Des. Codes Cryptogr. (2011) 59:59–68
DOI 10.1007/s10623-010-9467-8

Correlation of the two-prime Sidel'nikov sequence

Nina Brandstätter · Gottlieb Pirsic · Arne Winterhof

Received: 10 February 2009 / Revised: 17 April 2009 / Accepted: 1 August 2010 /
Published online: 30 December 2010

Abstract Motivated by the concepts of Sidel'nikov sequences and two-prime generator (or Jacobi sequences) we introduce and analyze some new binary sequences called two-prime Sidel'nikov sequences. In the cases of twin primes and cousin primes equivalent 3 modulo 4 we show that these sequences are balanced. In the general case, besides balancedness we also study the autocorrelation, the correlation measure of order k and the linear complexity profile of these sequences showing that they have many nice pseudorandom features.

Keywords Two-prime generator · Sidel'nikov sequences · (Auto-) correlation · Linear complexity · Cryptography · Pseudorandomness

Mathematics Subject Classification (2000) 11T71 · 11T24

1 Introduction

Several sequences with nice pseudorandomness properties in view of applications in cryptography and wireless communication have been defined using the Legendre symbol, see the surveys [10,11] and references therein. Among these sequences are the Sidel'nikov sequences and the two-prime generator defined as follows.

Let p be an odd prime and g be a primitive element of the finite field $\mathbb{F}_p$ of p elements. The *Sidel'nikov sequence* (σ_n), see [8], is defined by

N. Brandstätter · A. Winterhof (✉)
Johann Radon Institute for Computational and Applied Mathematics,
Austrian Academy of Sciences, Altenbergerstraße 69, 4040 Linz, Austria
e-mail: arne.winterhof@oeaw.ac.at

N. Brandstätter
e-mail: nina.brandstaetter@gmail.com

G. Pirsic
Institute of Financial Mathematics, Johannes Kepler University, Altenbergerstraße 69, 4040 Linz, Austria
e-mail: gpirsic@gmail.com

$$\sigma_n = \begin{cases} 1, & \text{if } \left(\frac{g^n+1}{p}\right) = -1, \\ 0, & \text{otherwise,} \end{cases} \qquad n \geq 0,$$

where $\left(\frac{\cdot}{\cdot}\right)$ denotes the Legendre symbol.

Let p and q be two distinct odd primes. Put

$$Q = \{q, 2q, \ldots, (p-1)q\}, \quad Q_0 = Q \cup \{0\}, \quad \text{and} \quad P = \{p, 2p, \ldots, (q-1)p\}.$$

The pq-periodic sequence (t_n) over $\mathbb{F}_2$, defined by

$$t_n = \begin{cases} 0, & \text{if } (n \bmod pq) \in Q_0, \\ 1, & \text{if } (n \bmod pq) \in P, \\ \left(1 - \left(\frac{n}{p}\right)\left(\frac{n}{q}\right)\right)/2, & \text{otherwise,} \end{cases}$$

is called the *two-prime generator* (or *generalized cyclotomic sequence of order* 2 or *Jacobi sequence*) (see [2], and [4, Chapt. 8.2]).

Here we introduce a new sequence combining the concepts of Sidel'nikov sequence and two-prime generator:

Let p and q be two different odd primes and g be a primitive element modulo both p and q. (If g_1 and g_2 are primitive roots modulo p and q, respectively, the Chinese Remainder Theorem guarantees the existence of an integer $g \equiv g_1 \bmod p$ and $g \equiv g_2 \bmod q$, which is primitive modulo both p and q.) Put $d = \gcd(p-1, q-1)$ and $t = (p-1)(q-1)/d$. With Q_0, P as above we define the *two-prime Sidel'nikov sequence* (s_n) by

$$s_n = \begin{cases} 0, & (g^n+1) \bmod pq \in Q_0, \\ 1, & (g^n+1) \bmod pq \in P, \\ \left(1 - \left(\frac{g^n+1}{p}\right)\left(\frac{g^n+1}{q}\right)\right)/2, & \gcd(g^n+1, pq) = 1, \end{cases} \tag{1}$$

for $n \geq 0$. Obviously, (s_n) is t-periodic.

