Exact Autocorrelation Values of the Hall's Sextic Residues Sequences

Hassan Aly

Department of Computer Science and Information
College of Science
Majmaah University
AzZulfi 11932, P.O. Box 1217, KSA

h.aly@mu.edu.sa

Department of Mathematics
Faculty of Science
Cairo University
Giza, P.O. Box 12653, Egypt

hassan@sci.cu.edu.eg

Abstract

This paper determines exact values of the autocorrelation function $AC_{\mathcal{H}}(w)$ of the Hall's sextic residues sequence $\mathcal{H}$ of prime period p with $0 \leq w \leq p-1$. Let $p = 6f + 1 = A^2 + 3B^2$ be an odd prime and m be the smallest positive integer that satisfies $g^m \equiv 2 \pmod{p}$, where g is a primitive element modulo p. The paper shows that the number of different values of $AC_{\mathcal{H}}(1), AC_{\mathcal{H}}(2), \cdots, AC_{\mathcal{H}}(p-1)$ is either $1, 2, 3, 4, 5$, or 6 depending on f and m. Moreover, it proves that the maximum absolute autocorrelation value is bounded by $c\sqrt{p}$ where $c = 1/\sqrt{3}, 2/\sqrt{3}, 3/\sqrt{3}$, or $10/\sqrt{3}$ according to different values of f and m. Some special cases for prime p with very small maximum absolute value are also discussed.

1 Introduction

Periodic binary sequences with good autocorrelation properties have different important applications in various areas of computer science and communication. These include stream ciphers, spread spectrum communication systems, ranging systems, multi-terminal identification system, code-division multiple access communication systems, software testing, circuit testing, and computer simulation. Let $S = s_0 s_1 s_2 \cdots$ be a binary sequence. The sequence S is periodic with period N if $s_i = s_{i+N}$ for all $i = 0, 1, 2, \cdots$. The autocorrelation function of S at shift w is defined as

$$AC_S(w) = \sum_{t=0}^{N-1} (-1)^{s_{t+w} - s_t}.$$

It is obvious that $AC_S(0) = N$. The autocorrelation of S is a measure of how much it differs from its translates. The values $AC_S(w)$, $w \in \{1, 2, \cdots, N-1\}$ are called the *out-of-phase autocorrelation values*. The main goal of designing periodic binary sequences is to obtain the sequence whose out-of-phase autocorrelation values are as small in absolute value as possible while minimizing the total number of distinct values. We say that S has *$k-$level autocorrelation* if $AC_S(w)$ takes on k distinct values for $w = 0, 1, 2, \cdots, N-1$. The sequence S is said to have *ideal autocorrelation* if $AC_S(w) = -1$ for all $w = 1, 2, \cdots, N-1$ if $N \equiv 3 \bmod 4$. Further, it said to have *optimal autocorrelation* if $AC_S(w) \in \{1, -3\}$ for $N \equiv 1 \pmod 4$, $AC_S(w) \in \{-2, 2\}$ for $N \equiv 2 \pmod 4$, and $AC_S(w) \in \{0, \pm 4\}$ for $N \equiv 0 \pmod 4$, see for example [2, 5, 12]. The set

$$1_S = \{i | 0 \leq i \leq N-1, \ and \ \ s_i = 1\},$$

is called the *support* of S; and S is referred to as the *characteristic sequence* of 1_S. Define the *difference function* of a subset R in $\mathbb{Z}_n$ by

$$\delta_R(w) = |(w + R) \cap R|,$$

where $w + R = \{w + x | x \in R\}$. It is easy to show that

$$AC_S(w) = N - 4\left(|1_S| - \delta_{1_S}(w)\right). \tag{1}$$

This property reduces the computation of $AC_S(w)$ to that of $\delta_{1_S}(w)$. It follows from (1) that $AC_S(w) \equiv N \pmod 4$ for each $1 \leq w \leq N-1$. A number of constructions for ideal autocorrelation binary sequences have been presented in literature, see [2]. The Hall's sextic residue sequence is one of the oldest constructions in this direction. It goes back to Hall [8] in his discovering of difference sets in sextic residues modulo a prime p. This sequence has ideal autocorrelation with value -1 if the period $p = A^2 + 27$. No specific results are obtained for the autocorrelation function in the none-ideal case of this sequence. The main objective in this paper is to exactly determine the out-phase-autocorrelation values of the sequence in its general case. Although the paper uses standard arguments in the proofs, no such results are known for the author in literature.

