DOI：10.19789/j.1004-9398.2023.06.001
文献引用：王艳，韩西林，闫联陶，等.两类广义分圆序列的自相关值[J].首都师范大学学报（自然科学版），2023，44（6）：1-7. WANG Y，HAN X L，YAN L T，et al. Autocorrelation values of two classes of generalized cyclotomic sequences[J]. Journal of Capital Normal University（Natural Science Edition），2023，44（6）：1-7.

两类广义分圆序列的自相关值*

王　艳，韩西林**，闫联陶，相乃姣
（西安建筑科技大学理学院，陕西 西安　710055）

摘要：基于广义分圆理论，构造了一类周期为2p的二元广义分圆序列和一类周期为pq的二元广义分圆序列，利用分圆数和差集理论讨论了这2类序列的自相关函数值。对于周期为2p的二元广义分圆序列，当$p \equiv 1 (\mathrm{mod}8)$时，该类序列具有几乎最优的自相关函数值；当$p \equiv 3 (\mathrm{mod}8)$时，该类序列的自相关函数值是四值。对于周期为$pq$的二元广义分圆序列，当$(p-1)(q-1)/4$是偶数时，该类序列具有几乎最优的自相关函数值；当$(p-1)(q-1)/4$是奇数时，该类序列的自相关函数值为四值。结果表明，构造的2类二元广义分圆序列都具有低值自相关性质。

关键词：流密码；自相关性；分圆；伪随机序列
中图分类号：TN918.4　　**文献标识码**：A

Autocorrelation values of two classes of generalized cyclotomic sequences*

WANG Yan，HAN Xilin**，YAN Liantao，XIANG Naijiao
（School of Science，Xi'an University of Architecture and Technology，Xi'an Shaanxi　710055）

Abstract：A class of generalized cyclotomic binary sequences with period 2p and a class of generalized cyclotomic binary sequences with periods pq are constructed based on generalized cyclotomic theory. The autocorrelation values of two classes of generalized cyclotomic binary sequences with periods 2p and pq are determined by cyclotomic number and different sets. The class of binary sequences with period 2p have almost optimal autocorrelation function values when $p \equiv 1 (\mathrm{mod}8)$ and 4-value autocorrelation when $p \equiv 3 (\mathrm{mod}8)$. The class of binary sequences with periods pq have almost optimal autocorrelation function values when $(p-1)(q-1)/4$ is even and 4-value autocorrelation when$(p-1)(q-1)/4$ is odd. Results show that the class of sequences with periods pq and 2p in this paper have low-value autocorrelation.

Keywords：stream cipher；autocorrelation；cyclotomy；pseudorandom sequence
CLC：TN918.4　　**DC**：A

收稿日期：2022-04-27
* 国家自然科学基金项目（61902304）
** 通信作者：hanxilin121@xauat.edu.cn

0 引 言

在伪随机序列构造中,周期自相关函数是衡量伪随机序列性质的一个重要指标。具有理想自相关值的序列在密码学及其他领域有着重要的应用[1-2],因此,二元序列和四元序列的自相关值得到了广泛深入的研究[3-4]。

伪随机序列的构造和自相关值的研究是密码学领域的核心问题。有限域F_2上的伪随机序列的自相关性在加密应用中占有十分重要的地位。基于模N剩余类环分割得到分圆类构造序列是构造伪随机序列的重要方法[1],其中N是序列的周期。当N为素数时,其割圆类称为经典分圆类;当N为合数时,其割圆类称为广义分圆类。相应地,基于经典分圆类构造的序列称为经典分圆序列;基于广义分圆类构造的序列称为广义分圆序列。Legendre序列是基于二阶分圆类构造得到的一类序列,其具有好的自相关性[5]。文献[6-9]研究了具有理想自相关值的二元序列;文献[10]研究了一类自相关函数为三值的广义分圆序列;Ding[11]构造了一类新的分圆类,并得到了一类循环码;Liu和Chen[12]确定了基于这类新的分圆类构造的广义分圆序列的自相关性和线性复杂度。基于二阶广义分圆类的构造方法,Kim等[13]定义了一类周期为$2p$的四元分圆序列,其中p为素数,并且得到了这类序列的自相关值[14]。另外,周期为pqr的伪随机序列的自相关值和线性复杂度也被进一步研究[15]。

