一类推广的二元 Legendre-Sidelnikov 序列的自相关分布

柯品惠*① 叶智钒① 常祖领②
①(福建省网络安全与密码技术重点实验室 福州 350117)
②(郑州大学数学与统计学院 郑州 450001)

摘 要：推广的 Legendre-Sidelnikov 序列较之原序列有更好的平衡性质，但是关于该序列的周期自相关函数，迄今仅知道一些特殊移位的情形。该文利用有限域上特征和的相关性质，给出了推广的二元 Legendre-Sidelnikov 序列的自相关函数的完整分布。结果表明当 $p\equiv 3 \pmod 4$ 且 $q \gg p$ 时，推广的 Legendre-Sidelnikov 序列较之原序列有更好的周期自相关函数的分布。

关键词：Legendre 序列；Sidelnikov 序列；平衡性；周期自相关；乘法特征
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2016)02-0303-07
DOI: 10.11999/JEIT150687

Autocorrelation Distribution of Binary Generalized Legendre-Sidelnikov Sequences

KE Pinhui① YE Zhifan① CHANG Zuling②
①(*Fujian Provincial Key Laboratory of Network Security and Cryptology*, *Fuzhou* 350117, *China*)
②(*School of Mathematics and Statistics*, *Zhengzhou University*, *Zhengzhou* 450001, *China*)

Abstract: Compared with the original Legendre-Sidelnikov sequence, the generalized Legendre-Sidelnikov sequence has a better balanced property. For its autocorrelation distribution, however, only some special cases are known. In this paper, using the character sums, the autocorrelation distribution of the generalized binary Legendre-Sidelnikov sequence is determined completely. The result shows that the generalized Legendre-Sidelnikov sequence possesses a better autocorrelation distribution if $p\equiv 3 \pmod 4$ and $q \gg p$.

Key words: Legendre sequence; Sidelnikov sequence; Balance; Periodic autocorrelation; Multiplicative character

1 引言

具有良好自相关特性的序列在通信系统、雷达和密码学等应用中起着重要的作用[1−4]。许多具有这些特性的序列是利用有限域的乘法特征来构造的。一个著名的例子是 Legendre 序列，该序列的构造是基于有限域 $\mathbb{F}_p$ 上的二次特征，其中 p 为素数。特别地，$\mathbb{F}_2$ 上的 Legendre 序列已被证明具有较高的线性复杂度和很好的伪随机特性，具体可参看文献[5,6]。另一个例子就是 Sidelnikov 序列，该序列也已被证明有良好的周期自相关特性[7−10]。最近，结合以上两个概念，文献[11,12]构造了一种新的序列 — Legendre-Sidelnikov 序列。文献[11]给出了 Legendre-Sidelnikov 序列的一些伪随机性质，例如在 $p=q$ 时该序列是平衡的，以及该序列的周期自相关分布和非周期自相关分布。进一步地，文献[12,13]分析了该序列的线性复杂度，并在某些特殊情况下给出了该序列线性复杂度的一个下界。

注意到 Legendre-Sidelnikov 序列仅在 $\gcd(p, q-1)=1$ 且 $p=q$ 时是平衡的。为了改进该序列的平衡性，即使得序列在更多的情形下都保持平衡性，人们对已有的 Legendre-Sidelnikov 序列进行了改进。一方面，利用有限域的乘法特征，文献[14]把 Legendre-Sidelnikov 序列推广到 d 元的情形，其中 d 是 $p-1$ 与 $q-1$ 的公因子。此时，d 元 Legendre-Sidelnikov 序列对任意的奇素数 p 和奇素数幂 q ($\gcd(p,q-1)=1$) 都是平衡的，即 d 元广义 Legendre-Sidelnikov 序列具有更好的平衡性。当 $d=2$ 时，与文献[11]定义的序列比较易知，两条序列在 $i\in R$ 时取值相同，但是在 $i\in P$ 和 $i\in Q^*$ 不同，

收稿日期：2015-06-08；改回日期：2015-09-11；网络出版：2015-11-19
*通信作者：柯品惠 keph@fjnu.edu.cn
基金项目：福建师范大学“网络与信息安全关键理论和技术”校创新团队(IRTL1207)，福建省自然科学基金(2015J01237)，国家自然科学基金联合基金(U1304604)
Foundation Items: Fujian Normal University Innovative Research Team (IRTL1207), Natural Science Foundation of Fujian Province (2015J01237), The Joint Funds of the National Natural Science Foundation of China (U1304604)

