One-Error Linear Complexity over F_p of Sidelnikov Sequences*

Yu-Chang Eun[1,**], Hong-Yeop Song[2], and Gohar M. Kyureghyan[3]

[1] SAMSUNG ELECTRONICS CO., LTD., Dong Suwon P.O.BOX-105, 416 Maetan-3Dong, Paldal-Gu, Suwon-City, Gyeonggi-Do, Korea, 442-600
yc.eun@samsung.com

[2] Center for Information Technology of Yonsei University, Coding and Information Theory Lab, Department of Electrical and Electronics Engineering, Yonsei University, 134 Shinchon-dong Seodaemun-gu, Seoul, Korea, 120-749
hy.song@coding.yonsei.ac.kr

[3] Otto-von-Guericke University, Magdeburg, Faculty of Mathematics, Postfach 4120, Magdeburg, Germany 39016
gohar.kyureghyan@mathematik.uni-magdeburg.de

Abstract. Let p be an odd prime and m be a positive integer. In this paper, we prove that the one-error linear complexity over F_p of Sidelnikov sequences of length $p^m - 1$ is $(\frac{p+1}{2})^m - 1$, which is much less than its (zero-error) linear complexity.

1 Introduction

Let p be an odd prime and m be a positive integer. Let F_{p^m} be the finite field with p^m elements, and α be a primitive element of F_{p^m}. The Sidelnikov sequence $S = \{s(t) \ : \ t = 0, 1, 2, ..., p^m - 2\}$ of period $p^m - 1$ is defined as [1]

$$s(t) = \begin{cases} 1 & \text{if } \alpha^t + 1 \in \mathrm{N} \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

where $\mathrm{N} = \{\alpha^{2t+1} \ : \ t = 0, 1, ..., \frac{p^m-1}{2} - 1\}$ is the set of quadratic nonresidues over F_{p^m}. In [1], it was shown that S has the optimal autocorrelation and balance property. Sidelnikov sequences were rediscovered by Lempel *et al* [2], and Sarwate pointed out that the sequences described by Lempel *et al* were in fact the same as the ones by Sidelnikov [3]. Sidelnikov sequences are a special case of the construction by No *et al* [4].

* This work was supported by Korea Research Foundation Grant (KRF-2003-041-D00417).

** He was with Dept. of Electrical and Electronics Engineering, Yonsei University, while he was doing this research.

T. Helleseth et al. (Eds.): SETA 2004, LNCS 3486, pp. 154–165, 2005.

Helleseth and Yang [5] originated the study of the linear complexity of Sidelnikov sequences over F_2. They found also a representation of the sequences using the indicator function $I(\cdot)$ and the quadratic character $\chi(\cdot)$ as

$$s(t) = \frac{1}{2}\left(1 - I(\alpha^t + 1) - \chi(\alpha^t + 1)\right), \tag{2}$$

where $I(x) = 1$ if $x = 0$ and $I(x) = 0$ otherwise, and $\chi(x)$ denotes the quadratic character of $x \in F_{p^m}$ defined by

$$\chi(x) = \begin{cases} +1, & \text{if } x \text{ is a quadratic residue} \\ 0, & \text{if } x = 0 \\ -1, & \text{if } x \text{ is a quadratic nonresidue.} \end{cases}$$

Kyureghyan and Pott [6] have extended the calculation of the linear complexity of the sequences over F_2 following the results in [5]. However, the determination of the linear complexity of S over F_2 turns out to be difficult since the characteristic of the field, which is 2, divides the length of the sequence [6].

Observing that it is more natural to consider the linear complexity over F_p since the sequences are constructed over F_p, Helleseth *et al* [7] derived the linear complexity over F_p (not over F_2) of the sequence S of length $p^m - 1$ as well as its trace representation for $p = 3, 5$, and 7, and finally, Helleseth *et al* [8] finished the calculation of the linear complexity over F_p of the sequence of length $p^m - 1$ for all odd prime p.

