On the linear complexity of Sidel'nikov Sequences over nonprime fields

Nina Brandstätter [a], Wilfried Meidl [b]

[a] *Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenbergerstrasse 69, 4040 Linz, Austria*

[b] *Sabancı University, MDBF, Orhanlı, 34956 Tuzla, İstanbul, Turkey*

Abstract

We introduce a generalization of Sidel'nikov sequences for arbitrary finite fields. We show that several classes of Sidel'nikov sequences over arbitrary finite fields exhibit a large linear complexity. For Sidel'nikov sequences over $\mathbb{F}_8$ we provide exact values for their linear complexity.

1 Introduction

For a prime power q let $\mathbb{F}_q$ be the finite field of order q and let d be a positive 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 primitive element α of $\mathbb{F}_q$.
For a prime divisor d of $q-1$, Sidel'nikov [24] introduced the $(q-1)$-periodic sequence $S = s_0, s_1, \ldots$ with terms in the finite field $\mathbb{F}_d$ (we will also write over the finite field $\mathbb{F}_d$) defined by

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

Independently in [16] Lempel, Cohn and Eastman studied the sequence (1) for $d = 2$.

In the following we suggest a natural generalization of the sequence (1) for arbitrary finite fields.

Suppose that the divisor $d = p^t$ of $q-1$ is a power of the prime p and let $\{\beta_0, \beta_1, \ldots, \beta_{t-1}\}$ be a basis of $\mathbb{F}_{p^t}$ over $\mathbb{F}_p$. Then we define the Sidel'nikov sequence $S = s_0, s_1, \ldots$ with period $q-1$ and terms in the finite field $\mathbb{F}_{p^t}$ by

$$\begin{aligned} s_n = \xi_j \quad &\Longleftrightarrow \quad \alpha^n + 1 \in D_j, \quad n = 0, \ldots, q-2, n \neq (q-1)/2, \\ s_{(q-1)/2} = 0, \quad &\text{and} \\ s_{n+q-1} = s_n, \quad &n \geq 0, \end{aligned} \tag{2}$$

where $\xi_j = j_0\beta_0 + j_1\beta_1 + \cdots + j_{t-1}\beta_{r-1}$ if $(j_0, j_1, \ldots, j_{t-1})_p$ is the p-ary representation of the integer j. We remark that the exact appearance of the Sidel'nikov sequence depends on the choice of the basis.

The *linear complexity* of an N-periodic sequence $S = s_0, s_1, \ldots$ over a finite field $\mathbb{F}_d$, denoted by $L(S)$, is the smallest nonnegative integer L for which there exist coefficients $c_1, c_2, \ldots, c_L \in \mathbb{F}_d$ such that

$$s_n + c_1 s_{n-1} + \ldots + c_L s_{n-L} = 0 \quad \text{for all } n \geq L.$$

The linear complexity is of fundamental importance as a complexity measure for periodic sequences used as a keystream for a stream cipher in cryptography (see [20], [21], [22], [23]).

The linear complexity of the binary Sidel'nikov sequence has been investigated in [13], [15] and [19]. For results on the linear complexity of the Sidel'nikov sequence defined by (1) for an arbitrary prime divisor d of $q-1$ we can refer to [4].

Since the finite field $\mathbb{F}_q$, $q = u^m$, plays an important role in the construction of the Sidel'nikov sequence S given by (1), it is also reasonable to interpret S as a sequence over the prime field $\mathbb{F}_u$. Results on the linear complexity of this sequence can be found in [7], [8], [11], [12] if $d = 2$, and in [2], [5] and [14] for arbitrary divisors d of $q-1$ (in this case d need not necessarily be a prime).

In this article we investigate the linear complexity of the generalization (2) of the Sidel'nikov sequence for arbitrary finite fields. After recalling some basic facts and techniques in Section 2, in Section 3 we establish good lower bounds on the linear complexity for several classes of sequences of the form (2). In Section 4 we present exact values for the linear complexity of Sidel'nikov sequences over $\mathbb{F}_8$.

2 Preliminaries

Let $d = p^t$ be a power of the prime p and let $S = s_0, s_1, \ldots$ be an N-periodic sequence over the finite field $\mathbb{F}_d$. 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 linear complexity $L(S)$ of the sequence S is then given by (cf. [6, Lemma 8.2.1])

$$L(S) = N - \deg(\gcd(X^N - 1, S(X))). \tag{3}$$

If $N = p^s r$ with $\gcd(p, r) = 1$, then we have $X^N - 1 = (X^r - 1)^{p^s}$. 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 $S(X)$. The multiplicity of roots of the polynomial $S(X)$ can be determined with the kth *Hasse derivative* (cf. [10]) $S(X)^{(k)}$ of $S(X)$, which is defined by

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

The multiplicity of γ as root of $S(X)$ is v if $S(\gamma) = S(\gamma)^{(1)} = \ldots = S(\gamma)^{(v-1)} = 0$ and $S(\gamma)^{(v)} \neq 0$ (cf. [17, Lemma 6.51]).
Consequently we are interested in the Hasse derivatives of the polynomial $S(X)$ which corresponds to the sequence (2):
The binomial coefficients modulo p appearing in $S(X)^{(k)}$ can be evaluated with *Lucas' congruence* (cf. [9,18])

$$\binom{n}{k} \equiv \binom{n_0}{k_0} \cdots \binom{n_c}{k_c} \bmod p,$$

if $n_0, ..., n_c$ and $k_0, ..., k_c$ are the digits in the p-ary representation of n and k, respectively. We immediately see that

$$\binom{n}{k} \equiv \binom{i}{k} \bmod p$$

for $k < p^c \leq d^l$ 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 we refer to [3,25].) Then for the kth Hasse derivative at 1 of the polynomial $S(X)$ corresponding to the sequence (2) we obtain

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

where $l = 1$ if $k = 0$ and $l = \lfloor \log_d(k) \rfloor + 1$ if $k \geq 1$.