For the number of $0 \leq n < t$ with $s_n = 1$ in Sect. 2 we prove an exact formula if $d = 2$ and an asymptotic formula if $d > 2$. For $d = 2$ this shows that (s_n) is balanced if and only if p and $q = p+2$ are twin primes or p and $q = p+4$ are cousin primes with $p \equiv 3 \bmod 4$.

For a t-periodic sequence (s_n) over $\mathbb{F}_2$ and $1 \leq l < t$ the (*periodic*) *autocorrelation function* is defined by

$$AC(s_n, l) = \sum_{n=0}^{t-1} (-1)^{s_{n+l}+s_n}.$$

The (periodic) autocorrelation reflects global randomness. If (s_n) is a random sequence then $|AC(s_n, l)|$ can be expected to be small compared to t. For the autocorrelation functions of Sidel'nikov sequence and two-prime generator see [2,4,8,10] and references therein. In Sect. 3 we prove a bound on the autocorrelation of the two-prime Sidel'nikov sequence.

In Mauduit and Sárközy [7] the *correlation measure of order k* of a binary sequence (s_n) (of length t) is introduced as

$$C_k(s_n) = \max_{M,D} \left| \sum_{n=0}^{M-1} (-1)^{s_{n+d_1}} \cdots (-1)^{s_{n+d_k}} \right|, \quad k \geq 1,$$

where the maximum is taken over all $D = (d_1, d_2, \ldots, d_k)$ with non-negative integers $d_1 < d_2 < \cdots < d_k$ and M such that $M - 1 + d_k \leq t - 1$. The correlation measure of order k reflects local randomness.

The *linear complexity profile* of a sequence (s_n) over $\mathbb{F}_2$ is the sequence $L(s_n, N)$, $N \geq 1$, where its Nth term is the smallest L such that a linear recurrence of order L over $\mathbb{F}_2$ can generate the first N terms of (s_n). The value

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

is called the *linear complexity over* $\mathbb{F}_2$ of the sequence (s_n). For the linear complexity of any periodic sequence of period t one easily verifies that

$$L(s_n) = L(s_n, 2t) \leq t.$$

Linear complexity and linear complexity profile are measures for the unpredictability of a sequence and thus for its suitability in cryptography.

In Sect. 4 we study the correlation measure of order k of (s_n) for arbitrary d as well as the linear complexity profile of (s_n).

2 Balancedness

First we consider the case $d = 2$. (Note that we have $d > 2$ if $p \equiv q \equiv 1 \bmod 4$.)

Theorem 1 *Let (s_n) be defined by (1) with $d = 2$. The number of $0 \leq n < t$ with $s_n = 1$ is equal to*

$$\frac{t}{2} + \frac{q-p}{4} - \frac{\delta+1}{2},$$

where $\delta = 0$ if $p \not\equiv q \bmod 4$ and $\delta = 1$ if $p \equiv q \equiv 3 \bmod 4$.

The sequence (s_n) with $d = 2$ is balanced if and only if p and $q = p + 2$ are twin primes or p and $q = p + 4$ are cousin primes with $p \equiv 3 \bmod 4$.

Proof First we verify that $g^n + 1 \equiv 0 \bmod pq$ if and only if p and q are both equivalent 3 mod 4 and $n = t/2$. The only possible element of the form g^n with $1 \leq n < t$ such that $g^{2n} \equiv 1 \bmod pq$ is $g^{t/2}$. The condition $-1 \equiv g^{t/2} \bmod pq$ implies $-1 \equiv g^{(p-1)(q-1)/4} \equiv (-1)^{(q-1)/2} \bmod p$ and $-1 \equiv g^{(p-1)(q-1)/4} \equiv (-1)^{(p-1)/2} \bmod q$ which is true if and only if $p \equiv q \equiv 3 \bmod 4$.