Let $p = 6f + 1$ be a prime. The *Hall's sextic residue sequence* $\mathcal{H} = h_0 h_1 h_2 \cdots$ of period p is defined as follows: Let g be a primitive element modulo p and

$$C_\ell = \{g^{6i+\ell} | i = 0, 1, \cdots, f-1\}, \quad \ell = 0, 1, \cdots, 5, \tag{2}$$

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

$$h_n = \begin{cases} 1 & \text{if } n \bmod p \in C_0 \cup C_1 \cup C_3, \\ 0 & \text{otherwise,} \end{cases} \qquad n = 0, 1, \ldots \tag{3}$$

The Hall's sextic residue sequence $\mathcal{H}$ is periodic with length p and balanced in the sense that, the number of 0's exceeds that of 1's just by a position. This sequence has several desirable features of pseudo-randomness if $p = 4u^2 + 27$ and g is chosen such that $3 \in C_1$. It has ideal 2-level autocorrelation (or equivalently $C_0 \cup C_1 \cup C_3$ is a difference set), see

[8]. Its linear complexity is p if $p \equiv 3 \pmod 8$ and is $\frac{p-1}{6}+1$ if $p \equiv 7 \pmod 8$, see [11]. It has large linear complexity over some other fields, see [6, 9, 7]. It has large k-error linear complexity over $\mathbb{F}_p$ for $k < (p-1)/2$, see [1].

Primes on the form $p = 6f + 1$ may be classified into two categories according to either f is odd or even. Define integer parameters A and B as $p = A^2 + 3B^2$ with $A \equiv 1 \pmod 3$. Given p, the parameter A is uniquely determined but B is determined only up to sign. In case if f is odd, then $p \equiv 7 \pmod{12}$. In this case A is always even and B is always odd. But if f is even, then $p \equiv 1 \pmod{12}$, A is odd and B is always even. Let m be the smallest positive integer that satisfies $g^m \equiv 2 \pmod p$. We may need to distinguish between two families of primes p depending on m as follows [4, 10]:

1. Firstly, if $m \equiv 0 \pmod 3$. Prime p will be on the form $p = A^2+27v^2$ where $B = 3v$. It is known here that the residue 2 is cubic residues modulo p, see [10]. Examples for primes are $307, 439$, and 499 if f is odd and are $109, 157$, and 229 if f is even. The set of all primitive elements modulo p splits up into two subsets: one generates the sequence $\mathcal{H}$ with support $C_0 \cup C_1 \cup C_3$ and the other generates the sequence with support $C_0 \cup C_3 \cup C_5$. The sign of B will accordingly determined. Any attempt to uniquely determine the sign of B, in this case, will add some restriction on the choice of g. The computation of $AC_{\mathcal{H}}$ in fact does not need such direction.

2. Secondly, if $m \not\equiv 0 \pmod 3$. In this case, p will be on the form $p = A^2 + 3B^2$ where $\gcd(B, 3) = 1$. The sign of B is uniquely determined from the relation $A + B \equiv 0 \pmod 3$ if $m \equiv 1 \pmod 3$ and from the relation $A - B \equiv 0 \pmod 3$ if $m \equiv 2 \pmod 3$. In the rest of this paper, we will fix the number k to be

$$k = \begin{cases} \frac{A+B}{3} & \text{if } m \equiv 1 \pmod 3, \\ \frac{A-B}{3} & \text{if } m \equiv 2 \pmod 3. \end{cases}$$

The paper is organized as follows. Section 2 introduces some important properties of the cyclotomic numbers of order 6. In section 3, exact values of the autocorrelation function of the sequence $\mathcal{H}$ defined over prime $p = A^2 + 27v^2$ are given. Some special interesting cases are presented and sharp upper bound for the absolute autocorrelation values is introduced. In section 4, exact values of the autocorrelation function of the sequence $\mathcal{H}$ defined with prime $p = A^2 + 3B^2$ where $\gcd(3, B) = 1$ are obtained. Section 5 introduces some final remarks and conclusion.

2 Cyclotomic numbers of order 6

To find exact values of the autocorrelation function $AC_{\mathcal{H}}(w)$ for $1 \le w \le p-1$, we need to recall some results on the cyclotomic numbers of order 6 with respect to $\mathbb{F}_p$. Define

$$(i, j)_6 = |\,(C_i + 1) \cap C_j|$$

where $i, j = 0, 1, 2, 3, 4, 5$. In other words, $(i, j)_6$ is the number of solutions $(x, y) \in C_i \times C_j$ of the difference

$$y - x \equiv 1 \pmod p.$$

The constants $(i,j)_6$ are called the cyclotomic numbers of order 6 over $\mathbb{F}_p$. Clearly, there are at most 36 distinct cyclotomic numbers of order 6. It has been proven that the 36 cyclotomic numbers $(i,j)_6$ depend sloely upon the decomposition A^2+3B^2 of the prime $p=6f+1$ [4, 8, 13]. It is known that these numbers satisfy the relation

$$(i,j)_6=(j+3,i+3)_6=(6-i,j-i)_6.$$

Tables 1 and 2 give the 36 cyclotomic numbers in terms of ten possible distinct ones where $(i,j)_6$ is in row i and column j for $i,j\equiv 0,1,2,3,4,5 \pmod 6$ for f odd and f even at respectively.

