On the Lower Bound of the Linear Complexity
over \( F_p \) of Sidelnikov Sequences

Moubariz Z. Garaev
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58089, Morelia, Michoacán, México
garaev@matmor.unam.mx

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58089, Morelia, Michoacán, México
fluca@matmor.unam.mx

Igor E. Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

Arne Winterhof
Johann Radon Institute for
Computational and Applied Mathematics
Austrian Academy of Sciences
Altenberger Straße 69, A-4040 Linz, Austria
arne.winterhof@oeaw.ac.at
Abstract

For a Sidelnikov sequence of period $p^m - 1$ we obtain tight lower bounds on its linear complexity $L$ over $\mathbb{F}_p$. In particular, these bounds imply that, uniformly over all $p$ and $m$, $L$ is close to its largest possible value $p^m - 1$.

Keywords. Sidelnikov sequences, linear complexity, character sums.

1 Introduction

Let $p \geq 3$ be a prime and let $m \geq 1$ be an integer. We fix a primitive root $g$ in the finite field $\mathbb{F}_{p^m}$ of $p^m$ elements.

Then the Sidelnikov sequence $s_i, i = 0, 1, \ldots$, corresponding to $g$ can be defined as follows (see [14]). We consider the set

$$S = \{g^{2^j - 1} - 1 \mid j = 1, \ldots, (p^m - 1)/2\}$$

and define

$$s_i = \begin{cases} 1, & \text{if } g^i \in S; \\ 0, & \text{otherwise; } \quad i = 0, 1, \ldots \end{cases}$$

(1)

In particular, $s_i$ is a periodic sequence with period $p^m - 1$. The same construction has also been proposed in [9].

It is known that every Sidelnikov sequence has optimal periodic autocorrelation (see [14]). We also refer to [1, 5, 6, 7, 8, 12] for further references.

Let $L$ denote the linear complexity over the field $\mathbb{F}$ of a Sidelnikov sequence $s_i$. That is, $L$ is the smallest positive integer for which there are some $c_1, \ldots, c_L \in \mathbb{F}$ such that

$$s_{i+L} = c_{L-1}s_{i+L-1} + \ldots + c_0s_i, \quad i = 0, 1, \ldots.$$

It is certainly natural to study the linear complexity over $\mathbb{F}_2$ as in [8, 12], however studying the linear complexity of this sequence over other fields and rings is of interest as well. For example, several results on the linear complexity $L$ over $\mathbb{F}_p$ of Sidelnikov sequences have recently been obtained (see [5, 6] and the references therein). It is well known that linear complexity is an important cryptographic characteristic of sequences and provides information on the predictability and thus unsuitability for cryptography. In particular, sequences with low linear complexity are not suitable for cryptographic applications.
Here, we show that the method of [2, 3, 4] allows us to obtain lower bounds for the linear complexity $L$ over $\mathbb{F}_p$. These results are based on studying the distribution of the sequence

$$a_n = 2^{-2n} \binom{2n}{n}, \quad n = 0, 1, \ldots,$$

in residue classes modulo $p$.

More precisely, in [6] it has been shown that

$$L = p^m - 1 - M_0,$$

where $M_0$ is the number of solutions to the congruence

$$a_n \equiv (-1)^{(p^m-1)/2} \pmod{p}, \quad n = 0, \ldots, \frac{p^m - 3}{2}.$$