We have $g^n + 1 \in Q_0$ whenever $n \equiv (q-1)/2 \bmod (q-1)$. The number of such n with $0 \leq n < t$ is $(p-1)/2$. We have $g^n + 1 \in P$ whenever $n \equiv (p-1)/2 \bmod (p-1)$ and $g^n + 1 \not\equiv 0 \bmod pq$. The number of such n with $0 \leq n < t$ is $(q-1)/2 - \delta$.

Note that for all n with $g^n + 1 \notin (P \cup Q_0)$ we have

$$(-1)^{s_n} = \left(\frac{g^n+1}{p}\right)\left(\frac{g^n+1}{q}\right).$$

Hence we get

$$\sum_{n=0}^{t-1}(-1)^{s_n} = \frac{p-1}{2} - \left(\frac{q-1}{2} - \delta\right) + S, \quad \text{where} \quad S = \sum_{n=0}^{t-1}\left(\frac{g^n+1}{p}\right)\left(\frac{g^n+1}{q}\right).$$

Next we show that $S = 1$.

We need the well-known relations

$$\sum_{x=0}^{p-1}\left(\frac{x}{p}\right) = 0 \quad \text{and} \quad \sum_{x=0}^{p-1}\left(\frac{x}{p}\right)\left(\frac{x+a}{p}\right) = -1 \quad \text{if } p \not| a,$$

see [1,5,6].

We have

$$S = \sum_{n=0}^{p-2} \left(\frac{g^n+1}{p}\right) \sum_{j=0}^{(q-3)/2} \left(\frac{g^{n+j(p-1)}+1}{q}\right).$$

Since $d = 2$ for $j = 0, 1, \ldots, (q-3)/2$ the elements $g^{j(p-1)}$ run through the quadratic residues x modulo q. Hence,

$$\begin{aligned} S &= \sum_{n=0}^{p-2} \left(\frac{g^n+1}{p}\right) \sum_{x=1}^{q-1} \left(\frac{g^n x+1}{q}\right) \left(1+\left(\frac{x}{q}\right)\right) \Big/ 2 \\ &= \frac{1}{2} \sum_{n=0}^{p-2} \left(\frac{g^n+1}{p}\right) \left(\underbrace{\sum_{x=1}^{q-1} \left(\frac{g^n x+1}{q}\right)}_{-1} + \left(\frac{g^n}{q}\right) \underbrace{\sum_{x=1}^{q-1} \left(\frac{x+g^{-n}}{q}\right)\left(\frac{x}{q}\right)}_{-1} \right) \\ &= -\frac{1}{2} \left(\underbrace{\sum_{n=0}^{p-2} \left(\frac{g^n+1}{p}\right)}_{-1} + \underbrace{\sum_{n=0}^{p-2} \left(\frac{g^n+1}{p}\right)\left(\frac{g^n}{q}\right)}_{-1} \right) = 1. \end{aligned}$$

(Note that $\left(\frac{g^n}{p}\right) = \left(\frac{g^n}{q}\right) = (-1)^n$, so we again have a sum of the form noted preliminarily.) Now the numbers $N_i, i = 0, 1$, of $0 \le n < t$ with $s_n = i$ can be easily determined from $N_0 + N_1 = t$ and $N_0 - N_1 = \sum_{n=0}^{t-1} (-1)^{s_n}$. □

For $d > 2$ we can prove a slightly weaker result.