二元流密码是一种对称密码系统,其中明文和密文是有限域上的有限序列,通过同一字符串的位加减法进行加密和解密。后一个字符串作为加密和解密密钥,在流密码中被称为密钥流。序列构造的核心是,密钥流应该是随机的,测量密钥流随机性的主要工具是自相关。给定一个周期为N的二元序列$s^\infty=(s_0,s_1,\cdots)$,其中$s_i\in \mathrm{GF}(2)$。周期为$N$的二元序列$s^\infty$的自相关函数被定义为

$$C_s(\omega)=\frac{1}{N}\sum_{i\in Z_N}(-1)^{s_{i+w}+s_i}, \tag{1}$$

式中$0\leqslant\omega\leqslant N-1$。二元序列的理想自相关值是二值,其自相关函数被定义为

$$C_s(\omega)=\begin{cases}1, & \omega=0,\\ 1/N, & \text{其他}。\end{cases} \tag{2}$$

具有理想自相关函数的伪随机序列在密码学、编码理论及通讯工程等领域应用广泛。

本文利用二阶分圆类的方法构造一类周期为pq的二元分圆序列和一类周期为$2p$的二元分圆序列,计算这2类序列的自相关值,并且讨论参数的选取,使得这类序列具有好的自相关性。

1 预备知识

1.1 构造周期为pq的二元序列

假设p、q是2个不同的素数,并且$\gcd(p-1,q-1)=2$。根据中国剩余定理[16],存在模p和模q的公共本元根q,整数x满足

$$x\equiv g(\mathrm{mod}p),x\equiv 1(\mathrm{mod}q), \tag{3}$$

中国剩余定理保证了上述同余方程组的解存在并且唯一。

定义周期$N=pq$,$e=(p-1)(q-1)/2$,由于g是模p和模q的公共本元根,根据中国剩余定理得

$$\mathrm{ord}_N(g)=\mathrm{lcm}(\mathrm{ord}_p(g),\mathrm{ord}_q(g))=\mathrm{lcm}(p-1,q-1)=e,$$

式中$\mathrm{ord}_N(g)$表示g模N得乘法阶。

二阶Whiteman广义分圆类D_0和D_1定义为[17]

$D_i=\{g^s x^i: s=0,1,\cdots,e-1\}$,$i=0,1$。

根据x的定义得

$$Z_{pq}^*=D_0\cup D_1, D_0\cap D_1=\varnothing,$$

式中$\varnothing$表示空集。

二阶广义分圆数定义为

$$(i,j)=|(D_i+1)\cap D_j|, i=0,1;\ j=0,1。 \tag{4}$$

对于Z_N上得任一子集A,$a\in Z_N$,定义

$A+a=\{x+a: x\in A\}$和$Aa=\{ax: x\in A\}$。

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

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

$R=\{0\}$,$C_0=R\cup P\cup D_0$,$C_1=Q\cup D_1$。

则

$$C_0\cup C_1=Z_{pq}, C_0\cap C_1=\varnothing。$$

关于模pq的二阶广义分圆序列$\{t_i\}$,$i\geqslant 0$定义为

$$S_i=\begin{cases}0, & i(\mathrm{mod}pq)\in C_0,\\ 1, & i(\mathrm{mod}pq)\in C_1。\end{cases} \tag{5}$$

上述序列可写成表达式$S_i=F(i\mathrm{mod}N)$,对于所有$0\leqslant i\leqslant N-1$,

$$F(i)=\begin{cases}0, & i\in R\cup P,\\ 1, & i\in Q,\\ (1-\left(\frac{i}{p}\right)\left(\frac{i}{p}\right))/2, & \text{其他},\end{cases} \tag{6}$$

式中$\left(\frac{i}{p}\right)$代表Legendre符号。

1.2　构造周期为2p的二元序列

设p是奇素数,g是奇数,且g是模p和2p的公共本原元,$< g^2 >$表示由g^2生成的子群,记模2p的剩余类环为$Z_{2p}=\{0,1,\cdots,2p-1\}$。

记

$$D_0^{(p)}=< g^2 >(\mathrm{mod}p)=\left\{g^{2k}(\mathrm{mod}p):k=0,1,\cdots,\frac{p-1}{2}-1\right\},$$

$$D_0^{(2p)}=< g^2 >(\mathrm{mod}2p)=\left\{g^{2k}(\mathrm{mod}2p):k=0,1,\cdots,\frac{p-1}{2}-1\right\},$$

$$D_1^{(p)}=gD_0^{(p)}=g< g^2 >(\mathrm{mod}p)=\left\{g^{2k+1}(\mathrm{mod}p):k=0,1,\cdots,\frac{p-1}{2}-1\right\},$$

$$D_1^{(2p)}=gD_0^{(2p)}=g< g^2 >(\mathrm{mod}2p)=\left\{g^{2k+1}(\mathrm{mod}2p):k=0,1,\cdots,\frac{p-1}{2}-1\right\},$$

