Computer Science and Application 计算机科学与应用, 2012, 2, 165-171
http://dx.doi.org/10.12677/csa.2012.24030 Published Online October 2012 (http://www.hanspub.org/journal/csa.html)

The Autocorrelation Values and Linear Complexity of a Class of Generalized Cyclotomic Ternary Sequence

Lili Yin, Xiwang Cao

College of Science, Nanjing University of Aeronautics and Astronautics, Nanjing
Email: nihaoma2331@126.com, xwcao@nuaa.edu.cn

Received: Jul. 11th, 2012; revised: Jul. 29th, 2012; accepted: Aug. 12th, 2012

Abstract: Pseudorandom sequences with good properties have wide application in information security and communications et al. This paper construct an almost balanced generalized cyclotomic ternary sequence with period p^{n+1} based on the definition of generalized cyclotomic. Further, the autocorrelation values and linear complexity of this sequence are calculated. The method are based on using the classical cyclotomic numbers of order six and the values of partial exponential sums of cyclotomic class of order six over an extension field of $GF(3)$. Results show that this sequence possesses good linear complexity.

Keywords: Generalized Cyclotomic; Cyclotomic Numbers; Autocorrelation Values; Linear Complexity

一类广义分圆三元序列的自相关值和线性复杂度

尹利利，曹喜望

南京航空航天大学理学院，南京
Email: nihaoma2331@126.com, xwcao@nuaa.edu.cn

收稿日期：2012 年 7 月 11 日；修回日期：2012 年 7 月 29 日；录用日期：2012 年 8 月 12 日

摘　要：具有良好性质的伪随机序列在信息安全与通信中有广泛的应用。根据广义分圆定义构造了一类周期为 p^{n+1} 的几乎平衡的 6 阶广义分圆三元序列。利用经典的 6 阶分圆数和部分指数和进一步计算了该序列的自相关值和线性复杂度。结果表明该序列有较好的线性复杂度。

关键词：广义分圆；分圆数；自相关值；线性复杂度

1. 引言

$GF(q)$ 是指只有 q 个元素的有限域，q 为素数。

设 $S=s_0,s_1,\cdots$ 为 $GF(q)$ 上周期为 N 的序列，其中 $s_i=s_{N+i}$。它的自相关函数定义为：

$$R_s(\tau)=\sum_{i=0}^{N-1}\omega^{s(i+\tau)-s(i)} \tag{1}$$

且 $0\le\tau\le N-1$，ω 为 q 次本原单位根。

而序列的线性复杂度是指：最小的 L 满足：$s_g=c_1s_{g-1}+c_2s_{g-2}+\cdots+c_Ls_{g-L}$，对所有的 $g\ge L$，其中 $c_1,c_2,\cdots c_L\in GF(q)$。

设 $S^N(x)=s_0+s_1x+s_2x^2+\cdots+s_{N-1}x^{N-1}$ 为序列 S 的生成多项式，则该序列的线性复杂度可以通过下面的公式算：

$$L(S)=N-\deg\left(\gcd\left(x^N-1,S^N(x)\right)\right) \tag{2}$$

伪随机序列在信息安全领域中有广泛的应用。序列的自相关值和线性复杂度是衡量序列伪随机性质的两个重要指标，根据这两个判断标准，国内外的诸多学者对伪随机序列进行了研究，得到了许多性质良好的序列。

1962 年，Whiteman 在[1]中提出了周期为 pq 的广

义分圆，并计算了 2、4 阶的广义分圆数，人们把这样的广义分圆称为 W-广义分圆。根据 W-广义分圆，丁存生教授给出了 2 阶分圆序列的自相关值[2]，表明了这类序列具有较好的密码学性质。白恩健[3]计算了 4 阶广义分圆序列的线性复杂度，得到了较好的结果。而阎统江在[4]中考虑了任意阶的二元序列的线性复杂度，给出了其上界和下界，表明大多数此类序列的线性复杂度都是好的。另外，在[5]中丁存生和 Helleseth 给出了另外一种广义分圆，人们称为 D-广义分圆。这种广义分圆不仅仅局限于周期为 pq 的情形，对于周期为 p^{n+1} 的序列同样适用。根据 D-广义分圆，阎统江利用剩余类环的多项式分别计算了周期为 pq 和 p^2 的分圆序列的线性复杂度和自相关值[6]。后来，Edemskiy 和阎统江用不同的方法计算了周期为 p^{n+1} 和 p^m 的广义分圆序列的线性复杂度，得到了较好的结果[7,8]。