Theorem 2 *Let (s_n) be defined by (1) with $d > 2$. The number of $0 \le n < t$ with $s_n = 1$ is*

$$\frac{t}{2} + \frac{q-p}{2d} + O\left(p^{1/2} q^{1/2}\right).$$

Proof Note that for a multiplicative character χ modulo q of order d we have

$$\sum_{k=0}^{d-1} \chi^k(x) = \begin{cases} d, & \text{if } x \text{ is a } d\text{th power residue mod } q, \\ 0, & \text{otherwise,} \end{cases} \quad x = 1, \ldots, q-1.$$

As in the proof of Theorem 1 we get

$$N_0 - N_1 = \frac{p-q}{d} + S + O(1),$$

where

$$\begin{aligned} S &= \sum_{n=0}^{p-2} \left(\frac{g^n+1}{p}\right) \sum_{j=0}^{(q-1-d)/d} \left(\frac{g^{n+j(p-1)}+1}{q}\right) \\ &= \sum_{n=0}^{p-2} \left(\frac{g^n+1}{p}\right) \sum_{x=1}^{q-1} \left(\frac{g^n x+1}{q}\right) \frac{1}{d} \sum_{k=0}^{d-1} \chi^k(x). \end{aligned}$$

Substituting $y = g^n x$ and interchanging sums we get

$$S = \frac{1}{d}\sum_{k=0}^{d-1}\sum_{n=0}^{p-2}\left(\frac{g^n+1}{p}\right)\psi^k(g^n)\sum_{y=1}^{q-1}\left(\frac{y+1}{q}\right)\chi^k(y),$$

where ψ is the character of order d of $\mathbb{F}_p$ defined by $\psi(g) = \overline{\chi}(g)$. For fixed k both factors are Jacobi sums and have absolute value $O(p^{1/2})$ and $O(q^{1/2})$, respectively, see for example [1,6]. □

3 Autocorrelation

Theorem 3 *Let (s_n) be defined by (1). The autocorrelation function of (s_n) satisfies*

$$AC(s_n, l) = O\left(\frac{p+q}{d} + p^{1/2}q^{1/2}\right), \quad 1 \le l < t.$$

Proof We have $AC(s_n, l) = S + O\left(\frac{p+q}{d}\right)$, where

$$S = \sum_{n=0}^{t-1}\left(\frac{(g^n+1)(g^{n+l}+1)}{p}\right)\left(\frac{(g^n+1)(g^{n+l}+1)}{q}\right).$$

If $l \equiv 0 \bmod (p-1)$ we get

$$\begin{aligned} S &= \sum_{n=0}^{t-1}\left(\frac{(g^n+1)(g^{n+l}+1)}{q}\right) + O\left(\frac{q}{d}\right) \\ &= \frac{p-1}{d}\sum_{n=0}^{q-2}\left(\frac{(g^n+1)(g^{n+l}+1)}{q}\right) + O\left(\frac{q}{d}\right) = O\left(\frac{p+q}{d}\right). \end{aligned}$$

In the same way, if $l \equiv 0 \bmod (q-1)$ we get $S = O\left((p+q)/d\right)$.
If $l \not\equiv 0 \bmod p-1$ and $\not\equiv 0 \bmod q-1$ we proceed as in the proof of Theorem 2 and get

$$\begin{aligned} S &= \sum_{n=0}^{p-2}\left(\frac{g^n+1}{p}\right)\left(\frac{g^{n+l}+1}{p}\right)\sum_{j=0}^{(q-1-d)/d}\left(\frac{g^{n+j(p-1)}+1}{q}\right)\left(\frac{g^{n+j(p-1)+l}+1}{q}\right) \\ &= \sum_{n=0}^{p-2}\left(\frac{g^n+1}{p}\right)\left(\frac{g^{n+l}+1}{p}\right)\sum_{x=1}^{q-1}\left(\frac{g^n x+1}{q}\right)\left(\frac{g^{n+l}x+1}{q}\right)\frac{1}{d}\sum_{k=0}^{d-1}\chi^k(x) \\ &= \frac{1}{d}\sum_{k=0}^{d-1}\sum_{n=0}^{p-2}\left(\frac{g^n+1}{p}\right)\left(\frac{g^{n+l}+1}{p}\right)\psi^k(g^n)\sum_{y=1}^{q-1}\left(\frac{y+1}{q}\right)\left(\frac{g^l y+1}{q}\right)\chi^k(y). \end{aligned}$$