	0	1	2	3	4	5
0	00	01	02	03	04	05
1	10	20	12	04	02	12
2	20	21	10	05	12	01
3	00	10	20	00	10	20
4	10	05	12	01	20	21
5	20	12	04	02	12	10

Table 1: Cyclotomic numbers of order 6 for f odd

	0	1	2	3	4	5
0	00	01	02	03	04	05
1	01	05	12	13	14	12
2	02	12	04	14	24	13
3	03	13	14	03	13	14
4	04	14	24	13	02	12
5	05	12	13	14	12	01

Table 2: Cyclotomic numbers of order 6 for f even

	$m\equiv 0 \pmod 3$	$m\equiv 1 \pmod 3$	$m\equiv 2 \pmod 3$
$36(0,0)_6$	$p-11-8A$	$p-11-2A$	$p-11-2A$
$36(0,1)_6$	$p+1-2A+12B$	$p+1+4A$	$p+1-2A-12B$
$36(0,2)_6$	$p+1-2A+12B$	$p+1-2A+12B$	$p+1-8A+12B$
$36(0,3)_6$	$p+1+16A$	$p+1+10A-12B$	$p+1+10A+12B$
$36(0,4)_6$	$p+1-2A-12B$	$p+1-8A-12B$	$p+1-2A-12B$
$36(0,5)_6$	$p+1-2A-12B$	$p+1-2A+12B$	$p+1+4A$
$36(1,0)_6$	$p-5+4A+6B$	$p-5-2A+6B$	$p-5+4A+6B$
$36(2,0)_6$	$p-5+4A-6B$	$p-5-2A-6B$	$p-5+4A-6B$
$36(1,2)_6$	$p+1-2A$	$p+1+4A$	$p+1+4A$
$36(2,1)_6$	$p+1-2A$	$p+1-8A+12B$	$p+1-8A-12B$

Table 3: Values of cyclotomic numbers of order 6 in terms of A,B, and p in case if f is odd.

Hall [8] showed that the number N_s of soultions (x,y) in $1_{\mathcal{H}}\times 1_{\mathcal{H}}$ of $y-x\equiv d \pmod p$ with d in class C_s is obtained by

$$\begin{aligned}N_s=&(-s,-s)_6+(1-s,-s)_6+(-s,1-s)_6+(1-s,1-s)_6+(-s,3-s)_6\\&+(3-s,-s)_6+(1-s,3-s)_6+(3-s,1-s)_6+(3-s,3-s)_6.\end{aligned}$$

	$m \equiv 0 \pmod 3$	$m \equiv 1 \pmod 3$	$m \equiv 2 \pmod 3$
$36(0,0)_6$	$p-17-20A$	$p-17-8A+6B$	$p-17-8A-6B$
$36(0,1)_6$	$p-5+4A+18B$	$p-5+4A+12B$	$p-5+4A+6B$
$36(0,2)_6$	$p-5+4A+6B$	$p-5+4A-6B$	$p-5-8A$
$36(0,3)_6$	$p-5+4A$	$p-5+4A-6B$	$p-5+4A+6B$
$36(0,4)_6$	$p-5+4A-6B$	$p-5-8A$	$p-5+4A+6B$
$36(0,5)_6$	$p-5+4A-18B$	$p-5+4A-6B$	$p-5+4A-12B$
$36(1,2)_6$	$p+1-2A$	$p+1-2A-6B$	$p+1-2A+6B$
$36(1,3)_6$	$p+1-2A$	$p+1-2A-6B$	$p+1-2A-12B$
$36(1,4)_6$	$p+1-2A$	$p+1-2A+12B$	$p+1-2A+6B$
$36(2,4)_6$	$p+1-2A$	$p+1+10A+6B$	$p+1+10A-6B$

Table 4: Values of cyclotomic numbers of order 6 in terms of A, B, and p in case if f is even.

The values for $s = 3, 4, 5$ will repeat those for $s = 0, 1, 2$ if f is odd but they are different if f is even. Using tables $1, 2, 3$, and 4 the values of N_s in terms of p, A, and B are given in table 5 and 6 for $s = 0, 1, 2, 3, 4, 5$. Notice that tables $1, 2, 3, 4$, and 5 are common in literature, see for example [4], [8], and [13]. But Table 6 may be computed only in this paper.