According to the results in both [7] and [8], the linear complexity over F_p is roughly the same as the period, and the sequences can be thought of having an "excellent" linear complexity. We noted that the linear complexity of the sequences obtained by deleting the term $I(\alpha^t + 1)$ in (2) is much smaller than the one of the original sequence. For example, the sequence of length $3^3 - 1 = 26$

1 1 1 1 0 1 1 0 1 1 0 0 0 **0** 0 1 0 0 1 1 1 0 0 0 1 0

has linear complexity 23 over F_3. But the sequence obtained by deleting the term $I(\alpha^t + 1)$ in (2) is

1 1 1 1 0 1 1 0 1 1 0 0 0 **2** 0 1 0 0 1 1 1 0 0 0 1 0

which has linear complexity 7 over F_3. We conjectured that this phenomenon may persist in all cases of Sidelnikov sequences, and this paper is the result of this investigation. In this paper we show that the value $(\frac{p+1}{2})^m - 1$, first appeared in [7] in the middle of the calculations, is indeed the one-error linear complexity over F_p of the sequence of period $p^m - 1$ for all odd prime p and all positive integers $m \geq 1$.

We give some notation and basic techniques for the calculation of the linear complexity of the sequences over F_p in Section 2. In Section 3, we prove that the "upper bound" on the one-error linear complexity of Sidelnikov sequences over F_p of period $p^m - 1$ is $(\frac{p+1}{2})^m - 1$, by constructing explicitly a one-error sequence. Note that this is already surprising enough since the true value of the one-error linear complexity is *at most* this number. In Section 4, we prove that the equality holds in the upper bound.

2 Preliminaries

Let p be an odd prime and $m \geq 1$. Denote the linear complexity over F_p of Sidelnikov sequence S defined in (1) or (2) by $L(S)$. Let $Z = \{z(t) : t = 0, 1, 2, ..., p^m - 2\}$ be a sequence of length $p^m - 1$ over F_p. Then the k-error linear complexity [9][10] of Sidelnikov sequence of length $p^m - 1$ over F_p is defined as

$$L_k(S) = \min_{0 \leq \mathrm{WH}(Z) \leq k} L(S + Z) \tag{3}$$

where $\mathrm{WH}(Z)$ denotes the Hamming weight of Z, *i.e.*, the number of components of Z that are non-zero. Assume $k = 1$ in (3) and

$$z^{(\tau,\lambda)}(t) = \frac{\lambda}{2} I(\alpha^{t-\tau} + 1), \quad 0 \leq \tau < p^m - 1, \quad \lambda \in F_p.$$

Then, any sequence over F_p of length $p^m - 1$ with Hamming weight ≤ 1 can be represented by the sequence $Z^{(\tau,\lambda)} = \{z^{(\tau,\lambda)}(t) | t = 0, 1, ..., p^m - 2\}$ for some $0 \leq \tau < p^m - 1$ and $\lambda \in F_p$.

Let $S_Z^{(\tau,\lambda)} = \{s_z^{(\tau,\lambda)}(t) : t = 0, 1, 2, ..., p^m - 2\}$ be defined as

$$\begin{aligned} s_z^{(\tau,\lambda)}(t) &\triangleq s(t) + z^{(\tau,\lambda)}(t) \\ &= \frac{1}{2}\left(1 - I(\alpha^t + 1) - \chi(\alpha^t + 1)\right) + \frac{\lambda}{2} I(\alpha^{t-\tau} + 1). \end{aligned} \tag{4}$$

Then the one-error linear complexity of S can be represented as

$$L_1(S) = \min_{\substack{\lambda \in F_p \\ 0 \leq \tau \leq p^m - 2}} L(S_Z^{(\tau,\lambda)}). \tag{5}$$

To compute the linear complexity in general, we use the Fourier transform in the finite field F_{p^m} defined for a p-ary sequence $Y = \{y(t)\}$ of period $n = p^m - 1$ by

$$A_i = \frac{1}{n} \sum_{t=0}^{n-1} y(t) \alpha^{-it}$$

where α is a primitive element of F_{p^m} and $A_i \in F_{p^m}$ [11][12]. The inverse Fourier transform is similarly represented as

$$y(t) = \sum_{t=0}^{n-1} A_i \alpha^{it}. \tag{6}$$

Then the linear complexity of Y is defined as [11][12]

$$L(Y) = \left| \{\, i \mid A_i \neq 0,\ 0 \leq i \leq n - 1 \,\} \right|.$$

3 Main Results

The Fourier transform of the Sidelnikov sequences is given in [7].

