On the linear complexity of Sidel'nikov Sequences over $\mathbb{F}_d$ *

Nina Brandstätter[1] and Wilfried Meidl[2]

[1] Johann Radon Institute for Computational and Applied Mathematics,
Austrian Academy of Sciences, Altenbergerstrasse 69,
4040 Linz, Austria
nina.brandstaetter@oeaw.ac.at
[2] Sabanci University, Orhanli, Tuzla,
34956 Istanbul, Turkey
wmeidl@sabanciuniv.edu

Abstract. We study the linear complexity of sequences over the prime field $\mathbb{F}_d$ introduced by Sidel'nikov. For several classes of period length we can show that these sequences have a large linear complexity. For the ternary case we present exact results on the linear complexity using well known results on cyclotomic numbers. Moreover, we prove a general lower bound on the linear complexity profile for all of these sequences. The obtained results extend known results on the binary case. Finally we present an upper bound on the aperiodic autocorrelation.

Keywords: Sidel'nikov sequence; Linear complexity; Linear complexity profile; Aperiodic autocorrelation

1 Introduction

For an odd prime power q let $\mathbb{F}_q$ be the finite field of order q and let d be a prime divisor of $q-1$. The *cyclotomic classes of order d* give a partition of $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$ defined by

$$D_0 := \{\alpha^{dn} \ : \ 0 \le n \le (q-1)/d - 1\} \quad \text{and} \quad D_j := \alpha^j D_0, \ 1 \le j \le d-1,$$

for a generating element α of $\mathbb{F}_q^*$.
In [14] Sidel'nikov introduced the $q-1$-periodic sequence $S = s_0, s_1, \ldots$ with terms in $\mathbb{F}_d$ defined by

$$\begin{aligned} s_n = j \quad &\Leftrightarrow \quad \alpha^n + 1 \in D_j, \quad n = 0, \ldots, q-2, n \ne (q-1)/2, \\ s_{(q-1)/2} &= 0, \quad \text{and} \\ s_{n+q-1} &= s_n, \quad n \ge 0. \end{aligned} \tag{1}$$

* The first author has been supported by the Austrian Science Fund (FWF) grant S83 and by the Austrian Academy of Sciences.

Independently in [9] Lempel, Cohn and Eastman studied the sequence (1) for $d = 2$.

The *linear complexity profile* of a sequence $S = s_0, s_1, \ldots$ over the field $\mathbb{F}_d$ is the function $L(S, N)$ defined for every positive integer N, as the least order L of a linear recurrence relation over $\mathbb{F}_d$

$$s_n = c_1 s_{n-1} + \ldots + c_L s_{n-L}, \tag{2}$$

for all $L \leq n \leq N-1$, which S satisfies. We use the convention that $L(S, N) = 0$ if the first N elements of S are all zero and $L(S, N) = N$ if the first $N-1$ elements of S are zero and $s_{N-1} \neq 0$. The value

$$L(S) = \sup_{N \geq 1} L(S, N)$$

is called the *linear complexity* of the sequence S. For the linear complexity of any periodic sequence of period t one easily verifies that $L(S) = L(S, 2t) \leq t$. Alternatively, the linear complexity of a periodic sequence with terms in $\mathbb{F}_d$ is the length of the shortest linear recurrence relation (2) the sequence satisfies for all $n \geq L$.

In Section 2 we recall some concepts and facts from the theory of linear recurring sequences over finite fields (see [10, Chapter 6] and [3]), and present a technique for determining the linear complexity of sequences of the form (1). Roughly speaking, we can determine the exact linear complexity whenever we know the value of certain cyclotomic numbers and the factorization of $X^{q-1} - 1$ over $\mathbb{F}_d$. Unconditionally we prove two results which yield good lower bounds on the linear complexity of sequences of the form (1) for several classes of period length. In Section 3 we use the results of Section 2 to obtain exact results on the linear complexity of the ternary Sidel'nikov sequence. In Section 4 we prove a general lower bound on the linear complexity profile. The results on the linear complexity and the linear complexity profile complement and extend results in previous works on the binary case by Helleseth and Yang [6], Kyureghyan and Pott [8], and Meidl and Winterhof [12]. Finally, in Section 5 we prove an upper bound on the aperiodic autocorrelation of the Sidel'nikov sequence which complements the results of [7] on the autocorrelation distribution.

2 Preliminaries

Let $S = s_0, s_1, \ldots$ be an N-periodic sequence over $\mathbb{F}_d$, then we can identify S with the polynomial $S(X) := s_0 + s_1 X + \ldots + s_{N-1} X^{N-1} \in \mathbb{F}_d[X]$ of degree at most $N-1$. The following well known lemma [3, Lemma 8.2.1] describes the computation of the linear complexity of a periodic sequence.

Lemma 1. *Let S be a sequence of period N over $\mathbb{F}_d$ and*

$$S(X) := s_0 + s_1 X + \ldots + s_{N-1} X^{N-1}.$$

Then the linear complexity of S is given by

$$N - \deg(\gcd(X^N - 1, S(X))).$$

If $N = d^s r$ with $\gcd(d, r) = 1$, then we have $X^N - 1 = (X^r - 1)^{d^s}$. Consequently, in order to calculate the linear complexity of S we are interested in the multiplicities of the rth roots of unity as roots of the polynomial $S(X)$. For the determination of the multiplicity of roots of the polynomial $S(X)$ we can employ the kth Hasse derivative (cf. [5]) $S(X)^{(k)}$ of $S(X)$, which is defined to be

$$S(X)^{(k)} = \sum_{n=k}^{N-1} \binom{n}{k} s_n X^{n-k}.$$

The multiplicity of ξ as root of $S(X)$ is v if $S(\xi) = S(\xi)^{(1)} = \ldots = S(\xi)^{(v-1)} = 0$ and $S(\xi)^{(v)} \neq 0$ (cf. [10, Lemma 6.51]).