近年来，由于三元序列和 q 元序列在编码与通信工程中的广泛应用也引起来了不少学者的关注与研究，例如[9-12]。我们都知道分圆数是构造序列的重要工具之一！本篇文章利用六阶分圆构造了周期为 p^{n+1} 的三元序列。

2. 相关理论

设 $p=ef+1$ 是奇素数，e,f 为两个正整数，g 是模 p^{n+1} 的原根，则 g 的阶为 $p^n(p-1)$ 且 $g^{(p-1)}\equiv 1\pmod p$[13,14]。已知 Z_N 代表模 N 的整数环，这里 $N=p^{n+1}$。Z_N^* 为 Z_N 中可逆元素的集合。设 $D_0=\langle g^e\rangle$，它是循环群 Z_N^* 的子群且 $|D_0|=p^n f$。令：$D_k=g^kD_0, k=0,1,\cdots,e-1$，$p^mD_k=\{p^ma;a\in D_k\}$，则 $|p^mD_k|=p^{n-m}f$。由[8]知，$Z_N=\bigcup_{m=0}^{n}\bigcup_{k=0}^{e-1}p^mD_k\bigcup\{0\}$。

我们称 D_k 为 e 阶广义分圆类，$k=0,1,\cdots,e-1$。

对应 e 阶广义分圆数定义为：

$$(i,j)^{(p^{n+1})}=|(D_i+1)\cap D_j|, i,j=0,1,\cdots,e-1,$$

且有下面的等式成立：

$$\begin{aligned}&|(D_{i_0}\cup D_{i_1}+\tau)\cap(D_{j_0}\cup D_{j_1})|=|(D_{i_0}+\tau)\cap D_{j_0}|\\&+|(D_{i_0}+\tau)\cap D_{j_1}|+|(D_{i_1}+\tau)\cap D_{j_0}|\\&+|(D_{i_1}+\tau)\cap D_{j_1}|,\end{aligned}$$

其中 $i_0,i_1,j_0,j_1=0,1,\cdots,e-1$。

本篇文章中，我们取 $e=6$，f 为偶数。构造一类六阶广义分圆序列(3)定义如下：

$$s_i=\begin{cases}0, i\pmod{p^{n+1}}\in\bigcup_{m=0}^{n}(p^mD_0\bigcup p^mD_3\cup\{0\})\\1, i\pmod{p^{n+1}}\in\bigcup_{m=0}^{n}(p^mD_1\bigcup p^mD_5)\\2, i\pmod{p^{n+1}}\in\bigcup_{m=0}^{n}(p^mD_2\bigcup p^mD_4)\end{cases}$$

下面我们就来计算一下此序列的自相关值和线性复杂度。

3. 自相关值

现在我们将利用经典的六阶分圆数来计算上述序列的自相关值，广义的六阶分圆数与经典的六阶分圆数之间的关系由下面的引理给出。

引理 1 ([5]) $(i,j)^{(p^m)}=p^{m-1}(i,j)^{(p)}, \in Z$。

我们还需知道经典六阶分圆数的值！所以下面的引理是必需的。

因为 $p=6f+1$，由[15]知：存在整数 A 和 B 使得 $p=A^2+3B^2, A\equiv 1\pmod 3$，除 B 的正负号外，A 和 B 由 p 唯一决定。

引理 2 设 $p=6f+1$ 是奇素数，f 为偶数

则六阶分圆的分圆数 $(i,j)^{(p)}, i,j=0,1,2,3,4,5$ 及其取值由附录中表 1 和表 2 给出。

在计算序列的自相关值的过程中也需要下面的两个引理。

引理 3[5] 对任意 $r\in Z_N,(r,p)\neq 1$，则

$$|(D_i+r)\bigcap D_j|=\begin{cases}\dfrac{p^n(p-1)}{6}, i=j\\0, i\neq j\end{cases}$$

引理 4 设 $p=6f+1$，若 f 为偶数，则 $-1\in D_0^{(p^m)}$，m 为整数。

证明略。

现在我们给出序列的自相关值。

定理 5 设 $GF(3)$ 上周期为 p^{n+1}（$p=6f+1$，f 为偶数）的六阶广义分圆序列 $S=(s_0,s_1,\cdots s_{p^{n+1}-1},\cdots)$ 定义如(3)式，则它的自相关值为：