前者取值为常数，而后者取值更随机。 文献[14]分析了该序列的一些重要的伪随机性质包括非周期自相关、k 阶相关性测度和线性复杂性等。另外，最近文献[15]也通过改变 P 和 Q 对应下标集的序列元素的赋值，构造了一类新的二元 Legendre-Sidelnikov 序列。与文献[14]中的定义的序列比较易知，对下标集 Q 对应的序列值仅相差一个常数。 但是，对下标集 P 对应的序列元素，两个构造得到的序列是不相同的。同时，文献[15]给出了该序列的自相关函数的分布，并指出该序列在一些情形具有较低的自相关性质。

关于文献[14]中的定义的 d 元广义 Legendre-Sidelnikov 序列的周期自相关分布，迄今仅知道一个特殊情形，即序列移位是 p 的倍数的情形(文献[14]引理 5)。 一般地，该序列自相关函数分布的完全确定较为困难。本文研究了文献[14]中推广的二元 Legendre-Sidelnikov 序列，即 $d=2$ 的情形， 给出了该序列完整的周期自相关分布。具体地，本文安排如下：第 2 节给出了本文需要的一些定义和引理；第 3 节计算了推广的二元 Legendre-Sidelnikov 序列的周期自相关分布；最后，对 Legendre-Sidelnikov 序列及其推广的相关性进行比较， 并提供了相应的实例。

2 预备知识

令 $n=p(q-1)$，其中 p 为奇素数， q 为奇素数幂且 $\gcd(p,q-1)=1$，以及 $P=\{0,p,2p,\cdots,p\cdot(q-2)\}$，$Q=\left\{\frac{q-1}{2},3\cdot\frac{q-1}{2},\cdots,(2p-1)\cdot\frac{q-1}{2}\right\}$。注意到 $P\cap Q=\left\{\frac{n}{2}\right\}$ 令 $Q^*=Q\setminus\left\{\frac{n}{2}\right\}$，$R=Z_n\setminus(P\cup Q^*)$。定义 $\mathbb{F}_2$ 上的 Legendre-Sidelnikov 序列 $S=\{s_i\}$ 如式(1)：

$$s_i=\begin{cases}1, & i\in P\\ 0, & i\in Q^*\\ \frac{1}{2}\cdot\left(1-\left(\frac{i}{p}\right)\eta(g^i+1)\right), & i\in R\end{cases}\tag{1}$$

其中 $\left(\frac{\cdot}{p}\right)$ 为 Legendre 符号， g 是 $\mathbb{F}_q$ 的本原元， η 是 $\mathbb{F}_q$ 上的二次特征。关于 Legendre 符号和二次特征的定义及更多的性质， 可参阅文献[16]。

文献[14]对上述概念进行了推广，给出了 d 元广义 Legendre-Sidelnikov 序列的定义。令 p 为奇素数 q 为奇素数的幂次且 $q\equiv 1(\bmod d)$， g 是有限域 $\mathbb{F}_q$ 的本原元。定义 $\mathbb{F}_q$ 上的 d 阶乘法特征 $\chi_q(\cdot)$： $\chi_q(g^i)=w^i$，$\chi_q(0)=0$，其中 w 是复数域上的 d 阶单位根。则 d 元广义 Legendre-Sidelnikov 序列 $S=\{s_i\}$ 定义为

$$s_i=\begin{cases}0, & i=n/2\\ \log_w\left(\chi_q(g^i+1)\right), & i\in P\setminus\left\{\frac{n}{2}\right\}\\ \log_w\left(\chi_p(i)\right), & i\in Q^*\\ \log_w\left(\chi_p(i)\cdot\chi_q\left(g^i+1\right)\right), & i\in R\end{cases}\tag{2}$$

其中 $\log_w(\cdot)$ 是定义在 $\mathbb{Z}_d$ 上以 w 为底数的离散对数函数。

通过改变 P 和 Q 对应下标集的序列元素的值， 文献[15]构造了一类新的二元 Legendre-Sidelnikov 序列。

令 $P_0=\{mp:m=0,2,\cdots,q-3\}$， $P_1=\{mp:m=1,3,\cdots,q-2\}$; $Q_0=\left\{n(q-1)+\frac{q-1}{2}:n\in\mathbb{Z}_p,\chi_p(2n+1)=1\right\}$，$Q_1=\left\{n(q-1)+\frac{q-1}{2}:n\in\mathbb{Z}_p,\ \chi_p(2n+1)=-1\right\}$。则一类周期为 $p(q-1)$ 的二元 Legendre-Sidelnikov 序列 $S=\{s_i\}$ 定义为

$$s_i=\begin{cases}0, & i\in P_0\cup Q_1\\ 1, & i\in P_1\cup Q_0\\ \frac{1}{2}\cdot\left(1-\left(\frac{i}{p}\right)\eta\left(g^i+1\right)\right), & i\in R\end{cases}\tag{3}$$