In order to obtain results on the linear complexity of the sequence (1) we are interested in the Hasse derivatives of the polynomial $S(X)$ which corresponds to the sequence (1).

The binomial coefficients modulo d appearing in $S(X)^{(k)}$ can be evaluated with *Lucas' congruence* (cf. [4, 11])

$$\binom{n}{k} \equiv \binom{n_0}{k_0} \cdots \binom{n_l}{k_l} \bmod d,$$

if $n_0, ..., n_l$ and $k_0, ..., k_l$ are the digits in the d-ary representation of n and k, respectively. We immediately see that

$$\binom{n}{k} \equiv \binom{i}{k} \bmod d \tag{3}$$

for $k < d^l$ and $n \equiv i \bmod d^l$.

As before we denote the cyclotomic classes of order δ by D_j, $j = 0, \ldots \delta - 1$, for a divisor δ of $q - 1$. The *cyclotomic numbers* $(i, j)_\delta$ of order δ are defined by

$$(i, j)_\delta = |(D_i + 1) \cap D_j|, \quad 0 \leq i, j \leq \delta - 1.$$

(For monographs on cyclotomic numbers see [2, 15].)

Put $l = 1$ if $k = 0$ and $l = \lfloor \log_d(k) \rfloor + 1$ if $k \geq 1$. For the sequence S defined by (1) we can express $S(1)^{(k)}$, $k = 0, 1, \ldots, d^l - 1$, in terms of cyclotomic numbers of order d^l using (3), namely

$$\begin{aligned} S(1)^{(k)} &= \sum_{n=k}^{q-2} \binom{n}{k} s_n = \sum_{i=k}^{d^l-1} \binom{i}{k} \sum_{n \equiv i \bmod d^l} s_n = \sum_{i=k}^{d^l-1} \binom{i}{k} \sum_{n \equiv i \bmod d^l} \sum_{m=1}^{d-1} \sum_{s_n = m} m \\ &= \sum_{i=k}^{d^l-1} \binom{i}{k} \sum_{j=0}^{d^{l-1}-1} \sum_{m=1}^{d-1} (i, dj + m)_{d^l} m. \end{aligned} \tag{4}$$

More general, if r is a divisor of $q - 1$ with $\gcd(r, d) = 1$, and ξ is a primitive rth root of unity over $\mathbb{F}_d$ then for the sequence S defined by (1) we can express

$S(\xi)^{(k)}$ in terms of cyclotomic numbers of order $d^l r$, namely

$$\begin{aligned} S(\xi)^{(k)} &= \sum_{n=k}^{q-2} \binom{n}{k} s_n \xi^{n-k} = \sum_{h=0}^{r-1} \sum_{\substack{n=k \\ n \equiv h+k \bmod r}}^{q-2} \binom{n}{k} s_n \xi^h \\ &= \sum_{h=0}^{r-1} \sum_{i=k}^{d^l-1} \binom{i}{k} \sum_{\substack{n \equiv i \bmod d^l \\ n \equiv h+k \bmod r}} s_n \xi^h \\ &= \sum_{h=0}^{r-1} \sum_{i=k}^{d^l-1} \binom{i}{k} \sum_{j=0}^{d^{l-1}r-1} \sum_{m=1}^{d-1} (u(h,i), dj+m)_{d^l r} m \xi^h, \end{aligned} \tag{5}$$

where $u(h,i)$ is (by the Chinese-Remainder-Theorem) the unique integer u with $0 \le u \le d^l r - 1$, $u \equiv h + k \bmod r$, and $u \equiv i \bmod d^l$.

Since in general the determination of cyclotomic numbers of order δ is difficult if δ is not small, we can utilize the above relations solely for small r. The following propositions on large prime factors r of $q-1$ enables us to obtain good lower bounds on the linear complexity for several classes of period length $q-1$. For certain classes of period length the propositions reduce the problem of determining the exact linear complexity to the problem of finding the multiplicity of ± 1 as a root of $S(X)$.

Proposition 1. *Let $r \neq d$ be a prime divisor of $q-1$. If d is a primitive root mod r and $r \ge q^{1/2}+1$ then for each r-th root of unity $\beta \neq 1$ we have $S(\beta) \neq 0$.*

Proof. Since $\beta^r = 1$ we get

$$S(\beta) = \sum_{n=0}^{q-2} s_n \beta^n = \sum_{h=0}^{r-1} \sum_{j=0}^{(q-1)/r-1} s_{h+jr} \beta^h.$$

Note that the least residue of $(q-1)/2$ modulo r is 0. Since d is a primitive root mod r the polynomial $\Phi_r(X) = 1 + X + \ldots + X^{r-1}$ is irreducible and thus the minimal polynomial of β over $\mathbb{F}_d$. Consequently $S(\beta) = 0$ implies

$$\sum_{j=0}^{(q-1)/r-1} s_{h+jr} = \sum_{j=0}^{(q-1)/r-1} s_{jr}, \quad h = 1, \ldots, r-1.$$