N_s	$m \equiv 0 \pmod 3$	$m \equiv 1 \pmod 3$	$m \equiv 2 \pmod 3$
$s = 0, 3$	$(9p-45+6B)/36$	$(9p-45-18B)/36$	$(9p-45+6A-6B)/36$
$s = 1, 4$	$(9p-27)/36$	$(9p-27-6A+12B)/36$	$(9p-27-6A-12B)/36$
$s = 2, 5$	$(9p-9-6B)/36$	$(9p-9-6A+6B)/36$	$(9p-9+16B)/36$

Table 5: The Values of N_s in terms of A, B, and p for odd f

N_s	$m \equiv 0 \pmod 3$	$m \equiv 1 \pmod 3$	$m \equiv 2 \pmod 3$
$s = 0$	$(9p-45+18B)/36$	$(9p-45+12A-6B)/36$	$(9p-45+12A-12B)/36$
$s = 1$	$(9p-45-12B)/36$	$(9p-45-18B)/36$	$(9p-45-12A-42B)/36$
$s = 2$	$(9p-9+6B)/36$	$(9p-9)/36$	$(9p-9-12A+30B)/36$
$s = 3$	$(9p-45-6B)/36$	$(9p-45-12A-30B)/36$	$(9p-45)/36$
$s = 4$	$(9p-9+12B)/36$	$(9p-9-12A+42B)/36$	$(9p-9+18B)/36$
$s = 5$	$(9p-9-18B)/36$	$(9p-9+12A+12B)/36$	$(9p-9+12A+6B)/36$

Table 6: The Values of N_s in terms of A, B, and p for even f

3 Autocorrelation function of $\mathcal{H}$ if $m \equiv 0 \pmod 3$

In this section we use the constants in the above six tables to exactly determine the autocorrelation values of the sequence $\mathcal{H}$ in the case if $m \equiv 0 \pmod 3$. Moreover, the maximum absolute value is sharply bounded. Some special interesting cases with maximum absolute autocorrelation values 5 or 11 are also discussed.

Theorem 1. *Let $p = 6f + 1 = A^2 + 27v^2$ be an odd prime. Let $\mathcal{H}$ be the Hall's sextic residue sequence defined in* (3) *of period p. Then the autocorrelation function $AC_{\mathcal{H}}(w)$ for $w \neq 0$ is obtained by*

$$AC_{\mathcal{H}}(w) = \begin{cases} -3 + 2v, & w \in C_0 \cup C_3, \\ -1, & w \in C_1 \cup C_4, \\ 1 - 2v, & w \in C_2 \cup C_5. \end{cases} \tag{4}$$

if f is odd, and

$$AC_{\mathcal{H}}(w) = \begin{cases} -3 + 6v, & w \in C_0, \\ -3 - 4v, & w \in C_1, \\ 1 + 2v, & w \in C_2, \\ -3 - 2v, & w \in C_3, \\ 1 + 4v, & w \in C_4, \\ 1 - 6v, & w \in C_5 \end{cases} \tag{5}$$

if f is even.

Proof. Recall first that $m \equiv 0 \pmod 3$ and set $B = 3v$. If f is odd, from table 5 and by substituting in (1) we find that

$$\begin{aligned} AC_{\mathcal{H}}(w) &= N - 4\left(|1_{\mathcal{H}}| - \delta_{1_{\mathcal{H}}}(w)\right) \\ &= p - 4\left(\frac{p-1}{2}\right) + 4\left(\frac{9p - 45 + 6B}{36}\right) \\ &= \left(-3 + \frac{2B}{3}\right) \\ &= -3 + 2v \end{aligned}$$

if $w \in C_0 \cup C_3$,

$$\begin{aligned} AC_{\mathcal{H}}(w) &= N - 4\left(|1_{\mathcal{H}}| - \delta_{1_{\mathcal{H}}}(w)\right) \\ &= p - 4\left(\frac{p-1}{2}\right) + 4\left(\frac{9p - 27}{36}\right) \\ &= -1, \end{aligned}$$

if $w \in C_1 \cup C_4$, and

$$\begin{aligned} AC_{\mathcal{H}}(w) &= N - 4\left(|1_{\mathcal{H}}| - \delta_{1_{\mathcal{H}}}(w)\right) \\ &= p - 4\left(\frac{p-1}{2}\right) + 4\left(\frac{9p-9-6B}{36}\right) \\ &= \left(1 - \frac{2B}{3}\right) \\ &= 1 - 2v \end{aligned}$$

if $w \in C_2 \cup C_5$. If f is even, from table 6 and by substituting in (1) the assertion in (5) is similarly obtained. □

Notice here that the primitive elements modulo p will split up into two sets: the first generates a sequence with out-of-phase autocorrelation values corresponding to the positive value of v and the second generates a sequence with out-of-phase autocorrelation values corresponding to the negative value of v. For example with f odd, if $p = 31$, the primitive elements $3, 12, 17, 24$ generate the sequence 01111010100010011100000011001011 which is the ideal autocorrelation one. While the other primitive elements $11, 13, 21, 22$ generate the sequence 01101000100101011000011100011011 which has $-5, -1, 3$ out-of-phase autocorrelation values. In addition, if the primitive element g generates the first sequence, then g^5 generates the other. The same is true for even f.

