cryptography

Article

Maximum-Order Complexity and Correlation Measures

Leyla Işık [1] and Arne Winterhof [2,*]

[1] Department of Mathematics, Salzburg University, Hellbrunner Str. 34, 5020 Salzburg, Austria; leyla.isik@sbg.ac.at

[2] Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenbergerstr. 69, 4040 Linz, Austria

* Correspondence: arne.winterhof@oeaw.ac.at

Academic Editor: Kwangjo Kim
Received: 29 March 2017; Accepted: 10 May 2017; Published: 13 May 2017

Abstract: We estimate the maximum-order complexity of a binary sequence in terms of its correlation measures. Roughly speaking, we show that any sequence with small correlation measure up to a sufficiently large order k cannot have very small maximum-order complexity.

Keywords: maximum-order complexity; correlation measure of order k; measures of pseudorandomness; cryptography

MSC: 11K36, 11T71, 94A55, 94A60

---

1. Introduction

For a positive integer N, the *Nth linear complexity* $L(\mathcal{S},N)$ of a binary sequence $\mathcal{S}=(s_i)_{i=0}^{\infty}$ is the smallest positive integer L such that there are constants $c_0,c_1,...,c_{L-1}\in\mathbb{F}_2$ with

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

(We use the convention $L(\mathcal{S},N)=0$ if $s_0=\ldots=s_{N-1}=0$ and $L(\mathcal{S},N)=N$ if $s_0=\ldots=s_{N-2}=0\neq s_{N-1}$.) The Nth linear complexity is a measure for the predictability of a sequence and thus its unsuitability in cryptography. For surveys on linear complexity and related measures of pseudorandomness see [1–6].

Let k be a positive integer. Mauduit and Sárközy introduced the (Nth) *correlation measure of order k* of a binary sequence $\mathcal{S}=(s_i)_{i=0}^{\infty}$ in [7] as

$$C_k(\mathcal{S},N)=\max_{U,D}\left|\sum_{i=0}^{U-1}(-1)^{s_{i+d_1}+s_{i+d_2}+...+s_{i+d_k}}\right|,$$

where the maximum is taken over all $D=(d_1,d_2,...,d_k)$ with non-negative integers $0\le d_1<d_2<...<d_k$ and U such that $U+d_k\le N$. (Actually, [7] deals with finite sequences $((-1)^{s_i})_{i=0}^{N-1}$ of length N over $\{-1,+1\}$.)

Brandstätter and the second author [8] proved the following relation between the Nth linear complexity and the correlation measures of order k:

$$L(\mathcal{S},N)\ge N-\max_{1\le k\le L(\mathcal{S},N)+1}C_k(\mathcal{S},N),\quad N\ge 1. \tag{1}$$

Roughly speaking, any sequence with small correlation measure up to a sufficiently large order k must have a high Nth linear complexity as well.

For example, the Legendre sequence $\mathcal{L} = (\ell_i)_{i=0}^{\infty}$ defined by

$$\ell_i = \begin{cases} 1, & \text{if } i \text{ is a quadratic non-residue modulo } p, \\ 0, & \text{otherwise,} \end{cases}$$

where $p > 2$ is a prime, satisfies

$$C_k(\mathcal{L}, N) \ll kp^{1/2} \log p, \quad 1 \le N \le p, \tag{2}$$

and thus (1) implies

$$N \ll L(\mathcal{L}, N)p^{1/2} \log p, \quad 1 \le N \le p.$$

Using $L(\mathcal{L}, N) \ge L(\mathcal{L}, p)$ for any $N > p$ we get

$$L(\mathcal{L}, N) \gg \frac{\min\{N, p\}}{p^{1/2} \log p}, \quad N \ge 1,$$

see [7,9] (Theorem 9.2). (Here $f(N) \ll g(N)$ is equivalent to $|f(N)| \le cg(N)$ for some absolute constant c.)