式中$D_0^{(n)}$和$D_1^{(n)}$表示二阶广义分圆类。记$Z_n^*=\{1\leqslant i\leqslant n-1:\gcd(i,n)=1\}$,则

$$Z_{2p}^*=D_0^{(2p)}\cup D_1^{(2p)},Z_p^*=D_0^{(p)}\cup D_1^{(p)},Z_2^*=\{1\},$$

进而,

$$Z_{2p}=D_0^{(2p)}\cup D_1^{(2p)}\cup 2D_0^{(p)}\cup 2D_1^{(p)}\cup\{0\}。$$

记

$$C_0=D_1^{(2p)}\cup 2D_1^{(p)}\cup\{0\},C_1=D_0^{(2p)}\cup 2D_0^{(p)}\cup pZ_2^*,$$

则$Z_{2p}=C_0\cup C_1$,并且$C_0\cap C_1=\varnothing$,其中$\varnothing$为空集。

构造周期为2p的广义分圆二元序列$\{s_i\}$:

$$s_i=\begin{cases}0, & i(\mathrm{mod}2p)\in C_1,\\ 1, & i(\mathrm{mod}2p)\in C_0。\end{cases}\tag{7}$$

2　主要结果

2.1　周期为pq的二元序列的自相关值

可利用如下定义的差集函数确定二元序列的自相关函数值。

$$d_S(i,j;\omega)=|C_i\cap(C_j+\omega)|,\ \omega\in Z_N,i=0,1;j=0,1。$$

计算周期为pq的二元序列的自相关值需要以下引理。

引理1[18]　对于任意$a\neq 0(\mathrm{mod}N)$,有

$$C_S(a)=1-\frac{4d_S(1,0;a)}{N}。\tag{8}$$

引理2[19]　对于任意$\omega\in Z_N^*$,则有

$$|(D_0+\omega)\cap D_1|=\begin{cases}(0,1), & \omega\in D_0,\\ (1,0), & \omega\in D_1。\end{cases}\tag{9}$$

引理3　对于任一$\omega\in P\cup Q$,有

$$|(D_0+\omega)\cap D_1|=\frac{(p-1)(q-1)}{4}。\tag{10}$$

引理4　对于任一$\omega\in P\cup Q$,有

$$|D_1\cap((P\cup R)+\omega)|=\begin{cases}0, & \omega\in P\cup R,\\ \frac{q-1}{2}, & 其他。\end{cases}\tag{11}$$

证明　如果$\omega\in P\cup Q$,显然$|D_1\cap((P\cup R)+\omega)|=0$;如果$\omega\notin P\cup R$,则存在$z$,使得$z=g^sx\in(P\cup R)+\omega$当且仅当

$$g^sx-\omega\equiv 0(\mathrm{mod}p),\tag{12}$$

注意到$x\equiv g(\mathrm{mod}p)$和$x\equiv 1(\mathrm{mod}q)$。设ω模q的逆是v,由于g是模p的本元根,所以一定存在整数t,$0\leqslant t\leqslant q-1$,使得$v\equiv g^t(\mathrm{mod}p)$。因此,式(12)等价于$g^{s-t}\equiv 1(\mathrm{mod}p)$,进一步等价于$s-t\equiv 0(\mathrm{mod}p-1)$。所以式(12)中$s(0\leqslant s\leqslant e-1)$的解的数目为$e/(q-1)$,即$(p-1)/2$。

引理5[16]　(广义中国剩余定理)设$m_1,\cdots,m_t$为正整数。对于整数集合$a_1,\cdots,a_t$,同余方程组$y\equiv a_i(\mathrm{mod}m_i),\ i=1,\cdots,t$有解当且仅当

$$a_i\equiv a_j(\mathrm{mod}\gcd(m_i,m_j)),\ i\neq j,1\leqslant i\leqslant t,1\leqslant j\leqslant t。\tag{13}$$

如果式(13)成立,则方程$\mathrm{lcm}(m_1,m_2,\cdots,m_t)$有唯一解。

引理6　如果$|p-q|/2$是奇数,则$-1\in D_1$;如果$|p-q|/2$是偶数,则$-1\in D_0$。

证明　由于

$$g^s\equiv -1(\mathrm{mod}pq),\tag{14}$$

当且仅当存在整数$s(0\leqslant s\leqslant e-1)$,由中国剩余定理知,其等价于$g^s\equiv -1(\mathrm{mod}p)$和$g^s\equiv -1(\mathrm{mod}q)$。因为$g$是模$p$和模$q$的公共本元根,所以$g^{(p-1)/2}\equiv -1(\mathrm{mod}p)$,$g^{(q-1)/2}\equiv -1(\mathrm{mod}q)$。其等价于$g^{s-(p-1)/2}\equiv 1(\mathrm{mod}p)$,$g^{s-(q-1)/2}\equiv 1(\mathrm{mod}q)$。由引理5可知,式(14)有解当且仅当$|p-q|/2$为偶数。

