Autocorrelation of Legendre–Sidelnikov Sequences

Ming Su and Arne Winterhof

Abstract—We combine the concepts of the \(p\)-periodic Legendre sequence, the \((q-1)\)-periodic Sidelnikov sequence and the two-prime generator to introduce a new \(p/(q-1)\)-periodic sequence called Legendre–Sidelnikov sequence. We show that this new sequence is balanced if \(p \equiv q\). For an arbitrary odd prime \(p\) and an arbitrary power \(q\) of an odd prime with \(gcd(p, q-1) = 1\) we determine the exact values of its (periodic) autocorrelation function and deduce an upper bound on its aperiodic autocorrelation function showing that it is small compared to its period.

Index Terms—Autocorrelation, binary sequences, cryptography, finite fields, Legendre sequence, quadratic character (Legendre symbol), Sidelnikov sequence, two-prime generator, wireless communication.

I. INTRODUCTION

Let \(q\) be the power of an odd prime and \(g\) be a primitive element of the finite field \(\mathbb{F}_q\) of \(q\) elements. Then we recall that the quadratic character \(\eta\) of \(\mathbb{F}_q\) is defined by

\[\eta(g^i) = (-1)^i, \quad i \geq 0, \quad \text{and} \quad \eta(0) = 0.\]

If \(q = p\) is a prime it coincides with the Legendre symbol

\[\left(\frac{n}{p}\right) = \eta(n), \quad n \geq 0.\]

Several sequences with nice pseudorandomness properties in view of applications in wireless communication and cryptography have been defined using the quadratic character of a finite field, see the recent surveys [10], [11], the monograph [4] and references therein. Among these sequences are the Legendre sequence, the Sidelnikov sequence and the two-prime generator.

Here we introduce a new sequence combining the concepts of these three sequences:

Let \(p\) be an odd prime and \(q\) the power of an odd prime such that \(gcd(p, q-1) = 1\). Put \(n := p(q-1)\)

\[Q := \left\{\frac{q-1}{2}, q-1 + \frac{q-1}{2}, 2(q-1) + \frac{q-1}{2}, \ldots, \right.\]
\[\left. (p-1)(q-1) + \frac{q-1}{2}\right\},\]

and

\[P := \{0, p, 2p, \ldots, (q-2)p\}.\]

Note that \(P \cap Q = \{\frac{p}{2}\}\) and put \(Q^* := Q \setminus \{\frac{p}{2}\}\) and \(R := \{0, 1, 2, \ldots, n-1\} \setminus (P \cup Q^*)\).

We consider the \(n\)-periodic sequence \((s_i)\) over \(\mathbb{F}_2\) defined by

\[s_i = \begin{cases} 1, & \text{if } (i \mod n) \in P, \\ 0, & \text{if } (i \mod n) \in Q^*, \\ \frac{1-(\frac{i}{2})\eta(g^{i+1})}{2}, & \text{if } (i \mod n) \in R. \end{cases} \quad (1)

In Section II we provide a formula for the number of 1’s in a period of \((s_i)\) which shows that \((s_i)\) is balanced if \(p = q\).

For a \(T\)-periodic sequence \((a_i)\) over \(\mathbb{F}_2\) and \(1 \leq l < T\) the aperiodic autocorrelation function is given by

\[\text{AAC}(a_i, u, v, l) := \sum_{i=0}^{v} (-1)^{a_i+l+\alpha}, \quad 0 \leq u < v < T,\]

and the (periodic) autocorrelation function by

\[\text{AC}(a_i, l) := \sum_{i=0}^{T-1} (-1)^{a_i+l+\alpha}.\]

The aperiodic autocorrelation reflects local randomness and the (periodic) autocorrelation global randomness. If \((a_i)\) is a random sequence then \[\text{AAC}(a_i, u, v, l)\] and \[\text{AC}(a_i, l)\] can be expected to be small compared to \(T\). For the autocorrelation functions of Legendre sequence, Sidelnikov sequence and two-prime generator see [1], [4], [9], [10] and references therein.