For fixed k both factors have absolute value $O(p^{1/2})$ or $O(q^{1/2})$, respectively, by the Weil bound, see [6, Theorem 5.41]. (Put $u = \operatorname{lcm}(d, 2)$ and note that

$$\left(\frac{(g^n+1)(g^{n+l}+1)}{p}\right)\psi^k(g^n) = \varphi((g^n+1)^{u/2}(g^{n+l}+1)^{u/2}g^{nku/d})$$

for a multiplicative character φ modulo p of order u. The sum over y can also be expressed with a character modulo q of order u.) □

4 Correlation Measure and Linear Complexity Profile

The bound on the correlation measure is based on the following Lemma.

Lemma 1 *Let $f(X) \in \mathbb{Z}[X]$ be a monic polynomial of degree $D \geq 1$ which is neither a square in $\mathbb{F}_p[X]$ nor $\mathbb{F}_q[X]$ with $f(0) \neq 0$ and let g be a primitive element modulo p and modulo q. Let $d = \gcd(p-1, q-1)$ and $t = (p-1)(q-1)/d$ be the order of g modulo pq. Then for $1 \leq N \leq t$ we have*

$$\left| \sum_{n=0}^{N-1} \left(\frac{f(g^n)}{p}\right)\left(\frac{f(g^n)}{q}\right) \right| = O\left(D^2 p^{1/2} q^{1/2} \log t\right).$$

Proof Put $e_t(x) = e^{2\pi i x/t}$. Then we have

$$\frac{1}{t}\sum_{a=0}^{t-1} e_t(ax) = \begin{cases} 0, & x \not\equiv 0 \bmod t \\ 1, & x \equiv 0 \bmod t. \end{cases} \tag{2}$$

Put

$$S_N = \sum_{n=0}^{N-1} \left(\frac{f(g^n)}{p}\right)\left(\frac{f(g^n)}{q}\right).$$

From (2) we get

$$S_N = \frac{1}{t}\sum_{a=0}^{t-1}\sum_{n=0}^{t-1}\left(\frac{f(g^n)}{p}\right)\left(\frac{f(g^n)}{q}\right)\sum_{m=0}^{N-1} e_t(a(n-m)) = \frac{1}{t}\sum_{a=0}^{t-1} S_a \sum_{m=0}^{N-1} e_t(-am),$$

where

$$\begin{aligned} S_a &= \sum_{n=0}^{t-1}\left(\frac{f(g^n)}{p}\right)\left(\frac{f(g^n)}{q}\right) e_t(an) \\ &= \frac{1}{d}\sum_{k=0}^{d-1}\sum_{n=0}^{p-2}\left(\frac{f(g^n)}{p}\right) e_{p-1}(\alpha n)\sum_{x=1}^{q-1}\left(\frac{f(g^n x)}{q}\right) e_{q-1}(\beta \mathrm{ind} x)\chi^k(x), \end{aligned}$$

where $\alpha \equiv ad(q-1)^{-1} \bmod (p-1)$, $\beta \equiv a(p-1)^{-1} \bmod (q-1)$, χ is again a character modulo q of order d and $\mathrm{ind}(g^n) = n$ is the discrete logarithm (or index) modulo q. Note that $\lambda_p(g^n) = e_{p-1}(\alpha n)$ and $\lambda_q(g^n) = e_{q-1}(\beta n)$ are multiplicative characters modulo p and q, respectively. For fixed k the sums over n and x are $O(Dp^{1/2})$ and $O(Dq^{1/2})$, respectively, by Weil's Theorem. (Note that the term $\left(\frac{f(g^n x)}{q}\right) e_{q-1}(\beta \mathrm{ind} x)\chi^k(x)$ can be expressed as $\eta(f(g^n x)^{u/2} x^{u/s+uk/d})$ with a character η of order $u = \mathrm{lcm}(s, d, 2)$, where s is the order of the character λ_q. The polynomial $f(X)^{u/2}X^{u/s+u/d}$ is not a uth power since $f(0) \neq 0$.) Since