Remark. As a more general result (which will not be used in this article since in general the determination of cyclotomic numbers of order δ is difficult if δ is not small) one can show that for a primitive rth root of unity γ over $\mathbb{F}_d$ we have

$$S(\gamma)^{(k)} = \sum_{h=0}^{r-1} \sum_{i=k}^{d^l-1} \binom{i}{k} \sum_{j=0}^{d^{l-1}r-1} \sum_{m=1}^{d-1} (u(h,i), dj+m)_{d^l r} \xi_m \gamma^h, \tag{5}$$

where $u(h,i)$ is (by the Chinese-Remainder-Theorem) the unique integer u with $0 \leq u \leq d^l r - 1$, $u \equiv h + k \bmod r$, and $u \equiv i \bmod d^l$. For details on the determination of formula (5) for prime fields we refer to [4,19].

For the construction of Sidel'nikov sequences of the form (2) with guaranteed large linear complexity we need bases of $\mathbb{F}_d$ over $\mathbb{F}_p$ with some special properties.

Let $\mathrm{Tr}(\xi)$ denote the trace function from $\mathbb{F}_d$ into its prime field $\mathbb{F}_p$. We call a basis $\{\beta_0, \beta_1, \ldots, \beta_{t-1}\}$ of $\mathbb{F}_{p^t}$ over $\mathbb{F}_p$ such that $\mathrm{Tr}(\beta_j) = 0$ for $1 \leq j \leq t-1$ and $\mathrm{Tr}(\beta_0) = 1$ a *one trace-one basis*.
As it is generally known, each finite field $\mathbb{F}_{p^t}$ has a normal basis $\mathcal{N} = \{\beta, \beta^p, \beta^{p^2}, \ldots, \beta^{p^{t-1}}\}$. Since otherwise the elements of $\mathcal{N}$ are linearly dependent over $\mathbb{F}_p$, the element β satisfies $\mathrm{Tr}(\beta) = c \neq 0$, and hence all elements of $\mathcal{N}$ have trace c. Consequently the basis $\mathcal{B} = \{c^{-1}\beta, \beta^p - \beta, \beta^{p^2} - \beta, \ldots, \beta^{p^{t-1}} - \beta\}$ is a one trace-one basis of $\mathbb{F}_{p^t}$ over $\mathbb{F}_p$.

For efficient calculation purposes one is interested in polynomial bases $\mathcal{P} = \{1, \beta, \beta^2, \ldots, \beta^{t-1}\}$ such that the minimal polynomial $f(X)$ of β over $\mathbb{F}_p$ has a small number of nonzero coefficients. In [1] Ahmadi and Menezes investigated polynomial one trace-one bases for the important case that $p = 2$:
Let $f(X) \in \mathbb{F}_p[X]$ be an irreducible trinomial (pentanomial) of degree t, i.e. a polynomial which has only three (five) nonzero coefficients, and let β be a root of $f(X)$, then $\mathcal{P} = \{1, \beta, \beta^2, \ldots, \beta^{t-1}\}$ is called a *trinomial (pentanomial) basis* of $\mathbb{F}_{p^t}$ over $\mathbb{F}_p$. Ahmadi and Menezes showed conditions under which irreducible trinomials and pentanomials, respectively, correspond to a basis $\mathcal{P}$ containing exactly one element having trace 1. Clearly, if the extension degree t is odd, then $\mathrm{Tr}(1) = 1$. For each of the 545 extension degrees $t \in [2, 1000]$ for which a trinomial basis with just one element having trace one exists, Ahmadi and Menezes presented a corresponding irreducible trinomial of degree t, and for all extension degrees $6 \leq t \leq 809$, they provided an irreducible pentanomial

for which the corresponding pentanomial basis has only one element with trace one.

3 Lower bounds on the linear complexity

In this section we establish lower bounds on the linear complexity of Sidel'nikov sequences $S = s_0, s_1 \ldots$ of the form (2). We assume that the Sidel'nikov sequence S over $\mathbb{F}_{p^t}$ is constructed with a (not necessarily polynomial) one trace-one basis $\mathcal{B} = \{\beta_0, \ldots, \beta_{t-1}\}$ of $\mathbb{F}_{p^t}$ over $\mathbb{F}_p$. We will use the following lemma.

Lemma 1 *Let χ_p denote the nontrivial multiplicative character of $\mathbb{F}_q$ with $\chi_p(\alpha^k) = \mathrm{e}^{2\pi\sqrt{-1}k/p}$, and let $\varepsilon_p = \mathrm{e}^{2\pi\sqrt{-1}/p}$. Then*

$$\varepsilon_p^{\mathrm{Tr}(s_n)} = \chi_p(\alpha^n + 1), \quad 0 \le n \le q-2,\ n \ne (q-1)/2. \tag{6}$$

Proof. Since we suppose that $\mathrm{Tr}(\beta_0) = 1$ and $\mathrm{Tr}(\beta_j) = 0$ for $1 \le j \le t-1$, we have $\mathrm{Tr}(s_n) = j_0$ if $s_n = j_0\beta_0 + j_1\beta_1 + \cdots + j_{t-1}\beta_{t-1}$. The identity (6) follows then from the definition of the Sidel'nikov sequence (2). □

With the next two propositions we can exclude some special $(q-1)$-th roots of unity of being roots of $S(X)$. This enables us in the following to establish good lower bounds on the linear complexity of Sidel'nikov sequences constructed with a one trace-one basis for several classes of period lengths.