Note that for $n \neq (q-1)/2$ we have that

$$\varepsilon_d^{s_n} = \chi_d(\alpha^n + 1), \tag{6}$$

where χ_d denotes the nontrivial multiplicative character with $\chi_d(\alpha^k) = \mathrm{e}^{2\pi\sqrt{-1}k/d}$ and $\varepsilon_d = \mathrm{e}^{2\pi\sqrt{-1}/d}$. Furthermore, note that

$$\prod_{j=0}^{(q-1)/r-1} \left(\alpha^{jr} X + 1\right) = 1 - X^{(q-1)/r}.$$

Hence,

$$\varepsilon_d^{\sum_{j=0}^{(q-1)/r-1} s_{h+jr}} = \prod_{j=0}^{(q-1)/r-1} \chi_d(\alpha^{h+jr}+1) = \chi_d(1-\alpha^{h(q-1)/r})$$

has the same value for all $h = 1, \ldots, r-1$. Now

$$\begin{aligned} r-1 &= \left|\sum_{h=0}^{r-1} \chi_d(1-\alpha^{h(q-1)/r})\right| = \frac{r}{q-1}\left|\sum_{h=0}^{q-2} \chi_d(1-\alpha^{h(q-1)/r})\right| \\ &\le \frac{r}{q-1}\left(\left(\frac{q-1}{r}-1\right)q^{1/2}+1\right) < q^{1/2} \end{aligned}$$

by Weil's bound for character sums (see e.g. [10, Theorem 5.41]) contradicting our assumption on r.

Proposition 2. *Let $r \neq d$ be a prime divisor of $q-1$ and $q \equiv 3 \bmod 4$. If d is a primitive element mod r and*

$$r \ge q^{1/2}\frac{1}{\min_{0\le a\le d-1}|\cos 2\pi a/d|} + 1 \tag{7}$$

then for each $2r$-th root of unity $\beta \neq \pm 1$ we have $S(\beta) \neq 0$.

Proof. For $\beta^r = 1$ the statement follows from Proposition 1.

If $\beta^r = -1$ we get

$$S(\beta) = \sum_{n=0}^{q-2} s_n\beta^n = \sum_{h=0}^{r-1}\sum_{j=0}^{(q-1)/r-1} (-1)^j s_{h+jr}\beta^h.$$

Again from the irreducibility of $\Phi_r(X) = 1 - X + \ldots - X^{r-2} + X^{r-1}$ we conclude that $\Phi_r(X)$ is the minimal polynomial of β over $\mathbb{F}_d$, and that $S(\beta) = 0$ implies

$$\sum_{j=0}^{(q-1)/r-1} (-1)^j s_{h+jr} = (-1)^h \sum_{j=0}^{(q-1)/r-1} (-1)^j s_{jr}, \quad h = 1, \ldots, r-1.$$

Denote the sum on the left side by $T(h)$. Then it is obvious that $T(h+r) = -T(h)$ and that $T(0) = T(2) = \ldots = T(2r-2) = -T(1) = -T(3) = \ldots = -T(2r-1)$.

Hence,

$$\begin{aligned} 2(r-1)\min_{0\le a\le d-1}|\cos 2\pi a/d| &\le \left|(r-1)\left(\varepsilon_d^{T(0)} + \varepsilon_d^{-T(0)}\right)\right| \\ &= \left|\sum_{\substack{h=1\\ h\neq r}}^{2r-1} \varepsilon_d^{\sum_{j=0}^{(q-1)/r-1}(-1)^j s_{h+jr}}\right|. \end{aligned} \tag{8}$$

Note that, provided that $q \equiv 3 \bmod 4$, we have

$$\prod_{j=0}^{(q-1)/r-1} \left(\alpha^{jr}X+1\right)^{(-1)^j} = \left(1+X^{(q-1)/2r}\right)\left(1-X^{(q-1)/2r}\right)^{-1},$$

where we denote the function on the right side by $f(X)$. Hence, for $1 \le h \le 2r-1$ except for $h = r$, it follows together with (6) that

$$\varepsilon_d^{\sum_{j=0}^{(q-1)/r-1}(-1)^j s_{h+jr}} = \prod_{j=0}^{(q-1)/r-1} \chi_d(\alpha^{h+jr}+1)^{(-1)^j} = \chi_d(f(\alpha^h)).$$

Now, together with (8) this yields

$$\begin{aligned} 2(r-1)\min_{0\le a\le d-1}|\cos 2\pi a/d| &\le \left|\sum_{h=0}^{2r-1}\chi_d(f(\alpha^h))\right| = \frac{2r}{q-1}\left|\sum_{h=0}^{q-2}\chi_d(f(\alpha^h))\right| \\ &\le \frac{2r}{q-2}\left(\left(\frac{q-2}{r}-1\right)q^{1/2}+1\right) < 2q^{1/2} \end{aligned}$$

by Weil's bound for character sums contradicting our assumption on r.

Propositions 1 and 2 immediately yield the lower bound $L(S) \ge 2(r-1)d^s$ for the sequence (1) over $\mathbb{F}_d$ with period length of the form $q-1 = 2ud^sr$, $u \ne d$ odd, d is a primitive root modulo the prime r and r satisfies (7). For instance, for $d = 5$ condition (7) equals $r \ge q^{1/2}\frac{1}{\cos 2\pi/d}+1 \approx 3.236q^{1/2}+1$.

