SCIENCE CHINA
Information Sciences

• LETTER •

September 2020, Vol. 63 199101:1–199101:3
https://doi.org/10.1007/s11432-019-2665-5

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*

Received 12 June 2019/Accepted 24 September 2019/Published online 26 March 2020

Citation Niu Z H, Yuan C, Chen Z X, et al. On the k-error linear complexity of $2p^2$-periodic binary sequences. Sci China Inf Sci, 2020, 63(9): 199101, https://doi.org/10.1007/s11432-019-2665-5

Dear editor,

Pseudorandom sequences play an important role in cryptography. In particular in symmetric cryptography they serve as the secret key. So the designs of pseudorandom sequences and cryptographic indicators are the critical research directions. The cryptographic indicators of sequences mainly include: balance, correlation, linear complexity, k-error linear complexity, and so on [1]. In this study, we compute the k-error linear complexity of $2p^2$-periodic binary sequences, so the concepts of linear complexity and k-error linear complexity of sequences are introduced.

Let $\mathbb{F}_2 = \{0, 1\}$ be the binary field. For an N-periodic sequence $s = (s_0, s_1, \ldots)$ over $\mathbb{F}_2$, the linear complexity, denoted by $\mathrm{LC}(s)$, is the length of shortest linear feedback shift register (LFSR) that generates the sequence, i.e., the smallest positive integer L such that $s_{u+L} = c_{L-1}s_{u+L-1} + \cdots + c_1 s_{u+1} + c_0 s_u$ for $u \geqslant 0$ and constants $c_0 \neq 0$, $c_1, \ldots, c_{L-1} \in \mathbb{F}_2$. Let s be a binary sequence with the first period $s^N = (s_0, s_1, \ldots, s_{N-1})$. The generating polynomial of s^N is defined as $s^N(x) = s_0 + s_1 x + \cdots + s_{N-1}x^{N-1}$. Then the linear complexity over $\mathbb{F}_2$ of s can be computed as

$$\mathrm{LC}(s) = N - \deg\left(\gcd\left(x^N - 1, s^N(x)\right)\right), \quad (1)$$

which is the degree of the minimal polynomial, $\frac{x^N-1}{\gcd(x^N-1, s^N(x))}$, of the sequence, see [2] for details.

For integers $k \geqslant 0$, the k-error linear complexity over $\mathbb{F}_2$ of s, denoted by $\mathrm{LC}_k(s)$, is the least linear complexity over $\mathbb{F}_2$ that can be obtained by changing at most k terms of the sequence per period, i.e.,

$$\mathrm{LC}_k(s) = \min_{wt(e) \leqslant k} \mathrm{LC}(s + e), \quad (2)$$

where e is the error sequence with period N and $wt(e)$ equals the number of nonzero terms of e per period, i.e., the weight of e. See [3] for details.

In this study, we always suppose $N = 2p^2$. Now we arrange the first period of the N-periodic binary sequence into matrix forms, and then discuss the k-error linear complexity of s by examining the column weight of the matrices, involving three matrix forms.

The first matrix form is a matrix of size $p \times 2p$, defined as

$$\mathfrak{M}_s = \begin{bmatrix} s_0 & \cdots & s_p & \cdots & s_{2p-1} \\ s_{2p} & \cdots & s_{3p} & \cdots & s_{4p-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ s_{2(p-1)p} & \cdots & s_{(2p-1)p} & \cdots & s_{2p^2-1} \end{bmatrix} \triangleq [M_0, M_1, \ldots, M_{2p-1}],$$

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 $0 \leqslant i < 2p$.

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

The second is a matrix of size $2p \times p$, defined as

$$\mathfrak{A}_s = \begin{bmatrix} s_0 & s_1 & \cdots & s_{p-1} \\ s_p & s_{p+1} & \cdots & s_{2p-1} \\ \vdots & \vdots & \vdots & \vdots \\ s_{p^2} & s_{p^2+1} & \cdots & s_{p^2+p-1} \\ \vdots & \vdots & \vdots & \vdots \\ s_{(2p-1)p} & s_{(2p-1)p+1} & \cdots & s_{2p^2-1} \end{bmatrix} \triangleq \left[\frac{\mathfrak{A}^{(1)}}{\mathfrak{A}^{(2)}}\right],$$

where $\mathfrak{A}^{(1)}$ and $\mathfrak{A}^{(2)}$ are both matrices of size $p \times p$, and $\mathfrak{A}^{(1)} \triangleq [\mathfrak{A}_0^{(1)}, \mathfrak{A}_1^{(1)}, \ldots, \mathfrak{A}_{p-1}^{(1)}]$, $\mathfrak{A}^{(2)} \triangleq [\mathfrak{A}_0^{(2)}, \mathfrak{A}_1^{(2)}, \ldots, \mathfrak{A}_{p-1}^{(2)}]$,

$$\mathfrak{A}_i^{(1)} = \begin{bmatrix} s_i \\ s_{i+p} \\ \vdots \\ s_{i+(p-1)p} \end{bmatrix} \text{ and } \mathfrak{A}_i^{(2)} = \begin{bmatrix} s_{i+p^2} \\ s_{i+(p+1)p} \\ \vdots \\ s_{i+(2p-1)p} \end{bmatrix}$$

are the $(i+1)$th column of $\mathfrak{A}^{(1)}$ and $\mathfrak{A}^{(2)}$ for $0 \leqslant i < p$, respectively.