In this paper, we determine the exact values of the periodic autocorrelation function of the sequence \((s_i)\) defined by (1) in Section III and an upper bound on the maximum absolute value of the aperiodic autocorrelation function in Section IV.

In [7] the correlation measure of order 2 of a finite binary sequence \((s_i)\) of length \(n\) is defined as

\[C_2(s_i) = \max_{M,D} \left|\sum_{i=0}^{M-1} (-1)^{s_i+d_1} (-1)^{s_i+d_2}\right|\]

where the maximum is taken over all \(D = (d_1, d_2)\) and \(M\) such that \(0 \leq d_1 < d_2 \leq n - M\). If \((s_i)\) is periodically continued with period \(n\) the correlation measure of order 2 can be bounded by the maximum of the aperiodic autocorrelation function. It was proved in [2] that for a truly random binary sequence of length \(n\) the correlation measure \(C_2(s_i)\) is “small”. More precisely, the order of magnitude of \(C_2(s_i)\) is \(n^{1/2} (\log n)^c\). Thus, a sequence \((s_i)\) can be considered as a “good” pseudorandom sequence if \(C_2(s_i)\) is small and is ideally greater than \(n^{1/2}\) only by at most a power of \(\log n\). For the Legendre–Sidelnikov this...
is true by our bound on the aperiodic autocorrelation if $p$ and $q$
are of the same size.

II. Balancedness

In this section, we show that $(s_i)$ is balanced for $p = q$.

**Theorem 1:** The number of 1s in the sequence $(s_i)$ defined by (1) is

$$N_1 = \frac{p(q-1) + q - p}{2}.$$ 

**Proof:** We have

$$N_1 = \sum_{i=0}^{\frac{p(q-1)-1}{2}} s_i = (q-1) + \sum_{i \in R} 1 - \left(\frac{i}{p}\right) \eta(g^i + 1)$$

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

By the Chinese Remainder Theorem, and the identity

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

we have

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

and the result follows.

III. Periodic Autocorrelation

In this section, we calculate the periodic autocorrelation function of the sequence $(s_i)$ defined by (1).

**Theorem 2:** The autocorrelation function of $(s_i)$ is given by the equation shown at the bottom of the page.

**Proof:** From (1) we deduce

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

If $l \in P \setminus \{0\}$ then we have

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

So we get

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

$$+ \eta(-g^{i+l} + 1) \sum_{i \in R} \eta(g^i + 1) \eta(g^{i+l} + 1).$$

Note that

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

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

and

$$\sum_{i \in R, i+l \in R} \eta(g^i + 1) \eta(g^{i+l} + 1)$$

$$= \sum_{i=0}^{p-1} \eta(g^i + 1) \eta(g^{i+l} + 1) - \sum_{i \in P} \eta(g^i + 1) \eta(g^{i+l} + 1)$$

