SCIENCE CHINA
Information Sciences

• **Supplementary File** •

On the k-error linear complexity of $2p^2$-periodic binary sequences

Zhihua NIU[1], Can YUAN[1], Zhixiong CHEN[2*], Xiaoni DU[3] & Tao ZHANG[1]

[1]*School of Computer Engineering and Science, Shanghai University, Shanghai* 200444*, China;*
[2]*Provincial Key Laboratory of Applied Mathematics, Putian University, Putian* 351100*, China;*
[3]*College of Mathematics and Statistics, Northwest Normal University, Lanzhou* 730070*, China*

Appendix A Lower bounds on linear complexity.

Appendix A.1 Proof of Lemma 1

Proof. We suppose $ord_{p^2}(2) = \mu$. First, we write $2^\lambda = 1 + ap$ for some integer a since $2^\lambda \equiv 1 \pmod{p}$. Then we have $2^{\lambda p} = (1+ap)^p = 1 + ap^2 + \cdots$, and hence $2^{\lambda p} \equiv 1 \pmod{p^2}$. This implies that μ is a divisor of λp. On the other hand, since $2^{p-1} \not\equiv 1 \pmod{p^2}$, we see that $p \nmid a$.

Second, the assumption of $2^{p-1} \not\equiv 1 \pmod{p^2}$ implies that $\mu \geqslant p$. So we can write $\mu = \lambda p^\omega$ for some positive integer $\omega \leqslant 1$. Suppose $\omega < 1$, then $2^{\lambda p^\omega} = (1+ap)^{p^\omega} = 1 + ap^{\omega+1} + \cdots$, which contradicts to $2^\mu = 2^{\lambda p^\omega} \equiv 1 \pmod{p^2}$. Hence $\omega = 1$ and $\mu = \lambda p$. This completes the proof of Lemma 1.

Appendix A.2 Proof of Theorem 1

Proof. Let $\Phi_1(x) = 1 + x + x^2 + \cdots + x^{p-1}$ and $\Phi_2(x) = 1 + x^p + x^{2p} + \cdots + x^{(p-1)p}$ over $\mathbb{F}_2$. We see that $x^{p^2} - 1 = (x-1)\Phi_1(x)\Phi_2(x)$ and $x^{2p^2} - 1 = (x-1)^2\Phi_1^2(x)\Phi_2^2(x)$ over $\mathbb{F}_2$.

Let the corresponding $p \times 2p$ matrix of s^N be $\mathfrak{M}_s \triangleq [M_0, M_1, \ldots, M_{2p-1}]$. Now if we suppose $\Phi_2^2(x) \,|\, s^N(x)$ and write $s^N(x) = H(x)\Phi_2^2(x)$ for some polynomial $H(x) = h_0 + h_1 x + \cdots + h_{2p-1}x^{2p-1} \in \mathbb{F}_2[x]$ of degree $< 2p$. Then we derive for $0 \leqslant i < 2p$, $M_i = \begin{bmatrix} s_i \\ s_{i+2p} \\ \vdots \\ s_{i+2(p-1)p} \end{bmatrix} = \begin{cases} (0,0,\ldots,0)^T, & \text{if } h_i = 0 \\ (1,1,\ldots,1)^T, & \text{if } h_i = 1 \end{cases}$, from which we get that the second row, the third row, $\ldots$, the pth row of the matrix $\mathfrak{M}_s$ are the same as the first row, hence $2p$ is the period of s. This is in contradiction to the least period of s being $2p^2$, hence $\Phi_2^2(x) \nmid s^N(x)$.

On the other hand, if $\Phi_2(x)$ happens to be rooted at the elements of degree p^2 over $\mathbb{F}_2$, then there exists a root β of $\Phi_2(x)$ such that $s^N(\beta) \neq 0$. And since the order of 2 modulo p^2 is λp, then $s^N\left(\beta^{2^j}\right) = s^N(\beta)^{2^j} \neq 0$ for $0 \leqslant j < \lambda p$, so $LC(s) \geqslant \lambda p$. This completes the proof of Theorem 1.

Appendix A.3 Proof of Lemma 2

Proof. Let s^N be arranged into matrices $\mathfrak{A}_s \triangleq \left[\frac{\mathfrak{A}^{(1)}}{\mathfrak{A}^{(2)}}\right]$ and $\mathfrak{A}^{(3)} = \mathfrak{A}^{(1)} + \mathfrak{A}^{(2)}$ defined in this study.

If $\left(x^{p^2} - 1\right) | s^N(x)$, then for $0 \leqslant i < p$ each column $\mathfrak{A}_i^{(3)}$ of matrix $\mathfrak{A}^{(3)}$ is $(0,0,\cdots,0)^T$, indicating $\mathfrak{A}^{(1)} = \mathfrak{A}^{(2)}$, i.e., $s_n = s_{n+p^2}$ for all $0 \leqslant n < p^2$. Hence the period of the sequence s drops to p^2, which contradicts to the least period $2p^2$. So $\left(x^{p^2} - 1\right) \nmid s^N(x)$. This completes the proof of Lemma 2.

* Corresponding author (email: ptczx@126.com)

Appendix A.4 Proof of Theorem 2

Proof. If 2 is a primitive root modulo p^2, then $\Phi_1(x)$ and $\Phi_2(x)$ are irreducible polynomial over $\mathbb{F}_2$. And from Theorem 1, we know $\Phi_2^2(x) \nmid s^N(x)$. So there are two cases:

(i) Suppose $\Phi_2(x) | s^N(x)$. Lemma 2 shows $\left(x^{p^2}-1\right) \nmid s^N(x)$, then the factor of $\gcd\left(x^{2p^2}-1, s^N(x)\right)$ must be one of the following five:

$$\Phi_1^2(x)\Phi_2(x), (x-1)^2\Phi_2(x), \Phi_1(x)\Phi_2(x), (x-1)\Phi_2(x), \Phi_2(x),$$

thereby the minimal polynomial of s must be one of the following five:

$$(x-1)^2\Phi_2(x), \Phi_1^2(x)\Phi_2(x), (x-1)^2\Phi_1(x)\Phi_2(x), (x-1)\Phi_1^2(x)\Phi_2(x), (x-1)^2\Phi_1^2(x)\Phi_2(x),$$

hence the linear complexity of s satisfies one of the following five:

$$LC(s) \in \left\{p^2-p+2, p^2+p-2, p^2+1, p^2+p-1, p^2+p\right\},$$

It can be written as $LC(s) = p^2-p+a$ where $a \in \{2, 2p-2, p+1, 2p-1, 2p\}$. Further, we obtain $p^2-p < LC(s) \leqslant p^2+p$.

(ii) Suppose $\Phi_2(x) \nmid s^N(x)$, then $\Phi_2^2(x) \nmid s^N(x)$, hence it is easy to get $LC(s) \geqslant 2\left(p^2-p\right)$, and the factor of $\gcd\left(x^{2p^2}-1, s^N(x)\right)$ must be one of the following nine:

$$(x-1)^2\Phi_1^2(x), (x-1)\Phi_1^2(x), \Phi_1^2(x), (x-1)^2\Phi_1(x), (x-1)^2, (x-1)\Phi_1(x), \Phi_1(x), (x-1), 1.$$

The minimal polynomial of s must be one of the following nine:

$$\Phi_2^2(x), (x-1)\Phi_2^2(x), (x-1)^2\Phi_2^2(x), \Phi_1(x)\Phi_2^2(x), \Phi_1^2(x)\Phi_2^2(x), (x-1)\Phi_1(x)\Phi_2^2(x),$$
$$(x-1)^2\Phi_1(x)\Phi_2^2(x), (x-1)\Phi_1^2(x)\Phi_2^2(x), (x-1)^2\Phi_1^2(x)\Phi_2^2(x).$$

Further, we obtain $LC(s) = 2\left(p^2-p\right)+b$ where $b \in \{0, 1, 2, p-1, 2p-2, p, p+1, 2p-1, 2p\}$.
This completes the proof of Theorem 2.