Lemma 1. [7] *Let the p-adic expansion of an integer i, where $0 \leq i \leq p^m - 2$, be given by*

$$i = \sum_{a=0}^{m-1} i_a p^a$$

where $0 \leq i_a \leq p-1$. Then the Fourier coefficient $A_{-i} \in F_{p^m}$ of the Sidelnikov sequence defined in (2) *of period $p^m - 1$ is given by*

$$A_{-i} = \frac{(-1)^i}{p-2}\left(-1 + (-1)^{-\frac{p^m-1}{2}} \prod_{a=0}^{m-1} \binom{i_a}{\frac{p-1}{2}}\right). \tag{7}$$

Then it is straightforward, that the Fourier coefficients of the one-error allowed Sidelnikov sequences are given as follows.

Lemma 2. *The Fourier coefficient $A_{-i}(\tau, \lambda)$ of the one-error allowed Sidelnikov sequence $S_Z^{(\tau,\lambda)}$ defined in* (4) *is given by*

$$A_{-i}(\tau,\lambda) = \frac{(-1)^i}{p-2}\left(-1 + \lambda\alpha^{\tau i} + (-1)^{-\frac{p^m-1}{2}} \prod_{a=0}^{m-1} \binom{i_a}{\frac{p-1}{2}}\right) \in F_{p^m} \tag{8}$$

where i_a is defined in Lemma 1.

Consider the case $\alpha^\tau = 1$ (or $\tau = 0$) and $\lambda = 1$. In this case we have

$$s_z^{(0,1)}(t) = \frac{1}{2}(1 - \chi(\alpha^t + 1)),$$

and

$$\begin{aligned} L\left(S_Z^{(0,1)}\right) &= |\{\, i \;:\; A_{-i}(0,1) \neq 0,\; 0 \leq i < p^m - 1 \,\}| \\ &= |I_{\text{nz}}| = \left(\frac{p+1}{2}\right)^m - 1 \end{aligned} \tag{9}$$

where

$$I_{\text{nz}} \triangleq \left\{ i \;:\; \prod_{a=0}^{m-1} \binom{i_a}{\frac{p-1}{2}} \neq 0,\; 0 \leq i < p^m - 1 \right\}. \tag{10}$$

Note that I_{nz} contains all the i's in the range $i = 0, 1, 2, ..., p^m - 2$ that satisfy $\frac{p-1}{2} \leq i_a \leq p - 1$ for all a.

Table 1. Comparison of L_0 and L_1 when $p = 3$

m	L_0	L_1	$n = 3^m - 1$	L_0/n (%)	L_1/n (%)
2	7	3	8	87.5	37.5
3	23	7	26	88.5	26.9
4	73	15	80	91.3	18.8
5	227	31	242	93.8	12.8
6	697	63	728	95.7	8.7
7	2123	127	2186	97.1	5.8
8	6433	255	6560	98.1	3.9

Table 2. Comparison of L_0 and L_1 when $p = 5$

m	L_0	L_1	$n = 5^m - 1$	L_0/n (%)	L_1/n (%)
2	21	8	24	87.5	33.3
3	117	26	124	94.4	21.0
4	608	80	624	97.4	12.8
5	3083	244	3124	98.7	7.8
6	15501	728	15624	99.2	4.7
7	77717	2186	78124	99.5	2.8
8	389248	6560	390624	99.6	1.7

