Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 13, Number 7 (2017), pp. 3497-3503

http://www.ripublication.com/gjpam.htm

Analysis of some ternary functions in terms of their Walsh-Hadamard transform

Deep Singh[1] **and Amit Paul**
Department of Mathematics,
Central University of Jammu, Samba, India.

Abstract

In this paper, we use the Walsh Hadamard transform (WHT) as a fundamental tool for analysis of some properties of generalized ternary functions. Some existing binary results obtained for cryptographic functions are generalized to the ternary case, and hence obtain some new characterization of ternary functions based on their spectral analysis. The WHT of ternary functions is expressed in terms of their decomposition functions. Further, the cross-correlation ternary functions is analyzed in terms of their WHT.

AMS subject classification:
Keywords: Boolean functions, Derivative, Ternary functions, Walsh-Hadamard transform (WHT), Cross-correlation.

1. Introduction

In the recent years, the Walsh-Hadamard transform (WHT) has been widely used in the cryptographic research, specially in the design and characterization of cryptographically significant functions. Several authors have made contributions toward the analysis of properties of these functions. Xiao and Massey [15] have studied correlation immune functions with the help of their WHT and analyze several properties of their WHT. Sarkar and Maitra [7] have generalized these results to study m correlation immune functions. The authors in [8, 14] have presented several important results for cryptographic functions by using WHT. It has been observed that almost every cryptogrphic analysis can be performed with the help of WHT of the functions.

[1]Corresponding author.

A Boolean function is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Several authors have proposed several generalization of Boolean functions. The ring of integers modulo m is $\mathbb{Z}_m$. The additive group $\mathbb{Z}_m$ is isomorphic to $\mathbb{U}_m = \{1, \xi, \ldots, \xi^{m-1}\}$, the multiplicative group of complex m^{th} roots of unity. Kumar et al. [5] have generalized the Boolean bent functions by considering functions from $\mathbb{Z}_m^n$ to $\mathbb{Z}_m$, where $m \geq 2$ and n are positive integers.

Suppose $\mathcal{T}_{n,3}$ is the set of all ternary functions. The Walsh-Hadamard transform of $f \in \mathcal{T}_{n,3}$ is defined as follows

$$\mathcal{W}_g(u) = \sum_{x \in \mathbb{Z}_3^n} \xi^{g(x)+<x,u>},$$

where $< x,\ u >= x_1u_1 + x_2u_2 + \cdots + x_nu_n$ in $\mathbb{Z}_3^n$.

A function $g \in \mathcal{T}_{n,3}$ is *ternary bent* if $|\mathcal{W}_g(u)| = 1$ for every $u \in \mathbb{Z}_3^n$. The Boolean *bent* functions were introduced by Rothaus [6]. According to Rothaus [6], bent functions can be constructed only for even number of variables. For more results on ternary (generalized) bent functions we refer to [1, 2, 3, 4, 12]. The authors in [10] have studied number of properties of such functions. They have introduced some new indicators to investigate the cross-correlation properties of these generalized functions. Ternary bent functions are widely applicable in many CDMA communications systems as well as in several other wireless communications channels[9].

The *derivative* of $g, h \in \mathcal{T}_{n,3}$ at $c \in \mathbb{Z}_3^n$ is defined as $D_{g,h}(c) = g(x) - h(x + c)$, and for $g = h$, $D_g(c) = g(x) - g(x + c)$ is called derivative of g at $c \in \mathbb{Z}_3^n$.

Let $g, h \in \mathcal{T}_{n,3}$. Then the sum

$$\mathcal{C}_{g,h}(a) = \sum_{x \in \mathbb{Z}_3^n} \xi^{g(x)-h(x+a)},$$

is the cross-correlation between g and h for $a \in \mathbb{Z}_3^n$. Moreover, for $g = h$, the sum $\mathcal{C}_{g,g}(a) = \mathcal{C}_g(a)$ is called the autocorrelation of g at a.

In this paper, we have analyzed some properties of ternary functions with the help of Walsh-Hadamard transform. Some existing binary results obtained for cryptographic functions are generalized to the ternary case, and hence obtain some new characterization of ternary functions based on their spectral analysis. The WHT of ternary functions is expressed in terms of the WHT of their decomposition functions. Further, the cross-correlation ternary functions is obtained in terms of their WHT.

The following Lemma 1.1 is an important property and extensively used in the paper.

Lemma 1.1. [10, Lemma 2.1] Let $a \in \mathbb{Z}_3^n$. Then

$$\sum_{\mathbf{x} \in \mathbb{Z}_3^n} \xi^{<a,\ \mathbf{x}>} = \begin{cases} 3^n, & \text{if } a = 0, \\ 0, & \text{otherwise .} \end{cases}$$

2. Main Results

In Theorem 2.1 and Theorem 2.3 below we generalize the results of Zhou et al. [14] to the ternary functions.