Corollary 2. *For prime period p of the sequence $\mathcal{H}$ on the form $p = 6f + 1 = A^2 + 243$ with odd f, we have*

$$AC_{\mathcal{H}}(w) = \begin{cases} 3, & w \in C_0 \cup C_3, \\ -1, & w \in C_1 \cup C_4, \\ -5, & w \in C_2 \cup C_5 \end{cases}$$

if $v = 3$, and

$$AC_{\mathcal{H}}(w) = \begin{cases} -9, & w \in C_0 \cup C_3, \\ -1, & w \in C_1 \cup C_4, \\ 7, & w \in C_2 \cup C_5 \end{cases}$$

if $v = -3$

Proof. By direct substitution in equations (4) the assertion follows. □

There are infinitely many primes p on the form $p = A^2 + 243$. Examples are $307, 439, 499$, and 643. Primes on the form $x^2 + 27y^2$ and their properties have been discussed with some details in chapter 4 in [3]. If g is any primitive element modulo p, one of g or g^5 will generate sequence $\mathcal{H}$ with maximum absolute out-of-phase autocorrelation values 5. This sequence has linear complexity L such that $L = \frac{5(p-1)}{6}$ if $p \equiv 7 \bmod 8$ and $L = \frac{p-1}{3}$ if $p \equiv 3 \pmod 8$ as obtained by Lemma 4 in [7]. It seems that this sequence possesses several pseudo-randomness properties for various applications.

Corollary 3. *For prime period p of the sequence $\mathcal{H}$ on the form $p = 6f + 1 = A^2 + 108$, with even f we have*

$$AC_{\mathcal{H}}(w) = \begin{cases} 9, & w \in C_0 \cup C_4, \\ -11, & w \in C_1 \cup C_5, \\ 5, & w \in C_2, \\ -7 & w \in C_3, \end{cases}$$

if $v = 2$, and

$$AC_{\mathcal{H}}(w) = \begin{cases} -15, & w \in C_0, \\ 5, & w \in C_1, \\ -3, & w \in C_2, \\ 1 & w \in C_3, \\ -7 & w \in C_4, \\ 13 & w \in C_5. \end{cases}$$

if $v = -2$

Proof. By direct substitution in equations (5) the assertion follows. □

Notice that the only possible case such that the sequence $\mathcal{H}$ has four out-of-phase autocorrelation values, for p on the form $p = 6f + 1 = A^2 + 27v^2$ with f even, is when $v = 2$.

Theorem 4. *Let $p = 6f + 1 = A^2 + 27v^2$ be an odd prime. Let $\mathcal{H}$ be the Hall's sextic residue sequence defined in* (3) *of period p. Then the autocorelation function $AC_{\mathcal{H}}(w)$ for $w \neq 0$ satisfies:*

$$\max_{1 \leq w \leq p-1} |AC_{\mathcal{H}}(w)| < 3 + 2\sqrt{p/27},$$

if f is odd, and

$$\max_{1 \leq w \leq p-1} |AC_{\mathcal{H}}(w)| < 3 + 2\sqrt{p/3},$$

if f is even.

Proof. It is easy to check that $\sqrt{p} = \sqrt{A^2 + 27v^2} > \sqrt{27}|v|$. If f is odd, from (4) we have

$$|-3 + 2v| \leq 3 + 2|v| < 3 + 2\sqrt{p/27},$$

and

$$|1 - 2v| \leq 1 + 2|v| < 3 + 2|v| < 3 + 2\sqrt{p/27}.$$

This proves the first assertion. Notice here that $3 + 2\sqrt{p/27} < 1 + \sqrt{p/3}$ except at $p = 31$ and $p = 43$. Using (5) the second assertion can similarly proven. □

4 Autocorrelation function of $\mathcal{H}$ if $m \not\equiv 0 \pmod 3$

This section examines the autocorrelation function $AC_{\mathcal{H}}(w)$ for primes in the form $p = A^2 + 3B^2$ where $\gcd(B, 3) = 1$. In this case m is either congruent to 1 modulo 3 or congruent to 2 modulo 3.