Alternatively, without specifically calculating $A_{-i}(0,1)$ for all i, we have

$$\begin{aligned} s_z^{(0,1)}(t) &= \frac{1}{2}\left(1 - \chi(\alpha^t + 1)\right) = \frac{1}{2}\left(1 - (\alpha^t + 1)^{\frac{p^m-1}{2}}\right) \\ &= \frac{1}{2}\left(1 - (\alpha^t + 1)^{\sum_{k=0}^{m-1}(\frac{p-1}{2})p^k}\right) \\ &= \frac{1}{2}\left(1 - \prod_{k=0}^{m-1}(\alpha^t + 1)^{(\frac{p-1}{2})p^k}\right) \\ &= \frac{1}{2}\left(1 - \prod_{k=0}^{m-1}(a_0 + a_1\alpha^t + \cdots + a_{\frac{p-1}{2}}\alpha^{\frac{p-1}{2}t})^{p^k}\right). \end{aligned} \tag{11}$$

where $a_i = \binom{\frac{p-1}{2}}{i}$. Since the characteristic is p and $a_i \not\equiv 0 \pmod p$ we obtain the same linear complexity as (9) by just counting all the sum-terms when (11) is represented as (6). This construction provides an upper bound on the one-error linear complexity of the Sidelnikov sequences.

Theorem 1. *Let S be the Sidelnikov sequence of period $p^m - 1$ for some odd prime p and a positive integer m. Then for the one-error linear complexity $L_1(S)$ of S it holds*

$$L_1(S) \le \left(\frac{p+1}{2}\right)^m - 1.$$

Even though the above bound was not explicitly mentioned in [7], we would like to add that it was first calculated there in the middle of the calculations. It is very surprising to have such an upper bound for $L_1(S)$. In fact there is an equality in Theorem 1, which may not be very unexpected.

Theorem 2 (main). *Let p be an odd prime and $m \geq 1$. Let S be the Sidelnikov sequence of period $p^m - 1$. Then the one-error linear complexity of S is*

$$L_1(S) = \left(\frac{p+1}{2}\right)^m - 1.$$

Tables I and II show some numerical data for $p = 3, 5$ and $1 < m \leq 8$. Observe that for $p = 5$ and $m = 8$, the one-error linear complexity becomes less than 2% of the period.

4 Proof of Main Theorem

Note first that it is enough to show that, for all τ and λ,

$$L(S_Z^{(\tau,\lambda)}) \geq \left(\frac{p+1}{2}\right)^m - 1,$$

where $S_Z^{(\tau,\lambda)}$ is given in (4). For this, we will denote α^τ by β, and take care of all possible cases of β and λ as follows:

1. CASE $\beta \notin F_p$ and $\lambda \neq 0$.
2. CASE $\beta \in F_p$.
   (a) case $\lambda = 0$.
   (b) case $\lambda \neq 0$. This case is further divided into the following:
      i. subcase $\beta = 1$.
      ii. subcase $\beta \neq 1$. This subcase is treated by several different methods according to the values of m as follows:
         A. for $m \geq 3$.
         B. for $m = 2$, or all even values of $m \geq 2$.
         C. for $m = 1$.

4.1 CASE $\beta \notin F_p$ and $\lambda \neq 0$

Note that if $\beta^i \notin F_p$, then we have $A_{-i}(\tau, \lambda) \neq 0$. Therefore,

$$L(S_Z^{(\tau,\lambda)}) \geq \left|\left\{\, i \;:\; \beta^i \notin F_p,\; 0 \leq i < p^m - 1 \,\right\}\right| \triangleq N.$$

If we let d be the least positive integer such that $\beta^d \in F_p$, then $d \geq 2$, and hence,

$$N = (p^m - 1)\left(1 - \frac{1}{d}\right) \geq \frac{p^m - 1}{2} \geq \left(\frac{p+1}{2}\right)^m - 1.$$

4.2 CASE $\beta \in F_p$

We will use

$$L(S_Z^{(\tau,\lambda)}) = n - |C| = p^m - 1 - |C|\,, \tag{12}$$

where

$$C \triangleq \{\, i \;:\; A_{-i}(\tau,\lambda) = 0,\ 0 \le i < p^m - 1 \,\}$$

and where $A_{-i}(\tau,\lambda)$ is given in Lemma 2. Observe that

$$C = \left\{ i \;:\; \prod_{a=0}^{m-1} \binom{i_a}{\frac{p-1}{2}} = (-1)^{\frac{p^m-1}{2}}(1-\lambda\beta^i),\quad 0 \le i < p^m - 1 \right\}. \tag{13}$$

