

A note on Hall's sextic residue sequence: correlation measure of order k and related measures of pseudorandomness

Hassan Aly¹ and Arne Winterhof²

¹ Department of Mathematics, Faculty of Science, Cairo University,
P.O. Box 12613, Giza, Egypt
E-mail: hassan@sci.cu.edu.eg

and

Department of Computer Science and Information, College of Science at Al-Zulfi,
Majmaah University, Saudi-Arabia

² Johann Radon Institute for Computational and Applied Mathematics,
Austrian Academy of Sciences, Altenberger Str. 69, 4040 Linz, Austria
E-mail: arne.winterhof@oeaw.ac.at

Abstract

It is known that Hall's sextic residue sequence has some desirable features of pseudorandomness: an ideal two-level autocorrelation and linear complexity of the order of magnitude of its period p . Here we study its correlation measure of order k and show that it is, up to a constant depending on k and some logarithmic factor, of order of magnitude $p^{1/2}$, which is close to the expected value for a random sequence of length p . Moreover, we derive from this bound a lower bound on the N th maximum order complexity of order of magnitude $\log p$, which is the expected order of magnitude for a random sequence of length p .

Keywords. Hall's sextic residue sequence, correlation measure of order k , maximum order complexity, linear complexity, pseudorandom sequence

MSC 2000. 11B50, 11K45, 11T22, 11T71, 94A55, 94A60

1 Introduction

1.1 Hall's sextic residue sequence

For a prime p of the form $p = 6f + 1$, Hall's sextic residue sequence $\mathcal{H} = (h_n)$ of period p is defined as follows: Let g be a primitive root modulo p and

$$C_\ell = \{g^{6i+\ell} | i = 0, 1, \dots, f-1\}, \quad \ell = 0, 1, \dots, 5, \quad (1)$$

be the cyclotomic cosets modulo p of order 6. Then we put

$$h_n = \begin{cases} 1 & \text{if } n \bmod p \in C_0 \cup C_1 \cup C_3, \\ 0 & \text{otherwise,} \end{cases} \quad n = 0, 1, \dots \quad (2)$$

Hall's sextic sequence has several desirable features of pseudorandomness:

- It has a small out-of-phase autocorrelation. In particular, if $p = 4u^2 + 27$ and g is chosen such that $3 \in C_1$, then it has ideal 2-level autocorrelation (or equivalently $C_0 \cup C_1 \cup C_3$ is a difference set), see [11].
- It has large linear complexity of order of magnitude p over \mathbb{F}_2 , see [20].
- It has large linear complexity over some other fields, see [8, 12].
- It has large k -error linear complexity over \mathbb{F}_p for $k < (p - 1)/2$, see [2].
- It has maximum 2-adic complexity, see [27] and also [16] for a short proof.

All these features of pseudorandomness consider a full period of the sequence. However, for cryptographic applications usually only a part of a period of the sequence is used. In this paper we deal with some aperiodic measures of pseudorandomness, the correlation measure of order k and the N th maximum order complexity.

1.2 Correlation measure of order k

The *correlation measure of order k* of a binary sequence (s_n) of length N is defined as

$$C_k(s_n) = \max_{M,D} \left| \sum_{n=0}^{M-1} (-1)^{s_{n+d_1} + s_{n+d_2} + \dots + s_{n+d_k}} \right|,$$

where the maximum is taken over all $D = (d_1, d_2, \dots, d_k)$ with non-negative integers $d_1 < d_2 < \dots < d_k$ and M such that $M - 1 + d_k \leq N - 1$. This measure of pseudorandomness was introduced by Mauduit and Sárközy in [21].

A sequence $\mathcal{S} = (s_n)$ is considered a good pseudorandom sequence if the value of $C_k(\mathcal{S})$ (at least for small k) is small in terms of N .

The main result of this paper is the following upper bound on the correlation measure of order k of Hall's sextic sequence.

Theorem 1 *Let $\mathcal{H} = \{h_0, h_1, \dots, h_{p-1}\}$ be a period of Hall's sextic sequence defined by (2). Then the correlation measure of order k of \mathcal{H} satisfies*

$$C_k(\mathcal{H}) = O \left(\left(\frac{14}{3} \right)^k k p^{1/2} \log p \right).$$

Here we used the notation $A = O(B)$ if $A \leq cB$ for a positive absolute constant c .