1) 当 $ind_g 2\equiv 0\pmod 3$ 时，

$$R_s(\tau)=\begin{cases}p^{n+1},\tau=0\\ M-N+2,\tau\in p^m(D_0\cup D_3),\\ M-N\left(1+\frac{1}{2}B\right)-1,\tau\in p^m(D_1\cup D_4),\\ M-N\left(1-\frac{1}{2}B\right)-1,\tau\in p^m(D_2\cup D_5),\end{cases}$$

2) 当 $ind_g 2\equiv 1(\bmod 3)$ 时，

$$R_s(\tau)=\begin{cases}p^{n+1},\tau=0\\ M-N\left(1+\frac{1}{2}B-A\right)+2,\tau\in p^m(D_0\cup D_3),\\ M-N(A+B+1)-1,\tau\in p^m(D_1\cup D_4),\\ M-N\left(1-\frac{3}{2}B\right)-1,\tau\in p^m(D_2\cup D_5),\end{cases}$$

3) 当 $ind_g 2\equiv 2(\bmod 3)$ 时，

$$R_s(\tau)=\begin{cases}p^{n+1},\tau=0\\ M-N\left(1-\frac{1}{2}B-A\right)+2,\tau\in p^m(D_0\cup D_3),\\ M-N\left(\frac{3}{2}B+1\right)-1,\tau\in p^m(D_1\cup D_4),\\ M-N(1-B+A)-1,\tau\in p^m(D_2\cup D_5),\end{cases}$$

其中 $m=0,1,\cdots,n$， $M=p^{n+1}-p^{n+1-m}$， $N=p^{n-m}$。

证明： 若 $\tau=0$，则 $R_s(\tau)=p^{n+1}$。

下设 $\tau\in p^mD_k, m=0,1,\cdots n, k=0,1,2,3,4,5$。

由引理 3 知 $-\tau\in p^mD_k$

$$\begin{aligned}R_s(\tau)&=\sum_{i=0}^{N-1}\omega^{s(i+\tau)-s(i)}\\ &=\sum_{i\in\bigcup_{m=0}^{n}\left(p^mD_0\cup p^mD_3\right)}\omega^{s(i+\tau)}+\sum_{i\in\bigcup_{m=0}^{n}\left(p^mD_1\cup p^mD_5\right)}\omega^{s(i+\tau)-1}\\ &+\sum_{i\in\bigcup_{m=0}^{n}\left(p^mD_2\cup p^mD_4\right)}\omega^{s(i+\tau)-2}+\omega^{s(\tau)}\\ &=U+V\omega+W\omega^2+\omega^{s(\tau)}+\omega^{-s(\tau)},\end{aligned}$$

其中

$$\begin{aligned}U=\sum_{m=0}^{n}\sum_{l=0}^{n}\Big[&\left|\left(p^mD_0\cup p^mD_3+\tau\right)+\left(p^lD_0\cup p^lD_3\right)\right|\\ &+\left|\left(p^mD_1\cup p^mD_5+\tau\right)+\left(p^lD_1\cup p^lD_5\right)\right|\\ &+\left|\left(p^mD_2\cup p^mD_4+\tau\right)+\left(p^lD_2\cup p^lD_4\right)\right|\Big],\end{aligned}$$

$$\begin{aligned}V=\sum_{m=0}^{n}\sum_{l=0}^{n}\Big[&\left|\left(p^mD_0\cup p^mD_3+\tau\right)+\left(p^lD_1\cup p^lD_5\right)\right|\\ &+\left|\left(p^mD_1\cup p^mD_5+\tau\right)+\left(p^lD_2\cup p^lD_4\right)\right|\\ &+\left|\left(p^mD_2\cup p^mD_4+\tau\right)+\left(p^lD_0\cup p^lD_3\right)\right|\Big],\end{aligned}$$

$$\begin{aligned}W=\sum_{m=0}^{n}\sum_{l=0}^{n}\Big[&\left|\left(p^mD_0\cup p^mD_3+\tau\right)+\left(p^lD_2\cup p^lD_4\right)\right|\\ &+\left|\left(p^mD_1\cup p^mD_5+\tau\right)+\left(p^lD_0\cup p^lD_3\right)\right|\\ &+\left|\left(p^mD_2\cup p^mD_4+\tau\right)+\left(p^lD_1\cup p^lD_5\right)\right|\Big].\end{aligned}$$