Appendix B k-error linear complexity

Appendix B.1 Proof of Lemma 3

Proof. It is easy to see that $\Phi_2(x) | s^N(x)$ but $\Phi_2^2(x) \nmid s^N(x)$ from $p^2-p < LC(s) \leqslant p^2+p$. Since

$$s^N(x) = \sum_{i=0}^{p^2-1} s_i x^i + x^{p^2} \sum_{i=0}^{p^2-1} s_{i+p^2} x^i = \sum_{i=0}^{p^2-1} (s_i + s_{i+p^2}) x^i \left(\mathrm{mod}\ x^{p^2}-1\right),$$

we have $\Phi_2(x) | \sum_{i=0}^{p^2-1} (s_i + s_{i+p^2}) x^i$. Thus, in matrix $\mathfrak{A}^{(3)} = \mathfrak{A}^{(1)} + \mathfrak{A}^{(2)} \triangleq \left[\mathfrak{A}_0^{(3)}, \mathfrak{A}_1^{(3)}, \ldots, \mathfrak{A}_{p-1}^{(3)}\right]$, each column is either $(0,0,\ldots,0)^T$ or $(1,1,\ldots,1)^T$, and at least one column is $(1,1,\ldots,1)^T$, otherwise it contradicts to the least period of s. For $0 \leqslant i < p$,

(i) if a column $\mathfrak{A}_i^{(3)}$ of $\mathfrak{A}^{(3)}$ is $(0,0,\ldots,0)^T$, then $\mathfrak{A}_i^{(1)} = \mathfrak{A}_i^{(2)}$, that is $wt\left(\mathfrak{A}_i^{(1)}\right) = wt\left(\mathfrak{A}_i^{(2)}\right)$. When this sequence is arranged into the matrix $\mathfrak{M}_s$, it satisfies $wt(M_i) = wt(M_{i+p})$.

(ii) if a column $\mathfrak{A}_i^{(3)}$ of $\mathfrak{A}^{(3)}$ is $(1,1,\ldots,1)^T$, then $\mathfrak{A}_i^{(1)}$ and $\mathfrak{A}_i^{(2)}$ are complementary. When this sequence is arranged into the matrix $\mathfrak{M}_s$, it satisfies $wt(M_i) + wt(M_{i+p}) = p$. Since at least one column $\mathfrak{A}_i^{(3)}$ of $\mathfrak{A}^{(3)}$ is $(1,1,\ldots,1)^T$, there must be $0 \leqslant i_0 < p$ such that $wt(M_{i_0}) + wt(M_{i_0+p}) = p$.
This completes the proof of Lemma 3.

Appendix B.2 Theorem 3 in the case of $p^2-p < LC(s) \leqslant p^2+p$

Let s be a binary sequence with the least period $N = 2p^2$, and let s^N be the first period of s. Let the corresponding $p \times 2p$ matrix be $\mathfrak{M}_s$, and the corresponding $2p \times p$ matrix be $\mathfrak{A}_s$, and the corresponding $p \times p$ matrix be $\mathfrak{A}^{(3)}$, and the generating polynomial of s^N be $s^N(x)$. Let $\mu_1 = 2 \cdot \sum_{0 \leqslant i < p} \min\{wt(M_i), p - wt(M_i)\}$, $\mu_2 = \mu_3 + 2\left\{\sum_{\substack{0 \leqslant i < p \\ wt\left(\mathfrak{A}_i^{(3)}\right)=p}} 1 - \max\{\mu_9, \mu_{10}\}\right\}$,

$$\mu_3 = p \cdot \sum_{\substack{0 \leqslant i < p \\ wt\left(\mathfrak{A}_i^{(3)}\right)=0}} 1,\ \mu_4 = p \cdot \sum_{\substack{0 \leqslant i < p \\ wt\left(\mathfrak{A}_i^{(3)}\right)=p}} 1,\ \mu_5 = \mu_4 + 2 \cdot \sum_{\substack{0 \leqslant i < p \\ wt\left(\mathfrak{A}_i^{(3)}\right)=0 \\ wt(M_i) \equiv 0 (\bmod 2)}} 1,\ \mu_6 = \mu_4 + 2 \cdot \sum_{\substack{0 \leqslant i < p \\ wt\left(\mathfrak{A}_i^{(3)}\right)=0 \\ wt(M_i) \equiv 1 (\bmod 2)}} 1,\ \mu_7 = 2,$$

$$\mu_8 = p,\ \mu_9 = \sum_{\substack{0 \leqslant i < p \\ wt\left(\mathfrak{A}_i^{(3)}\right)=p \\ i \equiv 0 (\bmod 2) \\ wt(M_i) \equiv 0 (\bmod 2)}} 1 + \sum_{\substack{0 \leqslant i < p \\ wt\left(\mathfrak{A}_i^{(3)}\right)=p \\ i \equiv 1 (\bmod 2) \\ wt(M_i) \equiv 1 (\bmod 2)}} 1,\ \mu_{10} = \sum_{\substack{0 \leqslant i < p \\ wt\left(\mathfrak{A}_i^{(3)}\right)=p \\ i \equiv 1 (\bmod 2) \\ wt(M_i) \equiv 0 (\bmod 2)}} 1 + \sum_{\substack{0 \leqslant i < p \\ wt\left(\mathfrak{A}_i^{(3)}\right)=p \\ i \equiv 0 (\bmod 2) \\ wt(M_i) \equiv 1 (\bmod 2)}} 1.$$

If 2 is a primitive root modulo p^2, then the k-error linear complexity of s satisfies the following formulas.

(i) If $LC(s) = p^2 - p + 2$, then

$$LC_k(s) = \begin{cases} p^2 - p + 2, & \text{if } 0 \leqslant k < \mu_1 \\ \leqslant 2p, & \text{if } k \geqslant \mu_1 \end{cases}.$$

(ii) If $LC(s) = p^2 + 1$, then

$$LC_k(s) = \begin{cases} p^2 + 1, & \text{if } 0 \leqslant k < \mu_2 \\ p^2 - p + 2, & \text{if } \mu_2 \leqslant k < \mu_1 \\ \leqslant 2p, & \text{if } k \geqslant \mu_1 \end{cases}, \text{for } \mu_2 < \mu_1;$$

or

$$LC_k(s) = \begin{cases} p^2 + 1, & \text{if } 0 \leqslant k < \mu_1 \\ \leqslant 2p, & \text{if } k \geqslant \mu_1 \end{cases}, \text{for } \mu_1 \leqslant \mu_2.$$

(iii) If $LC(s) = p^2 + p - 2$, then

$$LC_k(s) = \begin{cases} p^2 + p - 2, & \text{if } 0 \leqslant k < \mu_3 \\ p^2 + 1, & \text{if } \mu_3 \leqslant k < \mu_2 \\ p^2 - p + 2, & \text{if } \mu_2 \leqslant k < \mu_1 \\ \leqslant 2p, & \text{if } k \geqslant \mu_1 \end{cases}, \text{for } \mu_3 < \mu_4, \mu_2 < \mu_1;$$

or

$$LC_k(s) = \begin{cases} p^2 + p - 2, & \text{if } 0 \leqslant k < \mu_3 \\ p^2 + 1, & \text{if } \mu_3 \leqslant k < \mu_1 \\ \leqslant 2p, & \text{if } k \geqslant \mu_1 \end{cases}, \text{for } \mu_3 < \mu_4, \mu_3 < \mu_1 \leqslant \mu_2;$$

or

$$LC_k(s) = \begin{cases} p^2 + p - 2, & \text{if } 0 \leqslant k < \mu_4 \\ p^2 - 1, & \text{if } \mu_4 \leqslant k < \mu_5 \\ p^2 - p + 1, & \text{if } \mu_5 \leqslant k < \mu_6 \\ p^2 - p, & \text{if } \mu_6 \leqslant k < \mu_1 \\ \leqslant 2p, & \text{if } k \geqslant \mu_1 \end{cases}, \text{for } \mu_4 < \mu_3, \mu_5 < \mu_6 < \mu_1;$$

or

$$LC_k(s) = \begin{cases} p^2 + p - 2, & \text{if } 0 \leqslant k < \mu_4 \\ p^2 - 1, & \text{if } \mu_4 \leqslant k < \mu_5 \\ p^2 - p + 1, & \text{if } \mu_5 \leqslant k < \mu_1 \\ \leqslant 2p, & \text{if } k \geqslant \mu_1 \end{cases}, \text{for } \mu_4 < \mu_3, \mu_5 < \mu_1 \leqslant \mu_6;$$

or

$$LC_k(s) = \begin{cases} p^2 + p - 2, & \text{if } 0 \leqslant k < \mu_4 \\ p^2 - 1, & \text{if } \mu_4 \leqslant k < \mu_6 \\ p^2 - p, & \text{if } \mu_6 \leqslant k < \mu_1 \\ \leqslant 2p, & \text{if } k \geqslant \mu_1 \end{cases}, \text{for } \mu_4 < \mu_3, \mu_6 < \mu_5, \mu_6 < \mu_1;$$

or

$$LC_k(s) = \begin{cases} p^2 + p - 2, & \text{if } 0 \leqslant k < \mu_4 \\ p^2 - 1, & \text{if } \mu_4 \leqslant k < \mu_1 \\ \leqslant 2p, & \text{if } k \geqslant \mu_1 \end{cases}, \text{for } \mu_4 < \mu_3, \mu_4 < \mu_1, \mu_1 \leqslant \mu_5, \mu_1 \leqslant \mu_6;$$

or

$$LC_k(s) = \begin{cases} p^2 + p - 2, & \text{if } 0 \leqslant k < \mu_1 \\ \leqslant 2p, & \text{if } k \geqslant \mu_1 \end{cases}, \text{for } \mu_1 \leqslant \mu_3, \mu_1 \leqslant \mu_4.$$

