Some Results On Three-Valued Walsh Transforms from Decimations of Helleseth-Gong Sequences

Hasan Dilek, Ernin Tilenbaev, Zülfükar Saygı and Çetin Ürtiş

I. INTRODUCTION

Given two sequences \( \{a(t)\} \) and \( \{b(t)\} \) of period \( N \) with elements from a finite field \( F_p \). The cross-correlation between the sequences at shift \( \tau \) is defined by

\[
C_{a,b}(\tau) = \sum_{t=0}^{N-1} a(t+\tau)b(t)
\]

where \( \omega \) is a complex \( p \) th root of unity. In the particular case when two sequences are the same, we denote it by the autocorrelation \( A_{a,a}(\tau) \). A sequence \( \{a(t)\} \) is said to have (ideal) two-level autocorrelation if \( A_{a,a}(\tau) = -1 \) for all \( \tau \neq 0 \) (mod \( N \)). We say two vectors in a vector space of dimension \( n \) over the complex field is orthogonal if their inner product is equal to zero.

Recently, Gong, Helleseth, and Hu studied the Walsh transform of a subclass of Helleseth-Gong sequences as well as the Walsh transform of their certain decimations [1]. They found many decimation numbers which yield three-valued Walsh transforms by computer search. They proved two cases and also found additional values of decimation number which yield three-valued Walsh transform. Gong, Helleseth, Hu and Li proved two more cases with new observations. In this paper, for \( p = 5 \), \( k = 1 \), \( n = 5 \) and \( s = 2 \) we proved that the decimation value \( d = 481 \) yields a three-valued Walsh transform, which is not covered in previous studies. Also we present a conjecture for \( p = 3 \) at the end of the paper.

Index Terms—Autocorrelation, cross-correlation, m-sequences, p-ary sequences, Walsh transform, Helleseth-Gong sequences.

II. PRELIMINARIES

For any prime \( p \), and any positive integer \( n \), let \( F_{p^n} \) denote the finite field with \( p^n \) elements. Let \( \alpha \) be a primitive element in \( F_{p^n} \) and let

\[
\lambda = \sum_{x \in F_{p^n}} w^{f(x)+Tr_n(\lambda x)}.
\]

be the trace from the finite field \( F_{p^n} \) to the subfield \( F_{p^k} \) for some \( k | n \). In particular, we denote the (absolute) trace from \( F_{p^k} \) to \( F_p \) by \( Tr_n(x) \).

Definition 1: For any function \( f(x) \) from \( F_{p^n} \) to \( F_p \), and \( \lambda \in F_{p^n} \), the Walsh transform of \( f \) at \( \lambda \) is defined by

\[
\hat{f}(\lambda) = \sum_{x \in F_{p^n}} w^{f(x)-Tr_n(\lambda x)}.
\]

The Walsh transform is an important tool in cryptography and in design and analysis of sequences over finite fields. For binary and nonbinary functions, the Walsh transform determines the cross-correlation between a pair of \( p \)-ary sequences, the sequence defined by \( a(t) = f(\alpha^t) \) and the \( m \)-sequence given by \( b(t) = Tr_n(\alpha^t) \).

The cross-correlation at shift \( \tau \) between these two sequences is given by

\[
C_{a,b}(\tau) = \sum_{t=0}^{p^n-2} w^{a(t+\tau)-b(t)}
\]

where \( \lambda = -\omega^{-\tau} \).

Helleseth and Gong proved the following fact.

Fact 2: ([3]): Let \( \alpha \) be a primitive element of \( F_{p^n} \). Let \( n = (2m+1)k \) and let \( s \), \( 1 \leq s \leq 2m \), be an integer such that \( gcd(s, 2m+1) = 1 \). Let \( b_0 = 1 \), \( b_1 = b_{2m+1} \), and \( b_{is} = (-1)^s \) for \( i = 1, 2, \ldots, m \), where indices of \( b_{is} \) are taken mod \( 2m+1 \).
Let \( u_0 = b_0/2 = (p+1)/2 \) and \( u_i = b_{2i} \) for \( i = 1, 2, \ldots, m \).

Define

\[
 f(x) = \sum_{i=0}^{m} u_i x^{(2^k+1)/2}.
\]

Then the sequence over \( \mathbb{F}_p \) defined by

\[
 s(t) = T_{r_n}(f(\alpha^t))
\]

has an ideal two-level autocorrelation.