令 $S=(s_i)$ 是周期为 N 的二元序列。则该序列的周期自相关函数定义为

$$R_s(l)=\sum_{i=0}^{N-1}(-1)^{s_i+s_{i+l}},\quad 0\le l<N$$

下面我们给出一些引理， 这些引理将在正文的证明中被多次用到。

引理 1 令 p 为奇素数， q 为奇素数的幂次且 $\gcd(p,q-1)=1$， g 是 $\mathbb{F}_q$ 的本原元， η 是 $\mathbb{F}_q$ 上的二次特征。 P 和 Q^* 的定义同上, 则

(1)对任意的 l， $l\not\equiv 0\ (\bmod p)$，有

$$\sum_{i\in Q^*}\left(\frac{i}{p}\right)\cdot\left(\frac{i+l}{p}\right)=-1$$

(2)对任意的 l, $l\not\equiv 0(\bmod q-1)$ ，有

$$\sum_{i\in P}\eta\left(g^i+1\right)\eta\left(g^{i+l}+1\right)=-1-\eta\left(g^l\right)$$

(3) $\sum_{i\in P}\eta\left(-g^i+1\right)\eta\left(g^i+1\right)=-1-\eta\left(g^{-l}\right)$。

证明 对于任意的 $a\in\mathbb{F}_q^*$，易知： $\sum_{x\in F_q}\eta(x)\cdot\eta(x+a)=-1$。该结果可参看文献[17]。通过 Q^* 的定义

以及限制条件 $\gcd(p,q-1)=1$，不难发现 $Q^*(\bmod p)=\mathbb{F}_p^*$。由于 $\left(\frac{0}{p}\right)=0$，我们有

$$\sum_{i\in Q^*}\left(\frac{i}{p}\right)\left(\frac{i+l}{p}\right)=\sum_{i\in\mathbb{F}_p^*}\left(\frac{i}{p}\right)\left(\frac{i+l}{p}\right)=-1$$

因此，引理中的第 1 个等式成立。

对于第 2 个等式，我们有

$$\begin{aligned}\sum_{i\in P}&\eta\left(g^i+1\right)\eta\left(g^{i+l}+1\right)\\&=\eta\left(g^l\right)\sum_{i\in\mathbb{Z}_{q-1}}\eta\left(g^i+1\right)\eta\left(g^i+1-1+g^{-l}\right)\\&=\eta\left(g^l\right)\left(\sum_{x\in\mathbb{F}_q}\eta(x)\eta\left(x+g^{-l}-1\right)-\eta\left(g^{-l}\right)\right)\\&=-1-\eta\left(g^l\right)\end{aligned}$$

其中，第 1 个等式成立是因为 $P(\bmod q-1)=\mathbb{Z}_{q-1}$。同时，由于 $\{g^i+1:0\le i\le q-2\}=\mathbb{F}_q\setminus\{1\}$，所以第 2 个等式成立。由于 $l\not\equiv 0(\bmod q-1)$，$g^{-l}-1\ne 0$。最后，第 3 个等式由证明开始时提到的结论可得到。

证毕

3　推广的二元 Legendre-Sidelnikov 序列的周期自相关分布

利用上文已给定的符号，文献[14]推广的二元 Legendre-Sidelnikov 序列 $S=(s_i)$ 可以等价地定义为

$$s_i=\begin{cases}0, & i=n/2\\(1/2)\cdot\left(1-\eta\left(g^i+1\right)\right), & i\in P\setminus\{n/2\}\\(1/2)\cdot\left(1-(i/p)\right), & i\in Q^*\\(1/2)\cdot\left(1-(i/p)\eta\left(g^i+1\right)\right), & i\in R\end{cases}\tag{4}$$

平衡性是 Golomb 3 条随机性假设之一，即对于一个周期为偶数的二元序列，序列中 0 与 1 的个数是相同的[1]。注意到，在文献[14]亦指出了广义 Legendre-Sidelnikov 序列是平衡性的，但没有给出证明。为完整起见，下面给出一个简要的证明。

定理 1　式(4)定义的推广的二元 Legendre-Sidelnikov 序列是平衡的。

证明　对于周期为 n 的二元序列 (s_i)，易知 (s_i) 是平衡的当且仅当 $\sum_{i=0}^{n-1}(-1)^{s_i}=0$。由序列的定义知

$$(-1)^{s_i}=\begin{cases}1, & i=n/2\\\eta\left(g^i+1\right), & i\in P\setminus\{n/2\}\\(i/p), & i\in Q^*\\(i/p)\eta\left(g^i+1\right), & i\in R\end{cases}$$

那么，

$$\begin{aligned}\sum_{i=0}^{n-1}(-1)^{s_i}&=1+\sum_{i\in P\setminus\frac{n}{2}}\eta\left(g^i+1\right)\\&\quad+\sum_{i\in Q^*}\left(\frac{i}{p}\right)+\sum_{i\in R}\left(\frac{i}{p}\right)\eta\left(g^i+1\right)\end{aligned}$$