(iv) If $LC(s) = p^2 + p - 1$, then

$$LC_k(s) = \begin{cases} p^2 + p - 1, & \text{if } 0 \leqslant k < \mu_7 \\ p^2 + p - 2, & \text{if } \mu_7 \leqslant k < \mu_3 \\ p^2 + 1, & \text{if } \mu_3 \leqslant k < \mu_2 \\ p^2 - p + 2, & \text{if } \mu_2 \leqslant k < \mu_1 \\ \leqslant 2p, & \text{if } k \geqslant \mu_1 \end{cases}, \text{for } \mu_3 < \mu_4, \mu_2 < \mu_1;$$

or

$$LC_k(s) = \begin{cases} p^2 + p - 1, & \text{if } 0 \leqslant k < \mu_7 \\ p^2 + p - 2, & \text{if } \mu_7 \leqslant k < \mu_3 \\ p^2 + 1, & \text{if } \mu_3 \leqslant k < \mu_1 \\ \leqslant 2p, & \text{if } k \geqslant \mu_1 \end{cases}, \text{for } \mu_3 < \mu_4, \mu_3 < \mu_1 \leqslant \mu_2;$$

or

$$LC_k(s)=\begin{cases} p^2+p-1, & \text{if } 0\leqslant k<\mu_7 \\ p^2+p-2, & \text{if } \mu_7\leqslant k<\mu_4 \\ p^2-1, & \text{if } \mu_4\leqslant k<\mu_5 \\ p^2-p+1, & \text{if } \mu_5\leqslant k<\mu_6 \\ p^2-p, & \text{if } \mu_6\leqslant k<\mu_1 \\ \leqslant 2p, & \text{if } k\geqslant \mu_1 \end{cases}, \text{for } \mu_4<\mu_3, \mu_5<\mu_6<\mu_1;$$

or

$$LC_k(s)=\begin{cases} p^2+p-1, & \text{if } 0\leqslant k<\mu_7 \\ p^2+p-2, & \text{if } \mu_7\leqslant k<\mu_4 \\ p^2-1, & \text{if } \mu_4\leqslant k<\mu_5 \\ p^2-p+1, & \text{if } \mu_5\leqslant k<\mu_1 \\ \leqslant 2p, & \text{if } k\geqslant \mu_1 \end{cases}, \text{for } \mu_4<\mu_3, \mu_5<\mu_1\leqslant\mu_6;$$

or

$$LC_k(s)=\begin{cases} p^2+p-1, & \text{if } 0\leqslant k<\mu_7 \\ p^2+p-2, & \text{if } \mu_7\leqslant k<\mu_4 \\ p^2-1, & \text{if } \mu_4\leqslant k<\mu_6 \\ p^2-p, & \text{if } \mu_6\leqslant k<\mu_1 \\ \leqslant 2p, & \text{if } k\geqslant \mu_1 \end{cases}, \text{for } \mu_4<\mu_3, \mu_6<\mu_5, \mu_6<\mu_1;$$

or

$$LC_k(s)=\begin{cases} p^2+p-1, & \text{if } 0\leqslant k<\mu_7 \\ p^2+p-2, & \text{if } \mu_7\leqslant k<\mu_4 \\ p^2-1, & \text{if } \mu_4\leqslant k<\mu_1 \\ \leqslant 2p, & \text{if } k\geqslant \mu_1 \end{cases}, \text{for } \mu_4<\mu_3, \mu_4<\mu_1, \mu_1\leqslant\mu_5, \mu_1\leqslant\mu_6;$$

or

$$LC_k(s)=\begin{cases} p^2+p-1, & \text{if } 0\leqslant k<\mu_7 \\ p^2+p-2, & \text{if } \mu_7\leqslant k<\mu_1 \\ \leqslant 2p, & \text{if } k\geqslant \mu_1 \end{cases}, \text{for } \mu_1\leqslant\mu_3, \mu_1\leqslant\mu_4.$$

(v) If $LC(s)=p^2+p$, then

$$LC_k(s)=\begin{cases} p^2+p, & \text{if } 0\leqslant k<\mu_8 \\ p^2+p-2, & \text{if } \mu_8\leqslant k<\mu_3 \\ p^2+1, & \text{if } \mu_3\leqslant k<\mu_2 \\ p^2-p+2, & \text{if } \mu_2\leqslant k<\mu_1 \\ \leqslant 2p, & \text{if } k\geqslant \mu_1 \end{cases}, \text{for } \mu_8<\mu_3<\mu_4, \mu_2<\mu_1;$$

or

$$LC_k(s)=\begin{cases} p^2+p, & \text{if } 0\leqslant k<\mu_8 \\ p^2+p-2, & \text{if } \mu_8\leqslant k<\mu_3 \\ p^2+1, & \text{if } \mu_3\leqslant k<\mu_1 \\ \leqslant 2p, & \text{if } k\geqslant \mu_1 \end{cases}, \text{for } \mu_8<\mu_3<\mu_4, \mu_3<\mu_1\leqslant\mu_2;$$

or

$$LC_k(s)=\begin{cases} p^2+p, & \text{if } 0\leqslant k<\mu_8 \\ p^2+p-2, & \text{if } \mu_8\leqslant k<\mu_4 \\ p^2-1, & \text{if } \mu_4\leqslant k<\mu_5 \\ p^2-p+1, & \text{if } \mu_5\leqslant k<\mu_6 \\ p^2-p, & \text{if } \mu_6\leqslant k<\mu_1 \\ \leqslant 2p, & \text{if } k\geqslant \mu_1 \end{cases}, \text{for } \mu_4<\mu_3, \mu_5<\mu_6<\mu_1;$$

or

$$LC_k(s)=\begin{cases} p^2+p, & \text{if } 0\leqslant k<\mu_8 \\ p^2+p-2, & \text{if } \mu_8\leqslant k<\mu_4 \\ p^2-1, & \text{if } \mu_4\leqslant k<\mu_5 \\ p^2-p+1, & \text{if } \mu_5\leqslant k<\mu_1 \\ \leqslant 2p, & \text{if } k\geqslant \mu_1 \end{cases}, \text{for } \mu_4<\mu_3, \mu_5<\mu_1\leqslant\mu_6;$$

or

$$LC_k(s)=\begin{cases}p^2+p, & \text{if } 0\leqslant k<\mu_8\\ p^2+p-2, & \text{if } \mu_8\leqslant k<\mu_4\\ p^2-1, & \text{if } \mu_4\leqslant k<\mu_6\\ p^2-p, & \text{if } \mu_6\leqslant k<\mu_1\\ \leqslant 2p, & \text{if } k\geqslant\mu_1\end{cases},\text{for } \mu_4<\mu_3,\mu_6\leqslant\mu_5,\mu_6<\mu_1;$$

or

$$LC_k(s)=\begin{cases}p^2+p, & \text{if } 0\leqslant k<\mu_8\\ p^2+p-2, & \text{if } \mu_8\leqslant k<\mu_4\\ p^2-1, & \text{if } \mu_4\leqslant k<\mu_1\\ \leqslant 2p, & \text{if } k\geqslant\mu_1\end{cases},\text{for } \mu_4<\mu_3,\mu_4<\mu_1,\mu_1\leqslant\mu_5,\mu_1\leqslant\mu_6;$$

or

$$LC_k(s)=\begin{cases}p^2+p, & \text{if } 0\leqslant k<\mu_8\\ p^2+p-2, & \text{if } \mu_8\leqslant k<\mu_1\\ \leqslant 2p, & \text{if } k\geqslant\mu_1\end{cases},\text{for } \mu_8<\mu_1,\mu_1\leqslant\mu_3,\mu_1\leqslant\mu_4;$$

or

$$LC_k(s)=\begin{cases}p^2+p, & \text{if } 0\leqslant k<\mu_1\\ \leqslant 2p, & \text{if } k\geqslant\mu_1\end{cases},\text{for } \mu_1\leqslant\mu_8,\mu_1\leqslant\mu_4.$$

Proof.