We will prove Theorem 1 in Section 2.

By [1] for a sequence \mathcal{S} of length N with very high probability the correlation measure $C_k(\mathcal{S})$ is up to a constant depending on k of order of magnitude $\sqrt{N \log N}$. In this sense Hall's sextic sequence behaves (almost) like a random sequence.

Moreover, Theorem 1 implies bounds on two other measures of pseudorandomness for parts of a period of a sequence, the N th maximum order complexity and the N th linear complexity.

Note that bounds on the correlation measure of order k of characteristic sequences of *consecutive* unions of cyclotomic classes of order m were studied in [9]. However, Hall's sextic residue sequence is not covered by the construction of [9] and our approach is slightly different.

More precisely, [9] also deals with the case that the running index n is substituted by $f(n)$ for a polynomial $f(X)$ over \mathbb{F}_p of degree k which satisfies certain conditions. However, the result is trivial if $k > p^{1/2}$ but the polynomial used to define Hall's sequence has larger degree $k \geq (p+5)/6$:

Let C'_i be the i th cyclotomic class of order 6 with respect to the primitive element g^{-1} and note that $C_{6-i} = C'_i$ for $i = 0, 1, \dots, 5$. Then let $f(n)$ be the mapping which interchanges C_2 and C_3 , that is,

$$f(n) = \begin{cases} gn, & n \in C_2, \\ g^{-1}n, & n \in C_3, \\ n, & \text{otherwise.} \end{cases}$$

Then we have

$$h_n = \begin{cases} 0, & 1 \leq (\text{ind}_{g^{-1}}(f(n)) \bmod 6) \leq 3, \\ 1, & \text{otherwise,} \end{cases} \quad n = 1, \dots, p-1,$$

which is of the form of sequences which are studied in [9]. (Note that actually [9] deals with the sequence $((-1)^{h_n})_{n=0}^{p-1}$ over $\{-1, 1\}$.) Obviously, f cannot be represented by a polynomial $f(X)$ of degree one and is of the form

$$f(X) = X \sum_{i=0}^5 A_i X^{i(p-1)/6}$$

by [22, Theorem 1]. Hence, $\deg f \geq (p+5)/6$ and [9] does not give a nontrivial bound.

1.3 N th Maximum order complexity

The N th *maximum order complexity* $M(\mathcal{S}, N)$ of a binary sequence $\mathcal{S} = (s_n)$ 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

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

see [18, 19, 23].

By [17] for any binary sequence \mathcal{S} we have the following relation between the maximum order complexity and the correlation measure of order k :

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

Combining this relation and Theorem 1 we get the following lower bound on the maximum order complexity of Hall's sextic residue sequence.

Corollary 1 *For the N th maximum order complexity of Hall's sextic residue sequence we have*

$$M(\mathcal{H}, N) = \Omega \left(\log \left(\frac{\min\{N, p\}}{p^{1/2} \log^2 p} \right) \right).$$

Here $A = \Omega(B)$ is equivalent to $B = O(A)$.

The expected value of the N th maximum-order complexity is of order of magnitude $\log N$, see [18] as well as [23] (Remark 4) and references therein. Hence, the N th maximum order complexity of Hall's sextic residue sequence for any N with $p^{1/2} \log^3 p \leq N \leq p$ is at least of this desired order of magnitude.

1.4 N th linear complexity

For $N \geq 1$ the N th linear complexity $L(\mathcal{S}, N)$ over \mathbb{F}_2 of a binary sequence $\mathcal{S} = (s_n)$ is the shortest Length L of a linear recurrence relation over \mathbb{F}_2

$$s_{n+L} = c_{L-1}s_{n+L-1} + \cdots + c_0s_n, 0 \leq n \leq N - L - 1,$$

which is satisfied by the first N sequence elements. (We use the convention that $L(\mathcal{S}, N) = 0$ if the first N terms of the sequence are all 0 and $L(\mathcal{S}, N) = N$ if $S_0 = s_1 = \cdots = s_{N-2} = 0$ and $s_{N-1} = 1$.)

