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

Hasan Dilek, Ernist Tilenbaev, Zülfükar Saygı and Çetin Ürtiş

***Abstract*—The Walsh transform of two-level autocorrelation sequences has played an important role in construction of the set of sequences. For p-ary sequences, there are only two basic classes of two-level autocorrelation sequences with no subfield structures for an arbitrary odd prime p. One is the class of p-ary m-sequences and the other of p-ary Helleseth-Gong sequences. Gong, Helleseth, and Hu 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.**

I. INTRODUCTION

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

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

where w 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 $\tau \neq 0 \pmod{N}$. 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 of them. But later on, Gong, Helleseth, Hu, and Li present more decimation numbers for three-valued Walsh transform than in [1] which involves some new obversations [2]. There are some main differences between [1] and [2]. One is that u_i which will be defined later is not limited $(-1)^i$ as in [1], but it is relaxed to that in the definition of Helleseth-Gong sequences.

This paper is organized as follows. Section II contains necessary backgound on Helleseth-Gong sequences and the Walsh transform. Section III contains the known results and Section IV contains experimental results. Finally, the paper is concluded in Section V.

H.Dilek, Department of Mathematics, TOBB University of Economics and Technology
E.Tilanbaev, Department of Mathematics, TOBB University of Economics and Technology
Z.Saygi, Department of Mathematics, TOBB University of Economics and Technology
Ç.Ürtiş, Department of Mathematics, TOBB University of Economics and Technology

II. PRELIMINARIES

For any prime p, and any positive integer n, let $\mathbb{F}_{p^n}$ denote the finite field with p^n elements. Let α be a primitive element in $\mathbb{F}_{p^n}$ and let

$$Tr_k^n(x) = \sum_{i=0}^{\frac{n}{k}-1} x^{p^{ik}}$$

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

Definition 1: For any function $f(x)$ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, and $\lambda \in \mathbb{F}_{p^n}$, the Walsh transform of f at λ 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 τ between these two sequences is given by

$$\begin{aligned} C_{a,b}(\tau) &= \sum_{t=0}^{p^n-2} w^{a(t+\tau)-b(t)} \\ &= \sum_{t=0}^{p^n-2} w^{f(\alpha^\tau\alpha^t)-Tr_n(\alpha^t)} \\ &= \sum_{x\in F_{p^n}\setminus\{0\}} w^{f(x)+Tr_n(\lambda x)} \\ &= -w^{f(0)} + \hat{f}(\lambda), \end{aligned}$$

where $\lambda = -\alpha^{-\tau}$.

Helleseth and Gong proved the following fact.

Fact 2: ([3]): Let α be a primitive element of $\mathbb{F}_{p^n}$. Let $n = (2m+1)k$ and let s, $1 \leq s \leq 2m$, be an integer such that $gcd(s, 2m+1) = 1$. Let $b_0 = 1$,$b_i = b_{2m+1-i}$ and $b_{is} = (-1)^i$ for $i = 1, 2, ..., m$, where indices of b_{is} are taken $\bmod\ 2m+1$.

Let $u_0 = b_0/2 = (p+1)/2$ and $u_i = b_{2i}$ for $i = 1, 2, ..., m$. Define

$$f(x) = \sum_{i=0}^{m} u_i x^{(p^{2ki}+1)/2}.$$

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

$$s(t) = Tr_n(f(\alpha^t))$$

has an ideal two-level autocorrelation.

The fact above in the special case $s = 2$ gives $b_{2i} = u_i = (-1)^i (= b_{2m+1-i})$ for $i = 1, 2, ..., m$ 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 ρ. Let r be a nonsquare in $\mathbb{F}_q$ and define

$$S = \frac{1}{2}\left(\sum_{y\in\mathbb{F}_{p^n}} w^{Tr_k(Q(y))} + \sum_{y\in\mathbb{F}_{p^n}} w^{Tr_k(rQ(y))}\right)$$

Then

$$S = \begin{cases} 0, & \text{if } \rho \text{ is odd} \\ \pm\rho^{\frac{n}{k}-\frac{\rho}{2}}, & \text{if } \rho \text{ is even} \end{cases}$$