$$= p \sum_{j=0}^{q-2} \eta(g^j + 1) \eta(g^{j+l} + 1)$$

$$- \sum_{j=0}^{q-2} \eta(g^j + 1) \eta(g^{j+l} + 1)$$

$$= -p - 1 \eta(g^j + 1) + 1 = -(p - 1)(\eta(g^j + 1) + 1)$$

$$= -(p - 1)(\eta(g^j + 1) + 1)$$

$$= -(p - 1)((-1)^l + 1)$$

$$= -(p - 1)((-1)^l + 1)$$

$$= AC(s_i, l) = \begin{cases} q - 1 - (p - 1)((-1)^l + 1), & l \in P \setminus \{0\} \\ (-1)^{(l-1)/2} - 1 + \frac{1 - (-1)q^{-l}}{2} \left(\frac{i}{p}\right) \left(1 + (-1)^{\frac{l-1}{2}}\right), & l \in Q^* \\ p - q - 2 + (1 - (-1)(p-1)/2) \left(\frac{i}{p}\right), & l \in R, q - 1 \neq l \\ (-1)^l - 1 + \left(\frac{i}{p}\right) \left(1 + (-1)q^{-l/2} - \eta(-g^i + 1)(1 + (-1)g^{-l/2+q^{-l/2+l}})\right), & l \in R, q - 1 \neq l. \end{cases}$$
where we used
\[ \sum_{x \in F_q} \eta(x)\eta(x + a) = -1, \quad a \in F_q^* \]
see, e.g., [6, Lemma 7.3.7]. By (2), (3), (4) and (5), for \( l \in P \) we have
\[ AC(s_i, l) = q - 1 - (p - 1)(((q - 1)^l + 1). \]
If \( l \in Q^* \) then we have
\[
(-1)^{s_i + s_i + l} = \begin{cases} 
-1, & i = 0 \\
-\left( \frac{l}{p} \right) \eta(-g^l + 1), & i \in P \setminus \{0\}, \\
-\left( \frac{p}{p} \right) \eta(2), & i \in Q^* \\
-\left( \frac{i}{p} \right) \eta(g^i + 1), & i \in P, i + l \in P \\
-\left( \frac{i}{p} \right) \eta(g^i + 1), & i \in Q^*, i + l \in P \\
\left( \frac{i}{p} \right) \eta(g^i + 1), & i \in Q^*, i + l \in Q^* \\
\left( \frac{i}{p} \right) \eta(g^i + 1), & i \in R, i + l \in P \\
\left( \frac{i}{p} \right) \eta(g^i + 1), & i \in R, i + l \in Q^* \\
\left( \frac{i}{p} \right) \eta(g^i + 1), & i \in R, i + l \in R.
\end{cases}
\]
Therefore, we have
\[ AC(s_i, l) = -1 - \left( \frac{l}{p} \right) \sum_{i \in P} \eta(-g^i + 1) \]
\[ + \eta(2) \sum_{i \in Q^*} \left( \frac{i + l}{p} \right) - 1 \]
\[ - \left( \frac{-l}{p} \right) \sum_{i \in R} \eta(g^i + 1) \]
\[ + \eta(2) \sum_{i \in R} \left( \frac{i}{p} \right) \]
\[ + \sum_{i \in Q^*} \left( \frac{i}{p} \right) \left( \frac{i + l}{p} \right) \eta(g^i + 1)\eta(g^{i+l} + 1) \]
\[ = -1 + \left( \frac{l}{p} \right) - \eta(2) \left( \frac{l}{p} \right) - 1 \]
\[ + \left( \frac{-l}{p} \right) - \eta(2) \left( \frac{-l}{p} \right) \]
\[ + \sum_{i = 1}^{q-1} \left( \frac{i}{p} \right) \left( \frac{i + l}{p} \right) \eta(g^i + 1)\eta(g^{i+l} + 1). \]
By the Chinese Remainder Theorem the last sum equals
\[ \left( \sum_{i = 0}^{p-1} \left( \frac{i}{p} \right) \left( \frac{i + l}{p} \right) \right) \left( \sum_{i = 0}^{q-2} \eta(g^i + 1)\eta(g^{i+l} + 1) \right) \]
\[ = (-1)(-\eta(g^l) - 1) \]
\[ = (-1)(q-1)^l + 1 \]
and for \( l \in Q^* \) we have
\[ AC(s_i, l) = (-1)(q-1)^l + 1 \]