下面我们计算 U,V,W。

首先计算 U，

$$U=\sum_{m=0}^{n}\sum_{l=0}^{n}U_{ml}$$

$$\begin{aligned}U_{ml}=&\left|\left(p^mD_0+\tau\right)\bigcap p^lD_0\right|+\left|\left(p^mD_0+\tau\right)\bigcap p^lD_3\right|\\ &+\left|\left(p^mD_3+\tau\right)\bigcap p^lD_0\right|+\left|\left(p^mD_3+\tau\right)\bigcap p^lD_3\right|\\ &+\left|\left(p^mD_1+\tau\right)\bigcap p^lD_1\right|+\left|\left(p^mD_1+\tau\right)\bigcap p^lD_5\right|\\ &+\left|\left(p^mD_5+\tau\right)\bigcap p^lD_1\right|+\left|\left(p^mD_5+\tau\right)\bigcap p^lD_5\right|\\ &+\left|\left(p^mD_2+\tau\right)\bigcap p^lD_2\right|+\left|\left(p^mD_2+\tau\right)\bigcap p^lD_4\right|\\ &+\left|\left(p^mD_4+\tau\right)\bigcap p^lD_2\right|+\left|\left(p^mD_4+\tau\right)\bigcap p^lD_4\right|\end{aligned}$$

1) 当 $l<m$ 时，

$$U_{ml}=\begin{cases}0,\text{如果}\tau\in p^tD_k,\ 0\le t\le l-1;\\ \frac{p^{n-l}(p-1)}{3},\text{如果}\tau\in p^lD_k;\\ 0,\text{如果}\tau\in p^tD_k,\ l<t\le n.\end{cases}$$

2) 当 $l=m$ 时，

$$U_{ml}=\begin{cases}0,\text{如果}\tau\in p^tD_k,\ 0\le t\le l-1;\\ p^{n-m}U',\text{如果}\tau\in p^lD_k;\\ p^{n-m}(p-1),\text{如果}\tau\in p^tD_k,\ l<t\le n.\end{cases}$$

其中

$$\begin{aligned}U'=&(-k,-k)^{(p)}+(-k,3-k)^{(p)}+(3-k,-k)^{(p)}\\ &+(3-k,3-k)^{(p)}+(1-k,1-k)^{(p)}+(1-k,5-k)^{(p)}\\ &+(5-k,1-k)^{(p)}+(5-k,5-k)^{(p)}+(2-k,2-k)^{(p)}\\ &+(2-k,4-k)^{(p)}+(4-k,2-k)^{(p)}+(4-k,4-k)^{(p)}.\end{aligned}$$

3) 当 $l>m$ 时，

$$U_{ml}=\begin{cases}0, \text{如果}\tau\in p^tD_k,\ 0\le t\le m-1;\\ \dfrac{p^{n-m}(p-1)}{3}, \text{如果}\tau\in p^mD_k;\\ 0, \text{如果}\tau\in p^tD_k,\ m<t\le n.\end{cases}$$

所以

$$\begin{aligned}U_m&=U_{m0}+U_{m1}+\cdots+U_{mn}\\&=\begin{cases}\dfrac{p^{n-t}(p-1)}{3}, \text{如果}\tau\in p^tD_k,\ 0\le t\le m-1;\\ p^{n-m}U'+\dfrac{(n-m)p^{n-m}(p-1)}{3}, \text{如果}\tau\in p^mD_k;\\ p^{n-m}(p-1), \text{如果}\tau\in p^tD_k, m<t\le n.\end{cases}\end{aligned}$$

上述 $k=0,1,2,3,4,5$。

所以，当 $\tau\in p^mD_k, m=0,1,\cdots n, k=0,1,2,3,4,5$ 时

$$\begin{aligned}U&=U_0+U_1+\cdots U_n\\&=p^{n+1}-p^{n+1-m}+p^{n-m}U'+\frac{2(n-m)p^{n-m}(p-1)}{3}.\end{aligned}$$

其次计算 V，

$$V=\sum_{m=0}^{n}\sum_{l=0}^{n}V_{ml}$$

$$\begin{aligned}V_{ml}=&\left|(p^mD_o+\tau)\bigcap p^lD_1\right|+\left|(p^mD_0+\tau)\bigcap p^lD_5\right|\\&+\left|(p^mD_3+\tau)\bigcap p^lD_1\right|+\left|(p^mD_3+\tau)\bigcap p^lD_5\right|\\&+\left|(p^mD_1+\tau)\bigcap p^lD_2\right|+\left|(p^mD_1+\tau)\bigcap p^lD_4\right|\\&+\left|(p^mD_5+\tau)\bigcap p^lD_2\right|+\left|(p^mD_5+\tau)\bigcap p^lD_4\right|\\&+\left|(p^mD_2+\tau)\bigcap p^lD_0\right|+\left|(p^mD_2+\tau)\bigcap p^lD_3\right|\\&+\left|(p^mD_4+\tau)\bigcap p^lD_0\right|+\left|(p^mD_4+\tau)\bigcap p^lD_3\right|.\end{aligned}$$