注意到，$P(\bmod q)=\mathbb{Z}_{q-1}$ 与 $Q^*(\bmod p)=\mathbb{F}_p^*$。由于 $g^{n/2}=-1$ 和 $\eta(0)=0$，我们有

$$\sum_{i\in P\setminus\frac{n}{2}}\eta\left(g^i+1\right)=\sum_{j=0}^{q-2}\eta\left(g^j+1\right)=-\eta(1)=-1$$

$$\sum_{i\in Q^*}\left(\frac{i}{p}\right)=\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)=0$$

进一步地，由中国剩余定理可知

$$\sum_{i\in R}\left(\frac{i}{p}\right)\eta\left(g^i+1\right)=\sum_{i=0}^{p-1}\left(\frac{i}{p}\right)\sum_{i=0}^{q-2}\eta\left(g^i+1\right)=0$$

综上可得 $\sum_{i=0}^{n-1}(-1)^{s_i}=0$。　　证毕

定理 2　式(4)定义的推广的二元 Legendre-Sidelnikov 序列的周期自相关函数分布为

$$R_s(l)=\begin{cases}p\left(\eta\left(-g^l+1\right)+\eta\left(-g^{-l}+1\right)-(-1)^l-1\right), & l\in P\\\left(\left(\frac{l}{p}\right)+\left(-\frac{l}{p}\right)-1\right)\left(2(-1)^{\frac{q^2-1}{8}}-(-1)^l-1\right), & l\in Q^*\\(q-1)\left(\left(\frac{l}{p}\right)+\left(-\frac{l}{p}\right)-1\right), & (q-1)\mid l\\\left(\left(\frac{l}{p}\right)+\left(-\frac{l}{p}\right)-1\right)\left(\eta\left(-g^l+1\right)\right.\\\quad\left.+\eta\left(-g^{-l}+1\right)-(-1)^l-1\right), & \text{其它}\end{cases}$$

证明　根据 l，$0<l<p(q-1)$ 属于 $P\setminus\{0\}$，Q^* 或 R，证明可分为如下 3 部分。

(1)若 $l\in P\setminus\{0\}$，则

$$(-1)^{s_i+s_{i+l}}=\begin{cases}\eta\left(-g^l+1\right), & i=n/2\\\eta\left(-g^l+1\right), & i+l=n/2\\\eta\left(g^i+1\right)\eta\left(g^{i+l}+1\right), & i\in P\setminus\{n/2\},\\ & i+l\in P\setminus\{n/2\}\\\eta\left(-g^l+1\right), & i\in Q^*\\\eta\left(-g^l+1\right), & i\in R, i+l\in Q^*\\\eta\left(g^i+1\right)\eta\left(g^{i+l}+1\right), & i\in R, i+l\in R\end{cases}$$

进一步地，由引理 1 可知

$$\sum_{i\in P\setminus\left\{\frac{n}{2}\right\},i+l\in P\setminus\left\{\frac{n}{2}\right\}}\eta\left(g^i+1\right)\eta\left(g^{i+l}+1\right)$$
$$=\sum_{i\in P}\eta\left(g^i+1\right)\eta\left(g^{i+l}+1\right)=-1-\eta\left(g^l\right)$$

同理， 我们有

$$\sum_{i\in R,i+l\in Q^*}\eta\left(-g^{-l}+1\right)=\sum_{i+l\in Q^*}\eta\left(-g^{-l}+1\right)$$
$$=(p-1)\eta\left(-g^{-l}+1\right)$$

$$(-1)^{s_i+s_{i+l}}=\begin{cases}\left(\dfrac{l}{p}\right)\eta(2), & i=0\\ \left(\dfrac{l}{p}\right)\eta(2), & i=\dfrac{n}{2}\\ \left(\dfrac{l}{p}\right)\eta(-g^i+1)\eta(g^i+1), & i\in P\setminus\left\{0,\dfrac{n}{2}\right\}\\ \left(-\dfrac{l}{p}\right)\eta(2), & i\in Q^*,\ i+l\in P\setminus\left\{\dfrac{n}{2}\right\}\\ \left(\dfrac{i}{p}\right)\left(\dfrac{i+l}{p}\right)\eta(2), & i\in Q^*,\ i+l\in R\\ \left(-\dfrac{l}{p}\right)\eta(2), & i\in R,\ i+l=\dfrac{n}{2}\\ \left(-\dfrac{l}{p}\right)\eta\left(-g^i+1\right)\eta\left(g^i+1\right), & i\in R,\ i+l\in P\setminus\left\{\dfrac{n}{2}\right\}\\ \left(\dfrac{i}{p}\right)\left(\dfrac{i+l}{p}\right)\eta(2), & i\in R,\ i+l\in Q^*\\ \left(\dfrac{i}{p}\right)\left(\dfrac{i+l}{p}\right)\eta\left(g^i+1\right)\eta\left(g^{i+l}+1\right), & i\in R,\ i+l\in R\end{cases}$$