Theorem 5. *Let $p = 6f + 1 = A^2 + 3B^2$ be an odd prime where $\gcd(B, 3) = 1$ and f is odd. Let $\mathcal{H}$ be the Hall's sextic residue sequence defined in (3) of period p. Then the autocorrelation function $AC_{\mathcal{H}}(w)$ for $w \neq 0$ is obtained by*

$$AC_{\mathcal{H}}(w) = \begin{cases} -3 - 2B, & w \in C_0 \cup C_3, \\ -1 - 2(k - B), & w \in C_1 \cup C_4, \\ 1 + 2k, & w \in C_2 \cup C_5 \end{cases} \tag{6}$$

if $m \equiv 1 \bmod 3$, and

$$AC_{\mathcal{H}}(w) = \begin{cases} -3 + 2k, & w \in C_0 \cup C_3, \\ -1 - 2(k + B), & w \in C_1 \cup C_4, \\ 1 + 2B, & w \in C_2 \cup C_5 \end{cases} \tag{7}$$

if $m \equiv 2 \bmod 3$.

Proof. From Table 3 and by substituting in (1) we find that if $m \equiv 1 \pmod 3$,

$$\begin{aligned} AC_{\mathcal{H}}(w) &= N - 4\left(|1_{\mathcal{H}}| - \delta_{1_{\mathcal{H}}}(w)\right) \\ &= p - 4\left(\frac{p-1}{2}\right) + 4\left(\frac{9p - 45 - 18B}{36}\right) \\ &= -3 - 2B, \end{aligned}$$

if $w \in C_0 \cup C_3$, and

$$\begin{aligned} AC_{\mathcal{H}}(w) &= N - 4\left(|1_{\mathcal{H}}| - \delta_{1_{\mathcal{H}}}(w)\right) \\ &= p - 4\left(\frac{p-1}{2}\right) + 4\left(\frac{9p - 27 - 6A + 12B}{36}\right) \\ &= -1 - 2(k - B), \end{aligned}$$

if $w \in C_1 \cup C_4$, and

$$\begin{aligned} AC_{\mathcal{H}}(w) &= N - 4\left(|1_{\mathcal{H}}| - \delta_{1_{\mathcal{H}}}(w)\right) \\ &= p - 4\left(\frac{p-1}{2}\right) + 4\left(\frac{9p - 9 + 6A + 6B}{36}\right) \\ &= 1 + 2k, \end{aligned}$$

if $w \in C_2 \cup C_5$. If $m \equiv 2 \pmod 3$ the proof is very similar. □

Theorem 6. *Let $7 \neq p = 6f + 1 = A^2 + 3B^2$ be an odd prime with $\gcd(3, B) = 1$ and f is odd. Let $\mathcal{H}$ be the Hall's sextic residue sequence defined in (3) of period p. Then the autocorrelation function $AC_{\mathcal{H}}(w)$ for $w \neq 0$ satisfies:*

$$\max_{1 \leq w \leq p-1} |AC_{\mathcal{H}}(w)| < \sqrt{3p}.$$

Proof. Assume that $7 \neq p = 6f + 1 = A^2 + 3B^2$ be an odd prime with $\gcd(B, 3) = 1$ and f is odd. It is easy to see that $\sqrt{p} = \sqrt{A^2 + 3B^2} > \sqrt{3}|B|$ and $\sqrt{p} = \sqrt{A^2 + 3B^2} > |A|$. Then we have $|k| = |\frac{A \pm B}{3}| \leq \frac{|A|+|B|}{3} \leq \sqrt{p/3}(\frac{\sqrt{3}+1}{3}) < \sqrt{p/3}$, since $\frac{\sqrt{3}+1}{3} < 1$. Therefore, if $m \equiv 1 \pmod 3$, we have from (6) that:

$$| - 3 - 2B| \leq 3 + 2|B| < 3 + 2\sqrt{p/3} = 3 + 1.155\sqrt{p}.$$

$$\begin{aligned} | - 1 - 2(k - B)| &\leq 1 + 2|k - B| \\ &\leq 1 + \frac{2}{3}(|A| + 2|B|) \\ &< 1 + \frac{2}{3}\left(\sqrt{p} + \frac{2}{\sqrt{3}}\sqrt{p}\right) \\ &\leq 1 + \frac{2}{3}\sqrt{p}\left(\frac{\sqrt{3}+2}{\sqrt{3}}\right) = 1 + 1.4365\sqrt{p}, \end{aligned}$$

and

$$|1 + 2k| \leq 1 + 2|k| \leq 1 + 2\sqrt{p/3} = 1 + 1.155\sqrt{p}.$$

But we have $1 + 1.155\sqrt{p} < 3 + 1.155\sqrt{p} < 1 + 1.4365\sqrt{p} < \sqrt{3p}$. If $m \equiv 2 \pmod 3$, the proof is very similar. □

Some special cases have better upper bounds.