4) 当 $l<m$ 时，

$$V_{ml}=\begin{cases}0, \text{如果}\tau\in p^tD_k,\ 0\le t\le l-1;\\ \dfrac{p^{n-l}(p-1)}{3}, \text{如果}\tau\in p^lD_k;\\ 0, \text{如果}\tau\in p^tD_k, l<t\le n.\end{cases}$$

5) 当 $l=m$ 时，

$$V_{ml}=\begin{cases}0, \text{如果}\tau\in p^tD_k,\ 0\le t\le l-1;\\ p^{n-m}V', \text{如果}\tau\in p^lD_k;\\ 0, \text{如果}\tau\in p^tD_k, l<t\le n.\end{cases}$$

其中

$$\begin{aligned}V'=&(-k,1-k)^{(p)}+(-k,5-k)^{(p)}+(3-k,1-k)^{(p)}\\&+(3-k,5-k)^{(p)}+(1-k,2-k)^{(p)}+(1-k,4-k)^{(p)}\\&+(5-k,2-k)^{(p)}+(5-k,4-k)^{(p)}+(2-k,-k)^{(p)}\\&+(2-k,3-k)^{(p)}+(4-k,-k)^{(p)}+(4-k,3-k)^{(p)}.\end{aligned}$$

6) 当 $l>m$ 时，

$$V_{ml}=\begin{cases}0, \text{如果}\tau\in p^tD_k,\ 0\le t\le m-1;\\ \dfrac{p^{n-m}(p-1)}{3}, \text{如果}\tau\in p^mD_k;\\ 0, \text{如果}\tau\in p^tD_k, m<t\le n.\end{cases}$$

所以，当 $\tau\in p^mD_k, m=0,1,\cdots n, k=0,1,2,3,4,5$ 时

$$\begin{aligned}V&=V_0+V_1+\cdots+V_n\\&=p^{n-m}V'+\frac{2(n-m)p^{n-m}(p-1)}{3}.\end{aligned}$$

类似地，我们可以计算 W，

当 $\tau\in p^mD_k, m=0,1,\cdots n, k=0,1,2,3,4,5$ 时

$$W=p^{n-m}W'+\frac{2(n-m)p^{n-m}(p-1)}{3},$$

其中

$$\begin{aligned}W'=&(-k,2-k)^{(p)}+(-k,4-k)^{(p)}+(3-k,2-k)^{(p)}\\&+(3-k,4-k)^{(p)}+(1-k,-k)^{(p)}+(1-k,3-k)^{(p)}\\&+(5-k,-k)^{(p)}+(5-k,3-k)^{(p)}+(2-k,1-k)^{(p)}\\&+(2-k,5-k)^{(p)}+(4-k,1-k)^{(p)}+(4-k,5-k)^{(p)}.\end{aligned}$$

由六阶分圆数表知

当 $\tau\in p^mD_0\bigcup p^mD_3, m=0,1,\cdots,n$ 时，

$$\begin{aligned}R_s(\tau)&=U+V\omega+W\omega^2+\omega^0+\omega^0\\&=p^{n+1}-p^{n+1-m}+p^{n-m}\left[(0,0)^{(p)}+3(0,3)^{(p)}\right.\\&\left.+2(2,4)^{(p)}-3(1,3)^{(p)}-3(1,4)^{(p)}\right]+2.\end{aligned}$$

当 $\tau\in p^mD_1\bigcup p^mD_4, m=0,1,\cdots,n$ 时

$$\begin{aligned}R_s(\tau)&=U+V\omega+W\omega^2+\omega^2+\omega^1\\&=p^{n+1}-p^{n+1-m}+p^{n-m}\left[(0,0)^{(p)}+3(0,4)^{(p)}\right.\\&\left.+3(1,3)^{(p)}-3(1,2)^{(p)}-3(1,4)^{(p)}-(2,4)^{(p)}\right]-1.\end{aligned}$$

当 $\tau\in p^mD_2\bigcup p^mD_5, m=0,1,\cdots,n$ 时，

$$\begin{aligned}R_s(\tau) &= U + V\omega + W\omega^2 + \omega^2 + \omega^1 \\ &= p^{n+1} - p^{n+1-m} + p^{n-m}\left[(0,0)^{(p)} + 3(0,2)^{(p)}\right. \\ &\left. + 3(1,4)^{(p)} - 3(1,2)^{(p)} - 3(1,3)^{(p)} - (2,4)^{(p)}\right] - 1.\end{aligned}$$