Here, we use a slightly different but more convenient formula for $L$. By the Lucas theorem, we have

$$a_n \equiv \prod_{i=0}^{m-1} a_{n_i} \pmod{p}, \quad (2)$$

where

$$n = n_0 + n_1p + \ldots + n_{m-1}p^{m-1}, \quad 0 \leq n_0, \ldots, n_{m-1} \leq p - 1,$$

is the $p$-ary expansion of $n \leq p^m - 1$ (see also [5, 6]). It is easy to verify that

$$\binom{p-1}{(p-1)/2} = \prod_{j=1}^{(p-1)/2} \frac{p-j}{j} \equiv (-1)^{(p-1)/2} \pmod{p}$$

and that

$$\frac{p^m - 1}{p - 1} = p^{m-1} + \ldots + 1 \equiv m \pmod{2}.$$

Thus $(p - 1)m/2 \equiv (p^m - 1)/2 \pmod{2}$. In particular,

$$a_{(p^m-1)/2} \equiv \binom{p^m - 1}{(p^m-1)/2} \equiv \binom{p-1}{(p-1)/2}^m \equiv (-1)^{(p-1)/2} \equiv (-1)^{(p^m-1)/2} \pmod{p}$$
and thus,

\[ L = p^m - M, \]

where \( M \) is the number of solutions to the congruence

\[ a_n \equiv (-1)^{(p^m-1)/2} \pmod{p}, \quad n = 0, \ldots, \frac{p^m - 1}{2}. \]

It is also useful to note that

\[ \binom{2n}{n} \equiv 0 \pmod{p} \]

for \( (p + 1)/2 \leq n \leq p - 1 \).

We estimate \( M \) in Section 3. In particular, these estimates are based on bounds of character sums of the form

\[ S(\chi, N) = \sum_{n=0}^{N-1} \chi(a_n), \quad 1 \leq N \leq (p + 1)/2, \]

where \( \chi \) is a nontrivial multiplicative character of \( \mathbb{F}_p \). In fact, for our specific applications only the case \( N = (p + 1)/2 \) is relevant, but we believe estimates of such sums can find some other applications. Furthermore, when \( N < p/\log p \), better estimates can be obtained by using the Weil bound together with the standard technique of estimating incomplete sums. We refer to [2, 3, 4] for details.

In the final section, we apply the bounds on \( M \) to obtain lower and upper bounds on \( L \) over \( \mathbb{F}_p \). These bounds imply that, for any \( p \) and \( m \), \( L \) is asymptotically close to its largest possible value \( p^m - 1 \). In fact, we give precise and explicit estimates. These seem to be the first known results of this kind (the results of [5, 6] apply only to small values of \( p \)).

Finally, we note that our bounds can be combined with the results of [13] to produce lower bounds on the linear complexity of Sidelnikov sequences over other residue rings.

**Acknowledgements.** During the preparation of this paper, F. L. was supported in part by grants SEP-CONACYT 37259-E and 37260-E, I. S. was supported in part by ARC grant DP0556431, A. W. was supported in part by the Austrian Academy of Sciences and by FWF grant S8313.
2 Bounds of Character Sums

We need some analogues of the results of [3], which have been obtained for middle binomial coefficients and Catalan numbers,

\[ b_n = \binom{2n}{n} \quad \text{and} \quad c_n = \frac{1}{n+1} \binom{2n}{n}, \quad n = 0, 1, \ldots, \]
rather than for our sequence \( a_n \).

Let \( \mathcal{X} \) and \( \mathcal{X}^* \) denote the set of multiplicative characters and the set of nontrivial multiplicative characters modulo \( p \), respectively. We use the convention \( \chi(0) = 0 \) for all \( \chi \in \mathcal{X} \).

**Lemma 1.** Let \( N \) be an integer with \( 1 \leq N \leq (p+1)/2 \). Then the following bound holds

\[ \max_{\chi \in \mathcal{X}^*} |S(\chi, N)| < \left( \frac{8}{3} \right)^{1/4} N^{1/2} p^{3/8} + (3/2)^{1/2} p^{1/4}. \]

**Proof.** For any integer \( k \geq 0 \), we have

\[ \left| S(\chi, N) - \sum_{n=0}^{N-1} \chi(a_{n+k}) \right| \leq 2k. \quad (4) \]

Note that

\[ a_{n+k} \prod_{j=1}^{k} (2n + 2j) = a_n \prod_{j=1}^{k} (2n + 2j - 1), \quad (5) \]

and for \( k \leq (p-1)/2 \)

\[ \chi(a_{n+k}) = \chi \left( a_n \prod_{j=1}^{k} (2n + 2j - 1)(2n + 2j)^{-1} \right), \]