Proposition 2 *Let $r \ne p$ be a prime divisor of $q-1$. If p^t is a primitive root modulo r and $r \ge q^{1/2} + 1$, then for each r-th root of unity $\gamma \ne 1$ we have $S(\gamma) \ne 0$.*

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

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

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

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

Therefore we must have

$$\mathrm{Tr}\left(\sum_{j=0}^{(q-1)/r-1} s_{h+jr}\right) = \mathrm{Tr}\left(\sum_{j=0}^{(q-1)/r-1} s_{jr}\right)$$

or equivalently

$$\sum_{j=0}^{(q-1)/r-1} \mathrm{Tr}(s_{h+jr}) = \sum_{j=0}^{(q-1)/r-1} \mathrm{Tr}(s_{jr})$$

for all $h = 1, \ldots, r-1$. We note that

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

Hence with (6) we obtain that

$$\varepsilon_p^{\sum_{j=0}^{(q-1)/r-1} \mathrm{Tr}(s_{h+jr})} = \prod_{j=0}^{(q-1)/r-1} \chi_p(\alpha^{h+jr} + 1) = \chi_p(1 - \alpha^{h(q-1)/r})$$

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

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

by Weil's bound for character sums (see e.g. [17, Theorem 5.41]) contradicting our assumption on r. □

For odd characteristic we also have to consider $2r$-th roots of unity.

Proposition 3 *Let $p > 2$ and let $r \neq p$ be a prime divisor of $q - 1$. If p^t is a primitive root modulo r and*

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

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

Proof. For $\gamma^r = 1$ the statement follows from Proposition 2.

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

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

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 γ over $\mathbb{F}_{p^t}$, and that $S(\gamma) = 0$ 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 $G(h)$. Then it is obvious that $G(h+r) = -G(h)$ and that $G(0) = G(2) = \ldots = G(2r-2) = -G(1) = -G(3) = \ldots = -G(2r-1)$. Hence,

$$\begin{aligned} 2(r-1) \min_{0 \le a \le p-1} |\cos 2\pi a/p| &\le \left| (r-1) \left(\varepsilon_p^{\mathrm{Tr}(G(0))} + \varepsilon_p^{-\mathrm{Tr}(G(0))} \right) \right| \\ &= \left| \sum_{\substack{h=1 \\ h \ne r}}^{2r-1} \varepsilon_p^{\mathrm{Tr}\left(\sum_{j=0}^{(q-1)/r-1} (-1)^j s_{h+jr} \right)} \right|. \end{aligned} \tag{7}$$

Note that

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

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

$$\begin{aligned} \varepsilon_p^{\mathrm{Tr}\left(\sum_{j=0}^{(q-1)/r-1} (-1)^j s_{h+jr} \right)} &= \varepsilon_p^{\sum_{j=0}^{(q-1)/r-1} (-1)^j \mathrm{Tr}\left(s_{h+jr} \right)} \\ &= \prod_{j=0}^{(q-1)/r-1} \chi_p(\alpha^{h+jr} + 1)^{(-1)^j} = \chi_p(f(\alpha^h)). \end{aligned}$$

Now, together with (7) this yields

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

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

Propositions 2 and 3, and equation (3) immediately yield the following lower bounds for the linear complexity of the Sidel'nikov sequence S defined by (2) constructed with a one trace-one basis.

Theorem 4 *Suppose that $q - 1 = 2^s u r$, $u \ne r$, u odd, for a prime $r \ge q^{1/2} + 1$ and suppose that $d = 2^t$ is a primitive root modulo r. Then the linear*

complexity of the Sidel'nikov sequence S over $\mathbb{F}_d$ satisfies

$$L(S) \geq (r-1)2^s.$$

Example. Let $t = 3$ and S be the Sidel'nikov sequence over $\mathbb{F}_{2^3}$ of length $q - 1 = 2^3 * 11 = 88$. Then we have $L(S) \geq 80$.

Theorem 5 *Let $p > 2$ and $q - 1 = 2p^s ur$, $u \neq r$, u odd with $\gcd(u, p) = 1$, for a prime r with*

$$r \geq q^{1/2} \frac{1}{\min_{0 \leq a \leq p-1} |\cos 2\pi a/p|} + 1,$$

and suppose that $d = p^t$ is a primitive root modulo r. Then the linear complexity of the Sidel'nikov sequence S over $\mathbb{F}_d$ satisfies

$$L(S) \geq 2(r-1)p^s.$$

Example. Suppose $d = 3^3$ and let S be the Sidel'nikov sequence over $\mathbb{F}_{3^3}$ of length $q - 1 = 2 * 3^3 * 233 = 12582$, then $L(S) \geq 12528$.

Example. Suppose $d = 5^3$ and let S be the Sidel'nikov sequence over $\mathbb{F}_{5^3}$ of length $q - 1 = 2 * 5^3 * 2753 = 688248$, then $L(S) \geq 688000$.

4 Linear complexity for Sidel'nikov sequences over $\mathbb{F}_8$

Let β be a root of the polynomial $X^3 + X + 1 \in \mathbb{F}_2[X]$, then the basis $\mathcal{B} = \{1, \beta, \beta^2\}$ of $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3+X+1)$ satisfies $\mathrm{Tr}(1) = 1$ and $\mathrm{Tr}(\beta) = \mathrm{Tr}(\beta^2) = 0$.
Let $q = 8t + 1$ be a prime power, then we can consider the $(q-1)$-periodic Sidel'nikov sequence $S = s_0, s_1, \ldots$ over $\mathbb{F}_8$ defined as in (2) with the basis $\mathcal{B}$. Let $S(X) = s_0 + s_1 X + \cdots + s_{q-2} X^{q-2}$ be the polynomial corresponding to this Sidel'nikov sequence. Then we can determine the multiplicity of 1 as a root of $S(X)$ with equation (4), which in the considered case reduces to

