The Expansion Complexity of Ultimately Periodic Sequences over Finite Fields

Yi Zhang
Department of Foundational Mathematics
Xi'an Jiaotong-Liverpool University
Suzhou, China, 215123
Yi.Zhang03@xjtlu.edu.cn

Abstract

The expansion complexity is a new figure of merit for cryptographic sequences. In this paper, we present an explicit formula of the (irreducible) expansion complexity of ultimately periodic sequences over finite fields. We also provide improved upper and lower bounds on the Nth irreducible expansion complexity when they are not explicitly determined. In addition, for some infinite sequences with given nonlinear complexity, a tighter upper bound of their Nth expansion complexity is given. This a joint work with Zhimin Sun, Xiangyong Zeng, Chunlei Li, and Lin Yi.

1 Introduction

Pseudo-random sequences have many applications in digital communications and cryptography [4, 5, 15]. Such sequences can be generated by linear feedback shift registers (LFSRs). The *linear complexity* of a sequence is defined as the length of the shortest LFSRs that can generate the sequence. For a sequence of length n having linear complexity $l \leq n/2$, the Berlekamp-Massey algorithm [14] can produce the whole sequence when $2l$ consecutive elements of the sequence are given. There has been a great amount of research on linear complexity properties of sequences in the literature [1, 3, 18, 20, 23]. Sequences with large linear complexity are generally of more interest. However, such sequences may be generated by shorter nonlinear feedback shift registers. This observation leads to the study of *nonlinear complexity* of a sequence [9, 10, 12], which is defined as the length of the shortest feedback shift registers that generate the given sequence. Clearly a sequence with large nonlinear complexity has a large linear complexity. To further assess the unpredictability of a sequence and thus its suitability for cryptographic applications, the *Nth nonlinear complexity*, as well as *nonlinear complexity profile* were introduced [9]. Recent progress on nonlinear complexity can be found in [8, 12, 13, 19, 21, 22, 24].

A random sequence has an expected linear complexity close to half of its length [17]. An infinite sequence $\mathcal{S}$ is thus said to have perfect linear complexity profile if $|L_N(\mathcal{S}) - \frac{N}{2}| \leq 1$ for all positive integers N and have d-almost perfect linear complexity profile if $|L_N(\mathcal{S}) - \frac{N}{2}| \leq d$ for all N and certain integer d, where $L_N(\mathcal{S})$ is the Nth linear complexity of $\mathcal{S}$, namely, the length of shortest

LFSRs that generate the first N elements of $\mathcal{S}$. Based on the function expansion into expansion series, Xing and Lam in [23] presented a general construction of infinite sequences with optimal linear complexity, which seems to be appealing for cryptographic applications. Nevertheless, Diem showed that this type of sequences can be efficiently computed from a relatively short subsequence in [2], where he introduced the notion of the *Nth expansion complexity* and the *expansion complexity* of an infinite sequence. Certain progress in this research line was made recently [16, 6, 7].

In this paper, we first investigate the irreducible expansion complexity of ultimately periodic sequences $\mathcal{S} = (s_i)_{i=0}^{\infty}$ over the finite field $\mathbb{F}_q$, where q is a prime power. For characterizing the irreducible expansion complexity of an ultimately periodic sequence $\mathcal{S}$, we utilize the method of polynomial pseudo-division [11, Chapter 4] to prove that the defining ideal of $\mathcal{S}$ is actually generated by a polynomial $h(x, y) = f_1(x)y - f_0(x)$ with $f_0(x)/f_1(x)$ being the generating function of $\mathcal{S}$. This observation enables us to present an explicit formula of the Nth irreducible expansion complexity of $\mathcal{S}$ for all integers $N > N_0$ and thereby the irreducible expansion complexity of $\mathcal{S}$, where N_0 is a positive integer determined by the irreducible expansion complexity. In addition, we present an upper bound on the Nth expansion complexity of an infinite sequence over finite fields when its nonlinear complexity satisfies certain condition.

References

[1] Z. Chen, X. Du, "On the linear complexity of binary threshold sequences derived from Fermat quotients," *Des. Codes Cryptogr.*, vol. 67, pp. 317–323, 2013.

[2] C. Diem, "On the use of expansion series for stream ciphers," *LMS J. Comput. Math*, vol. 15, pp. 326-340, May 2012.