(since \( n+j \leq N+k < p \), this last expression is well-defined modulo \( p \)). For any integer \( 1 \leq K \leq (p+1)/2 \), from \( (4) \), we derive

\[ \left| KS(\chi, N) - \sum_{k=0}^{K-1} \sum_{n=0}^{N-1} \chi(a_{n+k}) \right| \leq \sum_{k=0}^{K-1} \left| S(\chi, N) - \sum_{n=0}^{N-1} \chi(a_{n+k}) \right| \]

\[ \leq 2 \sum_{k=0}^{K-1} k = K(K-1). \]
Therefore
\[
|S(\chi, N)| \leq \frac{1}{K} \left| \sum_{k=0}^{K-1} \sum_{n=0}^{N-1} \chi(a_{n+k}) \right| + (K - 1).
\]

Changing the order of summation, we obtain
\[
|S(\chi, N)| \leq \frac{1}{K} W + K - 1, \tag{6}
\]

where
\[
W = \sum_{n=0}^{N-1} \sum_{k=0}^{K-1} \chi(a_{n+k}) = \sum_{n=0}^{N-1} \sum_{k=0}^{K-1} \chi \left( a_n \prod_{j=1}^{k} (2n + 2j - 1)(2n + 2j)^{-1} \right) \]
\[
= \sum_{n=0}^{N-1} \sum_{k=0}^{K-1} \chi \left( \prod_{j=1}^{k} (2n + 2j - 1)(2n + 2j)^{-1} \right).
\]

We recall that for any \( \chi \in \mathcal{X} \) and any \( \lambda \in \mathbb{F}_p^* \), we have \( \overline{\chi}(\lambda) = \chi(\lambda^{-1}) \), where \( \overline{\chi} \) means the conjugate character. We also have \( |z|^2 = z \overline{z} \) for any complex \( z \).

Applying the Cauchy-Schwarz inequality, we derive
\[
W^2 \leq N \sum_{n=0}^{N-1} \sum_{k=0}^{K-1} \chi \left( \prod_{j=1}^{k} (2n + 2j - 1)(2n + 2j)^{-1} \right)^2
\]
\[
\leq N \sum_{n=0}^{p-1} \sum_{k=0}^{K-1} \chi \left( \prod_{j=1}^{k} (2n + 2j - 1)(2n + 2j)^{-1} \right)^2
\]
\[
\leq N \sum_{n=0}^{p-1} \sum_{k,m=0}^{K-1} \chi \left( \prod_{j=1}^{k} (2n + 2j - 1)(2n + 2j)^{-1} \right) \times \overline{\chi} \left( \prod_{j=1}^{m} (2n + 2j - 1)(2n + 2j)^{-1} \right)
\]
\[
= NKp + N \sum_{n=0}^{p-1} \sum_{0 \leq k < m < K} \chi(\Psi_{k,m}(n)) + N \sum_{n=0}^{p-1} \sum_{0 \leq k < m < K} \overline{\chi}(\Psi_{m,k}(n))
\]

where
\[
\Psi_{r,s}(X) = \prod_{j=r+1}^{s} (2X + 2j - 1)(2X + 2j)^{-1}. \tag{7}
\]
Changing the order of summation and noticing that
\[ \left| \sum_{n=0}^{p-1} \chi(\Psi_{k,m}(n)) \right| = \left| \sum_{n=0}^{p-1} \bar{\chi}(\Psi_{m,k}(n)) \right|, \]
we deduce
\[ W^2 \leq NKp + 2 \sum_{0 \leq k < m < K} \left| \sum_{n=0}^{p-1} \chi(\Psi_{k,m}(n)) \right|. \]

Clearly, for \( 0 \leq k < m < K \) the rational function \( \Psi_{k,m}(X) \) is not a power of another rational function over \( \mathbb{F}_p \) since \( K < p \).