引理7　对于任一$\omega\in Z_N^*$,有如下结果。

(1)

$$|Q\cap(D_0+\omega)|=\begin{cases}\dfrac{p-1}{2},\omega\in P,\\ 0,\quad\omega\in Q,\\ \dfrac{p-1}{2},\ \omega\in D_1,\ \dfrac{|p-q|}{2}\text{是偶数},\\ \dfrac{p-3}{2},\omega\in D_1,\ \dfrac{|p-q|}{2}\text{是奇数},\\ \dfrac{p-3}{2},\ \omega\in D_0,\ \dfrac{|p-q|}{2}\text{是偶数},\\ \dfrac{p-1}{2},\ \omega\in D_0,\ \dfrac{|p-q|}{2}\text{是奇数}。\end{cases}$$

(2)

$$|Q\cap((P\cup R)+\omega)|=\begin{cases}0,&\omega\in P,\\ 1,&\omega\in Q,\\ 1,&\omega\in D_0\cup D_1。\end{cases}\tag{15}$$

证明 (1)与引理4的证明类似,可以得到

$$|(P\cup R)\cap(D_0+\omega)|=\begin{cases}0,&\omega\in P\cup R,\\ \dfrac{p-1}{2},&\omega\notin P\cup R。\end{cases}\tag{16}$$

由引理6得

$$|R\cap(D_0+\omega)|=\begin{cases}0,&\omega\in P,\\ 0,&\omega\in D_1,\ \dfrac{|p-q|}{2}\text{是偶数},\\ 1,&\omega\in D_1,\ \dfrac{|p-q|}{2}\text{是奇数},\\ 1,&\omega\in D_0,\ \dfrac{|p-q|}{2}\text{是偶数},\\ 0,&\omega\in D_0,\ \dfrac{|p-q|}{2}\text{是奇数}。\end{cases}$$

又因为

$$|Q\cap(D_0+\omega)|=|(Q\cup R)\cap(D_0+\omega)|-|R\cap(D_0+\omega)|=\frac{p-1}{2}-|R\cap(D_0+\omega)|,$$

将$|R\cap(D_0+\omega)|$带入后可得结果。

(2)注意到

$$|Q\cap((P\cup R)+\omega)|=|Q\cap(P+\omega)|+|Q\cap(R+\omega)|=|Q\cap(P+\omega)|+|Q\cap\{\omega\}|,\tag{17}$$

所以,如果$\omega\in P$,则$|Q\cap((P\cup R)+\omega)|=0$;如果$\omega\in Q$,则$|Q\cap((P\cup R)+\omega)|=1$。

由P和Q的定义,对于任一给定$\omega\in Z_N^*$,有

$$up-vq\equiv\omega(\mathrm{mod}pq),\tag{18}$$

式中:$1\leqslant u\leqslant q-1$;$1\leqslant v\leqslant p-1$。假设上式有2个解$(u_1,v_1)$和$(u_2,v_2)$。则

$$u_1p-v_1q\equiv u_2p-v_2q(\mathrm{mod}pq),\tag{19}$$

因此,$u_1p\equiv u_2p(\mathrm{mod}q)$,$v_1q\equiv v_2q(\mathrm{mod}p)$,

又

$$0\leqslant u_1\leqslant q-1,0\leqslant u_2\leqslant q-1,$$
$$0\leqslant v_1\leqslant p-1,0\leqslant v_2\leqslant p-1,$$