\[ + (1 - \eta(2)) \left( \frac{l}{p} \right) \left( 1 - (-1)(q-1)^l \right). \]
The result follows in this case since \( \eta(2) = (-1)(q^2-1)^{l/2} \), see e.g., [5, Proposition 5.1.3].
If \( l \in R \) then we have
\[
(-1)^{s_i + s_i + l} = \begin{cases} 
-1, & i \in P, i + l \in Q^* \\
-\left( \frac{l}{p} \right) \eta(-g^l + 1), & i \in Q^*, i + l \in P \\
\left( \frac{i}{p} \right) \eta(g^i + 1), & i \in R, i + l \in P \\
\left( \frac{i}{p} \right) \eta(g^i + 1), & i \in R, i + l \in Q^* \\
\left( \frac{i}{p} \right) \eta(g^i + 1), & i \in R, i + l \in R.
\end{cases}
\]
There is exactly one \( i \in P \) with \( i + l \in Q^* \) and one \( i \in Q^* \) with \( i + l \in P \) giving the contribution \(-2\) to the autocorrelation function. The case \( i \in Q^* \) with \( i + l \in Q^* \) occurs only if \( l \equiv 0 \mod (q-1) \) giving the contribution \( p-2 \) in this case. Next we calculate all remaining sums contributing to \( AC(s_i, l) \).
We have
\[ \left( \frac{l}{p} \right) \sum_{i = 0}^{q-2} \eta(g^i + 1) = \left( \frac{l}{p} \right) \sum_{i = 0}^{q-2} \eta(g^{i+l} + 1) \]
\[ \eta(-g^l + 1) \sum_{i = 0}^{q-2} \left( \frac{i + l}{p} \right) = -\eta(-g^l + 1) \left( \frac{l}{p} \right) \]
\[ - \left( \frac{-l}{p} \right) \sum_{i = 0}^{q-2} \eta(g^i + 1) = \left( \frac{-l}{p} \right) \]
\[ \eta(-g^l + 1) \sum_{i = 0}^{q-2} \left( \frac{i}{p} \right) = -\eta(-g^l + 1) \left( \frac{-l}{p} \right) \]
and
\[ \sum_{i = 0}^{q-2} \left( \frac{i}{p} \right) \eta(g^i + 1) \left( \frac{i + l}{p} \right) \eta(g^{i+l} + 1) \]
\[ = \left( \sum_{i = 0}^{q-2} \left( \frac{i}{p} \right) \left( \frac{i + l}{p} \right) \right) \left( \sum_{i = 0}^{q-2} \eta(g^i + 1)\eta(g^{i+l} + 1) \right) \]
\[ = \left\{ \begin{array}{ll} 
2 - q, & \text{if } l \equiv 0 \mod (q-1), \\
1 + \eta(g^l), & \text{if } l \not\equiv 0 \mod (q-1). 
\end{array} \right. \]
By (6)–(9) and (10), we get the result after simple calculations. □
A particularly interesting case is given if \( p = q \equiv 3 \mod 4 \).
Corollary 1: If \( p = q \equiv 3 \mod 4 \), we have
\[
AC(s_i, l) = \begin{cases} 
(-1)^{(1-p)} & \text{if } l \in P \setminus \{0\}, \\
\frac{2}{p} \left( \frac{q^2-1}{p} \right)^l & \text{if } l \in R, \ p - 1 \not\equiv 0 \mod (p-1), \ l \text{ is even}, \\
-2 & \text{otherwise}.
\end{cases}
\]
Moreover, for \( p > 3 \) and \( 1 \leq l \leq p(p-1) - 1 \), we get
\[
|l: AC(s_i, l) = 1 - p| = \frac{p-3}{2}, \\
|l: AC(s_i, l) = p - 1| = \frac{p-1}{2}, \\
|l: AC(s_i, l) = -2| = \frac{3p^2+1}{4} - p
\]
and
\[
|l: AC(s_i, l) = 2| = \frac{p^2+3}{4} - p.
\]