The third is a matrix of size $p \times p$, defined as

$$\mathfrak{A}^{(3)} = \mathfrak{A}^{(1)} + \mathfrak{A}^{(2)} \triangleq \left[\mathfrak{A}_0^{(3)}, \mathfrak{A}_1^{(3)}, \ldots, \mathfrak{A}_{p-1}^{(3)}\right],$$

where $\mathfrak{A}_i^{(3)}$ is the $(i+1)$th column of $\mathfrak{A}^{(3)}$, and $\mathfrak{A}_i^{(3)} = \mathfrak{A}_i^{(1)} + \mathfrak{A}_i^{(2)}$ for $0 \leqslant i < p$.

Lower bounds on linear complexity. Let $\mathrm{ord}_m(2)$ denote the order of 2 modulo m, i.e., $\mathrm{ord}_m(2)$ is the least positive integer such that $2^{\mathrm{ord}_m(2)} \equiv 1 \pmod{m}$.

Lemma 1. Let $\mathrm{ord}_p(2) = \lambda$ with $1 < \lambda < p$. If $2^{p-1} \not\equiv 1 \pmod{p^2}$, then $\mathrm{ord}_{p^2}(2) = \lambda p$. See Appendix A.1 for the proof.

Theorem 1. If $2^{p-1} \not\equiv 1 \pmod{p^2}$, then the linear complexity of s satisfies $\mathrm{LC}(s) \geqslant \lambda p$, where $1 < \lambda < p$ is the order of 2 modulo p. See Appendix A.2 for the details of the proof.

The theorem can be generalized to arbitrary binary sequences of period $2p^r$ for $r > 1$, then $\mathrm{LC}(s) \geqslant \lambda p^{r-1}$.

Lemma 2. For the binary sequences with least period $N = 2p^2$, $(x^{p^2}-1) \nmid s^N(x)$. See Appendix A.3 for the proof.

Theorem 2. Let s be a binary sequence with the least period $N = 2p^2$. If 2 is a primitive root modulo p^2, then the linear complexity of s satisfies one of the following two cases.

(i) $p^2 - p < \mathrm{LC}(s) \leqslant p^2 + p$. In this case, there are five values of the linear complexity, which can be written as $\mathrm{LC}(s) = p^2 - p + a$ where $a \in \{2, 2p-2, p+1, 2p-1, 2p\}$.

(ii) $\mathrm{LC}(s) \geqslant 2(p^2-p)$. In this case, there are nine values of the linear complexity, which can be written as $\mathrm{LC}(s) = 2(p^2-p) + b$ where $b \in \{0, 1, 2, p-1, 2p-2, p, p+1, 2p-1, 2p\}$. See Appendix A.4 for the details of the proof.

k-error linear complexity. We first discuss the k-error linear complexity of s when $p^2 - p < \mathrm{LC}(s) \leqslant p^2 + p$.

Lemma 3. If $p^2 - p < \mathrm{LC}(s) \leqslant p^2 + p$, then for $0 \leqslant i < p$,

(i) $wt(M_i) = wt(M_{i+p})$;

(ii) $wt(M_i) + wt(M_{i+p}) = p$, and there must exist $0 \leqslant i_0 < p$ such that $wt(M_{i_0}) + wt(M_{i_0+p}) = p$.

See Appendix B.1 for the proof.

Theorem 3. Let s be a binary sequence with the least period $N = 2p^2$ and $\mu_1 = 2\sum_{0 \leqslant i < p} \min\{wt(M_i), p - wt(M_i)\}$. If 2 is a primitive root modulo p^2 and $\mathrm{LC}(s) = 2p^2 - 2p$, then

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

The other cases and proofs in Theorem 3 are presented in Appendix B.2.

Then we discuss the k-error linear complexity of s when $\mathrm{LC}(s) \geqslant 2(p^2-p)$.

Theorem 4. Let s be a binary sequence with the least period $N = 2p^2$. If 2 is a primitive root modulo p^2 and $\mathrm{LC}(s) = 2p^2 - 2p$, then the possible values of k-error linear complexity include $2p^2-2p$, p^2+p, p^2+p-2, p^2-p+2, p^2-p and some values $\leqslant 2p$, which correspond to some parameters μ_i. These parameters μ_i are related to the column weight of the corresponding matrices. The final values of k-error linear complexity are determined according to the ascending order of parameters μ_i. The determination of k-error linear complexity is similar when the linear complexity of s is other values.

The detailed content and proof of Theorem 4 are presented in Appendix B.3.