对于 $i\in P\setminus\{0,n/2\}$ 这种情形，由引理 1 可知：

$$\sum_{i\in P\setminus\left\{0,\frac{n}{2}\right\}}\left(\frac{l}{p}\right)\eta\left(-g^i+1\right)\eta\left(g^i+1\right)$$
$$=\left(\frac{l}{p}\right)\sum_{i\in P}\eta\left(g^i+1\right)\eta\left(g^{i+\frac{n}{2}}+1\right)$$
$$=-\left(\frac{l}{p}\right)(1+\eta(-1))$$

同理，由引理 1 得

$$\sum_{i\in Q^*,i+l\in R}\left(\frac{i}{p}\right)\left(\frac{i+l}{p}\right)\eta(2)=-\eta(2),$$

$$\sum_{i\in R,i+l\in P\setminus\left\{\frac{n}{2}\right\}}\left(-\frac{l}{p}\right)\eta(-g^i+1)\eta(g^i+1)$$
$$=-\left(-\frac{l}{p}\right)(1+\eta(-1))$$

$$\sum_{i\in R,i+l\in R}\eta\left(g^i+1\right)\eta\left(g^{i+l}+1\right)$$
$$=\sum_{i=0}^{n-1}\eta\left(g^i+1\right)\eta\left(g^{i+l}+1\right)\sum_{i\in P}\eta\left(g^i+1\right)\eta\left(g^{i+l}+1\right)$$
$$=(p-1)\sum_{j=0}^{q-2}\eta\left(g^j+1\right)\eta\left(g^{j+l}+1\right)$$
$$=-(p-1)\left(1+\eta\left(g^l\right)\right)$$

所以 $R_s(l)=p(\eta(-g^l+1)+\eta(-g^{-l}+1)-\eta(g^l)-1)$。

(2)若 $l\in Q^*$， 则

$$\sum_{i\in R,i+l\in Q^*}\left(\frac{i}{p}\right)\left(\frac{i+l}{p}\right)\eta(2)=-\eta(2)$$

最后，

$$\sum_{i\in R,i+l\in R}\left(\frac{i}{p}\right)\left(\frac{i+l}{p}\right)\eta\left(g^i+1\right)\eta\left(g^{i+l}+1\right)$$
$$=\sum_{i=0}^{n-1}\left(\frac{i}{p}\right)\left(\frac{i+l}{p}\right)\eta\left(g^i+1\right)\eta\left(g^{i+l}+1\right)$$
$$=\sum_{i=0}^{p-1}\left(\frac{i}{p}\right)\left(\frac{i+l}{p}\right)\sum_{i=0}^{q-2}\eta\left(g^i+1\right)\eta\left(g^{i+l}+1\right)$$
$$=1+\eta\left(g^l\right)=1+\eta(-1)$$

综上可得，$R_s(l)=\left(\left(\dfrac{l}{p}\right)+\left(-\dfrac{l}{p}\right)-1\right)(2\eta(2)-\eta(-1)-1)$。

由于 $\eta(2)=(-1)^{\frac{q^2-1}{8}}$ (参看文献[16])，故结论成立。

(3)若 $l\in R$， 则

$$(-1)^{s_i+s_{i+l}}=\begin{cases}\left(\dfrac{l}{p}\right), & i=\dfrac{n}{2},\ \ i+l\in Q^*\\ \left(\dfrac{l}{p}\right)\eta\left(-g^l+1\right), & i=\dfrac{n}{2},\ \ i+l\in R\\ \left(\dfrac{l}{p}\right)\eta\left(-g^{-l}+1\right), & i\in P\setminus\left\{\dfrac{n}{2}\right\},\ i+l\in Q^*\\ \left(\dfrac{l}{p}\right)\eta\left(g^i+1\right)\eta\left(g^{i+l}+1\right), & i\in P\setminus\left\{\dfrac{n}{2}\right\},\ \ i+l\in R\\ \left(-\dfrac{l}{p}\right), & i\in Q^*,\ \ i+l=\dfrac{n}{2}\\ \left(-\dfrac{l}{p}\right)\eta\left(-g^l+1\right), & i\in Q^*,\ \ i+l\in P\setminus\left\{\dfrac{n}{2}\right\}\\ \left(\dfrac{i}{p}\right)\left(\dfrac{i+l}{p}\right), & i\in Q^*,\ \ i+l\in Q^*\\ \left(\dfrac{i}{p}\right)\left(\dfrac{i+l}{p}\right)\eta\left(-g^l+1\right), & i\in Q^*,\ \ i+l\in R\\ \left(-\dfrac{l}{p}\right)\eta\left(-g^{-l}+1\right), & i\in R,\ \ i+l=\dfrac{n}{2}\\ \left(-\dfrac{l}{p}\right)\eta\left(g^i+1\right)\eta\left(g^{i+l}+1\right), & i\in R,\ \ i+l\in P\setminus\left\{\dfrac{n}{2}\right\}\\ \left(\dfrac{i}{p}\right)\left(\dfrac{i+l}{p}\right)\eta\left(-g^{-l}+1\right), & i\in R,\ \ i+l\in Q^*\\ \left(\dfrac{i}{p}\right)\left(\dfrac{i+l}{p}\right)\eta\left(g^i+1\right)\eta\left(g^{i+l}+1\right), & i\in R,\ \ i+l\in R\end{cases}$$