Proof: We focus on the number of \( 1 \leq l \leq p(p-1) - 1 \) with \( \left( \frac{q^2-1}{p} \right) = 1 \) for \( l \in R, \ l \not\equiv 0 \mod (p-1), \ l \text{ is even} \). First we have
\[
\left| \{ 1 \leq l \leq p(p-1) - 1 : \frac{p-1}{2} \not\equiv 0 \not\equiv \frac{3p^2+1}{4} \not\equiv \frac{p^2+3}{4} \not\equiv 0 \mod (p-1) \} \right| = \frac{(p-1)(p-3)}{2}. \quad (11)
\]

Note that the elements of \( l \in Q^* \) are odd. Then we have
\[
\sum_{l \in R, l \not\equiv 0 \mod (p-1)} \left( \frac{q^2-1}{p} \right)^l = \sum_{l = 0}^{p-1} \left( \frac{q^2-1}{p} \right)^l = \sum_{l = 0}^{p-1} \left( \frac{q^2-1}{p} \right)^l = 0. \quad (12)
\]
By (11) and (12), we get
\[
\left| l \in R, p - 1 \not\equiv 0 \not\equiv 0 \mod (p-1) \right| = \pm 1 = \frac{(p-1)(p-3)}{4}
\]
which immediately implies the distribution of the autocorrelation values of the sequence. \( \square \)

IV. APERIODIC AUTOCORRELATION

In this section, we prove the following upper bound for the aperiodic autocorrelation function.

Theorem 3: The aperiodic autocorrelation function of the sequence \( (s_i) \) defined by (1) satisfies
\[
AAC(s_i, u, v, l) = O(p^2 + p^{1/2}q^{1/2} \log pq)
\]
for \( 1 \leq l \leq n - 1 \).

Proof: If \( v - u = n - 1 \) then the result follows by Theorem 2 and we assume \( v - u = N - 1 < n - 1 \). Then we have
\[
AAC(s_i, u, v, l) = S + O(p + q)
\]
where
\[
S := \sum_{i=u}^{u+N-1} \left( \frac{i+i+l}{p} \right) \eta(g^i+1) \eta(g^{i+l}+1).
\]
For estimating \( S \) we have to distinguish three cases.
If \( l \equiv 0 \mod p, \ l \not\equiv 0 \), then we have
\[
S = \sum_{i=u}^{u+N-1} \eta(g^i+1) \eta(g^{i+l}+1) + O(q).
\]
Now if \( N = N_1(q-1) + N_0, \ 0 \leq N_0 < q - 1, \ 0 \leq N_1 < p \), then we have
\[
S = \sum_{i=u}^{u+N_1(q-1)-1} \eta(g^i+1) \eta(g^{i+l}+1) + O(q)
\]
\[
= N_1 \sum_{j=0}^{q^2} \eta(g^i+1) \eta(g^{i+l}+1) + O(q) = O(p + q).
\]
If \( l \equiv 0 \mod (q - 1), \ l \not\equiv 0 \), then we have
\[
S = \sum_{i=u}^{u+N_1(q-1)-1} \left( \frac{i+i+l}{p} \right) + O(p).
\]
Now if \( N = N_1p + N_0, \ 0 \leq N_0 < p, \ 0 \leq N_1 < q - 1 \), then we have
\[
S = \sum_{i=u}^{u+N_1(q-1)-1} \left( \frac{i+i+l}{p} \right) + O(p)
\]
\[
= N_1 \sum_{i=0}^{q^2} \left( \frac{i+i+l}{p} \right) + O(p)
\]
\[
= N_1 + O(p) = O(p + q).
\]
The last case is \( l \not\equiv 0 \mod (q - 1). \) Put \( e_n(x) = e^{2\pi i x/n} \). Then we have
\[
\sum_{a=0}^{n-1} e_n(ax) = \begin{cases} 
n & \text{if } x = 0, \\
0 & \text{if } x \neq 0.
\end{cases}
\]
Hence
\[
S = \frac{1}{n} \sum_{a=0}^{n-1} \sum_{i=0}^{n-1} \left( \frac{i+i+l}{p} \right) \eta(g^i+1) \eta(g^{i+l}+1) + \sum_{x=0}^{u+N-1} e_n(a(i-x)). \quad (13)
\]
Then we have
\[
|S| \leq \frac{N}{n} \sum_{i=0}^{n-1} \left| \left( \frac{i+i+l}{p} \right) \eta(g^i+1) \eta(g^{i+l}+1) \right| + \frac{1}{n} \Delta \Gamma. \quad (14)
\]
where