(i) Since $LC(s)=p^2-p+2$ is the minimum of the linear complexity of s, changing any bit of s does not cause a decrease on linear complexity as long as the period of s does not decrease. Hence we consider how many terms changed in s^N will cause the period to decline. We can obtain that the period of s will drop to $2p$ when each column of matrix $\mathfrak{M}_s$ is $(0,0,\ldots,0)^T$ or $(1,1,\ldots,1)^T$, thus according to Lemma 3, we only need to change $\min\{wt(M_i),p-wt(M_i)\}$ terms for each column, so we take $\mu_1=2\sum\limits_{0\leqslant i<p}\min\{wt(M_i),p-wt(M_i)\}$.

(ii) From the proof of Lemma 3, we know that if $\Phi_2(x)\,|s^N(x)$, then each column of matrix $\mathfrak{A}^{(3)}$ is either $(0,0,\ldots,0)^T$ or $(1,1,\ldots,1)^T$, and at least one column is $(1,1,\ldots,1)^T$. Based on this, if $\Phi_1(x)\Phi_2(x)\,|s^N(x)$, then each column of $\mathfrak{A}^{(3)}$ is $(1,1,\ldots,1)^T$, so we take $\mu_3=p\cdot\sum\limits_{\substack{0\leqslant i<p\\ wt\left(\mathfrak{A}_i^{(3)}\right)=0}}1$ to satisfy this condition. We can derive $\Phi_1(x)\Phi_2(x)\,|s^N(x)$ from $LC(s)=p^2+1$, so $\mu_3=0$ in this case. Next, we consider how to satisfy $\Phi_1^2(x)\Phi_2(x)\,|s^N(x)$. We conclude that each column of $\mathfrak{A}^{(3)}$ is $(1,1,\ldots,1)^T$ and the weight of adjacent columns in matrix $\mathfrak{M}_s$ will be different in parity. So μ_9 and μ_{10} are to determine the parity of the weight of adjacent columns, and we take $\mu_2=\mu_3+2\left\{\sum\limits_{\substack{0\leqslant i<p\\ wt\left(\mathfrak{A}_i^{(3)}\right)=p}}1-\max\{\mu_9,\mu_{10}\}\right\}$.

For $\mu_2<\mu_1$, changing k bits of s^N, if $0\leqslant k<\mu_2$, then $\Phi_1(x)\Phi_2(x)\,|s^N(x)$, hence $LC(s)=p^2+1$; if $\mu_2\leqslant k<\mu_1$, then $\Phi_1^2(x)\Phi_2(x)\,|s^N(x)$, hence $LC(s)=p^2-p+2$; if $k\geqslant\mu_1$, then $\Phi_2^2(x)\,|s^N(x)$, hence $LC(s)\leqslant 2p$. For $\mu_2\geqslant\mu_1$, changing k bits of s^N, if $0\leqslant k<\mu_1$, then $\Phi_1(x)\Phi_2(x)\,|s^N(x)$, hence $LC(s)=p^2+1$; if $k\geqslant\mu_1$, then $\Phi_2^2(x)\,|s^N(x)$, hence $LC(s)\leqslant 2p$.

Similarly, we can prove the other cases by referring to case (ii). This completes the proof of Theorem 3.

Appendix B.3 Theorem 4 in the case of $LC(s)\geqslant 2\left(p^2-p\right)$

Let symbols s, s^N, $\mathfrak{M}_s$, $\mathfrak{A}_s$, $\mathfrak{A}^{(3)}$, $s^N(x)$ be the same as Theorem 3. Let $\mu_1=\sum\limits_{0\leqslant i<2p}\min\{wt(M_i),p-wt(M_i)\}$, $\mu_2=\sum\limits_{0\leqslant i<p}wt\left(\mathfrak{A}_i^{(3)}\right)$, $\mu_3=\mu_2+2\cdot\sum\limits_{\substack{0\leqslant i<p\\ wt\left(\mathfrak{A}_i^{(3)}\right)=0\\ wt(M_i)\equiv 1\ (\mathrm{mod}\ 2)}}1$, $\mu_4=\mu_2+2\cdot\sum\limits_{\substack{0\leqslant i<p\\ wt\left(\mathfrak{A}_i^{(3)}\right)=0\\ wt(M_i)\equiv 0\ (\mathrm{mod}\ 2)}}1$, $\mu_5=p^2-\mu_2$, $\mu_6=\mu_5+2\mu_{17}$, $\mu_7=\sum\limits_{0\leqslant i<p}\min\left\{wt\left(\mathfrak{A}_i^{(3)}\right),p-wt\left(\mathfrak{A}_i^{(3)}\right)\right\}$, $\mu_8=\mu_7+\min\limits_{0\leqslant i<p}\left|p-2wt\left(\mathfrak{A}_i^{(3)}\right)\right|$, $\mu_9=\sum\limits_{\substack{0\leqslant i<2p\\ wt(M_i)\equiv 1\ (\mathrm{mod}\ 2)}}1$, $\mu_{10}=\sum\limits_{\substack{0\leqslant i<2p\\ wt(M_i)\equiv 0\ (\mathrm{mod}\ 2)}}1$, $\mu_{11}=2p-\max\{\mu_{18},\mu_{19}\}$, $\mu_{12}=\sum\limits_{\substack{0\leqslant i<p\\ wt\left(\mathfrak{A}_i^{(3)}\right)\equiv 1\ (\mathrm{mod}\ 2)}}1$, $\mu_{13}=\sum\limits_{\substack{0\leqslant i<p\\ wt\left(\mathfrak{A}_i^{(3)}\right)\equiv 0\ (\mathrm{mod}\ 2)}}1$, $\mu_{14}=1$, $\mu_{15}=\sum\limits_{\substack{0\leqslant i<p\\ (p-1)/2<wt\left(\mathfrak{A}_i^{(3)}\right)\leqslant p}}1$, $\mu_{16}=2$, $\mu_{17}=\sum\limits_{\substack{0\leqslant i<p\\ wt\left(\mathfrak{A}_i^{(3)}\right)=p}}1-\max\{\mu_{20},\mu_{21}\}$, $\mu_{18}=\sum\limits_{\substack{0\leqslant i<2p\\ i\equiv 0\ (\mathrm{mod}\ 2)\\ wt(M_i)\equiv 0\ (\mathrm{mod}\ 2)}}1+\sum\limits_{\substack{0\leqslant i<2p\\ i\equiv 1\ (\mathrm{mod}\ 2)\\ wt(M_i)\equiv 1\ (\mathrm{mod}\ 2)}}1$, $\mu_{19}=\sum\limits_{\substack{0\leqslant i<2p\\ i\equiv 1\ (\mathrm{mod}\ 2)\\ wt(M_i)\equiv 0\ (\mathrm{mod}\ 2)}}1+\sum\limits_{\substack{0\leqslant i<2p\\ i\equiv 0\ (\mathrm{mod}\ 2)\\ wt(M_i)\equiv 1\ (\mathrm{mod}\ 2)}}1$, $\mu_{20}=\sum\limits_{\substack{0\leqslant i<p\\ wt\left(\mathfrak{A}_i^{(3)}\right)=p\\ i\equiv 0\ (\mathrm{mod}\ 2)\\ wt(M_i)\equiv 0\ (\mathrm{mod}\ 2)}}1+\sum\limits_{\substack{0\leqslant i<p\\ wt\left(\mathfrak{A}_i^{(3)}\right)=p\\ i\equiv 1\ (\mathrm{mod}\ 2)\\ wt(M_i)\equiv 1\ (\mathrm{mod}\ 2)}}1$, $\mu_{21}=\sum\limits_{\substack{0\leqslant i<p\\ wt\left(\mathfrak{A}_i^{(3)}\right)=p\\ i\equiv 1\ (\mathrm{mod}\ 2)\\ wt(M_i)\equiv 0\ (\mathrm{mod}\ 2)}}1+$

$$\sum_{\substack{0\leqslant i<p\\ wt\left(\mathfrak{A}_i^{(3)}\right)=p\\ i\equiv 0\ (\bmod\ 2)\\ wt(M_i)\equiv 1\ (\bmod\ 2)}} 1.$$

If 2 is a primitive root modulo p^2, then the k-error linear complexity of s satisfies the following formulas.