最后由六阶分圆数的取值表代入即可得最后结果。

4. 线性复杂度

线性复杂度是序列的一个重要的性质。这一部分我们将计算序列(3)的线性复杂度。根据引言 1 我们知道 $L = N - \left|\left\{i \middle| S^N(\alpha^i) = 0, i = 0,1,\cdots,N-1\right\}\right|$，这里 $S^N(x) = s_0 + s_1 x + s_2 x^2 + \cdots + s_{N-1}x^{N-1}$ 是序列(2)的生成多项式。

本篇文章采用文献[8]的方法来计算该序列的线性复杂度。

设 $S_m^N(x) = \sum_{l \in p^m D_0} x^l, m = 0,1,\cdots,n$ 为辅助多项式，则 $S_m^N\left(\alpha^{g^k}\right) = \sum_{l \in p^m D_k} \alpha^l$，由序列(2)的定义我们可得到：

$$\begin{aligned}S^N(x) &= \sum_{m=0}^{n}\left[\sum_{i \in p^m D_1} x^i + \sum_{i' \in p^m D_5} x^i + 2\sum_{j \in p^m D_2} x^j + 2\sum_{j' \in p^m D_4} x^j\right] \\ &= \sum_{m=0}^{n}\left[S_m^N(x^g) + S_m^N\left(x^{g^5}\right) + 2S_m^N\left(x^{g^2}\right) + 2S_m^N\left(x^{g^4}\right)\right].\end{aligned}$$

设 α 为 p^{n+1} 次本原单位根，则

$$\begin{aligned}S^N(\alpha^i) = \sum_{m=0}^{n}\Big[&S_m^N\left(\alpha^{ig}\right) + S_m^N\left(\alpha^{ig^5}\right) \\ &+ 2S_m^N\left(\alpha^{ig^2}\right) + 2S_m^N\left(\alpha^{ig^4}\right)\Big]\end{aligned}, \quad i = 0,1,\cdots,N-1.$$

为了使计算更为简单，首先我们探索一下辅助多项式的性质。下面的三个引理告诉了我们辅助多项式的几个性质。

引理 6 对任意的 i,h，下面的等式成立

$$S_m^N\left(\alpha^{ig^{hd}}\right) = S_m^N\left(\alpha^i\right), S^N\left(\alpha^{ig^{hd}}\right) = S^N\left(\alpha^i\right).$$

引理 7 如果 p 不整除 i，则 $S_m^N\left(\alpha^i\right) = 0, m < n$。

引理 8 如果 p 不整除 i，则对于 $t = 0,1,\cdots,n$，有

$$S_m^N\left(\alpha^{p^t i}\right) = \begin{cases}0, t < n-m, \\ S_n^N\left(\alpha^i\right), t = n-m, \\ f, t > n-m.\end{cases}$$

以上三个引理的证明在文献[8]中已给出。由此引理我们可以看出计算序列(2)的线性复杂度和多项式 $S_n^N(x)$ 有关。

已知 g 是模 p^{n+1} 的原根，则 g 也是模 p 的原根。令 $H_0 = \left(g^6\right)$，是 Z_p^* 的子群，并且令 $T(x) = \sum_{l \in H_0} x^l$，设 $\beta = \alpha^{p^n}$，则 β 是 p 次本原单位根，所以有

$$S_n^N\left(\alpha^{g^t}\right) = T\left(\beta^{g^t}\right), t = 0,1,2,3,4,5.$$

因此我们需要计算在 x 取 β 的任意次方时多项式 $T(x)$ 的值。下面的引理告诉了我们多项式 $T(x)$ 的值。

引理 9 设 $p = 6f + 1$ 且 $4p = L^2 + 27M^2$，其中 $L \equiv 1 \pmod 3, 3 \mid M$。如果 f 为偶数，则 $3 \in H_0$。令 $T = \left(T(\beta), T\left(\beta^g\right), T\left(\beta^{g^2}\right), T\left(\beta^{g^3}\right), T\left(\beta^{g^4}\right), T\left(\beta^{g^5}\right)\right)$，其取值情况由附录中表 3 给出。