Using the Weil bound given in Example 12 of Appendix 5 of [15] (see also Theorem 3 of Chapter 6 in [11], or Theorem 5.41 and the comments to Chapter 5 of [10]), we see that
\[ \left| \sum_{n=0}^{p-1} \chi(\Psi_{k,m}(n)) \right| \leq (2(m-k) - 1)p^{1/2}. \]

Putting everything together, we get
\[ W^2 \leq N \left( Kp + 2 \sum_{0 \leq k < m < K} (2(m-k) - 1)p^{1/2} \right). \]

Taking \( K = \left\lceil (3/2)^{1/2} p^{1/4} \right\rceil \), by (6), we derive the result. \( \square \)

**Lemma 2.** Let \( N \) be an integer with \( 1 \leq N \leq (p+1)/2 \). The following bound holds
\[ \frac{1}{p-1} \sum_{\chi \in \mathcal{X}} |S(\chi, N)|^2 < 2 \cdot 3^{-1/2} N^{3/2} + 6N. \]

**Proof.** Arguing as in the proof of Lemma 1 (see (6), in particular), we derive that for any integer \( K \geq 1 \),
\[ \sum_{\chi \in \mathcal{X}} |S(\chi, N)|^2 \]
\[ \leq \sum_{\chi \in \mathcal{X}} \left( \frac{1}{K} \sum_{n=0}^{N-1} \sum_{k=0}^{K-1} \chi \left( \prod_{j=1}^{k} (2n + 2j - 1)(2n + 2j)^{-1} \right) + K - 1 \right)^2 \]
\[ < \frac{1}{K^2} \sigma_2 + 2 \frac{K - 1}{K} \sigma_1 + (K - 1)^2(p - 1), \]
where

$$\sigma_\nu = \sum_{\chi \in X} \left( \sum_{n=0}^{N-1} \sum_{k=0}^{K-1} \chi \left( \prod_{j=1}^{k} (2n + 2j - 1)(2n + 2j)^{-1} \right) \right)^\nu, \quad \nu = 1, 2.$$  

We recall the identity

$$\sum_{\chi \in X} \chi(u) = \begin{cases} 0, & \text{if } u \not\equiv 1 \pmod{p}, \\ p-1, & \text{if } u \equiv 1 \pmod{p}. \end{cases} \quad (8)$$

For

$$\sigma_1 = \sum_{n=0}^{N-1} \sum_{k=0}^{K-1} \sum_{\chi \in X} \chi \left( \prod_{j=1}^{k} (2n + 2j - 1)(2n + 2j)^{-1} \right)$$

we see that the sum over $\chi$ vanishes, unless

$$\prod_{j=1}^{k} (2n + 2j - 1)(2n + 2j)^{-1} \equiv 1 \pmod{p}.$$  

For every $k$ with $0 \leq k < K$, there are at most $k - 1$ solutions to this congruence. For each $k$, the above relation leads to a nontrivial polynomial congruence in $n$ of degree $k - 1$ (because the terms containing $X^k$ get canceled on both sides), and therefore it has at most $k - 1$ solutions $n$ with $0 \leq n \leq N - 1$. Thus,

$$\sigma_1 < \frac{1}{2} K(K - 1)(p - 1).$$

For $\sigma_2$, by the Cauchy-Schwarz inequality, as before, we derive

$$\sigma_2 \leq \left( \sum_{\chi \in X} \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \chi \left( \prod_{j=1}^{k} (2n + 2j - 1)(2n + 2j)^{-1} \right) \right|^2 \right)^{1/2}$$

$$= N \left( KN(p - 1) + 2 \sum_{0 \leq k < m < K} \sum_{n=0}^{N-1} \sum_{\chi \in X} \chi(\Psi_{k,m}(n)) \right),$$

where $\Psi_{r,s}(X)$ is given by (7).