(i) If $LC(s)=2p^2-2p$, then

$$LC_k(s)=\begin{cases}2p^2-2p, & \text{if } 0\leqslant k\\ p^2+p, & \text{if } (\mu_7\leqslant k)\,\&\&\,(\mu_{15}\equiv 1\,(\bmod\ 2))\\ p^2+p-2, & \text{if } (\mu_8\leqslant k)\,\&\&\,(\mu_{15}\equiv 1\,(\bmod\ 2)) \text{ or if } (\mu_7\leqslant k)\,\&\&\,(\mu_{15}\equiv 0\,(\bmod\ 2))\\ p^2-p+2, & \text{if } \mu_6\leqslant k\\ p^2-p, & \text{if } \mu_3\leqslant k\\ \leqslant 2p, & \text{if } \mu_1\leqslant k\end{cases}.$$

(ii) If $LC(s)=2p^2-2p+1$, then

$$LC_k(s)=\begin{cases}2p^2-2p+1, & \text{if } 0\leqslant k\\ p^2+p, & \text{if } (\mu_7\leqslant k)\,\&\&\,(\mu_{15}\equiv 1\,(\bmod\ 2))\\ p^2+p-2, & \text{if } (\mu_8\leqslant k)\,\&\&\,(\mu_{15}\equiv 1\,(\bmod\ 2)) \text{ or if } (\mu_7\leqslant k)\,\&\&\,(\mu_{15}\equiv 0\,(\bmod\ 2))\\ p^2-p+2, & \text{if } \mu_6\leqslant k\\ p^2-p+1, & \text{if } \mu_4\leqslant k\\ p^2-p, & \text{if } \mu_3\leqslant k\\ \leqslant 2p, & \text{if } \mu_1\leqslant k\end{cases}.$$

(iii) If $LC(s)=2p^2-2p+2$, then

$$LC_k(s)=\begin{cases}2p^2-2p+2, & \text{if } 0\leqslant k\\ 2p^2-2p, & \text{if } \mu_9\leqslant k\\ p^2+p, & \text{if } (\mu_7\leqslant k)\,\&\&\,(\mu_{15}\equiv 1\,(\bmod\ 2))\\ p^2+p-2, & \text{if } (\mu_8\leqslant k)\,\&\&\,(\mu_{15}\equiv 1\,(\bmod\ 2)) \text{ or if } (\mu_7\leqslant k)\,\&\&\,(\mu_{15}\equiv 0\,(\bmod\ 2))\\ p^2-p+2, & \text{if } \mu_6\leqslant k\\ p^2-p, & \text{if } \mu_3\leqslant k\\ \leqslant 2p, & \text{if } \mu_1\leqslant k\end{cases}.$$

(iv) If $LC(s)=2p^2-p-1$, then

$$LC_k(s)=\begin{cases}2p^2-p-1, & \text{if } 0\leqslant k\\ 2p^2-2p+1, & \text{if } \mu_{10}\leqslant k\\ 2p^2-2p, & \text{if } \mu_9\leqslant k,\\ p^2+p, & \text{if } (\mu_7\leqslant k)\,\&\&\,(\mu_{15}\equiv 1\,(\bmod\ 2))\\ p^2+p-2, & \text{if } (\mu_8\leqslant k)\,\&\&\,(\mu_{15}\equiv 1\,(\bmod\ 2)) \text{ or if } (\mu_7\leqslant k)\,\&\&\,(\mu_{15}\equiv 0\,(\bmod\ 2))\\ p^2-p+2, & \text{if } \mu_6\leqslant k\\ p^2-p, & \text{if } \mu_3\leqslant k\\ \leqslant 2p, & \text{if } \mu_1\leqslant k\end{cases}.$$

(v) If $LC(s)=2p^2-p$, then

$$LC_k(s)=\begin{cases}2p^2-p, & \text{if } 0\leqslant k\\ 2p^2-p-1, & \text{if } \mu_{16}\leqslant k\\ 2p^2-2p+1, & \text{if } \mu_{10}\leqslant k\\ 2p^2-2p, & \text{if } \mu_9\leqslant k\\ p^2+p, & \text{if } (\mu_7\leqslant k)\,\&\&\,(\mu_{15}\equiv 1\,(\bmod\ 2))\\ p^2+p-2, & \text{if } (\mu_8\leqslant k)\,\&\&\,(\mu_{15}\equiv 1\,(\bmod\ 2)) \text{ or if } (\mu_7\leqslant k)\,\&\&\,(\mu_{15}\equiv 0\,(\bmod\ 2))\\ p^2-p+2, & \text{if } \mu_6\leqslant k\\ p^2-p+1, & \text{if } \mu_4\leqslant k\\ p^2-p, & \text{if } \mu_3\leqslant k\\ \leqslant 2p, & \text{if } \mu_1\leqslant k\end{cases}.$$

(vi) If $LC(s)=2p^2-p+1$, then

$$LC_k(s)=\begin{cases}2p^2-p+1, & \text{if } 0\leqslant k\\ 2p^2-p-1, & \text{if } \mu_{12}\leqslant k\\ 2p^2-2p+2, & \text{if } \mu_{11}\leqslant k\\ (\text{carried over}) & \end{cases}.$$

$$LC_k(s)=\begin{cases}\text{(brought forward)}\\ 2p^2-2p, & \text{if } \mu_9\leqslant k\\ p^2+p, & \text{if } (\mu_7\leqslant k)\,\&\&\,(\mu_{15}\equiv 1\,(\mathrm{mod}\ 2))\\ p^2+p-2, & \text{if } (\mu_8\leqslant k)\,\&\&\,(\mu_{15}\equiv 1\,(\mathrm{mod}\ 2)) \text{ or if } (\mu_7\leqslant k)\,\&\&\,(\mu_{15}\equiv 0\,(\mathrm{mod}\ 2))\\ p^2+1, & \text{if } \mu_5\leqslant k\\ p^2-p+2, & \text{if } \mu_6\leqslant k\\ p^2-p, & \text{if } \mu_3\leqslant k\\ \leqslant 2p, & \text{if } \mu_1\leqslant k\end{cases}.$$

(vii) If $LC(s)=2p^2-2$, then

$$LC_k(s)=\begin{cases}2p^2-2, & \text{if } 0\leqslant k\\ 2p^2-p+1, & \text{if } \mu_{13}\leqslant k\\ 2p^2-p-1, & \text{if } \mu_{12}\leqslant k\\ 2p^2-2p+2, & \text{if } \mu_{11}\leqslant k\\ 2p^2-2p+1, & \text{if } \mu_{10}\leqslant k\\ 2p^2-2p, & \text{if } \mu_9\leqslant k\\ p^2+p, & \text{if } (\mu_7\leqslant k)\,\&\&\,(\mu_{15}\equiv 1\,(\mathrm{mod}\ 2))\\ p^2+p-2, & \text{if } (\mu_8\leqslant k)\,\&\&\,(\mu_{15}\equiv 1\,(\mathrm{mod}\ 2)) \text{ or if } (\mu_7\leqslant k)\,\&\&\,(\mu_{15}\equiv 0\,(\mathrm{mod}\ 2))\\ p^2+1, & \text{if } \mu_5\leqslant k\\ p^2-1, & \text{if } \mu_2\leqslant k\\ p^2-p+2, & \text{if } \mu_6\leqslant k\\ p^2-p, & \text{if } \mu_3\leqslant k\\ \leqslant 2p, & \text{if } \mu_1\leqslant k\end{cases}.$$