由于 $\gcd(p,q-1)=1$，由中国剩余定理可知，存在唯一的 $i,0\le i<n$ 同时满足 $i\in P$ 且 $i+l\in Q^*$。同理，存在唯一的 i 使得 $i\in Q^*$ 且 $i+l\in P$。$i=\dfrac{n}{2},i+l\in Q^*$，$i\in Q^*$ 且 $i+l\in Q^*$ 与 $i\in Q^*$ 且 $i+l=\dfrac{n}{2}$ 这 3 类情形只在 $l\equiv 0(\bmod q-1)$ 时出现。当 $l\equiv 0 \pmod{q-1}$ 时，还有 $i\in P\setminus\{n/2\}$ 且 $i+l\in R$，$i\in R\setminus\{n/2\}$ 且 $i+l\in P$ 和 $i\in R\setminus\{n/2\}$ 且 $i+l\in R$ 这 3 类情形。

通过上述分析及引理 1，我们有

$$\begin{aligned}&\sum_{i\in P\setminus\left\{\frac{n}{2}\right\},i+l\in R}\left(\frac{l}{p}\right)\eta\left(g^i+1\right)\eta\left(g^{i+l}+1\right)\\&=\left(\frac{l}{p}\right)\sum_{i\in P}\eta(g^i+1)\eta\left(g^{i+l}+1\right)\\&=\begin{cases}(q-2)\left(\dfrac{l}{p}\right), & l\equiv 0 \pmod{q-1}\\ -\left(\dfrac{l}{p}\right)\left(1+\eta\left(g^l\right)\right), & \text{其它}\end{cases}\end{aligned}$$

$$\begin{aligned}&\sum_{i\in R,i+l\in R}\left(\frac{i}{p}\right)\left(\frac{i+l}{p}\right)\eta\left(g^i+1\right)\eta\left(g^{i+l}+1\right)\\&=\sum_{i=0}^{n-1}\left(\frac{i}{p}\right)\left(\frac{i+l}{p}\right)\eta\left(g^i+1\right)\eta\left(g^{i+l}+1\right)\\&=\sum_{i=0}^{n-1}\left(\frac{i}{p}\right)\left(\frac{i+l}{p}\right)\eta\left(g^i+1\right)\eta\left(g^{i+l}+1\right)\\&=\sum_{i=0}^{p-1}\left(\frac{i}{p}\right)\left(\frac{i+l}{p}\right)\sum_{i=0}^{q-2}\eta\left(g^i+1\right)\eta\left(g^{i+l}+1\right)\\&=\begin{cases}2-q, & l\equiv 0 \pmod{q-1}\\ 1+\eta(g^l), & \text{其它}\end{cases}\end{aligned}$$

同理可得其余情形的结果，因此，如果 $l\equiv 0(\bmod q-1)$，那么 $R_s(l)=(q-1)\left(\left(\dfrac{l}{p}\right)+\left(-\dfrac{l}{p}\right)-1\right)$，否则 $R_s(l)=\left(\left(\dfrac{l}{p}\right)+\left(-\dfrac{l}{p}\right)-1\right)(\eta(-g^l+1)+\eta(-g^{-l}+1)-\eta(g^l)-1)$。综上可知结论成立。　　证毕

推论 1　式(4)定义的推广的二元 Legendre-Sidelnikov 序列的自相关函数的一个上界为 $\max\{4p,3(q-1),12\}$。

证明　由定理 2 我们不难发现，当 $l\in P$ 或 $l\equiv 0(\bmod q-1)$ 时，序列的周期相关分别是 p，$q-1$ 的倍数，且分别不超过 $4p$，$3(q-1)$。而在其余的情