Relation (8) implies that the sum over $\chi$ vanishes, unless $\Psi_{k,m}(n) \equiv 1 \pmod{p}$. For every $k$ and $m$ with $0 \leq k < m < K$, there are at most $m - k - 1$ solutions to this congruence. Thus,

$$\sigma_2 \leq N \left( KN(p - 1) + \frac{1}{3} K^2(K - 1)(p - 1) \right).$$

Taking $K = \lceil (3N)^{1/2} \rceil$, the desired result follows. \qed
3 Bounds on the Number of Solutions of Some Congruences

We start with a certain technical statement which can be of independent interest.

Lemma 3. If \( \ell_1 < \ldots < \ell_s \) are distinct positive integers then

\[
\sum_{i=1}^{s} \ell_i < \frac{3^{2/3}}{2} \left( \sum_{i=1}^{s} \ell_i^2 \right)^{2/3}.
\]

Proof. Put

\[ \sigma_\nu = \sum_{i=1}^{s} \ell_i^{\nu}, \quad \nu = 1, 2. \]

We assume that for a given \( \sigma_1 \) the positive integers \( \ell_1 < \ldots < \ell_s \) are such that \( \sigma_2 \) is minimal among all such sequences of \( s \) positive integers whose sum is \( \sigma_1 \). It clearly suffices to prove our inequality only for this sequence.

We now show that \( \ell_i + 1 - \ell_i \leq 2 \) for all \( i = 1, \ldots, s - 1 \). Indeed, assume that \( \ell_i + 1 - \ell_i > 2 \) for some \( i \in \{1, \ldots, s\} \). Then, replacing the pair \( (\ell_i, \ell_i + 1) \) by the pair \( (\ell_i + 1, \ell_i + 1) \) (which is again a pair of distinct integers), we do not change \( \sigma_1 \). However, the sum of squares of the new sequence becomes

\[
\sigma_2 + (\ell_i + 1)^2 + (\ell_i + 1 - 1)^2 - \ell_i^2 - \ell_{i+1}^2 = \sigma_2 - 2(\ell_{i+1} - \ell_i - 1) < \sigma_2.
\]

This contradicts our choice of \( \ell_1, \ldots, \ell_s \).

A positive integer \( i \in \{1, \ldots, s - 1\} \) will be called a gap if \( \ell_{i+1} - \ell_i = 2 \). We now show that there exists at most one gap. Indeed, assume that \( i < j \) are such that \( \ell_{i+1} - \ell_i = 2 \) and \( \ell_{j+1} - \ell_j = 2 \). Therefore, \( \ell_{j+1} = \ell_j + 2 \geq \ell_{i+1} + 2 = \ell_i + 4 \). Then, replacing the pair \( (\ell_i, \ell_{j+1}) \) by the pair \( (\ell_i + 1, \ell_{j+1} - 1) \) (which is a pair of unequal integers distinct from all \( \ell_\kappa \) with \( \kappa \neq i, j \)), we do not change \( \sigma_1 \). However, the sum of squares of the new sequence becomes

\[
\sigma_2 + (\ell_i + 1)^2 + (\ell_{j+1} - 1)^2 - \ell_i^2 - \ell_{j+1}^2 = \sigma_2 + 2(\ell_i - 2\ell_{j+1} + 2) < \sigma_2,
\]

which again contradicts our choice of \( \ell_1, \ldots, \ell_s \).
Thus, there exists at most one gap $1 \leq k \leq s$. We put $k = s + 1$ if there is no gap. Clearly, there is some integer $\ell \geq 0$ such that

$$\ell_j = \begin{cases} 
\ell + j + 1, & \text{for } k \leq j \leq s, \\
\ell + j, & \text{for } 1 \leq j \leq k - 1.
\end{cases}$$