Corollary 7. *Let $p = 6f + 1 = A^2 + 3$ be an odd prime with $|A| > 2$ and f is odd. Let $\mathcal{H}$ be the Hall's sextic residue sequence defined in* (3)*. Then the autocorrelation function $AC_{\mathcal{H}}(w)$ for $w \neq 0$ satisfies:*

$$\max_{1 \leq w \leq p-1} |AC_{\mathcal{H}}(w)| < \sqrt{p} + 1.$$

Proof. The assertion is valid for $p = 19$ since the autocorrelation values are $-1, 3, -5$. Now let p be an odd prime number greater than 19 on the form $p = 6f + 1 = A^2 + 3$ with odd f. This means that $|A| \geq 8$, i.e. $p \geq 67$. Then we have if $m \equiv 1 \bmod 3$,

$$| - 3 - 2B| \leq 5,$$

$$| - 1 - 2(k - B)| \leq 1 + 2|k - B| \leq 3 + \frac{2}{3}|A| \leq 3 + \frac{2}{3}\sqrt{p} \leq \sqrt{p} + 1,$$

and

$$|1 + 2k| \leq 1 + 2|k| \leq 1 + \frac{2}{3}|A + B| \leq 2 + \frac{2}{3}|A| \leq 1 + \sqrt{p}.$$

The other case for $m \equiv 2 \pmod 3$ is similar and the assertion satisfied. □

Other special cases like $p = A^2 + 75$ gives the same upper bound.

The results in this section show that $\mathcal{H}$ is 3-out-of-phase autocorrelation values in its general case with maximum absolute value of $O(\sqrt{p})$ if $p = A^2 + 3B^2$ with $\gcd(B, 3) = 1$ and f is odd. Now we discuss whether it is 2-out-of-phase autocorrelation values for certain choices of p.

Theorem 8. *The sequence $\mathcal{H}$ that defined in* (3) *for prime $p = A^2+3B^2$ with* $\gcd(B, 3) = 1$ *is 2-out-of-phase autocorrelation values if and only if p can be written on the forms $p = 13A^2 \pm 36A + 27$, $16p = 19A^2 \pm 36A + 108$, or $25p = 28A^2 \mp 18A + 27$. The sign in p depending on whether $m \equiv 1$ or $2 \pmod 3$.*

Proof. If $m \equiv 1 \pmod 3$, using (6) we have:

- If $1 + 2k = -1 - 2(k - B)$. Direct simplification gives $B = 3 + 2A$. Then we have $p = A^2 + 3v^2 = 13A^2 + 36A + 27$. Primes on this form include $379, 571$, and 3931. In this case $AC_{\mathcal{H}}(w) = -9 - 4A$ if $w \in C_0 \cup C_3$ and $3 + 2A$ otherwise.
- If $1 + 2k = -3 - 2B$. Then we have $B = \frac{-6-A}{4}$. Hence $16p = 19A^2 + 36A + 108$. Primes on this form include $631, 751$, and 6343. In this case $AC_{\mathcal{H}}(w) = -A - 3$ if $w \in C_1 \cup C_4$ and $A/2$ otherwise.
- If $-3 - 2B = -1 - 2(k - B)$. Then we have $B = \frac{A-3}{5}$. Hence $25p = 28A^2 - 18A + 27$. Primes on this form include $859, 1171$, and 3727. In this case $AC_{\mathcal{H}}(w) = (4A + 3)/5$ if $w \in C_2 \cup C_5$ and $(-9 - 2A)/5$ otherwise.

While if $m \equiv 2 \bmod 3$, using (7) we have:

- If $-3 + 2k = -1 - 2(k + B)$. Direct simplification gives $B = 3 - 2A$. Then we have $p = 13A^2 - 36A + 27$. Primes on this form include $151, 967$, and 3079. In this case $AC_{\mathcal{H}}(w) = 7 - 4A$ if $w \in C_2 \cup C_5$ and $-5 + 2A$ otherwise.
- If $-3 + 2k = 1 + 2B$. Then we have $B = \frac{A-6}{4}$. Hence $16p = 19A^2 - 36A + 108$. Primes on this form include $103, 271$, and 1303. In this case $AC_{\mathcal{H}}(w) = 1 - A$ if $w \in C_1 \cup C_4$ and $(A - 4)/2$ otherwise.
- If $1 + 2B = -1 - 2(k + B)$. Then we have $B = \frac{-A-3}{5}$. Hence $25p = 28A^2 + 18A + 27$. Primes on this form include $67, 3067, 7591$, and 10687. In this case $AC_{\mathcal{H}}(w) = (4A-13)/5$ if $w \in C_0 \cup C_3$ and $(-2A - 1)/5$ otherwise.