The Nth *maximum-order complexity* $M(\mathcal{S}, N)$ of a binary sequence $\mathcal{S} = (s_i)_{i=0}^{\infty}$ is the smallest positive integer M such that there is a polynomial $f(x_1, \dots, x_M) \in \mathbb{F}_2[x_1, \dots, x_M]$ with

$$s_{i+M} = f(s_i, s_{i+1}, \dots, s_{i+M-1}), \quad 0 \le i \le N - M - 1, \tag{3}$$

see [10–12]. Obviously we have

$$M(\mathcal{S}, N) \le L(\mathcal{S}, N)$$

and the maximum-order complexity is a finer measure of pseudorandomness than the linear complexity.

In this paper we analyze the relationship between maximum-order complexity $M(\mathcal{S}, N)$ and the correlation measures $C_k(\mathcal{S}, N)$ of order k. Our main result is the following theorem:

Theorem 1. *For any binary sequence $\mathcal{S}$ we have*

$$M(\mathcal{S}, N) \ge N - 2^{M(\mathcal{S},N)+1} \max_{1 \le k \le M(\mathcal{S},N)+1} C_k(\mathcal{S}, N), \quad N \ge 1.$$

Again, any nontrivial bound on $C_k(\mathcal{S}, N)$ for all k up to a sufficiently large order provides a nontrivial bound on $M(\mathcal{S}, N)$. For example, for the Legendre sequence we get immediately from (2)

$$N \ll 2^{M(\mathcal{L},N)} M(\mathcal{L}, N)p^{1/2} \log p, \quad 1 \le N \le p.$$

Now we have either $M(\mathcal{L}, N) > \log p$ and the bound (4) below is trivial or $M(\mathcal{L}, N) \le \log p$ which implies

$$M(\mathcal{L}, N) \ge \log(\min\{N, p\}/p^{1/2}) + O(\log \log p), \tag{4}$$

see also [9] (Theorem 9.3). (Here $f(N) = O(g(N))$ is equivalent to $f(N) \ll g(N)$.)

We prove Theorem 1 in the next section.

The expected value of the Nth maximum-order complexity is of order of magnitude $\log N$, see [10] as well as [12] (Remark 4) and references therein. Moreover, by [13] for a sequence of length N with very high probability the correlation measure $C_k(\mathcal{S}, N)$ is of order of magnitude $\sqrt{kN \log N}$ and thus by Theorem 1 $M(\mathcal{S}, N) \ge \frac{1}{2} \log N + O(\log \log N)$ which is in good correspondence to the result of [10].

In Section 3 we mention some straightforward extensions.

2. Proof of Theorem 1

Proof. Assume $\mathcal{S}$ satisfies (3). If $s_i = ... = s_{i+M-1} = 0$ for some $0 \le i \le N-M-1$, then $s_{i+M} = f(0,...,0)$. Equivalently, $(-1)^{s_i} = ... = (-1)^{s_{i+M-1}} = 1$ implies $(-1)^{s_{i+M}} = (-1)^{f(0,...,0)}$. Hence, for every $i = 0, ..., N-M-1$ we have

$$\left((-1)^{s_{i+M}} - (-1)^{f(0,\dots,0)}\right) \prod_{j=0}^{M-1} \left((-1)^{s_{i+j}} + 1\right) = 0.$$

Summing over $i = 0, ..., N-M-1$ we get

$$\sum_{i=0}^{N-M-1} \left((-1)^{s_{i+M}} - (-1)^{f(0,\dots,0)}\right) \prod_{j=0}^{M-1} \left((-1)^{s_{i+j}} + 1\right) = 0.$$