形下，周期自相关都不超过 12。 证毕

注 1 通过比较式(1)，式(3)和式(4)定义的序列的周期自相关函数的分布，不难发现在移位 $l \in \mathbb{Z}_n^*$ 时，三者的周期自相关差别都不大。当选取不同的 p ,q 时，在移位 $l \in P$ 或 $l \equiv 0 (\mathrm{mod}\, q-1)$ 时产生了较大的区别。具体地，在 $q \equiv 3 (\mathrm{mod}\, 4)$ 且移位 $l \in P$ 时，式(1)，式(3)和式(4)定义的序列的自相关函数的分布分别为

$$\begin{cases} q-1, & l\text{为奇数} \\ q-2p+1, & l\text{为偶数} \end{cases}$$

$$\begin{cases} 1-q+2(p-1)\left(\dfrac{\frac{1}{2}(q-1)}{p}\right)\eta\left(-g^l+1\right), & l\text{为奇数} \\ q-2p+1, & l\text{为偶数} \end{cases}$$

$$\begin{cases} 2p\eta\left(-g^l+1\right), & l\text{为奇数} \\ -2p, & l\text{为偶数} \end{cases}$$

在 $q \equiv 1 (\mathrm{mod}\, 4)$ 且移位 $l \in P$ 时，式(1)，式(3)和式(4)定义的序列的自相关函数的分布分别为

$$\begin{cases} q-1, & l\text{为奇数} \\ q-2p+1, & l\text{为偶数} \end{cases}$$

$$\begin{cases} 1-q, & l\text{为奇数} \\ q-2p+1+2(p-1)\left(\dfrac{\frac{q-1}{2}}{p}\right)\eta(-g^l+1), & l\text{为偶数} \end{cases}$$

$$\begin{cases} 0, & l\text{为奇数} \\ 2p(\eta(-g^l+1)-1), & l\text{为偶数} \end{cases}$$

在 $p \equiv 3 (\mathrm{mod}\, 4)$ 且移位 $l \equiv 0 (\mathrm{mod}\, q-1)$ 时， 式(1)，式(3)和式(4)定义的序列的自相关函数的分布分别为 $p-q-2$，$1-q$ 与 $1-q$ 。

在 $p \equiv 1 (\mathrm{mod}\, 4)$ 且移位 $l \equiv 0 (\mathrm{mod}\, q-1)$ 时，式(1)，式(3)和式(4)定义的序列的自相关函数的分布分别为 $p-q-2+2(l/p)$，$1-q$ 与 $(q-1)(2(l/p)-1)$ 。

因此， 在 $p \equiv 3 (\mathrm{mod}\, 4)$，$q >> p$ 时，式(4)对应的序列的自相关性质比较好。而 p 和 q 相差不大时，式(1)对应的序列的自相关性质比较好。

例 1 令 $p=3$，$q=23$，式(1)，式(3)和式(4)定义的序列分别如下：

[1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1,0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1,1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0];

[1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1,0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1,1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0];

[0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1,0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1,1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0];

对应地，它们的周期自相关分布如下：

[−2, −2, 22, 2, −2, 18, −2, 2, 22, 2, −2, 18, −2, −2, 22, 2, −2, 18, −2, 2, 22, −22, −2, 18, −2, −2, 22, −2, −2, 18, −2, −2, 22, −2, −2, 18, −2, −2, 22, −2, −2,18, −2, −22, 22, 2, −2, 18, −2, 2, 22, −2, −2, 18, −2, 2, 22, 2, −2, 18, −2, 2,22, −2, −2];

[−2, 2, −18, 2, 2, 18, −2, 2, −26, 2, 2, 18, 2, 2, −18, 2, 2, 18, −2, 2, −18, −22, −2, 18, −2, 2, −26, 2, −2, 18, 2, 2, −26, 2, 2, 18, −2, 2, −26, 2, −2, 18, −2, −22, −18, 2, −2, 18, 2, 2, −18, 2, 2, 18, 2, 2, −26, 2, −2, 18, 2, 2, −18,2, −2];

[2, 2, −6, 2, −2, −6, 2, 2, 6, 2, −2, −6, −2, 2, −6, 2, −2, −6, 2, 2, −6, −22,2, −6, 2, 2, 6, 2, 2, −6, −2, 2, 6, 2, −2, −6, 2, 2, 6, 2, 2, −6, 2, −22, −6, 2,2, −6, −2, 2, −6, 2, −2, −6, −2, 2, 6, 2, 2, −6, −2, 2, −6, 2, 2]。

4 结束语

对于任意的奇素数 p 和奇素数的幂次 q 且 $\gcd(p, q-1)=1$，由于 Ledendre-Sidelnikov 序列在支撑集为 P 与 Q^* 时取值总是固定的，所以它仅在 $p=q$ 时是平衡的。而推广的 Ledendre-Sidelnikov 序列在该部分是利用二次剩余来赋值。因此，推广的 Ledendre-Sidelnikov 序列总是平衡的，同时具有更好的的伪随机性质。本文给出了推广的二元 Legendre-Sidelnikov 序列自相关函数的分布。由结果可以看出，当 $p \equiv 3 (\mathrm{mod}\, 4)$，$q >> p$ 时，推广后的序列与原来的相比有更优的周期自相关函数的分布。

参 考 文 献

[1] GOLOMB G and GONG G. Signal Designs with Good Correlations: Forwireless Communications, Cryptography and Radar Applications[M]. Cambridge, U.K.: Cambridge University Press, 2005: 174–175.