The fact above in the special case \( s = 2 \) gives \( b_{2i} = u_i = (-1)^i(\equiv b_{2m+1-i}) \) for \( i = 1, 2, \ldots, m \) and \( b_0 = 2u_0 = 1 \), i.e., \( u_0 = (p+1)/2 \).

**Lemma 3:** (\( \{1\}, \{2\}, \{3\} \)): Let \( Q(y) \) be a quadratic form over \( \mathbb{F}_q \), \( q = p^k \) in \( n/k \) variables of rank \( \rho \). Let \( r \) be a nonsquare in \( \mathbb{F}_q \) and define

\[
 S = \frac{1}{2} \sum_{x \in \mathbb{F}_p} u_i x^{(2^k+1)/2}.
\]

Then

\[
 S = \begin{cases} 
 0, & \text{if } \rho \text{ is odd} \\
 \pm \rho^{\frac{n+1}{2}}, & \text{if } \rho \text{ is even} 
\end{cases}
\]

### III. KNOWN RESULTS

Helleseth and Gong proved the following theorem.

**Theorem 4:** (\( \{1\} \)): Let \( u_0 = (p+1)/2 \) and \( u_i = (-1)^i \) for \( i = 1, 2, \ldots, m \), and let \( d \in \{ 1, \ldots, p-1 \} \). The Walsh transform of

\[
 h(x) = T_{r_n}(\sum_{i=0}^{m} u_i x^{(2^k+1)/2})
\]

defined by

\[
 \hat{h}(\lambda) = \sum_{x \in \mathbb{F}_p} h(x) x^{-\lambda}
\]

has values in the set \( \{0, \pm \rho^{\frac{n+1}{2}}\} \). The distribution of \( \hat{h}(\lambda) \) when \( \lambda \) runs through \( \mathbb{F}_p \) is

\[
 0 \quad \text{occurs } p^m - p^{n-k} \quad \text{times} \\
 -p^{(n+k)/2} \quad \text{occurs } (p^{n-k} - p^{(n-k)/2})/2 \quad \text{times} \\
 p^{(n+k)/2} \quad \text{occurs } (p^{n-k} + p^{(n-k)/2})/2 \quad \text{times}
\]

Also some experimental results are given in Table 1.

**Theorem 5:** (\( \{2\} \)): Let \( p \) be an odd prime number, and \( q = p^k \). Let \( n = (2m+1)/2 \) and \( s = 1 \), \( 1 \leq s \leq 2m \), be an integer such that \( gcd(s, 2m+1) = 1 \). Let \( b_0 = 1, b_i = b_{2m+1-i} \) and \( b_{2i} = (-1)^i \) for \( i = 1, 2, \ldots, m \), where indices of \( b_{2i} \) are taken \( \text{mod} 2m+1 \). Let \( u_0 = b_0/2 = (p+1)/2 \) and \( u_i = b_{2i} \) for \( i = 1, 2, \ldots, m \). Define

\[
 f(x) = \sum_{i=0}^{m} u_i x^{(2^i+1)/2}.
\]

The Walsh transform of \( f(x) \) has values in the set \( \{0, \pm \rho^{\frac{n+1}{2}}\} \). The distribution of \( \hat{f}(\lambda) \) when \( \lambda \) runs through \( \mathbb{F}_p \) is

\[
 0 \quad \text{occurs } p^m - p^{n-k} \quad \text{times} \\
 -p^{(n+k)/2} \quad \text{occurs } (p^{n-k} - p^{(n-k)/2})/2 \quad \text{times} \\
 p^{(n+k)/2} \quad \text{occurs } (p^{n-k} + p^{(n-k)/2})/2 \quad \text{times}
\]

### Table I

**Experimental Data**

<table>
<thead>
<tr>
<th>Finite Field</th>
<th>s</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathbb{F}_{25} )</td>
<td>1</td>
<td>1,49,61</td>
</tr>
<tr>
<td>( \mathbb{F}_{27} )</td>
<td>2</td>
<td>7,23,35,49</td>
</tr>
<tr>
<td>( \mathbb{F}_{29} )</td>
<td>1</td>
<td>1,391</td>
</tr>
<tr>
<td>( \mathbb{F}_{31} )</td>
<td>2</td>
<td>61,169</td>
</tr>
<tr>
<td>( \mathbb{F}_{33} )</td>
<td>3</td>
<td>1,439</td>
</tr>
<tr>
<td>( \mathbb{F}_{37} )</td>
<td>1</td>
<td>1,3363</td>
</tr>
<tr>
<td>( \mathbb{F}_{41} )</td>
<td>2</td>
<td>547,1667</td>
</tr>
<tr>
<td>( \mathbb{F}_{43} )</td>
<td>4</td>
<td>1,3917</td>
</tr>
</tbody>
</table>