Hence,

$$\sigma_\nu = \sum_{i=1}^{s+1} (\ell + i)^\nu - (\ell + k)^\nu = f_\nu(\ell), \quad \nu = 1, 2,$$

where

$$f_1(\lambda) = s\lambda + \frac{(s+1)(s+2)}{2} - k,$$

$$f_2(\lambda) = s\lambda^2 + (s^2 + 3s + 2 - 2k)\lambda + \frac{(s+1)(s+2)(2s+3)}{6} - k^2.$$

Simple calculations show that

$$3f_2(\lambda) - 2sf_1(\lambda) = 3s\lambda^2 + (s^2 + 9s + 6 - 6k)\lambda + \frac{3(s+1)(s+2)}{2} - 3k^2 + 2sk > \frac{3(s+1)(s+2)}{2} - 3k^2 + 2sk \geq 0$$

for $\lambda \geq 0$ and $1 \leq k \leq s + 1$. Since

$$\frac{df_1(\lambda)}{d\lambda} = s \quad \text{and} \quad \frac{df_2(\lambda)}{d\lambda} = 2f_1(\lambda),$$

we derive that

$$\frac{d(9f_2^2(\lambda) - 8f_1^3(\lambda))}{d\lambda} = 36f_1(\lambda)f_2(\lambda) - 24sf_1^2(\lambda) = 12f_1(\lambda)(3f_2(\lambda) - 2sf_1(\lambda)) > 0$$

for $\lambda \geq 0$. Therefore,

$$\min_{\lambda \geq 0} (9f_2^2(\lambda) - 8f_1^3(\lambda)) = 9f_2^2(0) - 8f_1^3(0). \quad (9)$$
Now straightforward calculations show that

\[ 9f_2^2(0) - 8f_1^3(0) = \left( \frac{(s + 1)(s + 2)(2s + 3)}{2} - 3k^2 \right)^2 - ((s + 1)(s + 2) - 2k)^3 \]

\[ = 9k^4 + 8k^3 + 3(s + 1)(s + 2)k (2(s + 1)(s + 2) - (2s + 7)k) + \frac{(s + 1)^2(s + 2)^2}{4}. \]

If \( k \leq s - 1 \), then

\[ 2(s + 1)(s + 2) - (2s + 7)k \geq 0. \]

Finally, one can easily check that if \( k = s \) or \( k = s + 1 \), then the expression \( 9f_2^2(0) - 8f_1^3(0) \) is a polynomial of degree four with positive coefficients in \( s \). More precisely, for \( k = s + 1 \) this polynomial is \( (s(s + 1)/2)^2 \), and it has even larger coefficients when \( k = s \). Thus, \( 9f_2^2(0) - 8f_1^3(0) > 0 \), which together with (9) completes the proof. □

**Remark 4.** A more careful (but technically straightforward) analysis of the proof of Lemma 3 leads to the conclusion that the inequality

\[ 9 \left( \sum_{i=1}^{s} \ell_i^2 \right)^2 - 8 \left( \sum_{i=1}^{s} \ell_i \right)^3 \geq \left( \frac{s(s + 1)}{2} \right)^2 \]

holds for all positive integers \( \ell_1 < \ldots < \ell_s \) with equality if and only if \( \ell_i = i \) for all \( i = 1, \ldots, s \).

**Lemma 5.** For any \( N \leq (p + 1)/2 \) and any integer \( \lambda \), the number \( R(N, \lambda) \) of solutions to the congruence

\[ a_n \equiv \lambda \pmod{p}, \quad 0 \leq n \leq N - 1, \]

satisfies

\[ R(N, \lambda) < \frac{3^{2/3}}{2} N^{2/3}. \]

**Proof.** Since \( N \leq (p+1)/2 \), we have \( R(N, 0) = 0 \) and may assume that \( \lambda \neq 0 \pmod{p} \).
Let
\[ a_{n_1} \equiv a_{n_2} \equiv \ldots \equiv a_{n_r} \equiv \lambda \pmod{p} \]
be such that \( n_1 < n_2 < \ldots < n_r \), where \( r = R(N, \lambda) \). Let \( k_1 < \ldots < k_s \) be all distinct numbers of the form \( n_{i+1} - n_i \), \( 1 \leq i \leq r - 1 \). We assume that \( k_i \) occurs with multiplicity \( \ell_i \), \( i = 1, \ldots, s \).