且

$$\gcd(p,q)=1,\tag{20}$$

所以

$$(u_1,v_1)=(u_2,v_2)。\tag{21}$$

因此,当u跑遍$\{1,2,\cdots,q-1\}$且v跑遍$\{1,2,\cdots,q-1\}$时,函数$up-vq$在Z_N^*上取$(p-1)(q-1)$个不同的元,但是Z_N^*中仅有$(p-1)(q-1)$个元。所以,对于任一给定$\omega\in Z_N^*$,有

$$|Q\cap(P+\omega)|=1。$$

引理8 如果$(p-1)(q-1)/4$为偶数,则$(0,0)=(1,0)=(1,1)$且有2个差集分圆数

$$(0,0)=\frac{(p-2)(q-2)+1}{4},$$
$$(0,1)=\frac{(p-2)(q-2)-3}{4}。$$

如果$(p-1)(q-1)/4$为奇数,则$(0,0)=(1,0)=(1,1)$且有2个差集分圆数

$$(0,0)=\frac{(p-2)(q-2)+3}{4},$$
$$(0,0)=\frac{(p-2)(q-2)-1}{4}。$$

在下一部分需要用到以下公式:

$$d_s(1,0;\omega)=|C_1\cap(C_0+\omega)|=|(Q\cup D_1)\cap((R\cup P\cup D_0)+\omega)|=|(D_1\cap(D_0+\omega)|+|D_1\cap((P\cup R)+\omega)|+|Q\cap(D_0+\omega)|+|Q\cap((P\cup R)+\omega)|,\tag{22}$$

设各个符号定义同上,相应的主要结果如下。

定理1 设$(p-1)(q-1)/4$为偶数,则

$$C_S(w)=\begin{cases}\dfrac{-p+q+1}{pq},&w\in P,\\ \dfrac{-p+q-3}{pq},&w\in Q,\\ \dfrac{-1}{pq},&w\in Z_N^*。\end{cases}\tag{23}$$

证明 由式(22),引理2~4,7和8可得

$$d_s(1,0;\omega)=$$

$$\begin{cases}\dfrac{(p-1)(q-1)}{4}+0+\dfrac{p-1}{2}+0, & \omega\in P,\\ \dfrac{(p-1)(q-1)}{4}+\dfrac{p-1}{2}+0+1, & \omega\in Q,\\ \dfrac{(p-2)(q-2)-3}{4}+\dfrac{q-1}{2}+\dfrac{p-1}{2}+1, & \omega\in D_0,\\ \dfrac{(p-2)(q-2)}{4}+\dfrac{q-1}{2}+\dfrac{p-3}{2}+1, & \omega\in D_1,\end{cases}=$$

$$\begin{cases}\dfrac{pq+p-q-1}{4}, & \omega\in P,\\ \dfrac{pq+p-q+3}{4}, & \omega\in Q,\\ \dfrac{pq+1}{4}, & \omega\in D_0\cup D_1。\end{cases}\tag{24}$$

再由引理1可得如下定理。

定理2　设$(p-1)(q-1)/4$为奇数,则

$$C_S(w)=\begin{cases}\dfrac{-p+q-3}{pq}, & \omega\in P,\\ \dfrac{-p+q+1}{pq}, & \omega\in Q,\\ \dfrac{-3}{pq}, & \omega\in D_0,\\ \dfrac{1}{pq}, & \omega\in D_1。\end{cases}\tag{25}$$

证明与定理1的证明类似。

由定理1和定理2可以看出,当$|p-q|$非常小时,二阶广义分圆二元序列的自相关值差异很小。

对于二元序列的自相关值,最好的情形是$p-q=2$,即p和q是孪生素数。在这种情形下,当$(p-1)(q-1)/4$为偶数时,此类序列的自相关值$C_s(\omega)$是二值的,即这类序列具有理想自相关值;当$(p-1)(q-1)/4$为奇数时,此类序列的自相关值$C_s(\omega)$为四值。

另一种情形是当$p-q=4$时。在这种情形下,当$(p-1)(q-1)/4$为偶数时,此类序列的自相关值$C_s(\omega)$是四值;当$(p-1)(q-1)/4$为奇数时,此类序列的自相关值$C_s(\omega)$为三值。因此,这类序列具有好的自相关性。

2.2　周期为$2p$的二元序列的自相关值

引理9[4]　设$D_0^{(p)}$、$D_1^{(p)}$、$D_0^{(2p)}$、$D_1^{(2p)}$是由1.2节中定义的二阶广义分圆类,则

(1)$2\in D_0^{(p)}$当且仅当$p\equiv\pm1(\mathrm{mod}8)$;

(2)$2\in D_1^{(p)}$当且仅当$p\equiv\pm3(\mathrm{mod}8)$。

引理10[19]　设t是一个奇数,则对于$i=0,1$,有

(1) $2D_i^{(p)}+pt(\mathrm{mod}2p)=\begin{cases}D_i^{(2p)}, & 2\in D_0^{(p)},\\ D_{i+1}^{(2p)}, & 2\in D_1^{(p)}。\end{cases}$