Recall that, from earlier notation,

$$I_{\mathrm{nz}} = \left\{ i \;:\; \prod_{a=0}^{m-1} \binom{i_a}{\frac{p-1}{2}} \ne 0,\ 0 \le i < p^m - 1 \right\} \quad \text{and} \quad |I_{\mathrm{nz}}| = \left(\frac{p+1}{2}\right)^m - 1.$$

We will also consider its complement as follows:

$$I_{\mathrm{nz}}^{\mathrm{c}} \triangleq \{0,1,...,p^m-2\} \backslash I_{\mathrm{nz}} \quad \text{and hence} \quad |I_{\mathrm{nz}}^{\mathrm{c}}| = p^m - \left(\frac{p+1}{2}\right)^m.$$

Then, it is not difficult to show that

$$|I_{\mathrm{nz}}| \le |I_{\mathrm{nz}}^{\mathrm{c}}|.$$

Therefore, it is sufficient to prove that either $|C| \le |I_{\mathrm{nz}}|$ or $|C| \le |I_{\mathrm{nz}}^{\mathrm{c}}|$, since for both cases we have $|C| \le |I_{\mathrm{nz}}^{\mathrm{c}}|$, and therefore,

$$L(S_Z^{(\tau,\lambda)}) = p^m - 1 - |C| \ge p^m - 1 - |I_{\mathrm{nz}}^{\mathrm{c}}| = |I_{\mathrm{nz}}| = \left(\frac{p+1}{2}\right)^m - 1.$$

4.2.(a) case $\boldsymbol{\lambda = 0}$.
For $\lambda = 0$, we have

$$C = \left\{ i \;:\; \prod_{a=0}^{m-1} \binom{i_a}{\frac{p-1}{2}} = \pm 1,\quad 0 \le i < p^m - 1 \right\},$$

which implies $|C| \le |I_{\mathrm{nz}}|$. We will assume that $\lambda \ne 0$ in the remaining of the proof.

4.2.(b) case $\boldsymbol{\lambda \ne 0}$.

subcase $\beta = 1$.

If $\lambda = 1$, then $1 - \lambda\beta^i = 1 - \lambda = 0$, and hence, $|C| = |I_{\mathrm{nz}}^{\mathrm{c}}|$. If $\lambda \in F_p \setminus \{0,1\}$, then $1 - \lambda\beta^i = 1 - \lambda \ne 0$, and hence, $|C| \le |I_{\mathrm{nz}}|$.

subcase $\beta \ne 1$.

Note that in this case we have an initial estimation of the size of C from (13) as follows:

$$|C| \le \left|\{\, i \;:\; \beta^i = \lambda^{-1} \} \cap I_{\mathrm{nz}}^{\mathrm{c}}\right| + \left|\{\, i \;:\; \beta^i \ne \lambda^{-1} \} \cap I_{\mathrm{nz}}\right|. \tag{14}$$

Let $e > 1$ be the order of β over F_p, and hence, note that $e|(p-1)$. If there does not exist an integer u satisfying $\lambda^{-1} = \beta^u$ and $0 \le u < e$, then

$$|C| \le \left|\{\ i\ :\ \beta^i \ne \lambda^{-1}\} \cap I_{\mathrm{nz}}\right| \le |I_{\mathrm{nz}}|\,.$$

If such u exists, then (14) becomes,

$$|C| \le \left|\left\{i : \sum_{a=0}^{m-1} i_a \equiv u (\mathrm{mod}\ e)\right\} \cap I_{\mathrm{nz}}^{\mathrm{c}}\right| + \left|\left\{i : \sum_{a=0}^{m-1} i_a \not\equiv u (\mathrm{mod}\ e)\right\} \cap I_{\mathrm{nz}}\right|, \tag{15}$$

since

$$i = \sum_{a=0}^{m-1} i_a p^a \equiv \sum_{a=0}^{m-1} i_a \pmod{e}.$$

We need the following observation:

Lemma 3. *Let A be a set of k consecutive integers and e be a divisor of k, then*

$$\left|\left\{(x_0, \ldots, x_{m-1}) \in A^m : \sum_{j=0}^{m-1} x_j \equiv u \pmod{e}\right\}\right| = k^{m-1}\frac{k}{e},$$

for any $0 \le u \le e-1$. If e is not a divisor of k, then the above cardinality is $\ge k^{m-1}\lfloor \frac{k}{e} \rfloor$ and $\le k^{m-1}\lceil \frac{k}{e} \rceil$.