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 $i = 1, 2, ..., m$, and let $d \in \left\{1, \frac{p^n+1}{p^k+1}\right\}$.The Walsh tarnsform of

$$h(x) = Tr_n\left(\sum_{i=0}^{m} u_i x^{\frac{p^{2ki}+1}{2}d}\right)$$

defined by

$$\hat{h}(\lambda) = \sum_{x\in\mathbb{F}_{p^n}} w^{h(x)+Tr_n(\lambda x)}$$

has values in the set $\left\{0, \pm p^{\frac{n+k}{2}}\right\}$. The distribution of $\hat{h}(\lambda)$ when λ runs through $\mathbb{F}_{p^n}$ is

$$\begin{array}{cccc} 0 & \text{occurs} & p^n - p^{n-k} & \text{times} \\ -p^{(n+k)/2} & \text{occurs} & (p^{n-k} - p^{(n-k)/2})/2 & \text{times} \\ p^{(n+k)/2} & \text{occurs} & (p^{n-k} + p^{(n-k)/2})/2 & \text{times} \end{array}$$

Also some experimental results are given in Table 1.

Theorem 5: ([2]): Let p be an odd prime number, and $q = p^k$. Let $n = (2m+1)k$ and s, $1 \le s \le 2m$, be an integer such that $gcd(s, 2m+1) = 1$. Let $b_0 = 1$,$b_i = b_{2m+1-i}$ and $b_{is} = (-1)^i$ for $i = 1, 2, ..., m$, 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 $i = 1, 2, ..., m$. Define

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

The Walsh transform of $f(x)$ has values in the set $\left\{0, \pm p^{\frac{n+k}{2}}\right\}$. The distribution of $\hat{f}(\lambda)$ when λ runs through $\mathbb{F}_{p^n}$ is

$$\begin{array}{cccc} 0 & \text{occurs} & p^n - p^{n-k} & \text{times} \\ -p^{(n+k)/2} & \text{occurs} & (p^{n-k} - p^{(n-k)/2})/2 & \text{times} \\ p^{(n+k)/2} & \text{occurs} & (p^{n-k} + p^{(n-k)/2})/2 & \text{times} \end{array}$$

TABLE I
EXPERIMENTAL DATA

Finite Field	s	d
$\mathbb{F}_{3^5}$	1	$1, 49, 61$
	2	$7, 23, 35, 49$
$\mathbb{F}_{3^7}$	1	$1, 391$
	2	$61, 169$
	3	$1, 439$
$\mathbb{F}_{3^9}$	1	$1, 3361$
	2	$547, 1667$
	4	$1, 3937$
$\mathbb{F}_{3^{11}}$	1	$1, 29767$
	2	$4921, 14641$
	3	$1, 34571$
	4	$1, 35431$
	5	$1, 31639$
$\mathbb{F}_{3^{13}}$	1	$1, 266449$
	2	$44287, 133103$
	3	$1, 307105$
	4	$1, 318865$
	5	$1, 311105$
	6	$1, 284701$
$\mathbb{F}_{3^{15}}$	1	$1, 2393671$
	2	$398581, 1194649$
	4	$1, 2869783$
	7	$1, 2449831$

Theorem 6: ([2]): Let p be an odd prime number, and $q = p^k$. Let $n = (2m+1)k$ and s, $1 \le s \le 2m$, be an integer such that $gcd(s, 2m+1) = 1$. Let $b_0 = 1$,$b_i = b_{2m+1-i}$ and $b_{is} = (-1)^i$ for $i = 1, 2, ..., m$, 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 $i = 1, 2, ..., m$. Define

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

Let $1 < d < q^{2m+1} - 1$ be an integer satisfying

$$(q^{(m+1)s}+1)d \equiv 2q^h (\operatorname{mod} q^{2m+1s}-1) \text{ for } 0 \le h < 2m+1.$$

The Walsh transform of $g(x) = f(x^d)$ has values in the set $\left\{0, \pm p^{\frac{n+k}{2}}\right\}$. The distribution of $\hat{g}(\lambda)$ when λ runs through $\mathbb{F}_{p^n}$ is

$$\begin{array}{cccc} 0 & \text{occurs} & p^n - p^{n-k} & \text{times} \\ -p^{(n+k)/2} & \text{occurs} & (p^{n-k} - p^{(n-k)/2})/2 & \text{times} \\ p^{(n+k)/2} & \text{occurs} & (p^{n-k} + p^{(n-k)/2})/2 & \text{times} \end{array}$$

From Theorem 2 and Theorem 3, we see that the following decimation numbers and the corresponding correlation values remain open. For this reason, in the next section, we try to prove some of cases in Table 2.