$$\sum_{a=0}^{t-1}\left|\sum_{m=0}^{N-1} e_t(-am)\right| = O(t \log t)$$

we get altogether $S_N = O\left(D^2 p^{1/2} q^{1/2} \log t\right)$. □

Theorem 4 *For the sequence (s_n) defined by (1) we have*

$$\begin{aligned} C_k(s_n) &= O\left(k^2 p^{1/2} q^{1/2} \log t + k\frac{p+q}{d}\right), \quad k \geq 1 \text{ and } k \text{ odd}, \\ C_2(s_n) &= O((p^{1/2}+q^{1/2})p^{1/2}q^{1/2}\log t), \\ t - C_k(s_n) &= O(k(p+q)), \quad k > 2 \text{ and } k \text{ even} \end{aligned}$$

and

$$L(s_n, N) = \Omega\left(\min\left\{\frac{N^{1/2}}{p^{1/4}q^{1/4}\log^{1/2} t}, \frac{dN}{p+q}, p, q\right\}\right), \quad 1 \leq N \leq t.$$

Proof In each sum in the definition of $C_k(s_n)$ at most $O(k(p+q)/d)$ summands $(-1)^{s_{n+d_1}} \cdots (-1)^{s_{n+d_k}}$ cannot be expressed with the Legendre symbol. If k is odd we can apply Lemma 1 with $f(X) = (X + g^{-d_1}) \cdots (X + g^{-d_k})$.

If $k = 2$, $d_1 \not\equiv d_2 \bmod p-1$ and $d_1 \not\equiv d_2 \bmod q-1$ we can apply Lemma 1 to estimate $\sum_{n=0}^{M-1}(-1)^{n+d_1}(-1)^{n+d_2}$ by $O(p^{1/2}q^{1/2}\log t + p + q)$. If $k = 2$, $d_1 \equiv d_2 \bmod p-1$ and $d_1 \not\equiv d_2 \bmod q-1$, then $f(X) = (X + g^{-d_1})(X + g^{-d_2})$ is a square modulo p but not modulo $q-1$. As in the proof of Lemma 1 we get

$$\begin{aligned} |S_N| &\leq p \log t \max_{1 \leq j < d, 0 \leq a < q} \left| \sum_{x=1}^{q-1} \left(\frac{f(g^n x)}{q}\right) e_{q-1}(a(p-1)^{-1}\mathrm{ind} x)\chi^j(x) \right| \\ &= O(pq^{1/2}\log t). \end{aligned}$$

Similarly, if $k = 2$, $d_1 \not\equiv d_2 \bmod p-1$ and $d_1 \equiv d_2 \bmod q-1$ we get

$$S_N = O(p^{1/2} q \log t).$$

If $k > 2$ and k is even we choose

$$\{d_1, \ldots, d_k\} = \{j_1(p-1) + j_2(q-1) : 0 \leq j_1, j_2 < k/2,\ j_2 \equiv 2j_1 \text{ or } 2j_1 + 1 \bmod k/2\}.$$

For fixed j_1 we have two different lags d_i, d_j with $d_i \equiv d_j \bmod (q-1)$ and for fixed j_2 two different d_i, d_j with $d_i \equiv d_j \bmod (p-1)$. Hence, we have

$$\sum_{n=0}^{M-1} \left(\frac{(g^{n+d_1}+1)\cdots(g^{n+d_k}+1)}{p}\right)\left(\frac{(g^{n+d_1}+1)\cdots(g^{n+d_k}+1)}{q}\right) \geq M - k.$$

Choosing $M = t - (k/2-1)(p+q-2)$ gives the assertion.