Proof. If we take any $m-1$ elements $x_0, x_1, ..., x_{m-2}$ from A, there are still k/e choices for x_{m-1}. ■

Now, we try to estimate both terms on the RHS of the inequality (15) as follows. The first term is bounded as follows:

$$\begin{aligned}
&\left|\left\{i : \sum_{a=0}^{m-1} i_a \equiv u \pmod{e} \text{ and there is } i_a \text{ with } 0 \le i_a < \frac{p-1}{2}\right\}\right| \\
&= \left|\left\{i : \sum_{a=0}^{m-1} i_a \equiv u \pmod{e}, 0 \le i_a \le p-1\right\}\right| \\
&\qquad - \left|\left\{i : \sum_{a=0}^{m-1} i_a \equiv u \pmod{e}, \frac{p-1}{2} \le i_a \le p-1\right\}\right| \\
&\le p^{m-1}\left\lceil \frac{p}{e} \right\rceil - \left(\frac{p+1}{2}\right)^{m-1}\left\lfloor \frac{p+1}{2e} \right\rfloor,
\end{aligned}$$

where the last inequality follows from Lemma 3. The second term on the RHS of the inequality (15) is bounded as follows:

$$\begin{aligned}
&\left|\left\{i : \sum_{a=0}^{m-1} i_a \not\equiv u \pmod e \text{ with } \frac{p-1}{2} \le i_a \le p-1 \text{ for all } i_a\right\}\right| \\
&= |I_{\mathrm{nz}}| - \left|\left\{i : \sum_{a=0}^{m-1} i_a \equiv u \pmod e \text{ with } \frac{p-1}{2} \le i_a \le p-1 \text{ for all } i_a\right\}\right| \\
&\le \Big(\frac{p+1}{2}\Big)^m - \Big(\frac{p+1}{2}\Big)^{m-1}\Big\lfloor\frac{p+1}{2e}\Big\rfloor.
\end{aligned}$$

Therefore, the inequality (15) becomes

$$|C| \le p^{m-1}\Big\lceil\frac{p}{e}\Big\rceil + \Big(\frac{p+1}{2}\Big)^m - 2\Big(\frac{p+1}{2}\Big)^{m-1}\Big\lfloor\frac{p+1}{2e}\Big\rfloor \tag{16}$$

$$\le p^{m-1}\Big(\frac{p-1}{e}+1\Big) + \Big(\frac{p+1}{2}\Big)^m - \Big(\frac{p+1}{2}\Big)^{m-1}\Big(\frac{p-1}{e}-1\Big). \tag{17}$$

Observe, that for $p = 3$ (and thus $e = 2$) (16) directly implies that

$$|C| \le 3^m - 2^m = |I_{\mathrm{nz}}^{\mathrm{c}}|, \quad \text{for all} \quad m \ge 3.$$

Now, it is not difficult to show, if $p \ge 5$ and $m \ge 3$, then (17) does not exceed $p^m - \left(\frac{p+1}{2}\right)^m$. For this, we need to show that

$$\Big(\frac{p+1}{2}\Big)^{m-1}\Big(2\frac{p+1}{2} - \frac{p-1}{e} + 1\Big) \le p^{m-1}\Big(p - \frac{p-1}{e} - 1\Big)$$

which is the same as

$$\Big(\frac{p+1}{2p}\Big)^{m-1} \le \frac{p - \frac{p-1}{e} - 1}{p - \frac{p-1}{e} + 2}.$$

Note that, for $m \ge 3$ and $p \ge 5$, we have

$$\Big(\frac{p+1}{2p}\Big)^{m-1} \le \Big(\frac{p+1}{2p}\Big)^2 \le \Big(\frac{3}{5}\Big)^2 = \frac{9}{25},$$

and therefore it is enough to prove

$$\frac{p - \frac{p-1}{e} - 1}{p - \frac{p-1}{e} + 2} \ge \frac{6}{25}.$$

The last inequality holds, since

$$e \ge 2 > \frac{p-1}{p-2} > \frac{19p-19}{19p-37}$$

for $p \ge 5$.