Theorem 2.1. Let $g, h \in \mathcal{T}_{n,3}$, and L be a subspace of $\mathbb{Z}_3^n$ with $\dim(L) = k$. Then for any $b \in \mathbb{Z}_3^n$, we have

$$\sum_{a\in L} \mathcal{W}_g(a+b)\overline{\mathcal{W}_h(a)} = 3^k \sum_{e\in L^\perp} \mathcal{W}_{D_{g,h}(e)}(b),$$

where $L^\perp$ is the dual of a subspace V, i.e., $L^\perp = \{u \in \mathbb{Z}_3^n : \forall v \in L, u \cdot v = 0\}$.

Proof. By using Walsh-Hadamard transform, we obtain

$$\begin{aligned}
\sum_{a\in L} \mathcal{W}_g(a)\overline{\mathcal{W}_g(a+b)} &= \sum_{a\in L} \left(\frac{1}{3^{n/2}} \sum_{u\in\mathbb{Z}_3^n} \xi^{g(u)+<a,u>} \right) \overline{\left(\frac{1}{3^{n/2}} \sum_{v\in\mathbb{Z}_3^n} \xi^{h(v)+<a+b,v>} \right)} \\
&= \frac{1}{3^n} \sum_{a\in L} \sum_{u,v\in\mathbb{Z}_3^n} \xi^{g(u)+<a,u>-h(v)-<a+b,v>} \\
&= \frac{1}{3^n} \sum_{u,v\in\mathbb{Z}_3^n} \xi^{g(u)-h(v)-<b,v>} \sum_{a\in L} \xi^{<a,u-v>},
\end{aligned}$$

where $\sum_{a\in L} \xi^{<a,u-v>} \neq 0$ if and only if $u - v \in L^\perp$. Therefore, we have

$$\begin{aligned}
\frac{1}{3^n} \sum_{u,v\in\mathbb{Z}_3^n} \xi^{g(u)-h(v)-<b,v>} \sum_{a\in L} \xi^{<a,u-v>} &= 3^{k-n} \sum_{u,v\in\mathbb{Z}_3^n, u-v\in L^\perp} \xi^{g(u)-h(v)-<b,v>} \\
&= 3^{k-n} \sum_{u\in\mathbb{Z}_3^n} \sum_{e\in L^\perp, v=u-e} \xi^{g(u)-h(u-e)-<b,u-e>} \\
&= 3^{k-n} \sum_{e\in L^\perp} \xi^{<b,e>} \sum_{u\in\mathbb{Z}_3^n} \xi^{g(u)-h(u-e)-<b,u>} \\
&= 3^{k-n} \sum_{e\in L^\perp} \xi^{<b,e>} \overline{\sum_{u\in\mathbb{Z}_3^n} \xi^{-g(u)+h(u-e)+<b,u>}} \\
&= 3^{k-n} \sum_{e\in L^\perp} \xi^{<b,e>} \overline{\sum_{w\in\mathbb{Z}_3^n} \xi^{h(w)-g(w+e)+<b,w+e>}} \\
&= 3^{k-n} \sum_{e\in L^\perp} 3^{n/2} \overline{\mathcal{W}_{D_{h,g}(e)}(b)} \\
&= a^{\frac{2k-n}{2}} \sum_{e\in L^\perp} \overline{\mathcal{W}_{D_{h,g}(e)}(b)}.
\end{aligned}$$

■

The following result holds for the case $g = h$.

Corollary 2.2. Let $g, h \in \mathcal{T}_{n,3}$ and V be the subspace of $\mathbb{Z}_3^n$ with $\dim(L) = k$. Then

$$\sum_{a\in L} |\mathcal{W}_g(a+b)|^2 = 3^k \sum_{e\in L^\perp} \xi^{<b,e>} \overline{\mathcal{W}_{D_g(e)}(0)}, \ \forall\, b \in \mathbb{Z}_3^n.$$

Let M be a subspace of $\mathbb{Z}_3^n$ with $\dim(M) = k$. The constituent functions of g in M is the sequence $\{g_c : a \in L\}$, where L is a subspace such that $\mathbb{Z}_3^n$ is the direct sum of M and L, and g_a is the function of k variables from M to $\mathbb{Z}_3$, defined as $g_c(u) = g(c+u)$ for any $u \in M$. The following result investigate WHT of $g, h \in \mathcal{T}_{n,3}$ and the WHT of the constituent functions of g and h with respect to a subspace L of $\mathbb{Z}_3^n$.