(viii) If $LC(s)=2p^2-1$, then

$$LC_k(s)=\begin{cases}2p^2-1, & \text{if } 0\leqslant k\\ 2p^2-p+1, & \text{if } \mu_{13}\leqslant k\\ 2p^2-p-1, & \text{if } \mu_{12}\leqslant k\\ 2p^2-2p+2, & \text{if } \mu_{11}\leqslant k\\ 2p^2-2p+1, & \text{if } \mu_{10}\leqslant k\\ 2p^2-2p, & \text{if } \mu_9\leqslant k\\ p^2+p, & \text{if } (\mu_7\leqslant k)\,\&\&\,(\mu_{15}\equiv 1\,(\mathrm{mod}\ 2))\\ p^2+p-2, & \text{if } (\mu_8\leqslant k)\,\&\&\,(\mu_{15}\equiv 1\,(\mathrm{mod}\ 2)) \text{ or if } (\mu_7\leqslant k)\,\&\&\,(\mu_{15}\equiv 0\,(\mathrm{mod}\ 2))\\ p^2+1, & \text{if } \mu_5\leqslant k\\ p^2-1, & \text{if } \mu_2\leqslant k\\ p^2-p+2, & \text{if } \mu_6\leqslant k\\ p^2-p, & \text{if } \mu_3\leqslant k\\ \leqslant 2p, & \text{if } \mu_1\leqslant k\end{cases}.$$

(ix) If $LC(s)=2p^2$, then

$$LC_k(s)=\begin{cases}2p^2, & \text{if } 0\leqslant k\\ 2p^2-2, & \text{if } \mu_{14}\leqslant k\\ 2p^2-p+1, & \text{if } \mu_{13}\leqslant k\\ 2p^2-p-1, & \text{if } \mu_{12}\leqslant k\\ 2p^2-2p+2, & \text{if } \mu_{11}\leqslant k\\ 2p^2-2p+1, & \text{if } \mu_{10}\leqslant k\\ 2p^2-2p, & \text{if } \mu_9\leqslant k\\ p^2+p, & \text{if } (\mu_7\leqslant k)\,\&\&\,(\mu_{15}\equiv 1\,(\mathrm{mod}\ 2))\\ p^2+p-2, & \text{if } (\mu_8\leqslant k)\,\&\&\,(\mu_{15}\equiv 1\,(\mathrm{mod}\ 2)) \text{ or if } (\mu_7\leqslant k)\,\&\&\,(\mu_{15}\equiv 0\,(\mathrm{mod}\ 2))\\ p^2+1, & \text{if } \mu_5\leqslant k\\ p^2-1, & \text{if } \mu_2\leqslant k\\ p^2-p+2, & \text{if } \mu_6\leqslant k\\ p^2-p, & \text{if } \mu_3\leqslant k\\ \leqslant 2p, & \text{if } \mu_1\leqslant k\end{cases}.$$

After calculating $LC(s)$, we first write down the possible values of $LC_k(s)$ according to the corresponding case above, and calculate the corresponding values of μ_i. Then we compare μ_i and sort them in ascending order, and determine the values of $LC_k(s)$ depending on the order of μ_i. For $\mu_i \geqslant \mu_1$, the values of μ_i and its corresponding linear complexity are deleted; for the other μ_i, the corresponding linear complexity values need to be compared from the minimum μ_i to μ_1 sequentially. If $\mu_i < \mu_j$ and $LC_{\mu_i}(s) > LC_{\mu_j}(s)$, then their values are retained; if $\mu_i < \mu_j$ and $LC_{\mu_i}(s) < LC_{\mu_j}(s)$, then the values of μ_j and its corresponding linear complexity are deleted; if $\mu_i = \mu_j$ and $LC_{\mu_i}(s) > LC_{\mu_j}(s)$, then the values of μ_i and its corresponding linear complexity are deleted. Finally, the value range of k in the piecewise function is supplemented, and then the k-error linear complexity of s is obtained.

Proof. Since the proof is similar in other cases, we will show the proof of (i) only.

If each column of matrix $\mathfrak{M}_s$ is $(1,1,\ldots,1)^T$ or $(0,0,\ldots,0)^T$, then $\Phi_2^2(x)\,|s^N(x)$ and $LC(s) \leqslant 2p$, so we take $\mu_1 = \sum\limits_{0\leqslant i<2p} \min\{wt(M_i), p - wt(M_i)\}$. If $(x-1)^2\Phi_1^2(x)\,\Phi_2(x)\,|s^N(x)$, then each column of matrix $\mathfrak{A}^{(3)}$ is $(0,0,\ldots,0)^T$, and the weight of each column of $\mathfrak{M}_s$ is even, so we take $\mu_2 = \sum\limits_{0\leqslant i<p} wt\left(\mathfrak{A}_i^{(3)}\right)$, $\mu_3 = \mu_2 + 2\cdot \sum\limits_{\substack{0\leqslant i<p \\ wt\left(\mathfrak{A}_i^{(3)}\right)=0 \\ wt(M_i)\equiv 1 \pmod 2}} 1$. The parameter μ_6 in this theorem is the same as μ_2 in Theorem 3. If $(x-1)^2\Phi_2(x)\,|s^N(x)$, then the number of $(1,1,\ldots,1)^T$ in $\mathfrak{A}^{(3)}$ should be odd, but not equal to p; if $\Phi_2(x)\,|s^N(x)$, then the number of $(1,1,\ldots,1)^T$ in $\mathfrak{A}^{(3)}$ should be even, but not equal to 0. So we use $\mu_{15} = \sum\limits_{\substack{0\leqslant i<p \\ (p-1)/2<wt\left(\mathfrak{A}_i^{(3)}\right)\leqslant p}} 1$ to determine the number of $(1,1,\ldots,1)^T$ in $\mathfrak{A}^{(3)}$ when the changed terms in s are $\mu_7 = \sum\limits_{0\leqslant i<p} \min\left\{wt\left(\mathfrak{A}_i^{(3)}\right), p - wt\left(\mathfrak{A}_i^{(3)}\right)\right\}$ or $\mu_8 = \mu_7 + \min\limits_{0\leqslant i<p}\left|p - 2wt\left(\mathfrak{A}_i^{(3)}\right)\right|$.

From $LC(s) = 2p^2 - 2p$, we derive $(x-1)^2\Phi_1^2(x)\,|s^N(x)$. When $\mu_{15} \equiv 1 \pmod 2$, changing k bits of s^N, if $k \geqslant \mu_7$, then $\Phi_2(x)\,|s^N(x)$, hence $LC(s) = p^2 + p$; if $k \geqslant \mu_8$, then $(x-1)^2\Phi_2(x)\,|s^N(x)$, hence $LC(s) = p^2 + p - 2$. When $\mu_{15} \equiv 0 \pmod 2$, changing k bits of s^N, if $k \geqslant \mu_7$, then $(x-1)^2\Phi_2(x)\,|s^N(x)$, hence $LC(s) = p^2 + p - 2$. If we change $k \geqslant \mu_6$ bits of s^N, then $\Phi_1^2(x)\,\Phi_2(x)\,|s^N(x)$, hence $LC(s) = p^2 - p + 2$. If $k \geqslant \mu_3$, then $(x-1)^2\Phi_1^2(x)\,\Phi_2(x)\,|s^N(x)$, hence $LC(s) = p^2 - p$. If $k \geqslant \mu_1$, then $\Phi_2^2(x)\,|s^N(x)$, hence $LC(s) \leqslant 2p$.

Formula (2) shows that the k-error linear complexity of a sequence is the minimum of linear complexity obtained by changing up to k bits in a period of the sequence, so the parameters μ_i are sorted in ascending order, and the values of k-error linear complexity are determined according to the process described in this theorem. This completes the proof of Theorem 4.

Appendix C Application and numerical evidence

Appendix C.1 The definition of generalized cyclotomic binary sequences with period $2p^2$

Let p be an odd prime. Assume that 2 is a primitive root module p^2, then 2 is also a primitive root module p^k for $k \geqslant 1$. Since $2+p^k$ is odd, it is known that $2+p^k$ is also a primitive root module $2p^k$. Let $g = 2+p^2$, then g is a common primitive root modulo p, $2p$, p^2 and $2p^2$.