### Table II

**Experimental Data (Decimations numbers which have not been proved yet)**

<table>
<thead>
<tr>
<th>Finite Field</th>
<th>s</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathbb{F}_{35} )</td>
<td>2</td>
<td>7,23,35,49</td>
</tr>
<tr>
<td>( \mathbb{F}_{37} )</td>
<td>2</td>
<td>61,169</td>
</tr>
<tr>
<td>( \mathbb{F}_{39} )</td>
<td>2</td>
<td>547,1667</td>
</tr>
<tr>
<td>( \mathbb{F}_{41} )</td>
<td>2</td>
<td>4921,14041</td>
</tr>
<tr>
<td>( \mathbb{F}_{43} )</td>
<td>2</td>
<td>44287,131013</td>
</tr>
<tr>
<td>( \mathbb{F}_{47} )</td>
<td>2</td>
<td>398581,1194649</td>
</tr>
</tbody>
</table>
IV. EXPERIMENTAL RESULTS

We have implemented a SAGE code to find the exact cross-
correlation distribution of Helleseth-Gong sequences and its
decimated ones. Note that these cross-correlation values can
be easily obtained by (Table 2). For this reason we only
concentrated on the values of Walsh transform. For \( p = 3 \)
we have confirmed the decimation values given in Table 1.
Furthermore, in our search for \( p = 5, k = 1, n = 5 \) and
\( s = 2 \) we see that the decimation value \( d = 481 \) also yields a
three-valued Walsh transform.

We observe that this decimation numbers is not covered in
the results of [1] and [2]. In the following we state and prove
this observation. Also at the end of this section we give a
conjecture for \( p = 3 \) using Table 1 which was also confirmed
in our experiments for some values of \( n \).

**Theorem 7:** Let \( p = 5, k = 1, n = 5, s = 2 \) and \( d = 481 \).
and let \( u_i = (-1)^i \) for \( i = 0, 1, 2, ..., m \). The Walsh transform of
\[
\hat{h}(\lambda) = \sum_{x \in \mathbb{F}_5} w^{h(x)+Tr_{n}(\lambda x)}
\]
has values in the set \( \{ 0, \pm 5^3 \} \). The distribution of \( \hat{h}(\lambda) \) when
\( \lambda \) runs through \( \mathbb{F}_{5^5} \) is

- 0 occurs \( 5^5 - 5^4 \) = 2500 times
- \(-5^3\) occurs \( (5^4 - 5^2)/2 \) = 300 times
- \( 5^3\) occurs \( (5^4 + 5^2)/2 \) = 325 times

**Proof:** Define the function \( F(x) \) from \( \mathbb{F}_{5^3} \) to \( \mathbb{F}_{5} \) by
\[
F(x) = Tr_{5}(f(x^{481}) + \lambda x) = Tr_{5} \left( \sum_{i=0}^{2} u_i x^{2^i + 481} + \lambda x \right)
\]
and observe that
\[
\hat{h}(\lambda) = Tr_{5}(\lambda x) = Tr_{5}(f(x^{481}) + \lambda x) = F(x).
\]
It follows that \( F(rx) = rF(x) \) for any \( r \in \mathbb{F}_5 \), since
\[
\frac{5^{2i} + 1}{2} = 481 \cdot 1 \cdot 1 = 1 \mod 4
\]
Furthermore,
\[
F(x) = Tr_{5}(u_0 x^{481} + u_1 x^{13 \cdot 481} + u_2 x^{313 \cdot 481} + \lambda x) = Tr_{5}(u_0 x^{481} + u_1 x^5 + u_2 x^{601} + \lambda x).
\]
Now taking the \( 5^5 + 5 = 630 \) th power of \( x \), we obtained that
\[
F(x^{630}) = Tr_{5}(u_0 x^{2} + u_1 x^{26} + u_2 x^{626} + \lambda x^{630}) = Tr_{5}(u_0 x^{5^0 + 1} + u_1 x^{5^1 + 1} + u_2 x^{5^4 + 1} + \lambda x^{5^4 + 5}).
\]
Here we see that \( F(x^{630}) \) is a quadratic form over \( \mathbb{F}_5 \). Now
using the same technique in Lemma 1 and Lemma 2 of [1], we
complete the proof. Note this technique uses the results
from Trachtenberg [6] and Helleseth and Gong [3].