3 The ternary case $d = 3$

From Propositions 1 and 2 we know that a $2r$th root of unity $\beta \ne \pm 1$ is not a root of the polynomial $S(X)$ if r is a prime such that 3 is a primitive element modulo r and $r \ge 2q^{1/2}+1$, $q \equiv 3 \bmod 4$. If $q = 3^s2r+1$ is a prime power such that r is a prime and 3 is a primitive element modulo r, then we can obtain exact values for the linear complexity of the sequence (1) for the ternary case if we know the multiplicity of 1 and -1 as a root of $S(X)$. In the following we establish general results on the multiplicity of 1 and -1 as a root of $S(X)$. First we focus on the multiplicity of 1 and remark that $X-1$ will always be a divisor of $\gcd(X^{q-1}-1, S(X))$.

For the proof of our first result we will need cyclotomic numbers of order 3. For $q = 3t+1$ let L^2 and M^2 be the uniquely determined integers such that

$$4q = L^2 + 27M^2, \quad L \equiv 1 \bmod 3. \tag{9}$$

We remark that the sign of M is ambiguously determined, depending on the choice of the primitive element α. Then we have [3, p.92]

$$\begin{aligned} (1,1)_3 &= (2q-4-L-9M)/18, \\ (2,1)_3 &= (1,2)_3 = (q+1+L)/9 \quad \text{and} \\ (2,2)_3 &= (2q-4-L+9M)/18. \end{aligned} \tag{10}$$

Proposition 3. *(i)* $(X-1)^2$ *divides* $\gcd(X^{q-1}-1, S(X))$ *if and only if* $q \equiv 1 \bmod 9$.

(ii) $(X-1)^3$ *divides* $\gcd(X^{q-1}-1, S(X))$ *if and only if* $q \equiv 1 \bmod 9$ *and* $M \equiv 0 \bmod 3$, *where* M *is determined (up to sign) from the representation* (9) *of* q.

Proof. First we note that $(X-1)^2$ and $(X-1)^3$ divides $X^{q-1}-1$. To estimate the multiplicity of 1 as a root of $S(X)$ we employ the Hasse derivatives. With (4) we obtain

$$S(1)^{(1)} = (1,1)_3 + 2(1,2)_3 + 2(2,1)_3 + (2,2)_3, \text{ and}$$
$$S(1)^{(2)} = (2,1)_3 + 2(2,2)_3.$$

With (10) this yields

$$S(1)^{(1)} = (1,1)_3 + (1,2)_3 + (2,2)_3 = \frac{2q-4-L-9M}{18} + \frac{q+1+L}{9}$$
$$+\frac{2q-4-L+9M}{18} = \frac{q-1}{3} \equiv 0 \bmod 3$$

if and only if $q \equiv 1 \bmod 9$. For $S(1)^{(2)}$ we obtain

$$S(1)^{(2)} = \frac{q+1+L}{9} + 2\frac{2q-4-L+9M}{18} = \frac{q-1}{3} + M \equiv 0 \bmod 3.$$

Since we have to assume that $q \equiv 1 \bmod 9$ this yields $S(1)^{(2)} \equiv 0 \bmod 3$ if and only if $M \equiv 0 \bmod 3$.

The subsequent proposition presents results on the multiplicity of 2 as a root of $\gcd(X^{q-1}-1, S(X))$. Note that 6 divides $q-1$ and that 2 is a root of $X^{q-1}-1$ with multiplicity at least 3. The proof of the proposition uses the same technique as the proof of Proposition 3. For the sake of completeness the proof is added in the Appendix. Instead of cyclotomic numbers of order 3 we have to employ cyclotomic numbers of order 6 which depend upon the decomposition

$$q = 6f + 1 = A^2 + 3B^2 \tag{11}$$

of q with $A \equiv 1 \bmod 3$ and additionally $\gcd(A, q) = 1$ if $q = p^m$ and $p \equiv 1 \bmod 6$. The sign of B is ambiguously determined, depending on the choice of the primitive element α.

Proposition 4. *(i)* $X+1$ *and* $(X+1)^2$ *divide* $\gcd(X^{q-1}-1, S(X))$ *if and only if* $B \equiv 0 \bmod 3$,

(ii) $(X+1)^3$ *divides* $\gcd(X^{q-1}-1, S(X))$ *if and only if* $B \equiv 0 \bmod 9$, *where* B *is determined from the representation* (11) *of* q.

Remark 1. The condition $B \equiv 0 \bmod 3$ is satisfied if and only if 2 is a cube in $\mathbb{F}_q$ (cf. [2, Corollary 2.6.4]).

With the Propositions 1 – 4 we immediately obtain the following exact values for the linear complexity of the ternary Sidel'nikov sequence.