证明见文献[16]。

现在我们给出序列(3)的线性复杂度，结果如下面的定理所示：

定理 10 序列(3)的线性复杂度为 $L = \frac{2}{3}\left(p^{n+1} - 1\right)$

证明： 设 $i \in p^t D_k, t = 0,1,\cdots,n, k = 0,1,2,3,4,5,$

$$\begin{aligned}S^N(\alpha^i) &= \sum_{m=0}^{n}\left[S_m^N\left(\alpha^{ig}\right) + S_m^N\left(\alpha^{ig^5}\right) + 2S_m^N\left(\alpha^{ig^2}\right) + 2S_m^N\left(\alpha^{ig^4}\right)\right] \\ &= \sum_{m=0}^{n}\left[S_m^N\left(\alpha^{p^t g^{1+k}}\right) + S_m^N\left(\alpha^{p^t g^{5+k}}\right) + 2S_m^N\left(\alpha^{p^t g^{2+k}}\right) + 2S_m^N\left(\alpha^{p^t g^{4+k}}\right)\right] \\ &= \begin{cases}S_n^N\left(\alpha^{g^{1+k}}\right) + S_n^N\left(\alpha^{g^{5+k}}\right) + 2S_n^N\left(\alpha^{g^{2+k}}\right) \\ +2S_n^N\left(\alpha^{g^{4+k}}\right), t = 0 \\ S_n^N\left(\alpha^{g^{1+k}}\right) + S_n^N\left(\alpha^{g^{5+k}}\right) + 2S_n^N\left(\alpha^{g^{2+k}}\right) \\ +2S_n^N\left(\alpha^{g^{4+k}}\right) + \sum_{m=n-t+1}^{n} 6f, t > 0\end{cases} = \begin{cases}T\left(\beta^{g^{1+k}}\right) + T\left(\beta^{g^{5+k}}\right) + 2T\left(\beta^{g^{2+k}}\right) \\ +2T\left(\beta^{g^{4+k}}\right), t = 0 \\ T\left(\beta^{g^{1+k}}\right) + T\left(\beta^{g^{5+k}}\right) + 2T\left(\beta^{g^{2+k}}\right) + 2T\left(\beta^{g^{4+k}}\right) \\ + \sum_{m=n-t+1}^{n} 6f, t > 0.\end{cases}\end{aligned}$$

总之

$$S^N\left(\alpha^i\right)\equiv T\left(\beta^{g^{1+k}}\right)+T\left(\beta^{g^{5+k}}\right)+2T\left(\beta^{g^{2+k}}\right)+2T\left(\beta^{g^{4+k}}\right)\left(\mathrm{mod}\,3\right),$$

又 $S^N\left(\alpha^0\right)=S^N\left(1\right)\equiv 0\left(\mathrm{mod}\,3\right)$。

再由引理 9 的取值表可得

$$L=p^{n+1}-1-\frac{1}{3}\left(p^{n+1}-1\right)=\frac{2}{3}\left(p^{n+1}-1\right).$$

例 取 $p=61$, $n=1$。2 是模 61^2 的一个原根并且 $2^6\equiv 3\left(\mathrm{mod}\,61\right)$。根据序列(2)的定义，我们可以构造一个周期为 3721 的三元序列。通过 Magma，我们计算了这个序列的线性复杂度，结果为 2480，与定理 10 的结论相符。

5. 结束语

本篇文章，我们构造了一类广义三元分圆序列，计算出该序列的自相关值和线性复杂度。结果表明这类序列有较高的线性复杂度。类似于定理 5 和定理 10 的计算过程，我们可以计算当 f 为奇数时该序列的自相关值和线性复杂度，但结果和过程可能更为复杂。

参考文献 (References)

[1] L. Whiteman. A family of difference sets. Acta Arith, 1962, 6: 107-121.

[2] C. S. Ding. Autocorrelation values of generalized cyclotomic sequences of order two. IEEE Transactions on Information Theory, 1998, 44(4): 1698-1702.

[3] E. Bai, X. Fu and G. Xiao. On the linear complexity of generalized cyclotomic sequences of order four over Z_{pq}. IEICE Transactions on Fudanamentals, 2005, E88-A(1): 392-394.

[4] T. J. Yan. Linear complexity of Ding-Helleseth generalized cyclotomic binary sequences of any order. 2011, in press.

[5] C. S. Ding, T. Helleseth. New generalized cyclotomy and its applications. Finite Fields and Their Applications, 1998, 4(2): 140-166.

[6] T. Yan, R. Sun and G. Xiao. Autocorrelation and linear complexity of the new generalized cyclotomic sequences. IEICE Transactions on Fundamentals, 2007, E90-A(4): 857-864.