Finally, we prove the bound on the linear complexity profile. Put $L = L(s_n, N)$. Since the result is trivial otherwise we may assume that $L < \min\{p, q\} - 1$. We choose $c_0, \ldots, c_{L-1} \in \mathbb{F}_2$ such that

$$s_{n+L} = c_{L-1}s_{n+L-1} + \cdots + c_0 s_n, \quad 0 \leq n \leq N - L - 1.$$

Putting $c_L = 1$ we get for $0 \leq n \leq N - L - 1$ that

$$1 = \prod_{l=0}^{L} (-1)^{c_l s_{n+l}}, \quad 0 \leq n \leq N - L - 1.$$

We have

$$(-1)^{s_{n+l}} = \left(\frac{g^{n+l}+1}{p}\right)\left(\frac{g^{n+l}+1}{q}\right), \quad 0 \le l \le L,$$

for at least $N - L - (p+q-2)(L+1)/d$ different n with $0 \le n \le N-L-1$. Otherwise the right hand side is zero. Hence we get

$$\sum_{n=0}^{N-L}\left(\frac{f(g^n)}{p}\right)\left(\frac{f(g^n)}{q}\right) \ge N - L - (p+q-2)(L+1)/d,$$

where

$$f(X) = \prod_{l=0}^{L}(g^l X + 1)^{c_l}.$$

Since $L < \min\{p,q\} - 1$ the polynomial $f(X)$ is neither a square modulo p nor modulo q and Lemma 1 implies

$$N = O\left(L^2 p^{1/2} q^{1/2} \log t + L\frac{p+q}{d}\right)$$

and thus the result. □

5 Final remarks

1. For each balanced binary sequence (s_n) of period t we have

$$AC(l) \equiv t \bmod 4, \ 1 \le l \le t-1,$$

since if a_{ij} denotes the number of $0 \le n \le t-1$ with $s_n = i$ and $s_{n+l} = j$, then we have

$$AC(l) = \sum_{n=0}^{t-1}(-1)^{s_n + s_{n+l}} = a_{0,0} + a_{1,1} - a_{0,1} - a_{1,0} = 4a_{1,1} - t.$$

2. In the most important case, $d = 2$, for each l there are six different values of l' such that the sums $\sum_{y=1}^{q-1}\left(\frac{y(y+1)\left(g^{l'}y+1\right)}{q}\right)$ have the same absolute value. In some cases, for example if $l = (q-1)/2$, these sums can be exactly calculated, see [3].
3. Let us assume that $q - p$ is small and $d = 2$. We describe how the bound $L(s_n) \ge L(s_n, t) = \Omega(t^{1/4}\log^{-1/2} t)$ of Theorem 4 can be improved if t has a certain structure. Put

$$S(X) = \sum_{n=0}^{t-1} s_n X^t$$

and note that $L(s_n) = t - \deg(\gcd(X^t - 1, S(X))$, see [4].
If $t = 2^s r$ with an odd r, we have to count (in multiplicities) the number of rth roots of unity β with $S(\beta) = 0$.

We assume that r is small. Hence, we are only interested in the case $p \not\equiv q \bmod 4$ since $d = 2$. In this case we consider only $S(1)$ and get by Theorem 1

$$S(1) \equiv \frac{t}{2} + \frac{q-p}{4} - \frac{1}{2} \equiv \frac{q-p-2}{4} \bmod 2.$$

Now we have $S(1) \neq 0$ if and only if $q \equiv p + 6 \bmod 8$ and thus $L(s_n) \geq 2^s$ in this case, which is an improvement of $L(s_n) = \Omega(t^{1/4} \log^{-1/2} t)$ if, say, $q = 2^s r_1 + 1$ with $r_1 < t^{1/4} \log^{1/2} t \approx q^{1/2} \log^{1/2} q$.