Theorem 1. *Let S be the ternary Sidel'nikov sequence* (1) *with period $q-1$ for a prime power q of the form $q = 3^s 2r + 1$, where r is a prime such that 3 is a primitive root modulo r, and suppose that $r \geq 2q^{1/2} + 1$. If*

- $q \not\equiv 1 \bmod 9$, $B \not\equiv 0 \bmod 3$ *then* $L(S) = q - 2$,
- $q \equiv 1 \bmod 9$, $M \not\equiv 0 \bmod 3$, $B \not\equiv 0 \bmod 3$ *then* $L(S) = q - 3$,
- $q \not\equiv 1 \bmod 9$, $B \equiv 0 \bmod 3$, $B \not\equiv 0 \bmod 9$ *then* $L(S) = q - 4$,
- $q \equiv 1 \bmod 9$, $M \not\equiv 0 \bmod 3$, $B \equiv 0 \bmod 3$, $B \not\equiv 0 \bmod 9$ *then* $L(S) = q - 5$.

A remark to higher derivatives

In [1] Baumert and Fredricksen presented formulas for the cyclotomic numbers of order 9 and 18 for the case of a prime field $\mathbb{F}_p$. More precisely, if $p = 3^s 2r + 1$ with $s \geq 2$ and (γ being a 9th root of unity)

$$p = \left(\sum_{i=0}^{5} c_i \gamma^i\right)\left(\sum_{i=0}^{5} c_i \gamma^{-i}\right)$$

is a factorization of p in the field of 9th roots of unity, then each cyclotomic number of order 9 respectively of order 18 is expressed as a constant plus a linear combination of $p, L, M, c_0, \ldots, c_5$. We will indicate how we can use this results to obtain more information on the linear complexity of the Sidel'nikov-Lempel-Cohn-Eastman Sequence.
With the knowledge of the cyclotomic numbers of order 9 and 18 we are able to determine $S^{(k)}(1)$ and $S^{(k)}(2)$ for $k = 3, \ldots, 8$ from (4) and (5).

Here, we restrict ourselves to the 4th derivatives for the special case that $\operatorname{ind} 2 \equiv 0 \bmod 9$ and $\operatorname{ind} 3 \equiv 1 \bmod 3$. Applying the results of [1] with straightforward but longsome calculations we get

$$S^{(3)}(1) = c_2 \quad \text{and} \quad S^{(3)}(2) = \frac{c_2 - c_5}{2}.$$

Hence we obtain the following proposition for the considered special case.

Proposition 5. *(i)* $(X-1)^4$ *divides* $\gcd(X^{p-1} - 1, S(X))$ *if and only if* $p \equiv 1 \bmod 9$, $M \equiv 0 \bmod 3$ *and* $c_2 \equiv 0 \bmod 3$,
(ii) $(X+1)^4$ *divides* $\gcd(X^{p-1}-1, S(X))$ *if and only if* $B \equiv 0 \bmod 9$ *and* $c_2 - c_5 \equiv 0 \bmod 6$.

Consequently for this special case we can extend Theorem 1 as follows.

Theorem 2. *Let S and p satisfy the conditions of Theorem 1. Let* $\operatorname{ind} 2 \equiv 0 \bmod 9$ *and* $\operatorname{ind} 3 \equiv 1 \bmod 3$. *If*

- $p \equiv 1 \bmod 9$, $M \equiv 0 \bmod 3$, $c_2 \not\equiv 0 \bmod 3$, $B \equiv 0 \bmod 3$, $B \not\equiv 0 \bmod 9$ *then* $L(S) = p - 6$,
- $p \equiv 1 \bmod 9$, $M \not\equiv 0 \bmod 3$, $B \equiv 0 \bmod 9$, $c_2 - c_5 \not\equiv 0 \bmod 6$ *then* $L(S) = p - 6$,
- $p \equiv 1 \bmod 9$, $M \equiv 0 \bmod 3$, $c_2 \not\equiv 0 \bmod 3$, $B \equiv 0 \bmod 9$, $c_2 - c_5 \not\equiv 0 \bmod 6$ *then* $L(S) = p - 7$.

4 A lower bound on the Linear Complexity Profile

Theorem 3. *The linear complexity profile $L(S,N)$ of the Sidel'nikov sequence (1) satisfies*

$$L(S,N) \geq \min\left(\frac{N+1}{q^{1/2}\log q+3}, \frac{q-1}{q^{1/2}\log q+2}\right) - 1.$$

Proof. Suppose that S satisfies the recurrence relation (2) for $L \leq n \leq N-1$. If we put $c_0 = -1$ then we have

$$\sum_{l=0}^{L} c_l s_{n-l} = 0 \in \mathbb{F}_d \quad \text{for } L \leq n \leq \min(N, q-1+L) - 1.$$

Recall that for $m \neq (q-1)/2$ we have

$$\chi_d(\alpha^m + 1) = \varepsilon_d^{s_m}, \tag{12}$$

where χ_d denotes the nontrivial multiplicative character of order d with $\chi_d(\alpha^m) = \mathrm{e}^{2\pi\sqrt{-1}m/d}$ and $\varepsilon_d = \mathrm{e}^{2\pi\sqrt{-1}/d}$.

Thus, for all n satisfying $L \leq n \leq \min(N, q-1+L) - 1$ and $\frac{q-1}{2} \notin \{n, n-1, \ldots, n-L\}$, we get

$$\begin{aligned}\chi_d\left(\prod_{l=0}^{L}(\alpha^{n-l}+1)^{c_l}\right) &= \prod_{l=0}^{L}\chi_d(\alpha^{n-l}+1)^{c_l} \\ &= \prod_{l=0}^{L}\varepsilon_d^{c_l s_{n-l}} = \varepsilon_d^{\sum_{l=0}^{L} c_l s_{n-l}} = 1.\end{aligned}$$

Consequently,

$$\begin{aligned}\min(N-L, q-1) - 2(L+1) &\leq \sum_{n=L}^{\min(N,q-1+L)-1} \chi_d\left(\prod_{l=0}^{L}(\alpha^{n-l}+1)^{c_l}\right) \\ &\leq (L+1)q^{1/2}\log q,\end{aligned}$$

where the last step follows from [13, Lemma 3.3]. The bound immediately follows from the above inequality.