□

Notice here that although the sequence $\mathcal{H}$ has 2-out-of-phase autocorrelation values for the above forms of p, its support set $1_{\mathcal{H}}$ is not an almost-difference set.

Using the same technique in Theorem 1 and Table 6 one be able to prove the following results:

Theorem 9. *Let $p = 6f + 1 = A^2 + 3B^2$ be an odd prime where* $\gcd(B, 3) = 1$ *with even f. Let $\mathcal{H}$ be the Hall's sextic residue sequence defined in* (3) *of period p. Then the autocorrelation function $AC_{\mathcal{H}}(w)$ for $w \neq 0$ is obtained by*

$$AC_{\mathcal{H}}(w) = \begin{cases} -3 + 4k - 2B, & w \in C_0, \\ -3 - 2B, & w \in C_1, \\ 1, & w \in C_2, \\ -3 - 4k - 2B, & w \in C_3, \\ 1 - 4k + 6B, & w \in C_4, \\ 1 + 4k, & w \in C_5 \end{cases} \tag{8}$$

if $m \equiv 1 \bmod 3$, *and*

$$AC_{\mathcal{H}}(w) = \begin{cases} -3+4k, & w \in C_0, \\ -3-4k-6B, & w \in C_1, \\ 1-4k+2B, & w \in C_2, \\ -3, & w \in C_3, \\ 1+2B, & w \in C_4, \\ 1+4k+2B, & w \in C_5 \end{cases} \tag{9}$$

if $m \equiv 2 \pmod 3$.

Theorem 10. *Let* $7 \neq p = 6f+1 = A^2+3B^2$ *be an odd prime with* $\gcd(3,B)=1$ *and* f *is even. Let* $\mathcal{H}$ *be the Hall's sextic residue sequence defined in* (3) *of period* p. *Then the autocorrelation function* $AC_{\mathcal{H}}(w)$ *for* $w \neq 0$ *satisfies:*

$$\max_{1 \leq w \leq p-1} |AC_{\mathcal{H}}(w)| < 3 + 10\sqrt{p/3}.$$

5 Concluding Remarks

This paper presented exact values of the autocorrelation function of the Hall's sextic residues sequence $\mathcal{H}$ of prime period p on the form $p = 6f+1$. It is shown that $\mathcal{H}$ is 3-out-of-phase autocorrelation values in its general case if f is odd and 6-out-of-phase autocorrelation values if f is even. The maximum absolute autocorrelation value is bounded by $c\sqrt{p}$ with $c = 1/\sqrt{3}, 2/\sqrt{3}, 3/\sqrt{3}, 10/\sqrt{3}$ for different values of m and f. It is shown also that if p is on the forms $p = 13A^2 \pm 36A + 27$, $16p = 19A^2 \pm 36A + 108$, or $25p = 28A^2 \mp 18A + 27$ with even A, the sequence is 2-out-phase autocorrelation. If the period p on the form A^2+243, the sequence has 3-out-of-phase autocorrelation values $3, -1$, and -5.

References

[1] H. Aly, W. Meidl, and A. Winterhof, "On the k-error linear complexity of cyclotomic sequences." J. Math. Cryptol. 1 (2007), 1–14.

[2] Y. Cai and C. Ding, "Binary sequences with optimal autocorrelation." Theoretical Computer Science 410 (2009), 2316–2322.

[3] D. A. Cox "Primes of the Form x^2+ny^2: Fermat, Class Field Theory, and Complex Multiplication," A Wiley-Interscience Publication, John Wiley Sons, Inc. (1989).

[4] L. E. Dickson, "Cyclotomy, higher congruences, and Waring's problem." Amer. J. Math. vol 57 (1935) 391–424.

[5] C. Ding, T. Helleseth and K.Y. Lam, "Several classes of binary sequences with three-level autocorrelation." IEEE Trans. Inform. Theory 45 (1999), 2606–2612.

[6] 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.

[7] V.E. Edemskiy "On the linear complexity of binary sequences on the basis of biquadratic and sextic residue classes", Discrete Math. Appl., Vol 20, No. 1, (2010), 75–84.

[8] M. Hall, Jr., "A survey of difference sets." Proc. Amer. Math. Soc. 7 (1956), 975–986.

[9] 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.

[10] K. Ireland and M. Rosen, "A classical introduction to modern number theory," (Springer Verlag), Second Edition (1990).

[11] 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.

[12] W. Su, Y. Yang, and C. Fan, " New optimal binary sequences with period $4p$ via interleaving Ding-Helleseth- Lam sequences." Des. Codes, Cryptogr. 86 (2018) 1329–1338.

[13] A. I. Whiteman "The cyclotomic number of order twelve." Acta Arithmetica VI (1960), 53–76.