(2) $D_i^{(2p)}+2pt(\mathrm{mod}2p)=D_i^{(2p)}$。

设$D_0^{(p)}$、$D_1^{(p)}$是关于p的二阶广义分圆类,定义

$$(i,j)_p=|(D_i^{(p)}+1)\cap D_j^{(p)}|,\ i,j\in\{0,1\},\tag{26}$$

为模p的二阶分圆数。

引理11[19]　若$p\equiv1(\mathrm{mod}4)$,则

$$(0,1)_p=(1,0)_p=(1,1)_p=\frac{p-1}{4},$$

$$(0,0)_p=\frac{p-5}{4};$$

若$p\equiv3(\mathrm{mod}4)$,则

$$(1,0)_p=(0,0)_p=(1,1)_p=\frac{p-3}{4},$$

$$(0,1)_p=\frac{p+1}{4}。$$

引理12[19]　对于任意$\tau\in Z_p^*$,$i=0,1$,有

(1)

$$\left|(D_i^{(p)}+\tau)(\mathrm{mod}p)\cap D_i^{(p)}\right|=\begin{cases}(0,0), & \tau\in D_i^{(p)},\\ (1,1), & \tau\in D_{i+1}^{(p)}。\end{cases}$$

(2)

$$\left|(D_i^{(p)}+\tau)(\mathrm{mod}p)\cap D_{i+1}^{(p)}\right|=\begin{cases}(0,1), & \tau\in D_i^{(p)},\\ (1,0), & \tau\in D_{i+1}^{(p)}。\end{cases}$$

(3) 若$(-\tau)(\mathrm{mod}p)\cap D_i^{(p)}$,则

$$Z_p^*\cup\{0\}\subseteq(D_i^{(p)}+\tau)(\mathrm{mod}p)。$$

引理13　设$\tau\in2Z_p^*$,$i\in Z_2$,有

(1)若$2\in D_0^{(p)}$,则

$$\left|(D_i^{(2p)}+\tau)\cap 2D_i^{(p)}\right|=\begin{cases}(0,0), & \tau\in D_i^{(2p)},\\ (1,1), & \tau\in D_{i+1}^{(2p)}。\end{cases}$$

$$\left|(D_i^{(2p)}+\tau)\cap 2D_{i+1}^{(p)}\right|=\begin{cases}(0,1), & \tau\in D_i^{(2p)},\\ (1,0), & \tau\in D_{i+1}^{(2p)}。\end{cases}$$

$$\left|(2D_i^{(p)}+\tau)\cap D_i^{(2p)}\right|=\begin{cases}(0,0), & \tau\in D_i^{(2p)},\\ (1,1), & \tau\in D_{i+1}^{(2p)}。\end{cases}$$

$$\left|(2D_i^{(p)}+\tau)\cap D_{i+1}^{(2p)}\right|=\begin{cases}(0,1), & \tau\in D_i^{(2p)},\\ (1,0), & \tau\in D_{i+1}^{(2p)}。\end{cases}$$

(2)若$2\in D_1^{(p)}$,则

$$\left|(D_i^{(2p)}+\tau)\cap 2D_i^{(p)}\right|=\begin{cases}(0,1), & \tau\in D_i^{(2p)},\\ (1,0), & \tau\in D_{i+1}^{(2p)}。\end{cases}$$

$$\left|(D_i^{(2p)}+\tau)\cap 2D_{i+1}^{(p)}\right|=\begin{cases}(0,0), & \tau\in D_i^{(2p)},\\ (1,1), & \tau\in D_{i+1}^{(2p)}。\end{cases}$$

$$\left|(2D_i^{(p)}+\tau)\cap D_i^{(2p)}\right|=\begin{cases}(1,0), & \tau\in D_i^{(2p)},\\ (0,1), & \tau\in D_{i+1}^{(2p)}。\end{cases}$$

$$\left|(2D_i^{(p)}+\tau)\cap D_{i+1}^{(2p)}\right|=\begin{cases}(1,1), & \tau\in D_i^{(2p)},\\ (0,0), & \tau\in D_{i+1}^{(2p)}。\end{cases}$$