[3] C. Ding, "Linear complexity of generalized cyclotomic binary sequences of order 2," *Finite Fields Their Appl.*, vol. 3, pp. 159–174, 1997.

[4] S. Golomb, G. Gong, *Signal Design for Good Correlation: for Wireless Communication, Cryptography, and Radar*, U.K.: Cambridge Univ. Press, 2005.

[5] S. Golomb, *Shift Register Sequences*, 3rd Edition, World Scientific, 2017.

[6] D. Gómez-Pérez, L. Mérai, H. Niederreiter, "On the expansion complexity of sequences over finite fields," *IEEE Trans. Inf. Theory*, vol. 64, no. 6, pp. 4228–4232, Jun. 2018.

[7] D. Gómez-Pérez, L. Mérai, "Algebraic dependence in generating functions and expansion complexity", *Adv. Math. Commun.*, vol. 14, no. 2, pp. 307–318, May 2020.

[8] L. Işık, A. Winterhof, "Maximum-order complexity and correlation measures," *Cryptogr.*, vol. 1, no. 1, pp. 1–5, May 2017.

[9] C.J.A. Jansen, *Investigations on Nonlinear Stream Cipher Systems: Construction and Evaluation Methods*, Ph.D. dissertation, Technical University of Delft, Delft, 1989.

[10] C.J.A. Jansen, "The maximum order complexity of sequence ensembles," in *Advances in Cryptology - EUROCRYPT '91, Lect. Notes Comput. Sci.*, D.W. Davies (Ed.), Springer-Verlag, Berlin Heidelberg, vol. 547, Apr. 1991, pp. 153–159.

[11] D.E. Knuth, *The Art of Computer Programming*, Addison Wesley Publishing Company, 1981.

[12] K. Limniotis, N. Kolokotronis, N. Kalouptsidis, "On the nonlinear complexity and lempel−ziv complexity of finite length sequences," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 4293–4302, Nov. 2007.

[13] Y. Luo, C. Xing, L. You, "Construction of sequences with high nonlinear complexity from function fields," *IEEE Trans. Inform. Theory*, vol. 63, no. 12, pp. 7646–7650, Dec. 2017.

[14] J.L. Massey, "Shift register synthesis and BCH decoding," *IEEE Trans. Inf. Theory*, vol. 15, no. 1, pp. 122–127, Jan. 1969.

[15] A.J. Menezes, P.C. Van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[16] L. Mérai, H. Niederreiter, A. Winterhof, "Expansion complexity and linear complexity of sequences over finite fields," *Cryptogr. Commun.*, Vol. 9, pp. 501–509, 2017.

[17] H. Niederreiter, "The probabilistic theory of linear complexity," in *Advances in Cryptology - EUROCRYPT'88 (C.G. Günther, ed.), Lect. Notes Comput. Sci.*, vol. 330, Springer, Berlin, 1988, pp. 191–209.

[18] H. Niederreiter, "Linear complexity and related complexity measures for sequences," *Lect. Notes Comput. Sci.*, vol. 2904, pp. 1–17, 2003.

[19] J. Peng, X. Zeng, Z. Sun, "Finite length sequences with large nonlinear complexity," *Adv. Math. Commun.*, vol. 12, no. 1, pp. 215–230, Feb. 2018.

[20] A. Winterhof, "Linear complexity and related complexity measures," in *Selected topics in information and coding theory*, Ser. Coding Theory Crypto., 7, World Sci. Publ., Hackensack, NJ, 2010, pp. 3–40.

[21] Z. Sun, A. Winterhof, "On the maximum order complexity of subsequences of the Thue-Morse and Rudin-Shapiro sequence along squares," *Int. J. Comput. Math.*, vol. 4, no. 1, pp. 30–36, Jan. 2019.

[22] Z. Sun, X. Zeng, C. Li, T. Helleseth, "Investigations on periodic sequences with maximum nonlinear complexity," *IEEE Trans. Inf. Theory*, vol. 63, no. 10, pp. 6188–6198, Oct. 2017.

[23] C.P. Xing, K.Y. Lam, "Sequence with almost perfect linear complexity profiles and curves over finite fields," *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1267–1270, May 1999.

[24] Z. Xiao, X. Zeng, C. Li, Y. Jiang, "Binary sequences with period N and nonlinear complexity $N-2$," *Cryptogr. Commun.*, vol. 11, no. 4, pp. 735–757, 2019.