generalized cyclotomic sequences[J]. *IEICE Transactions on Fundamentals*, 2007, E90-A: 857–864.

[8] Yan T, Li S, and Xiao G. On the linear complexity of generalized cyclotomic sequences with the period p^m[J]. *Applied Mathematics Letters,* 2008, (21): 187–193.

[9] Edemskiy V. About computation of the linear complexity of generalized cyclotomic sequences with period p^{n+1}[J]. *Designs Codes Cryptography*, 2011, 61(3): 251–260.

[10] Zhang J W, Zhao C A, and Ma X. Linear complexity of generalized cyclotomic binary sequences of length $2p^m$[J]. *Applicable Algebra in Engineering, Communication and Computing*, 2010, (21): 93–108.

[11] Ke P H, Zhang J, and Zhang S Y. On the linear complexity and the autocorrelation of generalized cyclotomic binary sequences of length $2p^m$[J]. *Designs Codes Cryptography,* 2012, 67(3): 325–339.

[12] Ke P H and Zhang S Y. New classes of quaternary cyclotomic sequence of length $2p^m$ with high linear complexity[J]. *Information Processing Letters*, 2012, 12(16): 646–650.

[13] Hu L Q, Yue Q, and Wang M H. The linear complexity of Whiteman's generalized cyclotomic sequences of period $p^{m+1}q^{n+1}$[J]. *IEEE Transactions on Information Theory*, 2012, 58(8): 5534–5542.

[14] Du X N and Chen Z X. A generalization of the Hall's sixtic residue sequences[J]. *Information Sciences*, 2013, 222: 784–794.

[15] Chang Z L and Li D D. On the linear complexity of generalized cyclotomic binary sequences of length $2pq$[J]. *Concurrency and Computation: Practice and Experience*, 2013, DOI: 10.1002/cpe.3052.

李瑞芳： 女，1988 年生，硕士生，研究方向为序列设计.

柯品惠： 男，1978 年生，副教授，主要研究方向包括序列设计、现代密码学中的布尔函数.