$$S(1)^{(k)} = \sum_{i=k}^{7} \binom{i}{k} \sum_{m=1}^{7} (i, m)_8 \xi_m \tag{8}$$

for $0 \leq k \leq 7$. The cyclotomic numbers of order 8 contained in (8) are given in terms of the parameters x, y, a, b for which we have

$$q = x^2 + 4y^2 = a^2 + 2b^2, x \equiv a \equiv 1 \bmod 4,$$

and if $q = p^m$ with a prime $p \equiv 1 \bmod 4$ additionally $\gcd(q, x) = 1$, and $\gcd(a, q) = 1$ if $q = p^m$ with a prime $p \equiv 1$ or $3 \bmod 8$. Tables for the cyclotomic numbers of order 8 can be found in [3,6,25]. We recall these tables in the appendix at the end of this paper, and note that the sign of y is ambiguously determined, which is a consequence of the freedom to choose the primitive element α of $\mathbb{F}_q$. Since the cyclotomic numbers take different values, we have to distinguish between the cases Ia where $q \equiv 1 \bmod 16$ and 2 is a fourth power in $\mathbb{F}_q$, Ib where $q \equiv 1 \bmod 16$ and 2 is not a fourth power in $\mathbb{F}_q$, IIa where $q \equiv 9 \bmod 16$ and 2 is a fourth power in $\mathbb{F}_q$, and IIb where $q \equiv 9 \bmod 16$ and 2 is not a fourth power in $\mathbb{F}_q$. The next proposition deals with the case that $q \equiv 1 \bmod 16$. In the proof we will not go into all technical details.

Proposition 6 *Suppose that* $q \equiv 1 \bmod 16$. *Then*

(i) $X - 1$ *divides* $\gcd(X^{q-1} - 1, S(X))$,
(ii) $(X-1)^2$ *divides* $\gcd(X^{q-1} - 1, S(X))$ *if and only if* $4|y$,
(iii) $(X-1)^3$ *divides* $\gcd(X^{q-1} - 1, S(X))$ *if and only if* $4|y$ *and* $8|b$,
(iv) $(X-1)^4$ *divides* $\gcd(X^{q-1} - 1, S(X))$ *if and only if* $4|y$, $8|b$ *and* $(x-1)/8 \equiv y/4 \bmod 2$,
(v) $(X-1)^k$, $k = 5, 6, 7, 8$, *divides* $\gcd(X^{q-1} - 1, S(X))$ *if and only if* $4|y$, $8|b$ *and* $(x-1)/8 \equiv y/4 \equiv 0 \bmod 2$.

Proof. With (8) and the first table in the appendix we obtain

$$\begin{aligned} S(1) = &[(0,1)_8 + (0,3)_8 + (0,5)_8 + (0,7)_8]\beta \\ &+[(0,1)_8 + (0,2)_8 + (0,3)_8 + (0,5)_8 + (0,6)_8 \\ &+(0,7)_8 + (1,2)_8 + (1,3)_8 + (1,6)_8 + (2,5)_8]\beta^2. \end{aligned}$$

First we suppose that 2 is a fourth power of $\mathbb{F}_q$ and use the table in the appendix giving the cyclotomic numbers for the considered case to calculate the coefficients of β and β^2 in $S(1)$. Putting $\Delta = q - 7 + 2x + 4a$, for the coefficient of β we obtain

$$\begin{aligned} &(0,1)_8 + (0,3)_8 + (0,5)_8 + (0,7)_8 \\ &= \frac{\Delta + 16y + 16b}{64} + \frac{\Delta - 16y + 16b}{64} + \frac{\Delta + 16y - 16b}{64} + \frac{\Delta - 16y - 16b}{64} \\ &= \frac{y}{2} + \frac{y}{2} = 0, \end{aligned}$$

where the calculation is performed modulo 2. Since in the considered case $(1,2)_8 = (2,5)_8$ and $(1,3)_8 = (1,6)_8$, the coefficient of β^2 reduces to

$$(0,2)_8 + (0,6)_8 = \frac{q - 7 + 6x + 16y}{64} + \frac{q - 7 + 6x - 16y}{64} = \frac{y}{2} = 0,$$

where in the last step we use that 2 is a fourth power of $\mathbb{F}_q$ if and only if $4|y$ (cf. Theorem 7 in [25]). If 2 is not a fourth power in $\mathbb{F}_q$ then $(0,1)_8 = (0,3)_8 = (0,5)_8 = (0,7)_8$ and the coefficient of β in $S(1)$ vanishes. Since $(1,2)_8 = (2,5)_8$, the coefficient of β^2 reduces to

$$\begin{aligned}
&(0,2)_8 + (0,6)_8 + (1,3)_8 + (1,6)_8 \\
&= \frac{q-7-2x-8a-16y}{64} + \frac{q-7-2x-8a+16y}{64} + \\
&\quad \frac{q+1+2x-4a-16b}{64} + \frac{q+1+2x-4a-16b}{64} \\
&= \frac{y+b}{2}.
\end{aligned}$$