5 An upper bound on the Aperiodic Autocorrelation

Let $S = s_0, s_1, \ldots$ be an N-periodic sequence over the finite field $\mathbb{F}_d$. The *autocorrelation* of S is the complex-valued function defined by

$$\mathrm{A}_d(S,t) := \sum_{n=0}^{N-1} \varepsilon_d^{s_{n+t}-s_n}, \quad 1 \leq t \leq N-1,$$

where $\varepsilon_d = \mathrm{e}^{2\pi\sqrt{-1}/d}$.
In [7] Kim et al. presented results on the distribution of the autocorrelation of the Sidel'nikov sequence when t takes different values. In particular the autocorrelation of the Sidel'nikov sequence (1) was determined to be

$$\mathrm{A}_d(S,t) = \chi_d^{-1}(1-\alpha^t) + \chi_d(1-\alpha^{-t}) - \chi_d(\alpha^{-t}) - 1,$$

for $1 \le t \le N-1$.
While the autocorrelation reflects global randomness the *aperiodic autocorrelation*, which is defined by

$$\mathrm{AAC}_d(S,u,v,t) = \sum_{n=u}^{v} \varepsilon_d^{s_n - s_{n+t}}, \quad 0 \le u < v < N,\ 1 \le t < N,$$

reflects local randomness.
If S is a random sequence over $\mathbb{F}_d$ then $|\mathrm{A}_d(S,t)|$ and $|\mathrm{AAC}_d(S,u,v,t)|$ can be expected to be quite small. The security of many cryptographic systems depends upon the generation of pseudorandom, i. e., unpredictable quantities and a low (aperiodic) autocorrelation is a desirable feature for pseudorandom sequences.

Theorem 4. *The aperiodic autocorrelation* $\mathrm{AAC}_d(S,u,v,t)$ *of the Sidel'nikov sequence (1) over* $\mathbb{F}_d$ *can be estimated by*

$$|\mathrm{AAC}_d(S,u,v,t)| \le 2q^{1/2}\log q + 2,$$

for $0 \le u < v < q-1$ *and* $1 \le t < q-1$.

Proof. By definition and by (12) we have

$$\begin{aligned} |\mathrm{AAC}_d(S,u,v,t)| &= \left|\sum_{n=u}^{v} \varepsilon_d^{s_n - s_{n+t}}\right| \le \left|\sum_{n=u}^{v} \chi_d(\alpha^n+1)\chi_d^{d-1}(\alpha^{n+t}+1)\right| + 2 \\ &= \left|\sum_{n=u}^{v} \chi_d\left((\alpha^n+1)(\alpha^{n+t}+1)^{d-1}\right)\right| + 2 \le 2q^{1/2}\log q + 2, \end{aligned}$$

where the last inequality follows from [13, Lemma 3.3].

Remark 2. We remark that the estimate in Theorem 4 accords with

$$\max_{t=1,\ldots,q-2} |\mathrm{AAC}_d(S,0,N-1,t)| = \Omega(q^{1/2}),$$

where $N = (1/5-\varepsilon)q, \varepsilon > 0$.

Acknowledgement

Part of the research was done during a visit of the first author to the Sabanci University. She wishes to thank the university for hospitality.

We would like to thank Arne Winterhof for pointing out Remark 2.

References

1. L.D. Baumert and H. Fredricksen, The cyclotomic numbers of order eighteen with applications to difference sets, Math. Comp. 21 (1967), 204–219.
2. B. C. Berndt, R. J. Evans, and K. S. Williams, Gauss and Jacobi sums, Canadian Mathematical Society Series of Monographs and Advanced Texts. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1998.
3. T. W. Cusick, C. Ding, and A. Renvall, Stream Ciphers and Number Theory, North-Holland Publishing Co., Amsterdam, 1998.
4. A. Granville, Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers, in: Organic mathematics, Burnaby, BC, 1995, CMS Conf. Proc. 20, Amer. Math. Soc., Providence, RI, 1997, 253–276.
5. H. Hasse, Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit vollkommenem Konstantenkörper bei beliebiger Charakteristik, J. Reine Angew. Math. 175 (1936), 50–54.
6. T. Helleseth and K. Yang, On binary sequences with period $n = p^m - 1$ with optimal autocorrelation, In (T. Helleseth, P. Kumar, and K. Yang, eds.), Proceedings of SETA 01, (2002), 209–217.
7. Y.-S. Kim, J.-S. Chung, J.-S. No, and H. Chung, On the autocorrelation distributions of Sidel'nikov sequences, IEEE Trans. Inf. Th. 51 (2005), 3303–3307.
8. G. M. Kyureghyan and A. Pott, On the linear complexity of the Sidelnikov-Lempel-Cohn-Eastman sequences, Designs, Codes, and Cryptography 29 (2003), 149–164.
9. A. Lempel, M. Cohn, and W. L. Eastman, A class of balanced binary sequences with optimal autocorrelation properties. IEEE Trans. Inf. Th. 23 (1977), 38–42.
10. R. Lidl, H. Niederreiter, Finite Fields, Addison-Wesley, Reading, MA, 1983.
11. M. E. Lucas, Sur les congruences des nombres euleriennes et des coefficients differentiels des fuctions trigonometriques, suivant un-module premier, Bull. Soc. Math. France 6 (1878), 122–127.
12. W. Meidl and A. Winterhof, Some notes on the linear complexity of Sidel'nikov-Lempel-Cohn-Eastman sequences, Designs, Codes, and Cryptography 38 (2006), 159–178.
13. I. Shparlinski, Cryptographic Applications of Analytic Number Theory. Complexity Lower Bounds and Pseudorandomness. Progress in Computer Science and Applied Logic. 22, Birkhäuser, Basel, 2003.
14. V. M. Sidel'nikov, Some k-valued pseudo-random sequences and nearly equidistant codes. Problems of Information Transmission 5 (1969), 12–16.; translated from Problemy Peredači Informacii 5 (1969), 16–22 (Russian).
15. T. Storer, Cyclotomy and Difference Sets, Markham Publishing Co., Chicago, III. (1967).