The left-hand side contains one "main" term $\pm(N-M)$ and $2^{M+1} - 1$ terms of the form

$$\pm \sum_{i=0}^{N-M-1} (-1)^{s_{i+j_1} + s_{i+j_2} + \dots + s_{i+j_k}}$$

with $0 \le j_1 < j_2 < ... < j_k \le M$ and $1 \le k \le M+1$. Therefore we have

$$N - M \le 2^{M+1} \max_{1 \le k \le M+1} \left| \sum_{i=0}^{N-M-1} (-1)^{s_{i+j_1} + s_{i+j_2} + \dots + s_{i+j_k}} \right|$$

and the result follows. □

3. Further Remarks

Theorem 1 can be easily extended to m-ary sequences with $m > 2$ along the lines of [14]: Let ξ be a primitive mth root of unity. Then we have

$$\sum_{h=0}^{m-1} \xi^{hx} = 0 \quad \text{if and only if} \quad x \not\equiv 0 \bmod m.$$

As in the proof of Theorem 1 we get

$$\sum_{i=0}^{N-M-1} \left(\xi^{s_{i+M}} - \xi^{f(0,\dots,0)}\right) \prod_{j=0}^{M-1} \sum_{h=0}^{m-1} \xi^{h s_{i+j}} = 0.$$

We have one term of absolute value $N-M$ and $2m^M - 1$ terms of the form

$$\alpha \sum_{i=0}^{N-M-1} \xi^{h_1 s_{i+j_1} + h_2 s_{i+j_2} + \dots + h_k s_{i+j_k}} \tag{5}$$

with $1 \le h_1, \dots, h_k < m$, $0 \le j_1 < j_2 < \dots < j_k \le M$, $1 \le k \le M+1$ and $\alpha \in \{1, -\xi^{f(0,\dots,0)}\}$.

If m is a prime, then $x \mapsto hx$ is a permutation of $\mathbb{Z}_m$ for any $h \not\equiv 0 \bmod m$ and the sums in (5) can be estimated by the correlation measure $C_k(\mathcal{S}, N)$ of order k for m-ary sequences as it is defined in [15] and we get

$$M(\mathcal{S}, N) \ge N - 2m^{M(\mathcal{S},N)} \max_{1 \le k \le M(\mathcal{S},N)+1} C_k(\mathcal{S}, N), \quad N \ge 1.$$

If m is composite, $x \mapsto hx$ is not a permutation of $\mathbb{Z}_m$ if $\gcd(h, m) > 1$ and we have to substitute the correlation measure of order k by the power correlation measure of order k introduced in [14].

Now we return to the case $m = 2$.

Even if the correlation measure of order k is large for some small k, we may be still able to derive a nontrivial lower bound on the maximum-order complexity by substituting the correlation measure of order k by its analogue with bounded lags, see [16] for the analogue of (1). For example, the two-prime generator $\mathcal{T} = (t_i)_{i=0}^{\infty}$, see [17], of length pq with two odd primes $p < q$ satisfies

$$t_i + t_{i+p} + t_{i+q} + t_{i+p+q} = 0$$

if $\gcd(i, pq) = 1$ and its correlation measure of order 4 is obviously close to pq, see [18]. However, if we bound the lags $d_1 < \ldots < d_k < p$ one can derive a nontrivial upper bound on the correlation measure of order k with bounded lags including $k = 4$ as well as lower bounds on the maximum-order complexity using the analogue of Theorem 1 with bounded lags.

Finally, we mention that the lower bound (4) for the Legendre sequence can be extended to Legendre sequences with polynomials using the results of [19] as well as to their generalization using squares in arbitrary finite fields (of odd characteristic) using the results of [20,21]. For sequences defined with a character of order m see [15].

Acknowledgments: The authors are supported by the Austrian Science Fund FWF Projects F5504 and F5511-N26, respectively, which are part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications". L.I. would like to express her sincere thanks for the hospitality during her visit to RICAM.