The case $m = 2$ can be covered by direct calculations, using (15). Or, we may consider the following, which, in fact, works for all $p \geq 3$ and even values of $m \geq 2$. Let

$$H \triangleq \left\{ i \ : \ 0 \leq i_a \leq \frac{p-1}{2},\ 0 \leq i < p^m - 1,\ i \neq \frac{p^m-1}{2} \right\}. \tag{18}$$

Then

$$\left| \left\{ i : \sum_{a=0}^{m-1} i_a \not\equiv u \pmod e \right\} \cap I_{\mathrm{nz}} \right| = \left| \left\{ i : \sum_{a=0}^{m-1} i_a \not\equiv u \pmod e \right\} \cap H \right| \tag{19}$$

since

$$I_{\mathrm{nz}} = \left\{ i \ : \ \frac{p-1}{2} \leq i_a \leq p-1,\ 0 \leq i < p^m - 1 \right\}$$

and

$$\sum_{a=0}^{m-1} i_a = \sum_{a=0}^{m-1} \left(i_a - \frac{p-1}{2} \right) + m\frac{p-1}{2} \equiv \sum_{a=0}^{m-1} \left(i_a - \frac{p-1}{2} \right) \pmod e.$$

Since $H \subset I_{\mathrm{nz}}^{\mathrm{c}}$, the second term of (15) is upper bounded by

$$\left| \left\{ i \ : \ \sum_{a=0}^{m-1} i_a \not\equiv u \pmod e \right\} \cap I_{\mathrm{nz}}^{\mathrm{c}} \right|.$$

Therefore,

$$|C| \leq |I_{\mathrm{nz}}^{\mathrm{c}}|.$$

The proof will be complete if we show the following, for the case $m = 1$.

Lemma 4. *Let p be an odd prime and $\lambda \neq 0, \beta \in F_p$, and $\beta \neq 1$. Then,*

$$|C| = \left| \left\{ i : 0 \leq i \leq p-2,\ \binom{i}{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} (1 - \lambda\beta^i) \pmod p \right\} \right| \leq \frac{p-1}{2}.$$

Proof. Let $e > 1$ be the order of β. If there is no u with $1 - \lambda\beta^u = 0$, then obviously, by setting $(-1)^{\frac{p-1}{2}}(1 - \lambda\beta^i) = d(i) \pmod p$,

$$|C| = \left| \left\{ i : \frac{p-1}{2} \leq i \leq p-2,\ \binom{i}{\frac{p-1}{2}} = d(i) \not\equiv 0 \pmod p \right\} \right| \leq \frac{p-1}{2}.$$

Suppose, there is $0 \leq u < e$ with $1 - \lambda\beta^u = 0$, implying $1 - \lambda\beta^w = 0$ for any $w \equiv u \pmod e,\ 0 \leq w \leq p-2$. Then

$$\begin{aligned} |C| = &\left| \left\{ i : 0 \leq i < \tfrac{p-1}{2}, \tbinom{i}{\frac{p-1}{2}} \equiv d(i) \equiv 0 \pmod p \right\} \right| \\ &+ \left| \left\{ i : \tfrac{p-1}{2} \leq i \leq p-2, \tbinom{i}{\frac{p-1}{2}} \equiv d(i) \not\equiv 0 \pmod p \right\} \right|. \end{aligned} \tag{20}$$

Since it is obvious $\left(\frac{i}{\frac{p-1}{2}}\right) \neq d(i)$ for $i = \frac{p-1}{2}$, this case can be excluded from the second term of (20). Then the second term is equal to

$$\left|\left\{i : \frac{p-1}{2} < i \leq p-2\right\}\right| - \left|\left\{i : \frac{p-1}{2} < i \leq p-2,\ i \equiv u \pmod{e}\right\}\right|$$
$$= \frac{p-1}{2} - 1 - \left\lfloor \frac{p-1}{2e} - \frac{1}{e} \right\rfloor.$$