Obviously,
\[
\sum_{i=1}^{s} \ell_i = r - 1 \quad \text{and} \quad \sum_{i=1}^{s} \ell_i k_i = n_r - n_1 \leq N - 1. \tag{10}
\]

Thus, for a given \( i \), the number \( \ell_i \) is the number of solutions of the congruence
\[ a_{n+k_i} \equiv a_n \equiv \lambda \pmod{p}, \quad 0 \leq n \leq N - k_i - 1. \]

This congruence and (5) imply
\[
\prod_{j=1}^{k_i} (2n + 2j - 1)(2n + 2j)^{-1} \equiv 1 \pmod{p}.
\]

Examining the roots of the polynomials
\[
\prod_{j=1}^{k_i} (2X + 2j - 1) \quad \text{and} \quad \prod_{j=1}^{k_i} (2X + 2j),
\]

one easily concludes that these polynomials are distinct modulo \( p \). Thus, the above congruence has no more than \( k_i - 1 \) solutions. Therefore, \( \ell_i \leq k_i - 1 \), \( i = 1, \ldots, s \), and (10) implies
\[
\sum_{i=1}^{s} \ell_i (\ell_i + 1) = \sum_{i=1}^{s} \ell_i^2 + r - 1 \leq N - 1. \tag{11}
\]

Now, Lemma 3 together with (10) and (11) implies the inequality
\[
\frac{2^{3/2}}{3} (r - 1)^{3/2} + r - 1 \leq N - 1.
\]

Remarking that
\[
\frac{2^{3/2}}{3} r^{3/2} \leq \frac{2^{3/2}}{3} (r - 1)^{3/2} + r
\]
for \( r \geq 1 \), we conclude the proof. \( \square \)
Put
\[ \mathcal{N}_r = \{ n = n_0 + n_1 p + \ldots + n_{r-1} p^{r-1} : 0 \leq n_0, n_1, \ldots, n_{r-1} \leq (p-1)/2 \}. \]

Note that by the Lucas congruence (2), we have that \( a_n \not\equiv 0 \pmod{p} \) for all \( n \in \mathcal{N}_r \).

For \( \lambda \not\equiv 0 \pmod{p} \), let \( Q_r(\lambda) \) be the number of solutions to the congruence
\[ a_n \equiv \lambda \pmod{p}, \quad n \in \mathcal{N}_r. \]

**Lemma 6.** For any integers \( r \geq 2 \) and \( \lambda \) we have
\[ \left| Q_r(\lambda) - \frac{(p+1)^r}{2^r(p-1)} \right| < 1.2 p^{(7r-2)/8}. \]

**Proof.** By (8), we have
\[ Q_r(\lambda) = \frac{1}{p-1} \sum_{n \in \mathcal{N}_r} \sum_{\chi \in \mathcal{X}} \chi(\lambda^{-1}a_n) = \frac{1}{p-1} \sum_{\chi \in \mathcal{X}} \chi(\lambda^{-1}) \sum_{n \in \mathcal{N}_r} \chi(a_n). \]

Separating the term
\[ \frac{\#\mathcal{N}_r}{p-1} = \frac{(p+1)^r}{2^r(p-1)}, \]
corresponding to the trivial character, we obtain
\[ \left| Q_r(\lambda) - \frac{(p+1)^r}{2^r(p-1)} \right| \leq \frac{1}{p-1} \sum_{\chi \in \mathcal{X}^*} \left| \sum_{n \in \mathcal{N}_r} \chi(a_n) \right|. \]

We now see that, by the Lucas congruence (2),
\[ \sum_{n \in \mathcal{N}_r} \chi(a_n) = (S(\chi, (p+1)/2))^r. \]