引理14[19] 设$\tau\in Z_{2p}^*, i\in Z_2$,

(1)若$2\in D_0^{(p)}$, 则

$$\left|(\mathrm{D}_i^{(2p)}+\tau)\cap D_i^{(2p)}\right|=\begin{cases}(0,0), & \tau\in D_i^{(p)},\\ (1,1), & \tau\in D_{i+1}^{(p)}。\end{cases}$$

$$\left|(D_i^{(2p)}+\tau)\cap D_{i+1}^{(2p)}\right|=\begin{cases}(0,1), & \tau\in D_i^{(p)},\\ (1,0), & \tau\in D_{i+1}^{(p)}。\end{cases}$$

$$\left|(2D_i^{(p)}+\tau)\cap 2D_i^{(p)}\right|=\begin{cases}(0,0), & \tau\in D_i^{(p)},\\ (1,1), & \tau\in D_{i+1}^{(p)}。\end{cases}$$

$$\left|(2D_i^{(p)}+\tau)\cap 2D_{i+1}^{(p)}\right|=\begin{cases}(0,1), & \tau\in D_i^{(p)},\\ (1,0), & \tau\in D_{i+1}^{(p)}。\end{cases}$$

(2)若$2\in D_1^{(p)}$, 则

$$\left|(D_i^{(2p)}+\tau)\cap D_i^{(2p)}\right|=\begin{cases}(1,1), & \tau\in D_i^{(p)},\\ (0,0), & \tau\in D_{i+1}^{(p)}。\end{cases}$$

$$\left|(D_i^{(2p)}+\tau)\cap D_{i+1}^{(2p)}\right|=\begin{cases}(1,0), & \tau\in D_i^{(p)},\\ (0,1), & \tau\in D_{i+1}^{(p)}。\end{cases}$$

$$\left|(2D_i^{(p)}+\tau)\cap 2D_i^{(p)}\right|=\begin{cases}(0,0), & \tau\in D_i^{(p)},\\ (1,1), & \tau\in D_{i+1}^{(p)}。\end{cases}$$

$$\left|(2D_i^{(p)}+\tau)\cap 2D_{i+1}^{(p)}\right|=\begin{cases}(0,1), & \tau\in D_i^{(p)},\\ (1,0), & \tau\in D_{i+1}^{(p)}。\end{cases}$$

定理3 设$\{s_i\}$是由1.2节中定义的二元广义分圆序列,p是奇素数。

(1)当$p\equiv 1(\mathrm{mod}8)$时,序列$\{s_i\}$的自相关函数$C_s(\tau)$满足

$$C_s(\tau)=\begin{cases}2p, & \tau=0,\\ 2p-4, & \tau=p,\\ -2, & \tau\in Z_{2p}^*\cup 2Z_p^*。\end{cases}\tag{27}$$

(2)当$p\equiv 3(\mathrm{mod}8)$时,序列$\{s_i\}$的自相关函数$C_s(\tau)$满足

$$C_s(\tau)=\begin{cases}2p, & \tau=0,\\ -2p, & \tau=p,\\ 2, & \tau\in Z_{2p}^*,\\ -2, & \tau\in 2Z_p^*。\end{cases}\tag{28}$$

证明 (1)当$p\equiv 1(\mathrm{mod}8)$时,根据引理9可知,$2\in D_0^{(p)}$,所以

$$C_s(\tau)=\sum_{i=0}^{2p-1}(-1)^{s_{i+\tau}-s_i}=\sum_{i\in\{0,p\}}(-1)^{s_{i+\tau}-s_i}+\sum_{i\in D_0^{(2p)}\cup D_1^{(2p)}}(-1)^{s_{i+\tau}-s_i}+\sum_{i\in 2D_0^{(p)}\cup 2D_1^{(p)}}(-1)^{s_{i+\tau}-s_i}。$$

若$\tau=0$,则$C_s(\tau)=2p$。

若$\tau=p$,则$\sum_{i\in\{0,p\}}(-1)^{s_{i+\tau}-s_i}=-2$,由引理10可知$D_i^{(2p)}+p=2D_i^{(p)}, i=0,1$。因此

$$C_s(\tau)=-2+2p-2=2p-4。$$

若$\tau\in D_0^{(2p)}$,则$s_\tau=0$,由引理10可知,$p+\tau\in p+D_0^{(2p)}\in 2D_0^{(p)}$,所以$s_{p+\tau}=0$。因此

$\sum_{i\in\{0,p\}}(-1)^{s_{i+\tau}-s_i}=0$,再根据引理12和引理13可知

$$\sum_{t\in D_0^{(2p)}\cup D_1^{(2p)}}(-1)^{s_{t+\tau}-s_t}+\sum_{t\in 2D_0^{(p)}\cup 2D_1^{(p)}}(-1)^{s_{t+\tau}-s_t}=2((0,1)-(1,0)+(0,0)-(1,1))=-2,$$

所以$C_s(\tau)=-2$。

同理可得,若$\tau\in D_1^{(2p)}$,则$C_S(\tau)=-2$;若$\tau\in 2D_0^{(p)}$,则$C_S(\tau)=-2$;若$\tau\in 2D_1^{(p)}$,则$C_S(\tau)=-2$。