[4, Theorem 1] gives a lower bound on the N th linear complexity of \mathcal{S} in terms of the correlation measure of order k :

$$L(\mathcal{S}, N) \geq N - \max_{1 \leq k \leq L(\mathcal{S}, N)+1} C_k(\mathcal{S}), \quad N \geq 1.$$

Combining this bound with Theorem 1 we get for Hall's sextic residue sequence \mathcal{H}

$$L(\mathcal{H}, N) = \Omega \left(\log \left(\frac{\min\{N, p\}}{p^{1/2} \log^2 p} \right) \right).$$

The implied constant can be explicitly calculated. This result can be even obtained in a simpler way from Corollary 1 observing that

$$L(\mathcal{H}, N) \geq M(\mathcal{H}, N)$$

with a slightly weaker implied constant.

Some experiments indicate that $L(\mathcal{H}, N)$ is much larger and we consider it an interesting open problem to improve this lower bound on $L(\mathcal{H}, N)$.

Note that there is another figure of merit closely related to the correlation measure of order k , the *arithmetic autocorrelation*. Rather moderate bounds on the arithmetic autocorrelation of Hall's sextic residue sequence can be obtained combining Theorem 1 and [13].

2 Proof of Theorem 1

Let η be a multiplicative character of \mathbb{F}_p of order 3 and put

$$\delta_1(n) = \frac{1 + \eta(n) + \eta^2(n)}{3}, \quad n \in \mathbb{F}_p^*.$$

Then we have

$$\delta_1(n) = \begin{cases} 1 & \text{if } n \in C_0 \cup C_3, \\ 0 & \text{if } n \in C_1 \cup C_2 \cup C_4 \cup C_5. \end{cases}$$

Let χ be a multiplicative character of \mathbb{F}_p of order 6 and put

$$\omega = \chi(g),$$

where g is the primitive root modulo p fixed for the definition of the cyclotomic cosets in (1) and

$$\delta_2(n) = \frac{1 + \omega^{-1}\chi(n) + \omega^{-2}\chi^2(n) + \cdots + \omega^{-5}\chi^5(n)}{6}.$$

Then we have

$$\delta_2(n) = \begin{cases} 1, & \text{if } n \in C_1, \\ 0, & \text{if } n \in C_0 \cup C_2 \cup C_3 \cup C_4 \cup C_5, \end{cases} \quad n \in \mathbb{F}_p^*.$$

Now $\delta(n)$ defined by

$$\delta(n) = \delta_1(n) + \delta_2(n), \quad n \in \mathbb{F}_p^*,$$

is the characteristic function of $C_0 \cup C_1 \cup C_3 \subset \mathbb{F}_p^*$. Hence, Hall's sextic sequence $\mathcal{H} = (h_n)$ defined by (2) satisfies

$$h_n = \delta(n), \quad n = 1, 2, \dots, p-1,$$

and we have

$$\begin{aligned} (-1)^{h_n} &= 1 - 2\delta(n) \\ &= \frac{-2}{3} (\eta(n) + \eta^2(n)) - \frac{1}{3} (\omega^{-1}\chi(n) + \omega^{-2}\chi^2(n) + \cdots + \omega^{-5}\chi^5(n)) \end{aligned}$$

for $n = 1, 2, \dots, p-1$. Note that $\eta \in \{\chi^2, \chi^4\}$. Now

$$\left| \sum_{n=1}^{M-1} (-1)^{h_{n+d_1} + \cdots + h_{n+d_k}} \right|$$

can be estimated by 7^k sums of the form

$$\left(\frac{2}{3} \right)^k \left| \sum_{n=1}^{M-1} \chi((n+d_1)^{m_1} \cdots (n+d_k)^{m_k}) \right|$$

with $1 \leq m_1, \dots, m_k \leq 5$. A variant of Weil's theorem for incomplete character sums, see for example [25, Lemma 3.4], gives the bound

$$O(kp^{1/2} \log p)$$

for the absolute value of the inner character sums. Collecting everything, Theorem 1 follows. \square

3 Legendre sequence and Ding-Helleseth-Lam sequence

There are several other cyclotomic sequences with similar features of pseudorandomness. We mention only the Legendre sequence and the Ding-Helleseth-Lam sequence.