Before we apply the character sum bounds, we remark that
\[ \frac{p+1}{2} < p^{7/8} \quad \text{for } p \leq 61, \]
and
\[ (8/3)^{1/4}(p+1)^{1/2} p^{3/8} + (3/2)^{1/2} p^{1/4} < p^{7/8} \quad \text{for } p \geq 67. \]
Also,
\[
\left( \frac{p+1}{2} \right)^2 < 1.2p^{3/2} \quad \text{for } p \leq 17,
\]
and
\[
2 \cdot 3^{-1/2} \left( \frac{p+1}{2} \right)^{3/2} + 3(p+1) < 1.2p^{3/2} \quad \text{for } p \geq 19.
\]

Applying Lemma 1 for \( p \geq 19 \), Lemma 2 for \( p \geq 67 \), and the trivial bound \(|S(\chi, (p+1)/2)| \leq (p+1)/2\) for small \( p \), we obtain that for any \( p \)
\[
\max_{\chi \in \mathcal{X}^*} |S(\chi, (p+1)/2)| < p^{7/8} \quad \text{and} \quad \frac{1}{p-1} \sum_{\chi \in \mathcal{X}} |S(\chi, (p+1)/2)|^2 < 1.2p^{3/2}.
\]

Therefore,
\[
\frac{1}{p-1} \sum_{\chi \in \mathcal{X}^*} \left| \sum_{n \in \mathcal{N}_r} \chi(a_n) \right| \leq \frac{1}{p-1} \sum_{\chi \in \mathcal{X}^*} |S(\chi, (p+1)/2)|^r
< \frac{1}{p-1} p^{7(r-2)/8} \sum_{\chi \in \mathcal{X}} |S(\chi, (p+1)/2)|^2
< 1.2p^{(7r-2)/8},
\]
which concludes the proof. \( \square \)

For \( r = 1 \), we can simply use Lemma 1 to obtain an upper bound on \( Q_1(\lambda) \). Note that the lower bound is trivial in this case. However, the above upper bound is weaker than that of Lemma 5.

### 4 Main Results

By (3), to obtain bounds on the linear complexity \( L \) over \( \mathbb{F}_p \) of Sidelnikov sequences, it is enough to estimate \( M \).

For \( m = 1 \), we use Lemma 5.

**Theorem 7.** For the linear complexity \( L \) over \( \mathbb{F}_p \) of a Sidelnikov sequence \( s_i \) given by (1), the following bound holds:

\[
L > p - 3^{2/3}2^{-5/3}p^{2/3}.
\]
For \( m \geq 2 \), we use Lemma 6.

**Theorem 8.** For any integer \( m \geq 2 \) for the linear complexity \( L \) over \( \mathbb{F}_p \) of a Sidelnikov sequence \( s_i \) given by (1), the following bound holds:

\[
\left| L - p^m + \frac{(p+1)^m}{2^m(p-1)} \right| < 1.2p^{(7m-2)/8}.
\]

For small \( p \), we can improve Theorem 8 by determining explicitly the values of the \( S(\chi, (p+1)/2) \). For example, for \( p = 3 \), we immediately get \( S(\chi, 2) = 0 \) for the only nontrivial character \( \chi \) of \( \mathbb{F}_3 \) and thus (cf. [5, Theorem 3]),

\[
L = 3^m - 2^{m-1}.
\]

For \( p = 5 \), we get

\[
Q_m(1) = \frac{1}{4} \left( 3^m + (2 - \sqrt{-1})^m + 1 + (2 + \sqrt{-1})^m \right).
\]

Thus,

\[
L = 5^m - \frac{1}{4} \left( 3^m + (2 - \sqrt{-1})^m + 1 + (2 + \sqrt{-1})^m \right).
\]

Hence,

\[
\left| L - 5^m + \frac{3^m}{4} \right| \leq \frac{1}{2}5^{m/2} + \frac{1}{4}.
\]

**References**