6 Appendix

For the proof of Proposition 4 we will utilize the following relation between the cyclotomic numbers of order d (cf. [3, p.84]]. Let $q = df + 1$, then

$$(i,j)_d = (d-i, j-i)_d = \begin{cases} (j,i)_d, & f \text{ even} \\ (j+d/2, i+d/2)_d, & f \text{ odd} \end{cases}. \tag{13}$$

We will then need the following cyclotomic numbers of order 6 given in [3, Appendix B]. Let $q \equiv 1 \bmod 6$ with decomposition (11) and let $2 = \alpha^m$.

Case Ia: $q \equiv 1 \bmod 12$*,* $m \equiv 0 \bmod 3$

$$(0,1)_6 = (q-5+4A+18B)/36,\ (0,2)_6 = (q-5+4A+6B)/36,$$
$$(0,4)_6 = (q-5+4A-6B)/36,\ \ (0,5)_6 = (q-5+4A-18B)/36,$$
$$(1,2)_6 = (1,3)_6 = (1,4)_6 = (2,4)_6 = (q+1-2A)/36.$$

Case Ib: $q \equiv 1 \bmod 12$*,* $m \equiv 1 \bmod 3$

$$(0,1)_6 = (q-5+4A+12B)/36,\ (0,5)_6 = (q-5+4A-6B)/36,$$
$$(1,3)_6 = (q+1-2A-6B)/36,\ \ (1,4)_6 = (q+1-2A+12B)/36.$$

Case Ic: $q \equiv 1 \bmod 12$*,* $m \equiv 2 \bmod 3$

$$(0,1)_6 = (q-5+4A+6B)/36,\ \ (0,5)_6 = (q-5+4A-12B)/36,$$
$$(1,3)_6 = (q+1-2A-12B)/36,\ (1,4)_6 = (q+1-2A+6B)/36.$$

Case IIa: $q \equiv 7 \bmod 12$*,* $m \equiv 0 \bmod 3$

$$(1,0)_6 = (q-5+4A+6B)/36,\ (0,1)_6 = (0,2)_6 = (q+1-2A+12B)/36,$$
$$(1,1)_6 = (q-5+4A-6B)/36,\ (1,2)_6 = (2,1)_6 = (q+1-2A)/36,$$
$$(0,4)_6 = (0,5)_6 = (q+1-2A-12B)/36.$$

Case IIb: $q \equiv 7 \bmod 12$*,* $m \equiv 1 \bmod 3$

$$(0,2)_6 = (q+1-2A+12B)/36,\ (0,4)_6 = (q+1-8A-12B)/36,$$
$$(1,0)_6 = (q-5-2A+6B)/36,\ \ (1,1)_6 = (q-5+4A-6B)/36.$$

Case IIc: $q \equiv 7 \bmod 12$*,* $m \equiv 2 \bmod 3$

$$(0,2)_6 = (q+1-8A+12B)/36,\ (0,4)_6 = (q+1-2A-12B)/36,$$
$$(1,0)_6 = (q-5+4A+6B)/36,\ \ (1,1)_6 = (q-5-2A-6B)/36.$$

Proof of Proposition 4:
With (5) we obtain

$$\begin{aligned} S(2) = {} & (0,1)_6 + (0,4)_6 + (4,1)_6 + (4,4)_6 + (2,1)_6 + (2,4)_6 \\ & +2(0,2)_6 + 2(0,5)_6 + 2(4,2)_6 + 2(4,5)_6 + 2(2,2)_6 + 2(2,5)_6 \\ & +2(3,1)_6 + 2(3,4)_6 + 2(1,1)_6 + 2(1,4)_6 + 2(5,1)_6 + 2(5,4)_6 \\ & +(3,2)_6 + (3,5)_6 + (1,2)_6 + (1,5)_6 + (5,2)_6 + (5,5)_6. \end{aligned}$$