TABLE II
EXPERIMENTAL DATA (DECIMATIONS NUMBERS WHICH HAVE NOT BEEN PROVED YET)

Finite Field	s	d
$\mathbb{F}_{3^5}$	2	$7, 23, 35, 49$
$\mathbb{F}_{3^7}$	2	$61, 169$
$\mathbb{F}_{3^9}$	2	$547, 1667$
$\mathbb{F}_{3^{11}}$	2	$4921, 14641$
$\mathbb{F}_{3^{13}}$	2	$44287, 133103$
$\mathbb{F}_{3^{15}}$	2	$398581, 1194649$

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 concantrated 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 tarnsform of

$$h(x) = Tr_n\left(\sum_{i=0}^{2} u_i x^{\frac{5^{2i}+1}{2}481}\right)$$

defined by

$$\hat{h}(\lambda) = \sum_{x\in\mathbb{F}_{p^n}} w^{h(x)+Tr_n(\lambda x)}$$

has values in the set $\left\{0, \pm 5^3\right\}$. The distribution of $\hat{h}(\lambda)$ when λ 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 $\mathbb{F}_{5^5}$ to $\mathbb{F}_5$ by

$$F(x) = Tr_5(f(x^{481}) + \lambda x) = Tr_5\left(\sum_{i=0}^{2} u_i x^{\frac{5^{2i}+1}{2}481} + \lambda x\right)$$

and observe that

$$h(x) + Tr_5(\lambda x) = Tr_5(f(x^{481}) + \lambda x) = F(x).$$

It follows that $F(rx) = rF(x)$ for any $r \in \mathbb{F}_5$, since

$$\frac{5^{2i}+1}{2} \cdot 481 = 1 \cdot 1 = 1 \text{ mod } 4$$

Furthermore,

$$\begin{aligned} F(x) &= Tr_5(u_0 x^{481} + u_1 x^{13\cdot 481} + u_2 x^{313\cdot 481} + \lambda x) \\ &= Tr_5(u_0 x^{481} + u_1 x^5 + u_2 x^{601} + \lambda x). \end{aligned}$$

Now taking the $5^4 + 5 = 630$ th power of x, we obtained that

$$\begin{aligned} F(x^{630}) &= Tr_5(u_0 x^2 + u_1 x^{26} + u_2 x^{626} + \lambda x^{630}) \\ &= Tr_5(u_0 x^{5^0+1} + u_1 x^{5^2+1} + u_2 x^{5^4+1} + \lambda x^{5^4+5}). \end{aligned}$$

Here we see that $F(x^{630})$ is a quadratic form over $\mathbb{F}_5$. Now using the same technique in Lemma 1 and Lemma2 of [1], we complete the proof. Note that 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 $d = \frac{p^{n-2}+1}{p+1}$.The Walsh transform of

$$h(x) = Tr_n\left(\sum_{i=0}^{m} u_i x^{\frac{p^{2i}+1}{2}d}\right)$$

defined by

$$\hat{h}(\lambda) = \sum_{x\in\mathbb{F}_{p^n}} w^{h(x)+Tr_n(\lambda x)}$$

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

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

We have tried to prove this conjecture using similar technique 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 can not 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 decimations 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

```
""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)*I;
  return value;
def u(i):
    if i==0:
        return coerce(int, (p+1)/2);
    return (-1)^i;
d_degerleri = [];
```

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

print "\n tum degerler...\n";
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 ULAKBİM, High Performance and Grid Computing Center (TRUBA Resources).

REFERENCES

[1] G. Gong, T. Helleseth and H. Hu, ”A three-valued Walsh transform from decimations of Helleseth-Gong sequences,” IEEE Trans. Inf. Theory, vol. 58, no. 2,pp. 1158-1162, Feb. 2012.

[2] G. Gong, T. Helleseth, H. Hu and C. Li, ”New three valued walsh transforms from decimations of Helleseth-Gong sequences,” Proceeding of International Conference on Sequences and Their Applications SETA 2012, LNCS 7280, pp. 327-337, Sep. 2012.

[3] T. Helleseth and G. Gong, ”New nonbinary sequences with ideal two-level autocorrelation,” IEEE Trans. Inf. Theory, vol. 48, no. 11, pp. 2868-2872, Nov. 2002.

[4] H. M. Trachtenberg, ”On the cross-correlation functions of maximal linear sequences, ” Ph.D. thesis, Univ. Southern California, Los Angeles, CA, 1970.

[5] T. Helleseth, ”Some results about the cross-correlation function between two maximal linear sequences,” Discr. Math., vol.48, no. 11, pp. 209-232, Nov. 1976.

[6] R. Lidl and H. Niederreiter, Finite Fields. Cambridge University Press, Cambridge, 2nd edition, 1997.