(2)当$p\equiv 3(\mathrm{mod}8)$时,证明与(1)类似。

定理3表明当$p\equiv 1(\mathrm{mod}8)$时,序列$\{s_i\}$的自相关函数是三值;当$p\equiv 3(\mathrm{mod}8)$时,序列$\{s_i\}$的自相关函数是四值,即这类序列具有低值自相关性。

3 结束语

基于广义分圆类,本文分别构造了两类周期为pq和$2p$的二元广义分圆序列,利用分圆数和差集理论确定了这2类序列的自相关函数值。当$(p-1)(q-1)/4$为偶数时,周期为pq的二元序列自相关函数值为三值;当$(p-1)(q-1)/4$为奇数时,周期为pq的二元序列自相关函数值为四值。当$p\equiv 1(\mathrm{mod}8)$时,周期为$2p$的二元序列自相关函数值为三值;当$p\equiv 3(\mathrm{mod}8)$时,周期为$2p$的二元序列自相关函数值为四值。结果表明,这2类序列都具有好的密码学性质。

参考文献

[1] WANG Y, HAN X L, WANG W Q, et al. Linear complexity over F_q and 2-adic complexity of a class of binary generalized cyclotomic sequences with low-value autocorrelation[J]. Designs, Codes and Cryptography, 2022, 90: 1695-1712.

[2] TOPUZOGGLU A, WINTERHOF A. Pseudorandom sequences[J]. Topics in Geometry, Coding Theory and

Cryptography, Algebra and Applications, 2006, 6(AA): 135-166.

[3] CHEN X, LIU H, Autocorrelation values of generalized cyclotomic sequences with period p^n+1[J]. Mathematics, 2019, 7(10): 950.

[4] WANG Q, KONG W, YAN Y, et al. Autocorrelation of a class of quaternary sequences of period $2p^m$[J]. arXiv: 2002.00375, 2020.

[5] DING C, HELLESETH T, SHAN W. On the linear complexity of Legendre sequences[J]. IEEE Transaction on Communications, 1998, 44: 1276-1278.

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

[7] LIM T, NO J S, CHUNG H. New construction of quaternary sequences with good correlation using binary sequences with good correlation[J]. IEICE Transaction, Fundamentals, 2011, 94(8): 1701-1705.

[8] EDEMSKIY V, IVANOV A. The linear complexity of balanced quaternary sequences with optimal autocorrelation value [J]. Cryptography and Communications, 2015, 7(4): 485-496.

[9] TANG X, DING C. New classes of balanced quaternary and almost balanced binary sequences with optimal autocorrelation value [J]. IEEE Transactions on Information Theory, 2010, 56(12): 6398-6405.

[10] CHUNG J H, HAN Y K, YANG K. New quaternary sequences with even period and three-valued autocorrelation[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2010, 93(1): 309-315.

[11] DING C. Cyclotomic constructions of cyclic codes with length being the product of two primes[J]. IEEE Transactions on Information Theory, 2011, 58(4): 2231-2236.

[12] LIU H, CHEN X. Autocorrelation values and linear complexity of new generalized cyclotimic sequences[J]. Acta Mathematica Sinica (Chinese Series), 2019, 62(2): 233-246.

[13] KIM Y J, HONG Y P, SONG H Y. Autocorrelation of some quaternary cyclotomic sequences of length $2p$[J]. IEICE Transaction on Fundamentals of Electronics, Communications and Computer Sciences, 2008, 91(12): 3679-3684.

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

[15] JIA W J, GAO J T, ZHANG P. Linear complexity and autocorrelation of a new class of binary generalized cyclotomic sequences of order two and length pqr[J]. Journal of Systems Engineering and Electronics, 2019, 30(4): 651-661.

[16] PEI D, SALOMAA A, DING C. Chinese remainder theorem: applications in computing, coding, cryptography [M]. Hongkong: World Scientific, 1996.

[17] WHITEMAN A L. A family of difference sets[J]. Illinois Journal of Mathematics, 1962, 6(1): 107-121.

[18] DING C S. Autocorrelation values of generalized cyclotomic sequences of order two[J]. IEEE Transactions on Information Theory, 1998, 44(4): 1699-1702.

[19] KE P H, ZHANG J, ZHANG S Y. On the linear complexity and the autocorrelation of generalized cyclotomic binary sequences of length $2p^m$[J]. Designs, Codes and Cryptography, 2013, 67(3): 325-339.

(责任编辑:马田田)