Comparison of the methods. For calculating the k-error linear complexity of $2p^2$-periodic binary sequences, the available methods are based on the algorithms in [4, 5] introducing different cost vectors, which are iterative algorithms. The difficulty of these algorithms is to calculate and update the values of cost vectors in each iteration. These algorithms can only compute one value of k once. To obtain all the k-error linear complexity, the algorithms should be executed repeatedly.

With the matrix method proposed in this study, we can quickly arrange the sequences into three

matrix forms. Once the values of relevant parameters μ_i and their ascending order are obtained, all the final values of k-error linear complexity and the corresponding range of k can be determined directly according to the relevant conclusion. The whole process does not require repeat.

Application and numerical evidence. We use the method introduced by Ding and Helleseth [6] to construct a class of generalized cyclotomic binary sequences with least period $2p^2$, and obtain some conclusion about the k-error linear complexity of the sequences by the matrix method.

See Appendix C.1 for the detailed definition of the sequences.

Lemma 4. Let s^N be the first period ($N = 2p^2$) of the generalized cyclotomic binary sequence. If s^N is arranged into the $2p \times p$ matrix form $\mathfrak{A}_s \triangleq [\frac{\mathfrak{A}^{(1)}}{\mathfrak{A}^{(2)}}]$, then $\mathfrak{A}^{(1)}$ and $\mathfrak{A}^{(2)}$ are complementary, i.e., $s_n + s_{n+p^2} = 1$, for all $0 \leqslant n < p^2$. See Appendix C.2 for the proof.

Theorem 5. Let s be the generalized cyclotomic binary sequence with period $N = 2p^2$ mentioned above, then $\mathrm{LC}(s) = p^2 + 1$, and if $k = p - 1$, then $\mathrm{LC}_k(s) \leqslant 2p$. See Appendix C.3 for the details of the proof.

We give an example of generalized cyclotomic binary sequences (applying Theorem 3) in Appendix C.4.1 and found that such sequences are not "good" pseudorandom sequences. In recent years, the pseudorandom sequences derived from Fermat quotients have attracted extensive attention [7–9], these sequences are of high linear complexity, and the problem of their k-error linear complexity deserves further study. We also give another numerical example (applying Theorem 4) in Appendix C.4.2.

Conclusion. In this study, we propose the matrix method to calculate the k-error linear complexity of binary sequences with the least period $2p^2$. We first analyze the lower bounds on linear complexity and conclude that there are two cases, $p^2 - p < \mathrm{LC}(s) \leqslant p^2 + p$ and $\mathrm{LC}(s) \geqslant 2(p^2 - p)$. Then according to these two cases, we discuss the k-error linear complexity by arranging the sequences into three matrix forms and calculating the column weight. If the linear complexity of a sequence is obtained, then all the values of k-error linear complexity and the corresponding range of k can be obtained directly by using this matrix method. Finally, we apply the matrix method to a class of generalized cyclotomic binary sequences with period $2p^2$ defined by Ding and Helleseth. The results show that the stability on linear complexity of the sequences is poor, and their linear complexity will decrease from $p^2 + 1$ to less than $2p$ by changing $k = p - 1$ terms.

Acknowledgements Zhihua NIU, Can YUAN and Tao ZHANG were partially supported by State Key Program of National Nature Science Foundation of China (Grant No. 61936001), National Nature Science Foundation of Shanghai (Grant Nos. 16ZR1411200, 17ZR1409800, 19ZR1417700), Research and Development Program in Key Areas of Guangdong Province (Grant No. 2018B010113001), and National Nature Science Foundation of China (Grant No. 61572309). Zhixiong CHEN was partially supported by National Natural Science Foundation of China (Grant No. 61772292) and Projects of International Cooperation and Exchanges NSFC-RFBR (Grant No. 61911530130). Xiaoni DU was partially supported by National Natural Science Foundation of China (Grant No. 61772022).

Supporting information Appendixes A–C. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Ding C S, Xiao G Z, Shan W J. The Stability Theory of Stream Ciphers. Berlin: Springer, 1991
2 Cusick T W, Ding C S, Renvall A. Stream Ciphers and Number Theory. Amsterdam: North-Holland Publishing Co., 1998
3 Kurosawa K, Sato F, Sakata T, et al. A relationship between linear complexity and k-error linear complexity. IEEE Trans Inform Theor, 2000, 46: 694–698
4 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: 221–224
5 Zhou J Q. On the k-error linear complexity of sequences with period $2p^n$ over GF(q). Des Codes Cryptogr, 2011, 58: 279–296
6 Ding C S, Helleseth T. New generalized cyclotomy and its applications. Finite Fields Their Appl, 1998, 4: 140–166
7 Chen Z X, Niu Z H, Wu C H. On the k-error linear complexity of binary sequences derived from polynomial quotients. Sci China Inf Sci, 2015, 58: 092107
8 Chen Z X. Trace representation and linear complexity of binary sequences derived from Fermat quotients. Sci China Inf Sci, 2014, 57: 112109
9 Niu Z H, Chen Z X, Du X N. Linear complexity problems of level sequences of Euler quotients and their related binary sequences. Sci China Inf Sci, 2016, 59: 032106