This yields

$$|C| \leq \left\lceil \frac{p-1}{2e} \right\rceil + \frac{p-1}{2} - 1 - \left\lfloor \frac{p-1}{2e} - \frac{1}{e} \right\rfloor. \tag{21}$$

If $2e|p-1$, RHS of (21) is obviously equal to $\frac{p-1}{2}$. If not, it is enough to prove

$$\left\lfloor \frac{p-1}{2e} - \frac{1}{e} \right\rfloor = \left\lfloor \frac{p-1}{2e} \right\rfloor.$$

Let $p-1 \equiv k \pmod{2e}$. Since k is even and ≥ 2, we get

$$\left\lfloor \frac{p-1}{2e} \right\rfloor = \frac{p-1}{2e} - \frac{k}{2e} \leq \frac{p-1}{2e} - \frac{1}{e}.$$

Together with

$$\left\lfloor \frac{p-1}{2e} - \frac{1}{e} \right\rfloor \leq \left\lfloor \frac{p-1}{2e} \right\rfloor,$$

we can complete the proof.

References

1. V. M. Sidelnikov, "Some k-valued pseudo-random and nearly equidistant codes," *Probl. Pered. Inform.*, vol. 5, no. 1, pp. 16–22, 1969.
2. A. Lempel, M. Cohn, and W. L. Eastman, "A class of balanced binary sequences with optimal autocorrelation properties," *IEEE Trans. Inform. Theory*, vol. 23, no. 1, pp. 38–42, Jan. 1977.
3. D. V. Sarwate, "Comments on 'A Class of Balanced Binary Sequences with Optimal Autocorrelation Properties'," *IEEE Trans. Inform. Theory*, vol. 24, no. 1, pp. 128–129, Jan. 1978.
4. J.-S. No, H. Chung, H.-Y. Song, K. Yang, J.-D. Lee and T. Helleseth, "New Construction for Binary Sequences of period p^m-1 with Optimal Autocorrelation Using $(z+1)^d + az^d + b$," *IEEE Trans. Inform. Theory*, vol. 47, no. 4, pp. 1638–1644, May 2001.
5. T. Helleseth and K. Yang, "On binary sequences of period p^m-1 with optimal autocorrelation," in *Proc. 2001 Conf. Sequences and Their Applications* (SETA '01), Bergen, Norway, May 13-17 2001, pp. 29–30.
6. G. M. Kyureghyan and A. Pott, "On the linear complexity of the Sidelnikov-Lempel-Cohn-Eastman sequences," *Design, Codes and Cryptography.*, vol. 29, pp. 149–164, 2003.
7. T. Helleseth, S.-H. Kim, and J.-S. No, "Linear complexity over F_p and trace representation of Lempel-Cohn-Eastman sequences," *IEEE Trans. Inform. Theory*, vol. 49, no. 6, pp. 1548–1522, June 2003.

8. T. Helleseth, M. Maas, J.E. Mathiassen and T. Segers, "Linear complexity over F_p of Sidelnikov sequences," *IEEE Trans. Inform. Theory*, vol. 50, no. 10, pp. 2468-2472, Oct. 2004.
9. M. Stamp and C. F. Martin, "An algorithm for the k-linear complexity of binary sequences with period 2^n," *IEEE Trans. Inform. Theory*, vol. 39, no. 4, pp. 1398–1401, July. 1993.
10. T. W. Cusick, C. Ding, and A. Renvall, *Stream Ciphers and Number Theory.* North-Holland Mathematical Library 55. Amsterdam: North-Holland/Elsevier, 1998.
11. R. E. Blahut, "Transform techniques for error control codes," *IBM J. Res. Develop.*, vol. 23, pp. 299–315, 1979.
12. R. E. Blahut, *Theory and Practice of Error Control Codes.* New York: Addison-Wesley, 1983.