We also have

$$\frac{y+b}{2} = \sum_{m=0}^{7} (1,m)_8 \equiv 0 \bmod 2, \tag{9}$$

which is one of the elementary relationships between the cyclotomic numbers (cf. Lemma 3(d) of [25]). Consequently $X-1$ divides $\gcd(X^{q-1}-1, S(X))$. The coefficients of 1, β and β^2 in $S(1)^{(k)}$, $k = 1, \ldots 7$, are obtained similarly with (8) and the tables in the appendix giving the cyclotomic numbers of order 8. The results relevant for our considerations are listed below in Table 1 and Table 2. In the case that 2 is not a fourth power in $\mathbb{F}_q$, i.e. $4 \not| y$, $(X+1)^2$ does not divide $S(X)$ since (9) implies that $b/2$ is odd, which is the coefficient of β in $S(1)^{(1)}$. Hence in the following we suppose that $4|y$. Therefore, from (9) we get $4|b$. From Table 1 we see that $S(1)^{(1)} = (b/2)\beta = 0$. Moreover, $S(1)^{(2)} = (b/4)\beta^2 = 0$ if and only if $8|b$. Supposing that $8|b$ we obtain $S(1)^{(3)} = ((1-x)/8 - y/4)\beta^2$, which vanishes if and only if $(x-1)/8 \equiv y/4 \bmod 2$. This yields the conditions for $(X+1)^k$ dividing $\gcd(X^{q-1}-1, S(X))$, $k = 1, 2, 3, 4$. If $16|(q-1)$ and 2 is a fourth power in $\mathbb{F}_q$ then $16|(x-a)$ which can be seen from $(2,5)_8 - (2,4)_8 = (x-a)/16$. Therefore, assuming that $8|b$, we obtain that $S(1)^{(4)} = (y/4)\beta^2$, which vanishes if and only if $y/4 \equiv 0 \bmod 2$. As it is easy to see, under the above established conditions, namely $8|b$ and $(x-1)/8 \equiv y/4 \equiv 0 \bmod 2$, all (further) coefficients in Table 1 are zero, which completes the proof of the proposition. □

For the case that $q \equiv 9 \bmod 16$ we obtain the following proposition.

Proposition 7 *Suppose that* $q \equiv 9 \bmod 16$. *Then* $X-1$ *divides* $\gcd(X^{q-1}-1, S(X))$ *and* $(X-1)^2$ *does not divide* $\gcd(X^{q-1}-1, S(X))$.

Proof. We start with the observation that $q = x^2 + 4y^2 \equiv 9 \bmod 16$, $x \equiv 1 \bmod 4$, implies $x \equiv 5 \bmod 8$.
First we consider the case that 2 is a fourth power in $\mathbb{F}_q$, or equivalently $4|y$, and point out that then $4 \not| b$. From $(2,1)_8 - (0,0)_8 = (4+x-a)/16$ we see that $8|(4+x-a)$. Suppose that $4|b$, then $(1,2)_8 - (1,3)_8 = (-x+a+$

$2b)/8 = (-x+a)/8+b/4$ and $8|(x-a)$ which is a contradiction. With Table 3 (the polynomials in Table 3 and Table 4 are again obtained with (8) and the adequate tables in the appendix) we obtain that $S(1) = ((1-x)/4+b/2))\beta^2$ which vanishes since $x \equiv 5 \bmod 8$ implies $(x-1)/4 \equiv 1 \bmod 2$. Since the coefficient of β (and β^2) in $S(1)^{(1)}$ equals $(y+b)/2 \equiv 1 \bmod 2$, the polynomial $(X+1)^2$ does not divide $\gcd(X^{q-1}-1, S(X))$.
If 2 is not a fourth power in $\mathbb{F}_q$, then with Table 4 we get $((x+1+2a)/4)\beta^2$ for $S(1)$. From $x \equiv 5 \bmod 8$ we obtain $8|(x+1+2a)$, and consequently $S(1) = 0$. Since the coefficient of β^2 in $S(1)^{(1)}$ equals $y/2 \equiv 1 \bmod 2$, the polynomial $(X+1)^2$ again does not divide $\gcd(X^{q-1}-1, S(X))$. □

Before we state the main result of this section we need to show a numbertheoretical lemma.

Lemma 8 *If the prime $q = x^2+4y^2 \equiv 1 \bmod 16$, $x \equiv 1 \bmod 4$, is of the form $q = 2^s r+1$ for a prime $r \neq 3$ such that 8 is a primitive root modulo r, then we either have $x \equiv 1 \bmod 16$ and $4|y$, or $x \equiv 9 \bmod 16$ and $4 \not| y$.*

Proof. Clearly $8 = 2^3$ can only be a primitive root modulo a prime r if $\gcd(3, r-1) = 1$, which implies $r = 3$ or $r \equiv 2 \bmod 3$. For a prime $r \equiv 2 \bmod 3$ the number $q = 2^s r+1$ is not divisible by 3 if and only if s is odd. Consequently the prime q must be of the form $q = 2^s r+1$ with an odd integer s.
We recall that $q \equiv 1 \bmod 16$ implies $x \equiv 1 \bmod 8$, and consider the case that $x \equiv 9 \bmod 16$ and $4|y$. In this case we have $q = (9+16k)^2+64l^2 = 2^4(5+18k+16k^2+4l^2)+1$ for some integers k, l. Thus $s = 4$ is even, which contradicts q being a prime. With the same argument we see that $x \equiv 1 \bmod 16$ and $4 \not| y$ implies $s = 4$, which leads to the same contradiction. □

We are now able to obtain exact values for the linear complexity of the Sidel'nikov sequence over $\mathbb{F}_8$ for certain period lengths.

Theorem 9 *Let $q \equiv 1 \bmod 8$ be a prime with $q = x^2+4y^2 = a^2+2b^2, x \equiv a \equiv 1 \bmod 4$, and let S be the $(q-1)$-periodic Sidel'nikov sequence over $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3+X+1)$ defined by (2) with the basis $\mathcal{B} = \{1, \beta, \beta^2\}$, where β is a root of the polynomial X^3+X+1. If q is of the form $q = 2^s r+1$, $s > 3$, where $r \geq q^{1/2}+1$ is an odd prime such that 8 is a primitive root modulo r, then the linear complexity $L(S)$ of S satisfies*

(i) $L(S) = q-2$ *if* $4 \not| y$,
(ii) $L(S) = q-3$ *if* $4|y$ *and* $8 \not| b$,
(iii) $L(S) = q-4$ *if* $4|y$, $8 \not| y$ *and* $8|b$,
(iv) $q-1-2^s \leq L(S) \leq q-9$ *if* $8|y$ *and* $8|b$.