Define $D_0^{(p^j)} = \langle g^2\rangle \pmod{p^j}$, $D_0^{(2p^j)} = \langle g^2\rangle \pmod{2p^j}$, $D_1^{(p^j)} = gD_0^{(p^j)} \pmod{p^j}$, $D_1^{(2p^j)} = gD_0^{(2p^j)} \pmod{2p^j}$, where $D_0^{(n)}$ and $D_1^{(n)}$ denote the generalized cyclotomic classes of order two with respect to n for $n = p^j$ or $2p^j$, $j = 1, 2$.

It is well known that

$$Z_{2p^j}^* = D_0^{(2p^j)} \cup D_1^{(2p^j)},\ Z_{p^j}^* = D_0^{(p^j)} \cup D_1^{(p^j)},\ Z_2^* = \{1\},\ Z_{2p^2} = \bigcup_{k=0}^{1}\bigcup_{j=1}^{2}\left(p^{2-j}D_k^{(2p^j)} \cup 2p^{2-j}D_k^{(p^j)}\right) \cup p^2Z_2^* \cup \{0\},$$

where Z_n^* denotes the set of the residue classes coprime with n.

The generalized cyclotomic binary sequence $s = (s_0, s_1, \ldots)$ of order two with period $2p^2$ is defined as

$$s_i = \begin{cases} 1, & \text{if } i \pmod{2p^2} \in C_1 \\ 0, & \text{if } i \pmod{2p^2} \in C_0 \end{cases}, \text{ for all } i \geqslant 0,$$

where $C_0 = p^2Z_2^* \cup D_0^{(2p^2)} \cup 2D_0^{(p^2)} \cup pD_0^{(2p)} \cup 2pD_0^{(p)}$ and $C_1 = \{0\} \cup D_1^{(2p^2)} \cup 2D_1^{(p^2)} \cup pD_1^{(2p)} \cup 2pD_1^{(p)}$.

Appendix C.2 Proof of Lemma 4

Proof. For any $0 \leqslant n < p^2$,

(i) If $n \in \{0\} \subset C_1$, then $n + p^2 \in p^2Z_2^* \subset C_0$, hence $s_0 + s_{p^2} = 1$;

(ii) If $n \in Z_{2p^2}^*$, and write $n \equiv g^{2m_0+i} \pmod{2p^2}$. It is easy to see that $n+p^2 \in 2Z_{p^2}^*$, we suppose $\frac{n+p^2}{2} \equiv g^{n_0} \pmod{p^2}$, and hence $\frac{n+p^2}{2} = g^{n_0} + lp^2$ for some integer l, we derive $n = 2g^{n_0} + (2l-1)p^2$, i.e., $n \equiv 2g^{n_0} \pmod{p^2}$. So we get $n \equiv g^{2m_0+i} \equiv 2g^{n_0} \pmod{p^2}$. Since $2 \equiv g^{2v+1} \pmod{p^2}$, we furtherly get $g^{2m_0+i} \equiv g^{2v+1+n_0} \pmod{p^2}$. Hence, if $i = 0$, i.e., $n \in D_0^{(2p^2)} \subset C_0$, we have that n_0 is odd, i.e., $n + p^2 \in 2D_1^{(p^2)} \subset C_1$; and if $i = 1$, i.e., $n \in D_1^{(2p^2)} \subset C_1$, we have that n_0 is even, i.e., $n + p^2 \in 2D_0^{(p^2)} \subset C_0$. Similarly, if $n \in 2D_0^{(p^2)} \subset C_0$, then $n + p^2 \in D_1^{(2p^2)} \subset C_1$; and if $n \in 2D_1^{(p^2)} \subset C_1$, then $n + p^2 \in D_0^{(2p^2)} \subset C_0$. Then we have $s_n + s_{n+p^2} = 1$.

(iii) In a similar way as in (ii), we can prove that if $n \in pD_0^{(2p)} \subset C_0$, then $n+p^2 \in 2pD_1^{(p)} \subset C_1$; and if $n \in pD_1^{(2p)} \subset C_1$, then $n+p^2 \in 2pD_0^{(p)} \subset C_0$. If $n \in 2pD_0^{(p)} \subset C_0$, then $n+p^2 \in pD_1^{(2p)} \subset C_1$; and if $n \in 2pD_1^{(p)} \subset C_1$, then $n+p^2 \in pD_0^{(2p)} \subset C_0$. Hence $s_n + s_{n+p^2} = 1$.

This completes the proof of Lemma 4.

Appendix C.3 Proof of Theorem 5

Proof. From Lemma 4, we obtain $s_n + s_{n+p^2} = 1$ for all $0 \leqslant n < p^2$. This implies each column of $\mathfrak{A}^{(3)}$ is $(1,1,\ldots,1)^T$, and there exists $\Phi_1(x)\Phi_2(x)|s^N(x)$ or $\Phi_1^2(x)\Phi_2(x)|s^N(x)$.

Arrange s^N into $p \times 2p$ matrix $\mathfrak{M}_s = [M_0, M_1, \ldots, M_{2p-1}]$, where $M_i = \begin{bmatrix} s_i \\ s_{i+2p} \\ \vdots \\ s_{i+2(p-1)p} \end{bmatrix}$ is the $(i+1)$ th column of $\mathfrak{M}_s$ for $0 \leqslant i < 2p$. If each column of $\mathfrak{M}_s$ is $(0,0,\ldots,0)^T$ or $(1,1,\ldots,1)^T$, then $\Phi_2^2(x)|s^N(x)$, thus the period of s drops to $2p$.

Observe the subscript $\begin{bmatrix} i \\ i+2p \\ \vdots \\ i+2(p-1)p \end{bmatrix}$ of each column M_i of $\mathfrak{M}_s$ for $0 \leqslant i < 2p$. It can be analyzed in four cases:

(1) If i is odd and $i \neq p$, then $i + 2kp \pmod{2p^2} \in Z_{2p^2}^*$ for $0 \leqslant k < p$, i.e., $\gcd(i+2kp, 2p^2) = 1$. Let $i + 2kp \equiv g^{j_k} \pmod{2p^2}$ for $0 \leqslant k < p$, and the index j_k is related to k. Note that $i + 2kp \equiv g^{j_k} \pmod{2p^2} \Leftrightarrow i \equiv g^{j_k} \pmod{p}$, therefore, if j_k is even, then $i \pmod{p} \in D_0^{(p)}$; if j_k is odd, then $i \pmod{p} \in D_1^{(p)}$. That is, if $i \pmod{p} \in D_0^{(p)}$, then $s_{i+2kp} = 0$; if $i \pmod{p} \in D_1^{(p)}$, then $s_{i+2kp} = 1$. This implies that the columns mentioned above are either $(0,0,\ldots,0)^T$ or $(1,1,\ldots,1)^T$.

(2) If i is even, write $i = 2i_1$ for $0 \leqslant i_1 < p$, then we can get $i_1 + kp \pmod{p^2} \in Z_{p^2}^*$ for $0 \leqslant i_1 < p$, i.e., $\gcd(i_1 + kp, p^2) = 1$. The subscript of each column of $\mathfrak{M}_s$ can be written as $\begin{bmatrix} i \\ i+2p \\ \vdots \\ i+2(p-1)p \end{bmatrix} = 2\begin{bmatrix} i_1 \\ i_1+p \\ \vdots \\ i_1+(p-1)p \end{bmatrix}$. Let $i_1 + kp \equiv g^{j_k} \pmod{p^2}$ for $0 \leqslant k < p$. If j_k is even, then $i_1 + kp \pmod{p^2} \in D_0^{(p^2)}$; if j_k is odd, then $i_1 + kp \pmod{p^2} \in D_1^{(p^2)}$. That is, if $i_1 + kp \pmod{p^2} \in D_0^{(p^2)}$, then $s_{i+2kp} = s_{2(i_1+kp)} = 0$; if $i_1 + kp \pmod{p^2} \in D_1^{(p^2)}$, then $s_{i+2kp} = s_{2(i_1+kp)} = 1$. This implies that the columns mentioned above are either $(0,0,\ldots,0)^T$ or $(1,1,\ldots,1)^T$.