3.1 Legendre sequence

Similar results are known for the Legendre sequence $\mathcal{L} = (\ell_n)$ of prime period $p > 2$ which is the characteristic sequence of the quadratic residues modulo p , that is, a cyclotomic sequence of order 2:

- It has small out-of-phase autocorrelation and in particular ideal 2-level autocorrelation if $p \equiv 3 \pmod{4}$, see [24].
- It has large linear complexity of order of magnitude p , see [7, 26].
- It has k th error linear complexity over \mathbb{F}_p of order of magnitude p for $k < (p-1)/2$, see [3].
- Its 2-adic expansion is maximal, see [27, 16, 15].
- It has small correlation measure of order k of order of magnitude $kp^{1/2} \log p$, see [21].
- Its N th maximum order complexity is at least $\log(\min\{N, p\}/p^{1/2}) + O(\log \log p)$, see [17].
- Its N th linear complexity is at least of order of magnitude $\min\{N, p\}/(p^{1/2} \log p)$, see [25, Theorem 9.2] or combine [21] and [4].
- Its arithmetic autocorrelation is moderately small, see [14].

3.2 Ding-Helleseth-Lam sequence

Ding et al. [5] introduced a cyclotomic generator of order 4. Let $C_0 = \{x^4 : x \in \mathbb{F}_p^*\}$ be the subgroup of \mathbb{F}_p^* of bi-squares and $C_1 = gC_0$ for a primitive root g modulo p . Then the *Ding-Helleseth-Lam sequence* $\mathcal{D} = (d_n)$ is the characteristic sequence of $C_0 \cup C_1$.

- Its out-of-phase autocorrelation is small and it has optimum three-level autocorrelation (or equivalently $C_0 \cup C_1$ is an almost difference set) if $p = x^2 + 4$ with $x \equiv 1 \pmod{4}$, see [5, Theorem 4].
- It has linear complexity close to its period, see [6], if $2 \in D_0$.
- It has maximum 2-adic complexity, see [27, 16].
- For $k < (p-1)/2$ it has k -error linear complexity over \mathbb{F}_p of order of magnitude p , see [2].
- Its correlation measure of order k is estimated in [9].

- Its N th maximum order complexity can be lower bounded by combining [17] and [9].

It is possible to extend the results of this paper to cyclotomic sequences of higher order m . For the special case of characteristic sequences of the union of consecutive cyclotomic classes see [9]. However, for odd m the correlation measure of order k can be very large, see [9], and for even m the implied constant in the bound on the correlation measure of order k either depends on m (non-consecutive case) or we have an additional factor of $(\log p)^k$ (consecutive case [9]). Hence, the Hall sequence, the Legendre sequence and the Ding-Helleseth-Lam sequence are certainly the most attractive candidates for cryptographic applications.

Moreover, there are several other sequence constructions using characters of finite fields or elliptic curves over finite fields, see for example [10] and references therein.

Acknowledgment

This paper was partly written during a pleasant visit of the first author at RICAM. He wishes to thank for hospitality and financial support. The second author is supported by the Austrian Science Fund FWF Project P 30405-N32.

References

- [1] N. Alon, Y. Kohayakawa, C. Mauduit, C.G. Moreira and V. Rödl, "Measures of pseudorandomness for finite sequences: typical values." *Proc. Lond. Math. Soc.* 95 (2007), 778–812.
- [2] H. Aly, W. Meidl, and A. Winterhof, "On the k -error linear complexity of cyclotomic sequences." *J. Math. Cryptol.* 1 (2007), 1–14.
- [3] H. Aly and A. Winterhof, "On the k -error linear complexity over \mathbb{F}_p of Legendre and Sidelnikov sequences." *Des. Codes Cryptogr.* 40 (2006), 369–374.
- [4] N. Brandstätter and A. Winterhof, "Linear complexity profile of binary sequences with small correlation measure." *Period. Math. Hungar.* 52 (2006), 1–8.
- [5] C. Ding, T. Hellesteth and K.Y. Lam, "Several classes of binary sequences with three-level autocorrelation." *IEEE Trans. Inform. Theory* 45 (1999), 2606–2612.
- [6] C. Ding, T. Hellesteth and K.Y. Lam, "Duadic sequences of prime lengths." *Discrete Math.* 218 (2000), 33–49.
- [7] C. Ding, T. Hellesteth and W. Shan, "On the linear complexity of Legendre sequences." *IEEE Trans. Inform. Theory* 44 (1998), 1276–1278.
- [8] V. Edemskiy and N. Sokolovskiy, "On the linear complexity of Hall's sextic residue sequences over $GF(q)$." *J. Appl. Math. Comput.* 54 (2017), 297–305.