If $q \equiv 1 \bmod 12$ with (13) we obtain $S(2) = 2(0,1)_6 + (0,5)_6 + (1,3)_6 + 2(1,4)_6$. For the Case Ia, i.e. 2 is a cube which implies $B \equiv 0 \bmod 3$, we then get

$$\begin{aligned} S(2) &= 2\frac{q-5+4A+18B}{36} + \frac{q-5+4A-18B}{36} + \frac{q+1-2A}{36} \\ &\quad +2\frac{q+1-2A}{36} \\ &= -\frac{q-5+4A+18B}{36} + \frac{q-5+4A-18B}{36} = -B = 0. \end{aligned}$$

In the Case Ib, where $B \not\equiv 0 \bmod 3$, we obtain

$$S(2) = 2\frac{q-5+4A+12B}{36} + \frac{q-5+4A-6B}{36} + \frac{q+1-2A-6B}{36} + 2\frac{q+1-2A+12B}{36} = \frac{-18B}{36} + \frac{-18B}{36} = -B \neq 0.$$

Finally for Case Ic (again $B \not\equiv 0 \bmod 3$) we get

$$S(2) = 2\frac{q-5+4A+6B}{36} + \frac{q-5+4A-12B}{36} + \frac{q+1-2A-12B}{36} + 2\frac{q+1-2A+6B}{36} = \frac{-18B}{36} + \frac{-18B}{36} = -B \neq 0.$$

If $q \equiv 7 \bmod 12$ (13) yields $S(2) = 2(0,4)_6 + 2(1,1)_6 + (0,2)_6 + (1,0)_6$. Consequently for the Case IIa we obtain

$$S(2) = 2\frac{q+1-2A-12B}{36} + 2\frac{q-5+4A-6B}{36} + \frac{q+1-2A+12B}{36} + \frac{q-5+4A+6B}{36} = \frac{24B}{36} + \frac{12B}{36} = B = 0.$$

For the Case IIb respectively for the Case IIc we get

$$S(2) = 2\frac{q+1-8A-12B}{36} + 2\frac{q-5+4A-6B}{36} + \frac{q+1-2A+12B}{36} + \frac{q-5-2A+6B}{36} = \frac{6A+24B}{36} + \frac{-6A+12B}{36} = B \neq 0,$$

respectively

$$S(2) = 2\frac{q+1-2A-12B}{36} + 2\frac{q-5-2A-6B}{36} + \frac{q+1-8A+12B}{36} + \frac{q-5+4A+6B}{36} = \frac{-6A+24B}{36} + \frac{6A+12B}{36} = B \neq 0.$$

Summarizing $S(2) = 0$ if and only if 2 is a cube or equivalently $B \equiv 0 \bmod 3$.

With (5) we obtain

$$\begin{aligned} S(2)^{(1)} = {} & (1,1)_6 + 2(1,2)_6 + (1,4)_6 + 2(1,5)_6 + 2(5,1)_6 + (5,2)_6 \\ & + 2(5,4)_6 + (5,5)_6 + 2(4,1)_6 + (4,2)_6 + 2(4,4)_6 + (4,5)_6 \\ & + (2,1)_6 + 2(2,2)_6 + (2,4)_6 + 2(2,5)_6. \end{aligned}$$

If $q \equiv 1 \bmod 12$ with (13) this yields $S(2)^{(1)} = (0,5)_6 + (0,1)_6 + 2(2,4)_6 + 2(0,2)_6 + (1,2)_6 + 2(0,4)_6$, and hence for $m \equiv 0 \bmod 3$, the only case of interest, we get

$$\begin{aligned} S(2)^{(1)} = {} & \frac{q-5+4A-18B}{36} + \frac{q-5+4A+18B}{36} + 2\frac{q+1-2A}{36} \\ & + 2\frac{q-5+4A+6B}{36} + \frac{q+1-2A}{36} + 2\frac{q-5+4A-6B}{36} \\ = {} & \frac{-12B}{36} + \frac{12B}{36} = 0. \end{aligned}$$

If $q \equiv 7 \bmod 12$ with (13) we have $S(2)^{(1)} = (0,2)_6 + (0,4)_6 + 2(0,5)_6 + 2(2,1)_6 + (1,2)_6 + 2(0,1)_6$, which again vanishes if $m \equiv 0 \bmod 3$ (Case IIa).

Finally (5) yields $S(2)^{(2)} = (2,1)_6 + (2,4)_6 + 2(2,2)_6 + 2(2,5)_6 + 2(5,1)_6 + 2(5,4)_6 + (5,2)_6 + (5,5)_6$. Using (13) for the Case Ia we obtain

$$\begin{aligned} S(2)^{(2)} &= (2,4)_6 + 2(0,4)_6 + 2(1,2)_6 + (0,1)_6 \\ &= \frac{q+1-2A}{36} + 2\frac{q-5+4A-6B}{36} + 2\frac{q+1-2A}{36} \\ &\quad + \frac{q-5+4A+18B}{36} = \frac{2B}{3}, \end{aligned}$$

and for the Case IIa we obtain

$$\begin{aligned} S(2)^{(2)} &= (2,1)_6 + 2(0,1)_6 + 2(1,2)_6 + (0,4)_6 \\ &= \frac{q+1-2A}{36} + 2\frac{q+1-2A+12B}{36} + 2\frac{q+1-2A}{36} \\ &\quad + \frac{q+1-2A-12B}{36} = -\frac{2B}{3}. \end{aligned}$$

Consequently $S(2)^{(2)} = 0$ if and only if $B \equiv 0 \bmod 9$. □