(3) If $i = 0$, write $2kp = 2p \cdot i_1$ for $0 \leqslant k < p$, then $\begin{bmatrix} 0 \\ 2p \\ \vdots \\ 2(p-1)p \end{bmatrix} = 2p\begin{bmatrix} 0 \\ 1 \\ \vdots \\ p-1 \end{bmatrix}$, hence when i_1 passes through $\{0,1,2,\ldots,p-1\}$, $i_1 \pmod{p} \in D_0^{(p)}$ appears $\frac{p-1}{2}$ times and $i_1 \pmod{p} \in D_1^{(p)} \cup \{0\}$ appears $\frac{p+1}{2}$ times. Therefore, there are $\frac{p-1}{2}$ many 0's and $\frac{p+1}{2}$ many 1's in this column.

(4) If $i = p$, write $(1+2k)p = p \cdot i_1$ for $0 \leqslant k < p$, then $\begin{bmatrix} p \\ 3p \\ \vdots \\ (2p-1)p \end{bmatrix} = p\begin{bmatrix} 1 \\ 3 \\ \vdots \\ 2p-1 \end{bmatrix}$, hence when i_1 passes through $\{1,3,5,\ldots,2p-1\}$, $i_1 \pmod{2p} \in D_0^{(2p)} \cup p^2 Z_2^*$ appears $\frac{p+1}{2}$ times and $i_1 \pmod{2p} \in D_1^{(2p)}$ appears $\frac{p-1}{2}$ times. Therefore, there are $\frac{p+1}{2}$ many 0's and $\frac{p-1}{2}$ many 1's in this column.

From the proof (ii) in Theorem 3, we conclude that in matrix $\mathfrak{M}_s$, the weight of adjacent columns will vary in parity if $\Phi_1^2(x)\Phi_2(x)|s^N(x)$. It can be seen from the above analysis that the generalized cyclotomic sequence does not satisfy the parity condition, hence only $\Phi_1(x)\Phi_2(x)|s^N(x)$ holds, therefore $LC(s) = p^2 + 1$. And if changing the columns discussed in case(3) and case(4), i.e., changing $k = p-1$ terms, then each column of $\mathfrak{M}_s$ becomes $(0,0,\ldots,0)^T$ or $(1,1,\ldots,1)^T$, hence $LC_k(s) \leqslant 2p$. This finishes the proof of Theorem 5.

Appendix C.4 Numerical evidence

Appendix C.4.1

let $p=5$ and s^{50} =10011 01100 00011 11100 10011 01100 10011 11100 00011 01100 be the generalized cyclotomic binary sequence of period 50 defined in C.1, then the corresponding 10×5 matrix is $\mathfrak{A}_s=\begin{bmatrix}1&0&0&1&1\\0&1&1&0&0\\0&0&0&1&1\\1&1&1&0&0\\1&0&0&1&1\\0&1&1&0&0\\1&0&0&1&1\\1&1&1&0&0\\0&0&0&1&1\\0&1&1&0&0\end{bmatrix}\triangleq\begin{bmatrix}\mathfrak{A}^{(1)}\\\mathfrak{A}^{(2)}\end{bmatrix}$. It's easy to obtain $\mathfrak{A}^{(3)}=\mathfrak{A}^{(1)}+\mathfrak{A}^{(2)}=\begin{bmatrix}1&1&1&1&1\\1&1&1&1&1\\1&1&1&1&1\\1&1&1&1&1\\1&1&1&1&1\end{bmatrix}$. The corresponding 5×10 matrix is $\mathfrak{M}_s=\begin{bmatrix}1&0&0&1&1&0&1&1&0&0\\0&0&0&1&1&1&1&1&0&0\\1&0&0&1&1&0&1&1&0&0\\1&0&0&1&1&1&1&1&0&0\\0&0&0&1&1&0&1&1&0&0\end{bmatrix}$, we can see accurately each column of $\mathfrak{M}_s$ conforms to the four cases mentioned in Theorem 5, thus $LC(s)=26$. When the 0's in the first column are changed to 1's and the 1's in the sixth column are changed to 0's, each column of $\mathfrak{M}_s$ becomes $(0,0,\ldots,0)^T$ or $(1,1,\ldots,1)^T$. From this, we obtain $LC_4(s)\,(=6)\leqslant 10$. If we apply the conclusion of case (ii) in Theorem 3, we calculate $\mu_1=\mu_2=4$, then $LC_k(s)=\begin{cases}26, & \text{if } 0\leqslant k<4\\ \leqslant 10, & \text{if } k\geqslant 4\end{cases}$.

Theorem 5 and the example above indicate that the linear complexity of the generalized cyclotomic binary sequences decreases dramatically only by changing $p-1$ terms. Moreover, in the matrix $\mathfrak{M}_s$, there are $2p-2$ columns which are $(0,0,\ldots,0)^T$ or $(1,1,\ldots,1)^T$. This distribution is very bad, so the sequences are not "good" pseudorandom sequences.

Appendix C.4.2

Let s be a binary sequence of period $N=2\times 5^2$, with s^{50} = 00100 10100 00011 11001 00101 00000 00101 10100 11000 00110, then the corresponding 10×5 matrix is $\mathfrak{A}_s=\begin{bmatrix}0&0&1&0&0\\1&0&1&0&0\\0&0&0&1&1\\1&1&0&0&1\\0&0&1&0&1\\0&0&0&0&0\\0&0&1&0&1\\1&0&1&0&0\\1&1&0&0&0\\0&0&1&1&0\end{bmatrix}\triangleq\begin{bmatrix}\mathfrak{A}^{(1)}\\\mathfrak{A}^{(2)}\end{bmatrix}$, the corresponding 5×5 matrix is $\mathfrak{A}^{(3)}=\mathfrak{A}^{(1)}+\mathfrak{A}^{(2)}=\begin{bmatrix}0&0&1&0&0\\1&0&0&0&1\\1&0&1&1&1\\0&0&0&0&1\\0&0&0&1&1\end{bmatrix}$, and the corresponding 5×10 matrix is $\mathfrak{M}_s=\begin{bmatrix}0&0&1&0&0&1&0&1&0&0\\0&0&0&1&1&1&1&0&0&1\\0&0&1&0&1&0&0&0&0&0\\0&0&1&0&1&1&0&1&0&0\\1&1&0&0&0&0&0&1&1&0\end{bmatrix}$. We can obtain $LC(s)=41$ by the algorithm 1 in [1], thus, by case (ii) in Theorem 4 we have $\mu_1=14$, $\mu_2=10$, $\mu_3=12$, $\mu_4=10$, $\mu_5=15$, $\mu_6=15$, $\mu_7=7$, $\mu_8=8$, $\mu_{15}=1$, satisfying $\mu_{15}\equiv 1\,(\mathrm{mod}\ 2)$, and the undetermined value of k-error linear complexity is $LC_k(s)=\begin{cases}2p^2-2p+1, & \text{if } 0\leqslant k\\ p^2+p, & \text{if } \mu_7\leqslant k\\ p^2+p-2, & \text{if } \mu_8\leqslant k\\ p^2-p+2, & \text{if } \mu_6\leqslant k\\ p^2-p+1, & \text{if } \mu_4\leqslant k\\ p^2-p, & \text{if } \mu_3\leqslant k\\ \leqslant 2p, & \text{if } \mu_1\leqslant k\end{cases}$. Since the ascending order of μ_i is $\mu_7<\mu_8<\mu_4<\mu_3<\mu_1<\mu_6$, then it is easy to

$$\text{get } LC_k(s) = \begin{cases} 41, & \text{if } 0 \leqslant k < 7 \\ 30, & \text{if } 7 \leqslant k < 8 \\ 28, & \text{if } 8 \leqslant k < 10 \\ 21, & \text{if } 10 \leqslant k < 12 \\ 20, & \text{if } 12 \leqslant k < 14 \\ \leqslant 10, & \text{if } k \geqslant 14 \end{cases}.$$

We run the program of algorithm 2 in [2] and obtain that the k-error linear complexity of s accords with the case (ii) in Theorem 4. We further verify all possible cases in Theorem 3 and 4, and the conclusion is consistent.

References

1 Wei S M, Xiao G Z, Chen Z. A fast algorithm for determining the minimal polynomial of a sequence with period $2p^n$ over GF(q). IEEE Trans Inf Theory, 2002, 48(10): 2754–2758

2 Wei S M. An efficient algorithm for determining the k-error linear complexity of binary sequences with periods $2p^n$. Int J Comput Sci Netw Secur, 2008, 8(4): 221–224