- [9] K. Gyarmati, "On a fast version of a pseudorandom generator." In: General theory of information transfer and combinatorics, 326–342, Lecture Notes in Comput. Sci. 4123, Springer, Berlin, 2006.
- [10] K. Gyarmati, "Measures of pseudorandomness." In: Finite fields and their applications, 43–64, Radon Ser. Comput. Appl. Math. 11, De Gruyter, Berlin, 2013.
- [11] M. Hall, Jr., "A survey of difference sets." Proc. Amer. Math. Soc. 7 (1956), 975–986.
- [12] X. He, L. Hu and D. Li, "On the $GF(p)$ linear complexity of Hall's sextic sequences and some cyclotomic-set-based sequences." Chin. Ann. Math. Ser. B, 37 (2016), 515–522.
- [13] R. Hofer, L. Mérai and A. Winterhof, "Measures of pseudorandomness: arithmetic autocorrelation and correlation measure." Number theory – Diophantine problems, uniform distribution and applications, 303–312, Springer, Cham, 2017.
- [14] R. Hofer and A. Winterhof, "On the arithmetic autocorrelation of the Legendre sequence." Adv. Math. Commun. 11 (2017), 237–244.
- [15] R. Hofer and A. Winterhof, "On the 2-adic complexity of the two-prime generator." IEEE Trans. Inf. Theory 64 (2018), 5957–5960.
- [16] H. Hu, "Comments on "A new method to compute the 2-adic complexity of binary sequences"." IEEE Trans. Inform. Theory 60 (2014), 5803–5804.
- [17] L. Isik and A. Winterhof, "Maximum-order complexity and correlation measures." Cryptography 1, 7.
- [18] C.J.A. Jansen, "Investigations on Nonlinear Streamcipher Systems: Construction and Evaluation Methods." Ph.D. Thesis, Technische Universiteit Delft, 1989.
- [19] C.J.A. Jansen, "The maximum order complexity of sequence ensembles." In: Advances in Cryptology—EUROCRYPT'91, Lecture Notes in Comput. Sci. 547, 153–159, Springer, Berlin, 1991.
- [20] J.-H. Kim and H.-Y. Song "On the linear complexity of Hall's sextic residue sequences." IEEE Trans. Inform. Theory 47 (2001), 2094–2096.
- [21] C. Mauduit and A. Sárközy, "On finite pseudorandom binary sequences I: Measures of pseudorandomness, the Legendre symbol." Acta Arith. 82 (1997), 365–377.
- [22] H. Niederreiter and A. Winterhof, "Cyclotomic \mathcal{R} -orthomorphisms of finite fields." Discrete Math. 295 (2005), 161–171.
- [23] H. Niederreiter and C. Xing, "Sequences with high nonlinear complexity." IEEE Trans. Inf. Theory 60 (2014), 6696–6701.

- [24] R.E.A.C. Paley, "On orthogonal matrices." J. Math. Phys., Mass. Inst. Techn. 12 (1933), 311–320.
- [25] I. Shparlinski, "Cryptographic Applications of Analytic Number Theory: Complexity Lower Bounds and Pseudorandomness." Progress in Computer Science and Applied Logic 22. Birkhäuser, Basel, 2003.
- [26] R.J. Turyn, "The linear generation of Legendre sequence." J. Soc. Indust. Appl. Math. 12 (1964), 115–116.
- [27] H. Xiong, L. Qu and C. Li, "A new method to compute the 2-adic complexity of binary sequences." IEEE Trans. Inform. Theory 60 (2014), 2399–2406.