[7] T. Yan, S. Li and G. Xiao. On the linear complexity of generalized cyclotomic sequences with period p^m. Mathematics Letters, 2008, 21: 187-193.

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

[9] T. Hoholdt, J. Justesen. Ternary sequences with perfect periodic autocorrelation. IEEE Transactions on Information Theory, 1983, 29(4): 596-600.

[10] T. Helleseth, P. V. Kumar. A new family of ternary sequences with ideal two-level autocorrelation function. Designs, Codes and Cryptography, 2011, 23(2): 157-166.

[11] W. A. Jackson, P. R. Wild. Relations between two perfect ternary sequence constructions. Designs, Codes and Cryptography, 1992, 2: 325-332.

[12] J. A. Chang. Ternary sequences with zero-correlation. Proceedings of the IEEE, 1967, 55(7): 1211-1213.

[13] K. Ireland, M. Rosen. A classical introduction to modern number theory. Berlin: Springer, 1982.

[14] K. Ireland, M. Rosen. A classical introduction to modern number theory. 2nd Edition, Berlin: Springer-Verlag, 2003.

[15] L. E. Dickson. Cyclotomy, higher congruences and Waing's problem. American Journal of Mathematics, 1935, 57: 391-424.

[16] L. Q. Hu, Q. Yue and M. L. Lei. The linear complexity of cyclotomic sequences of order six over *GF*(3), preprint.

附录：

Table1. When *f* is even, the cyclotomic numbers of order six
表 1. *f* 为偶数时六阶分圆数表

(h,k)	0	1	2	3	4	5
0	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)
1	(0,1)	(0,5)	(1,2)	(1,3)	(1,4)	(1,2)
2	(0,2)	(1,2)	(0,4)	(1,4)	(2,4)	(1,3)
3	(0,3)	(1,3)	(1,4)	(0,3)	(1,3)	(1,4)
4	(0,4)	(1,4)	(2,4)	(1,3)	(0,2)	(1,2)
5	(0,5)	(1,2)	(1,3)	(1,4)	(1,2)	(0,1)

Table 2. When *f* is even, the values of cyclotomic numbers
表 2. *f* 为偶数时六阶分圆数的取值表

	$ind_g 2 \equiv 0 \pmod 3$	$ind_g 2 \equiv 1 \pmod 3$	$ind_g 2 \equiv 2 \pmod 3$
36(0,0)	$p-17-20A$	$p-17-8A+6B$	$p-17-8A-6B$
36(0,1)	$p-5+4A+18B$	$p-5+4A+12B$	$p-5+4A+6B$
36(0,2)	$p-5+4A+6B$	$p-5+4A-6B$	$p-5-8A$
36(0,3)	$p-5+4A$	$p-5+4A-6B$	$p-5+4A+6B$
36(0,4)	$p-5+4A-6B$	$p-5-8A$	$p-5+4A+6B$
36(0,5)	$p-5+4A-18B$	$p-5+4A-6B$	$p-5+4A-12B$
36(1,2)	$p+1-2A$	$p+1-2A-6B$	$p+1-2A+6B$
36(1,3)	$p+1-2A$	$p+1-2A-6B$	$p+1-2A-12B$
36(1,4)	$p+1-2A$	$p+1-2A+12B$	$p+1-2A+6B$
36(2,4)	$p+1-2A$	$p+1+10A+6B$	$p+1+10A-6B$

Table 3. The values of $T=\left(T(\beta),T(\beta^g),T(\beta^{g^2}),T(\beta^{g^3}),T(\beta^{g^4}),T(\beta^{g^5})\right)$
表 3. $T=\left(T(\beta),T(\beta^g),T(\beta^{g^2}),T(\beta^{g^3}),T(\beta^{g^4}),T(\beta^{g^5})\right)$ 的值

	$ind_g 2 \equiv 0 \pmod 3$	$ind_g 2 \equiv 1 \pmod 3$	$ind_g 2 \equiv 2 \pmod 3$
$p \equiv 1 \pmod{36}$	$(0,0,0,0,0,2)$	$(1,0,1,2,0,1)$	$(0,1,1,0,2,1)$
$p \equiv 13 \pmod{36}$	$(0,1,1,1,1,1)$	$(2,0,1,2,2,1)$	$(2,1,0,2,1,2)$
$p \equiv 25 \pmod{36}$	$(1,2,2,2,2,2)$	$(0,0,2,0,1,2)$	$(0,2,0,0,2,1)$