Moreover, based on numerical results on SAGE, we have the
following conjecture for \( p = 3 \).

**Conjecture 8:** Let \( p = 3, n = 2m + 1, n \geq 5, u_0 = (p+1)/2 \) and \( u_i = (-1)^i \) for \( i = 1, 2, ..., m \), and let \( d = p^{n+1} \). The Walsh transform of
\[
h(x) = Tr_{n} \left( \sum_{i=0}^{m} u_i x^{2^i + d} \right)
\]

is defined by
\[
\hat{h}(\lambda) = \sum_{x \in \mathbb{F}_{p^n}} w^{h(x)+Tr_{n}(\lambda x)}
\]
has values in the set \( \{ 0, \pm p^{n+1} \} \). The distribution of \( \hat{h}(\lambda) \) when \( \lambda \) runs through \( \mathbb{F}_{p^n} \) is

- 0 occurs \( p^n - p^{n-k} \) times
- \(-p^{(n+1)/2} \) occurs \( (p^{n-k} - p^{(n-k)/2})/2 \) times
- \( p^{(n+1)/2} \) occurs \( (p^{n-k} + p^{(n-k)/2})/2 \) times

We have tried to prove this conjecture using similar tech-
nique in [1] and [2]. After some point in the proof we get a
form having higher degrees instead of a quadratic form. The
crucial part of the proofs in [1] and [2] based on getting a
quadratic form in the computation of Walsh transform. For
this reason, we can prove the case \( p = 5, n = 5 \) and \( d = 481 \),
but we cannot complete our conjecture.

V. CONCLUSION

Gong, Helleseth, and Hu studied the Walsh transform of a
subclass of Helleseth-Gong sequences as well as the Walsh
transform of their certain decimations. They give many dec-
imations numbers which have not been proved yet. We have
made some numerical computations. Based on these results we
present a conjecture which requires some more techniques to
be proved. Also for \( p = 5, k = 1, n = 5 \) and \( s = 2 \) we proved
that the decimation value \( d = 481 \) yields a three-valued Walsh
transform.

**APPENDIX**

**SAGE CODE**

```sage
""Defining variables.."
import fractions;
m=2;
p=5;
k=1;
n=(2*m+1)*k;
q=p^n;
Fq.<a>=GF(q,'a');
def correct(value):
    value = coerce( complex,value );
    value = round( value.real, 4 ) +
    round( value.imag, 4 )*1;
    return value;
def u(i):
    if i==0:
        return coerce(int, (p+1)/2);
    return (-1)^i;
d_degerleri = [];
```
```python

d_karaliste = [];
d = 481;
"""Defining h(x)..."""

```python

def h(x):
    sum = 0;
    for i in range(m+1):
        sum = sum + u(i)*x**( (p**(2*k*i)+1)*d/2 );
    return sum.trace();

"""Defining walsh transform"

```python

def h_head(lam):
    sum = 0;
    for x in Fq:
        y = h(x)+(lam*x).trace();
        y = coerce( int, coerce(str,y) );
        sum = sum + exp(2*pi*I*( y )/p);  # EXPRESSION NOT COMPLETE
    return sum;

print "\n tum degerler...\n";

```python

h_head_values = [];
Unique_h_values = [];
for x in range(q-1):
    value = h_head(a**x);
    value = numerical_approx( value );
    value = correct( value );
    print value;
    h_head_values.append(value);
    for i in h_head_values:
        if i not in Unique_h_values:
            Unique_h_values.append(i);
    if len(Unique_h_values)>3:
        d_karaliste.append(d);
        z = 1;
        while (d*p^z % (q-1) != d):
            d_karaliste.append(d*p^z % (q-1));
            z = z + 1;
        break;
else:
    d_degerleri.append(d);
    z = 1;
    while (d*p^z % (q-1) != d):
        d_degerleri.append(d*p^z % (q-1));
        z = z + 1;

```

ACKNOWLEDGMENT

The authors would like to thank the anonymous referee for their valuable and helpful comments and also the first and the third authors were partially supported by TÜBİTAK under Grant no. TBAG-109T344. The numerical calculations reported in this paper were performed at TÜBİTAK ULAKBIM, High Performance and Grid Computing Center (TRUBA Resources).

References