If q is of the form $q = 8r+1$ with an odd prime $r \geq q^{1/2}+1$ such that 8 is a primitive root modulo r, then $L(S) = q-2$.

Proof. The case where $q = 8r + 1$ immediately follows from Propositions 2 and 7, and equation (3).
The statements (i) and (ii) immediately follow from Proposition 2, Proposition 6(i)–(iii), and equation (3).
If $4|y$ then by Lemma 8 we have $(x-1)/8 \equiv y/4 \bmod 2$ if and only if $y/4 \equiv 0 \bmod 2$. Therefore (iii) of Proposition 6 coincides with $8 \not| y$, (iv) of Proposition 6 is not possible for the considered class of primes, and (v) of Proposition 6 coincides with $8|y$. Together with Proposition 2 and equation (3) we obtain then the statements (iii) and (iv) of the theorem. □

Example.

(1) $q = 1697 = 2^5 * 53 + 1$. We have $x = 41$, $y = 2$, $a = -27$, $b = 22$. Hence, $L(S) = q - 2 = 1695$.
(2) $q = 1889 = 2^5 * 59 + 1$. We have $x = 17$, $= y = 20$, $a = 33$, $b = 20$. Hence, $L(S) = q - 3 = 1886$.
(3) $q = 288257 = 2^9 * 563 + 1$. We have $x = -31$, $y = 268$, $a = 513$, $b = 112$. Hence, $L(S) = q - 4 = 288253$.
(4) $q = 8609 = 2^5 * 269 + 1$. We have $x = -47$, $y = 40$, $a = 81$, $b = 32$. Hence, $q - 1 - 2^s = 8576 \leq L(S) \leq q - 9 = 8600$.
(5) $q = 89 = 2^3 * 11 + 1$. Hence, $L(S) = q - 2 = 87$.

Table 1: Subcase Ia.

$S(1) = \frac{y}{2}\beta^2$	$S(1)^{(4)} = \frac{y}{2} + \frac{b}{4}\beta + \frac{x+2y-a}{8}\beta^2$
$S(1)^{(1)} = \frac{b}{2}\beta + \frac{y}{2}\beta^2$	$S(1)^{(5)} = \frac{y}{2} + \frac{1-x-2y-2b}{8}\beta + \frac{x-a}{8}\beta^2$
$S(1)^{(2)} = \frac{b}{2} + \frac{y+b}{2}\beta + \frac{b}{2}\beta^2$	$S(1)^{(6)} = \frac{1-x-2y-2b}{8} + \frac{b}{4}\beta + \frac{b}{4}\beta^2$
$S(1)^{(3)} = \frac{b}{2} + \frac{b}{2}\beta + \frac{1-x-2y-2b}{8}\beta^2$	$S(1)^{(7)} = \frac{1-x-2y-2b}{8}(1 + \beta + \beta^2)$

Table 2: Subcase Ib. $S(1) = \frac{y+b}{2}\beta^2 \quad S(1)^{(1)} = \frac{y}{2}\beta + \frac{y+b}{2}\beta^2$
Table 3: Subcase IIa. $S(1) = \frac{y}{2}\beta + \frac{1-x+2b}{4}\beta^2 \quad S(1)^{(1)} = \frac{y}{2} + \frac{y+b}{2}\beta + \frac{y+b}{2}\beta^2$
Table 4: Subcase IIb. $S(1) = \frac{1+x+2a}{4}\beta^2 \quad S(1)^{(1)} = \frac{b}{2}\beta + \frac{y}{2}\beta^2$

References

[1] O. Ahmadi, A. Menezes, On the number of trace-one elements in polynomial bases for $\mathbb{F}_{2^n}$, Designs, Codes and Cryptography 37 (2005), 493–507.

[2] H. Aly, W. Meidl, On the linear complexity and k-error linear complexity over $\mathbb{F}_p$ of the d-ary Sidel'nikov sequence, IEEE Trans. Inform. Theory, to appear.

[3] 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.

[4] N. Brandstätter and W. Meidl, "On the linear complexity of Sidel'nikov sequences over $\mathbb{F}_d$," in *Proceedings of SETA'06, Lecture Notes in Computer Science* 4086 (G. Gong et al., Eds.), Springer-Verlag, Berlin Heidelberg, 2006, pp. 47–60.

[5] J.H. Chung, K. Yang, "Bounds on the linear complexity and the 1-error linear complexity over $\mathbb{F}_p$ of M-ary Sidel'nikov sequences," in *Proceedings of SETA'06, Lecture Notes in Computer Science* 4086 (G. Gong et al., Eds.), Springer-Verlag, Berlin Heidelberg, 2006, pp. 74–87.

[6] T. W. Cusick, C. Ding, and A. Renvall, Stream Ciphers and Number Theory, North-Holland Publishing Co., Amsterdam, 1998.

[7] Y. Eun, H. Song, and G. Kyureghyan, "One-error linear complexity over $\mathbb{F}_p$ of Sidel'nikov Sequences," in *Proceedings of SETA'04, Lecture Notes in Computer Science* 3486 (T. Helleseth et al., Eds.), Springer-Verlag, Berlin Heidelberg, 2005, pp. 154–165.

[8] M.Z. Garaev, F. Luca, I.E. Shparlinski, and A. Winterhof, "On the linear complexity over $\mathbb{F}_p$ of Sidelnikov Sequences," *IEEE Trans. Inform. Theory* 52, pp. 3299–3304, 2006.

[9] 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.