\[
\Delta := \max_{\alpha \neq 0} \left| \sum_{i=0}^{n-1} \left( \frac{i(i + L)}{p} \right) \eta(g^i + 1)\eta(g^{i+t} + 1)e_n(\alpha i) \right| \\
= \max_{\alpha \neq 0} \left( \sum_{i=0}^{n-1} \left( \frac{i(i + L)}{p} \right) e_p(\alpha \bar{x}) \right) \cdot \left( \sum_{i=0}^{n-1} \eta(g^i + 1)\eta(g^{i+t} + 1)e_{q-1}(\alpha \beta i) \right)
\]

where \( \alpha = (q - 1)^{-1} \mod p, \beta = p^{-1} \mod (q - 1), \) and

\[
\Gamma := \sum_{i=1}^{n-1} \sum_{x=0}^{l-N-1} e_n(-\alpha x) = O(n \log n) \tag{15}
\]

see e.g., [3, Th. 1]. By Weil’s theorem for hybrid character sums [8, Th. II.2G], we have

\[
\sum_{i=0}^{n-1} \left( \frac{i(i + L)}{p} \right) e_p(\alpha \bar{x}) = O(p^{1/2}). \tag{16}
\]

Verify that \( \varphi(g^x) = e_{q-1}(\alpha \beta x) \) is a multiplicative character of \( F_q \). Let \( s \) be the order of \( \varphi \) and put \( t = \log \alpha s, 2 \). Then we have

\[
\eta(g^i + 1)\eta(g^{i+t} + 1)e_{q-1}(\alpha \beta i) = \psi \left( g^i + 1\right)^{t/2} g^{i+t} + 1\right)^{t/2} g^{i+t/s} \]

with a multiplicative character \( \psi \) of order \( t \). Note that

\[
(X + 1)^{t/2}(g^t X + 1)^{t/2} X^{t/s}
\]

is not (up to a multiplicative constant) a \( t \)th power of a polynomial and we can apply Weil’s bound for multiplicative character sums [8, Th. II.2C’],

\[
\left| \sum_{i=0}^{n-1} \eta(g^i + 1)\eta(g^{i+t} + 1)e_{q-1}(\alpha \beta i) \right| = O(q^{1/2}) \tag{17}
\]

Furthermore, by the Chinese Remainder Theorem we get

\[
\left| \sum_{i=0}^{n-1} \left( \frac{i(i + L)}{p} \right) \eta(g^i + 1)\eta(g^{i+t} + 1) \right| \\
= \left| \sum_{i=0}^{n-1} \left( \frac{i(i + L)}{p} \right) \right| \cdot \left| \sum_{i=0}^{n-2} \eta(g^i + 1)\eta(g^{i+t} + 1) \right| \\
\leq 2^n. \tag{18}
\]

Therefore, combining (13), (14), (15), (16), (17) and (18), we get

\[
S = O(p^{1/2} q^{1/2} \log p q).
\]

**References**


**Ming Su** received the Bachelor degree in 1999 and the Ph.D. degree in mathematics in 2004, both from the College of Mathematics of Nankai University, China.

He took intern in Microsoft Research Asia from March 2002 to September 2002, and stayed in IBM China Research Lab from December 2003 to August 2004. From 2005 to 2007, he was in the College of Information Technical Science as a postdoctoral researcher. From February 2009 to July 2009, he stayed in RICAM, Austrian Academy of Sciences, Linz, Austria as an ÖAD scholar. Currently, he is with the Department of Computer Science, Nankai University. His main research interests include sequences and algorithm-related topics.

**Arne Winterhof** received the diploma in 1994 and the Ph.D. degree in mathematics in 1996, both from the Technical University of Braunschweig, Germany. In 2001, he received the postdoctoral lecture qualification (Habilitation) from the University of Vienna, Austria. He awarded the Hlawka Prize in 2004. In 2001 to 2002, he worked as research scientist at the Institute of Discrete Mathematics, Austrian Academy of Sciences, Vienna, Austria, and from 2002 to 2003 at Temasek Laboratories, National University of Singapore. Since 2003, he has been with the Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Linz, Austria. His main research interests include finite fields and their applications; in particular, cryptography and pseudorandom number generation.