Author Contributions: The authors contributed in equal parts.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Gyarmati, K. Measures of pseudorandomness. Finite Fields and Their Applications. In *Radon Series on Computational and Applied Mathematics*; De Gruyter: Berlin, Germany, 2013; Volume 11, pp. 43–64.
2. Meidl, W.; Winterhof, A. Linear complexity of sequences and multisequences, Section 10.4 of the Handbook of Finite Fields. In *Discrete Mathematics and its Applications (Boca Raton)*; Mullen, G.L., Panario, D., Eds.; CRC Press: Boca Raton, FL, USA, 2013; pp. 324–336.
3. Niederreiter, H. Linear complexity and related complexity measures for sequences. In *Progress in Cryptology-INDOCRYPT 2003*; Lecture Notes in Computer Science, 2904; Springer: Berlin, Germany, 2003; pp. 1–17.
4. Sárközy, A. On finite pseudorandom binary sequences and their applications in cryptography. *Tatra Mt. Math. Publ.* **2007**, *37*, 123–136.
5. Topuzoğlu, A.; Winterhof, A. Pseudorandom sequences. In *Topics in Geometry, Coding Theory and Cryptography*; Algebra Applications, 6; Springer: Dordrecht, The Netherlands, 2007; pp. 135–166.
6. Winterhof, A. Linear complexity and related complexity measures. In *Selected Topics in Information and Coding Theory*; Series on Coding Theory and Cryptology, 7; World Science Publishing: Hackensack, NJ, USA, 2010; pp. 3–40.
7. Mauduit, C.; Sárközy, A. On finite pseudorandom binary sequences. I. Measure of pseudorandomness, the Legendre symbol. *Acta Arith.* **1997**, *82*, 365–377.
8. Brandstätter, N.; Winterhof, A. Linear complexity profile of binary sequences with small correlation measure. *Period. Math. Hung.* **2006**, *52*, 1–8.
9. Shparlinski, I. *Cryptographic Applications of Analytic Number Theory. Complexity Lower Bounds and Pseudorandomness*; Progress in Computer Science and Applied Logic, 22; Birkhäuser Verlag: Basel, Switzerland, 2003.
10. Jansen, C.J.A. Investigations on Nonlinear Streamcipher Systems: Construction and Evaluation Methods. Ph.D. Thesis, Technische Universiteit Delft, Delft, The Netherlands, 1989; p. 195.
11. Jansen, C.J.A. The maximum order complexity of sequence ensembles. In *Advances in Cryptology—EUROCRYPT'91, LNCS 547*; Davies, D.W., Ed.; Springer: Berlin/Heidelberg, Germany, 1991; pp. 153–159.
12. Niederreiter, H.; Xing, C. Sequences with high nonlinear complexity. *IEEE Trans. Inf. Theory* **2014**, *60*, 6696–6701.

13. Alon, N.; Kohayakawa, Y.; Mauduit, C.; Moreira, C.G.; Rödl, V. Measures of pseudorandomness for finite sequences: Typical values. *Proc. Lond. Math. Soc.* **2007**, *95*, 778–812.
14. Chen, Z.; Winterhof, A. Linear complexity profile of *m*-ary pseudorandom sequences with small correlation measure. *Indag. Math.* **2009**, *20*, 631–640.
15. Mauduit, C.; Sárközy, A. On finite pseudorandom sequences of *k* symbols. *Indag. Math.* **2002**, *13*, 89–101.
16. He, J.J.; Panario, D.; Wang, Q.; Winterhof, A. Linear complexity profile and correlation measure of interleaved sequences. *Cryptogr. Commun.* **2015**, *7*, 497–508.
17. Brandstätter, N.; Winterhof, A. Some notes on the two-prime generator of order 2. *IEEE Trans. Inf. Theory* **2005**, *5*, 3654–3657.
18. Rivat, J.; Sárközy, A. Modular constructions of pseudorandom binary sequences with composite moduli. *Period. Math. Hung.* **2005**, *51*, 75–107.
19. Goubin, L.; Mauduit, C.; Sárközy, A. Construction of large families of pseudorandom binary sequences. *J. Number Theory* **2004**, *106*, 56–69.
20. Mérai, L.; Yayla, O. Improving results on the pseudorandomness of sequences generated via the additive order of a finite field. *Discret. Math.* **2015**, *338*, 2020–2025.
21. Sárközy, A.; Winterhof, A. Measures of pseudorandomness for binary sequences constructed using finite fields. *Discret. Math.* **2009**, *309*, 1327–1333.