4. The *k-error linear complexity* $L_k(s_n)$ of (s_n) is defined as

$$L_k(s_n) = \min_{(y_n)} L(y_n),$$

where the minimum is taken over all t-periodic sequences (y_n) over $\mathbb{F}_2$, for which the Hamming distance of the vectors $(s_0, s_1, \ldots, s_{t-1})$ and $(y_0, y_1, \ldots, y_{t-1})$ is at most k. We can also prove a lower bound on the k-error linear complexity of order of magnitude $\min\{t^{1/2} \log^{-1/2} t, t/k\}$, if $k = o(t)$ and $q - p$ is small.

5. It is easy to extend the concept of two-prime Sidel'nikov sequences to prime powers p^r and q^s using quadratic characters and two different primitive elements of $\mathbb{F}_{p^r}$ and $\mathbb{F}_{q^s}$. However, the generation of these sequences via evaluating the character values is slower than evaluating the Jacobi symbols $\left(\frac{\cdot}{p}\right)\left(\frac{\cdot}{q}\right)$ using the quadratic reciprocity law.

6. Apart from the two-prime generator and the two-prime Sidel'nikov sequence it is also natural to study the following related sequence (u_n) called *Legendre-Sidel'nikov sequence* defined by

$$u_n = \begin{cases} 1, & \text{if } p|n, \\ 0, & \text{if } n \equiv (q-1)\big/2 \bmod q-1,\ p \not| n, \\ \left(1 - \left(\frac{n}{p}\right)\left(\frac{g^n+1}{q}\right)\right)\big/2, & \text{otherwise,} \end{cases}$$

for $n \geq 0$. The autocorrelation of (u_n) has been studied in [9].

Acknowledgment The research of the authors has been supported by the Austrian science foundation (FWF) grants P-19004 and S9609.

References

1. Berndt B.C., Evans R.J., Williams K.S.: Gauss and Jacobi sums. Canadian Mathematical Society Series of Monographs and Advanced Texts. A Wiley-Interscience Publication. Wiley, New York (1998).
2. Brandstätter N., Winterhof A.: Some notes on the two-prime generator of order 2. IEEE Trans. Inform. Theory **51**(10), 3654–3657 (2005).
3. Burde, K.: Über allgemeine Sequenzen der Länge 3 von Legendresymbolen. (German) J. Reine Angew. Math. **272**, 203–216 (1974).
4. Cusick T.W., Ding C., Renvall A.: Stream ciphers and number theory. North-Holland Mathematical Library, vol. 66. Elsevier Science B.V., Amsterdam (2004).
5. Jungnickel D.: Finite fields. Structure and arithmetics. Bibliographisches Institut, Mannheim (1993).
6. Lidl R., Niederreiter H.: Finite fields. Encyclopedia of Mathematics and its Applications, vol. 20. Cambridge University Press, Cambridge (1997).
7. Mauduit C., Sárközy A.: On finite pseudorandom binary sequences. I. Measure of pseudorandomness, the Legendre symbol. Acta Arith. **82**(4), 365–377 (1997).
8. Sidel'nikov V. M.: Some k-valued pseudo-random sequences and nearly equidistant codes. Probl. Inf. Transm. **5**, 12–16 (1969) (translated from Problemy Peredači Informacii **5**, 16–22 (1969) (Russian)).
9. Su M., Winterhof A.: Autocorrelation of Legendre-Sidel'nikov sequences. IEEE Trans. Inform. Theory **56**(4), 1714–1718 (2010).

10. Topuzoğlu A., Winterhof A.: Pseudorandom sequences. In: Topics in Geometry, Coding Theory and Cryptography, Algebra and Applications, vol. 6, pp. 135–166. Springer, Dordrecht (2007).
11. Winterhof A.: Linear complexity and related complexity measures. In: Woungang I. et al. (eds.) Selected Topics in Information and Coding Theory. World Scientific, Singapore (2010).