[2] ARASU K T, DING C, HELLESETH T, *et al.* Almost difference sets and their sequences with optimal autocorrelation[J]. *IEEE Transactions on Information Theory*, 2001, 47(7): 2934–2943.

[3] 陈晓玉, 许成谦, 李玉博. 新的完备高斯整数序列的构造方法[J]. 电子与信息学报, 2014, 36(9): 2081–2085. doi: 10.3724/SP.

J.1146.2103.01697.

CHEN Xiaoyu, XU Chengqian, and LI Yubo. New constructions of perfect Gaussian integer sequences[J]. *Journal of Electronics & Information Technology*, 2014, 36 (9): 2081–2085. doi: 10.3724/SP.J.1146.2103.01697.

[4] 李瑞芳, 柯品惠. 一类新的周期为 $2pq$ 的二元广义分圆序列的线性复杂度[J]. 电子与信息学报, 2014, 36(3): 650–654. doi: 10.3724/SP.J.1146.2103.00751.

LI Ruifang and KE Pinhui. The linear complexity of a new class of generalized cyclotomic sequence with period $2pq$[J]. *Journal of Electronics & Information Technology*, 2014, 36 (3): 650–654. doi: 10.3724/SP.J.1146.2103.00751.

[5] DING C, HELLESETH T, and SAN W. On the linear complexity of Legendre sequences[J]. *IEEE Transactions on Information Theory*, 1998, 44(3): 1276–1278.

[6] DING C. Pattern distributions of Legendre sequences[J]. *IEEE Transactions on Information Theory*, 1998, 44(4): 1693–1698.

[7] SIDELNIKOV V M. Some k-valued pseudo-random sequences and nearly equidistant codes[J]. *Problems of Information Transmission*, 1969, 5(1): 12–16.

[8] 岳婴, 高军涛, 谢佳. 双素数 Sidel'nikov 序列的自相关函数[J]. 电子与信息学报, 2013, 35 (11): 2602–2607. doi: 10.3724/SP.J.1146.2103.00147.

YUE Zhao, GAO Juntao, and XIE Jia. Autocorrelation of the two-prime Sidel'nikov sequence[J]. *Jounal of Electronics & Information Technology*, 2013, 35(11): 2602–2607. doi: 10.3724/SP.J.1146.2103.00147.

[9] KIM Youngtae, SONG Minkyu, KIM Daesan, *et al*. Properties and crosscorrelation of decimated sidelnikov sequences[J]. *IEICE Transactions on Fundamentals*, 2014, 97-A(12): 2562–2566.

[10] KIM Youngtae, KIM Daesan, and SONG Hongyeop. New M-Ary sequence families with low correlation from the array structure of sidelnikov sequences[J]. *IEEE Transactions on Information Theory*, 2015, 61(1): 655–670.

[11] SU M and WINTERHOF A. Autocorrelation of Legendre-Sidelnikov sequences[J]. *IEEE Transactions on Information Theory*, 2010, 56(4): 1714–1718.

[12] SU M. On the linear complexity of Legendre-Sidelnikov sequences[J]. *Design Codes and Cryptography,* 2015, 74(3): 703–717.

[13] SU M and WINTERHOF A. Correlation measure of order k and linear complexity profile of legendre-sidelnikov sequences[C]. Proceedings of Fifth International Workshop on Signal Design and its Applications in Communications, Guilin, China, 2011: 6–8.

[14] SU M. ON the d-ary Generalized Legendre-Sidelnikov Sequence[J]. *LNCS*, 2012, 7280: 233–244.

[15] YAN T, LIU H, and SUN Y. Autocorrelation of modified Legendre-Sidelnikov sequences[J]. *IEICE Transactions on Fundamentals*, 2015, E98-A(2): 771–775.

[16] BURTON D M. Elementary Number Theory[M]. Maidenhead: UK, McGraw-Hill Education Press, 1998: 92–105.

[17] LIDL R and NIEDERREITER H. Finite Fields[M]. MA: Addision-Wesley, 1983: 217–225.

柯品惠：　男，1978 年生，副教授，主要研究方向为编码密码学.

叶智钒：　男，1991 年生，硕士生，研究方向为序列设计.

常祖领：　男，1976 年生，副教授，主要研究方向为编码密码学.