[10] H. Hasse, Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit vollkommenem Konstantenkörper bei beliebiger Characteristik, J. Reine Angew. Math. Vol. 175 (1936), pp. 50–54.

[11] T. Helleseth, S.-H. Kim, and J.-S. No, "Linear complexity over $\mathbb{F}_p$ and trace representation of Lempel-Cohn-Eastman sequences," *IEEE Trans. Inform. Theory* 49, pp. 1548–1552, 2003.

[12] T. Helleseth, M. Maas, J.E. Mathiassen, and T. Segers, "Linear complexity over $\mathbb{F}_p$ of Sidel'nikov sequences," *IEEE Trans. Inform. Theory* 50, pp. 2468–2472, 2004.

[13] T. Helleseth and K. Yang, "On binary sequences with period $n = p^m - 1$ with optimal autocorrelation," in *Proceedings of SETA'01*, (T. Helleseth, P. Kumar, and K. Yang, Eds.), Springer-Verlag, Berlin Heidelberg, 2002, pp. 209–217.

[14] Y.-S. Kim, J.-S. Chung, J.-S. No, and H. Chung, "On the linear complexity over $\mathbb{F}_p$ of M-ary Sidel'nikov sequences," in *Proceedings 2005 IEEE Inter. Symp. Inform. Theory* (ISIT 2005), pp. 2007–2011, 2005.

[15] G. M. Kyureghyan and A. Pott, "On the linear complexity of the Sidelnikov-Lempel-Cohn-Eastman sequences," *Designs, Codes, and Cryptography* 29, pp. 149–164, 2003.

[16] A. Lempel, M. Cohn, and W. L. Eastman, "A class of balanced binary sequences with optimal autocorrelation properties," *IEEE Trans. Inform. Theory* 23, pp. 38–42, 1977.

[17] R. Lidl, H. Niederreiter, Finite Fields, Addison-Wesley, Reading, MA, 1983.

[18] M.E. Lucas, "Sur les congruences des nombres euleriennes et des coefficients differentiels des functions trigonometriques, suivant un-module premier," *Bull. Soc. Math. France* 6, pp. 49–54, 1878.

[19] W. Meidl and A. Winterhof, "Some notes on the linear complexity of Sidel'nikov-Lempel-Cohn-Eastman sequences," *Designs, Codes, and Cryptography* 38, pp. 159–178, 2006.

[20] H. Niederreiter, "Some computable complexity measures for binary sequences," in *Proceedings of SETA'98*, (C. Ding, T. Helleseth, and H. Niederreiter, Eds.), London: Springer-Verlag, 1999, pp. 67–78.

[21] H. Niederreiter, "Linear complexity and related complexity measures for sequences," in *Progress in cryptology—INDOCRYPT 2003, Lecture Notes in Computer Science* 2904, (T. Johansson, S. Maitra, Eds.), Berlin, Germany: Springer-Verlag, 2003, pp. 1–17.

[22] R. A. Rueppel, Analysis and Design of Stream Ciphers, Springer-Verlag, Berlin, 1986.

[23] R. A. Rueppel, "Stream ciphers," in *Contemporary Cryptology: The Science of Information Integrity*, (G.J. Simmons, Ed.) New York: IEEE Press, 1992, pp. 65–134.

[24] V. M. Sidel'nikov, "Some k-valued pseudo-random sequences and nearly equidistant codes" *Problems of Information Transmission* 5, pp. 12–16, 1969.; translated from *Problemy Peredači Informacii* 5, pp. 16–22, 1969, (Russian).

[25] T. Storer, Cyclotomy and Difference Sets, Markham Publishing Co., Chicago, III. (1967).

5 Appendix

Case I: The relation between the cyclotomic numbers of order 8 if $q \equiv 1 \bmod 16$:

$$
\begin{array}{ll}
(0,1)_8 = (1,0)_8 = (7,7)_8; & (0,2)_8 = (2,0)_8 = (6,6)_8 \\
(0,3)_8 = (3,0)_8 = (5,5)_8; & (0,4)_8 = (4,0)_8 = (4,4)_8 \\
(0,5)_8 = (5,0)_8 = (3,3)_8; & (0,6)_8 = (6,0)_8 = (2,2)_8 \\
(0,7)_8 = (7,0)_8 = (1,1)_8 &
\end{array}
$$

$$
\begin{array}{l}
(1,2)_8 = (2,1)_8 = (1,7)_8 = (7,1)_8 = (6,7)_8 = (7,6)_8 \\
(1,3)_8 = (3,1)_8 = (2,7)_8 = (7,2)_8 = (5,6)_8 = (6,5)_8 \\
(1,4)_8 = (4,1)_8 = (3,7)_8 = (7,3)_8 = (4,5)_8 = (5,4)_8 \\
(1,5)_8 = (5,1)_8 = (3,4)_8 = (4,3)_8 = (4,7)_8 = (7,4)_8 \\
(1,6)_8 = (6,1)_8 = (2,3)_8 = (3,2)_8 = (5,7)_8 = (7,5)_8 \\
(2,4)_8 = (4,2)_8 = (2,6)_8 = (6,4)_8 = (4,6)_8 = (6,4)_8 \\
(2,5)_8 = (5,2)_8 = (3,5)_8 = (5,3)_8 = (3,6)_8 = (6,3)_8
\end{array}
$$

The cyclotomic numbers of order 8 for the case that $q \equiv 1 \bmod 16$, $q = x^2 + 4y^2 = a^2 + 2b^2, x \equiv a \equiv 1 \bmod 4$:

Case Ia: 2 is a fourth power in $\mathbb{F}_q$

$$
\begin{array}{l}
(0,0)_8 = (q - 23 - 18x - 24a)/64 \\
(0,1)_8 = (q - 7 + 2x + 4a + 16y + 16b)/64 \\
(0,2)_8 = (q - 7 + 6x + 16y)/64 \\
(0,3)_8 = (q - 7 + 2x + 4a - 16y + 16b)/64 \\
(0,4)_8 = (q - 7 - 2x + 8a)/64 \\
(0,5)_8 = (q - 7 + 2x + 4a + 16y - 16b)/64 \\
(0,6)_8 = (q - 7 + 6x - 16y)/64 \\
(0,7)_8 = (q - 7 + 2x + 4a - 16y - 16b)/64 \\
(1,2)_8 = (1,4)_8 = (1,5)_8 = (2,5)_8 = (q + 1 + 2x - 4a)/64 \\
(1,3)_8 = (1,6)_8 = (q + 1 - 6x + 4a)/64 \\
(2,4)_8 = (q + 1 - 2x)/64
\end{array}
$$

Case Ib: 2 is not a fourth power in $\mathbb{F}_q$

$(0,0)_8 = (q - 23 + 6x)/64$

$(0,1)_8 = (0,3)_8 = (0,5)_8 = (0,7)_8 = (q - 7 + 2x + 4a)/64$

$(0,2)_8 = (q - 7 - 2x - 8a - 16y)/64$

$(0,4)_8 = (q - 7 - 10x)/64$

$(0,6)_8 = (q - 7 - 2x - 8a + 16y)/64$

$(1,2)_8 = (q + 1 - 6x + 4a)/64$

$(1,3)_8 = (q + 1 + 2x - 4a - 16b)/64$

$(1,4)_8 = (q + 1 + 2x - 4a + 16y)/64$

$(1,5)_8 = (q + 1 + 2x - 4a - 16y)/64$

$(1,6)_8 = (q + 1 + 2x - 4a + 16b)/64$

$(2,4)_8 = (q + 1 + 6x + 8a)/64$

$(2,5)_8 = (q + 1 - 6x + 4a)/64$

Case II: The relation between the cyclotomic numbers of order 8 if $q \equiv 9 \bmod 16$:

$$
\begin{array}{ll}
(0,0)_8 = (4,0)_8 = (4,4)_8; & (0,1)_8 = (3,7)_8 = (5,4)_8 \\
(0,2)_8 = (2,6)_8 = (6,4)_8; & (0,3)_8 = (1,5)_8 = (7,4)_8 \\
(0,5)_8 = (1,4)_8 = (7,3)_8; & (0,6)_8 = (2,4)_8 = (6,2)_8 \\
(0,7)_8 = (3,4)_8 = (5,1)_8 & \\
(1,0)_8 = (3,3)_8 = (4,1)_8 = (4,5)_8 = (5,0)_8 = (7,7)_8 & \\
(1,1)_8 = (3,0)_8 = (4,3)_8 = (4,7)_8 = (5,5)_8 = (7,0)_8 & \\
(1,2)_8 = (2,7)_8 = (3,6)_8 = (5,3)_8 = (6,5)_8 = (7,1)_8 & \\
(1,3)_8 = (1,6)_8 = (2,5)_8 = (6,3)_8 = (7,2)_8 = (7,5)_8 & \\
(1,7)_8 = (2,3)_8 = (3,5)_8 = (5,2)_8 = (6,1)_8 = (7,6)_8 & \\
(2,0)_8 = (2,2)_8 = (4,2)_8 = (4,6)_8 = (6,0)_8 = (6,6)_8 & \\
(2,1)_8 = (3,1)_8 = (3,2)_8 = (5,6)_8 = (5,7)_8 = (6,7)_8 &
\end{array}
$$

The cyclotomic numbers of order 8 for the case that $q \equiv 9 \bmod 16$, $q = x^2 + 4y^2 = a^2 + 2b^2, x \equiv a \equiv 1 \bmod 4$:

Case IIa: 2 is a fourth power in $\mathbb{F}_q$

$(0,0)_8 = (q - 15 - 2x)/64$

$(0,1)_8 = (0,5)_8 = (q + 1 + 2x - 4a + 16y)/64$

$(0,2)_8 = (q + 1 + 6x + 8a - 16y)/64$

$(0,3)_8 = (0,7)_8 = (q + 1 + 2x - 4a - 16y)/64$

$(0,4)_8 = (q + 1 - 18x)/64$

$(0,6)_8 = (q + 1 + 6x + 8a + 16y)/64$

$(1,0)_8 = (1,1)_8 = (q - 7 + 2x + 4a)/64$

$(1,2)_8 = (q + 1 - 6x + 4a + 16b)/64$

$(1,3)_8 = (2,1)_8 = (q + 1 + 2x - 4a)/64$

$(1,7)_8 = (q + 1 - 6x + 4a - 16b)/64$

$(2,0)_8 = (q - 7 - 2x - 8a)/64$

Case IIb: 2 is not a fourth power in $\mathbb{F}_q$

$(0,0)_8 = (q - 15 - 10x - 8a)/64$

$(0,1)_8 = (0,3)_8 = (q + 1 + 2x - 4a - 16b)/64$

$(0,2)_8 = (q + 1 - 2x + 16y)/64$

$(0,4)_8 = (q + 1 + 6x + 24a)/64$

$(0,5)_8 = (0,7)_8 = (q + 1 + 2x - 4a + 16b)/64$

$(0,6)_8 = (q + 1 - 2x - 16y)/64$

$(1,0)_8 = (q - 7 + 2x + 4a + 16y)/64$

$(1,1)_8 = (q - 7 + 2x + 4a - 16y)/64$

$(1,2)_8 = (q + 1 + 2x - 4a)/64$

$(1,3)_8 = (2,1)_8 = (q + 1 - 6x + 4a)/64$

$(1,7)_8 = (q + 1 + 2x - 4a)/64$

$(2,0)_8 = (q - 7 + 6x)/64$