Theorem 2.3. Suppose M is a subspace of $\mathbb{Z}_3^n$ with $\dim(M) = k$, and $\{g_c : c \in L\}$ and $\{h_c : c \in L\}$ are decomposition functions of g and h with respect to M. Then

$$\sum_{a\in M^\perp} \mathcal{W}_g(a)\overline{\mathcal{W}_h(a)} = 3^k \sum_{c\in L} \mathcal{W}_{g_c}(0)\overline{\mathcal{W}_{h_c}(0)}$$

Proof. For any $e \in \mathbb{Z}_3^n$, we have

$$\begin{aligned}
\mathcal{C}_{g,h}(e) &= \sum_{w\in\mathbb{Z}_3^n} \xi^{g(w)-h(w+e)} \\
&= \sum_{c\in L}\sum_{u\in M} \xi^{g_c(u)-h_c(u+e)} \\
&= \sum_{c\in L}\sum_{u\in M} \xi^{g(c+u)-h(c+u+e)}
\end{aligned}$$

From Theorem 2.1, for $b = 0$, we have

$$\begin{aligned}
\sum_{a\in M^\perp} \mathcal{W}_g(a)\overline{\mathcal{W}_h(a)} &= 3^k \sum_{e\in M} \mathcal{C}_{g,h}(e) = 3^k \sum_{e\in M} \left(\sum_{w\in\mathbb{Z}_3^n} \xi^{g(w)-h(w+e)} \right) \\
&= 3^k \sum_{e\in M} \left(\sum_{c\in L}\sum_{u\in M} \xi^{g(c+u)-h(c+u+e)} \right) \\
&= 3^k \sum_{c\in L}\sum_{u\in M} \xi^{g(c+u)} \sum_{e\in M} \xi^{-h(c+u+e)} \\
&= 3^k \sum_{c\in L}\sum_{u\in M} \xi^{g(c+u)} \sum_{v\in M} \xi^{-h(c+v)} \\
&= 3^k \sum_{c\in L} \mathcal{W}_{g_c}(0)\overline{\mathcal{W}_{h_c}(0)}.
\end{aligned}$$

■

The following result holds for the case $g = h$.

Corollary 2.4. Let M be a subspace of $\mathbb{Z}_3^n$ of dimension k and suppose $(g_c : c \in L)$ be the decomposition function of g with respect to M. Then

$$\sum_{a \in M^{\perp}} |\mathcal{W}_g(a)|^2 = 3^{\frac{2k-n}{2}} \sum_{\mathbf{a} \in L} |\mathcal{W}_{g_c}(0)|^2.$$

For any $a \in \mathbb{Z}_3^n$, we have

$$| W_g(a) |^2 = \sum_{a \in \mathbb{Z}_3^n} \xi^{<c,a>} \overline{C_g(c)} = \sum_{c \in \mathbb{Z}_3^n} \xi^{<-c,a>} C_g(c).$$

In particular, if $a = 0$ then

$$| W_g(0) |^2 = \sum_{c \in \mathbb{Z}_3^n} C_g(c).$$

Theorem 2.5. Let $g, h, k \in \mathcal{T}_{n,3}$ be such that $k(u) = g(u) - h(u)$. Then

$$\mathcal{W}_k(b) = \frac{1}{3^{n/2}} \sum_{a \in \mathbb{Z}_3^n} \mathcal{W}_g(a+b)\overline{\mathcal{W}_h(a)}, \ \forall\, b \in \mathbb{Z}_3^n.$$

Proof. For any $b \in \mathbb{Z}_3^n$, using Lemma 1.1, we have

$$\begin{aligned}
\sum_{a \in \mathbb{Z}_3^n} \mathcal{W}_g(a+b)\overline{\mathcal{W}_h(a)} &= \frac{1}{3^n} \sum_{a \in \mathbb{Z}_3^n} \sum_{u \in \mathbb{Z}_3^n} \xi^{g(u)+\langle a+b,u \rangle} \sum_{\mathbf{y} \in \mathbb{Z}_3^n} \xi^{-h(b)-\langle a,b \rangle} \\
&= \frac{1}{3^n} \sum_{u,v \in \mathbb{Z}_3^n} \xi^{g(u)-h(b)+\langle b,u \rangle} \sum_{a \in \mathbb{Z}_3^n} \xi^{\langle a,u-v \rangle} \\
&= 3^n \sum_{u \in \mathbb{Z}_3^n} \xi^{g(u)-h(u)+\langle b,u \rangle} \\
&= 3^n \sum_{u \in \mathbb{Z}_3^n} \xi^{k(u)+\langle b,u \rangle} \\
&= 3^{n/2} \mathcal{W}_k(b).
\end{aligned}$$

Hence the result. ∎

3. Conclusion

In this article, ternary functions are analysed with the help of their WHT. It is established fact that cryptographic functions and their properties are closely dependent to the nature

of their WHT. The ternary functions are not much studied as compare to the Boolean functions. This article presents an effort in this direction. The article contains generalization of some results from binary case and investigated based on their spectral analysis. The WHT of ternary functions is expressed in terms of their decomposition functions. The cross-correlation ternary functions is analyzed in terms of their WHT.

Acknowledgement

The second author thanks to UGC, India for providing financial support through "Rajiv Gandhi National Fellowship".

References

[1] Carlet, C., and Dubuc, C., 2001 "On generalized bent and q-ary perfect nonlinear functions", Finite Fields and Applications 1999, pp. 81–94.

[2] Hou, X., 1998, "q-ary bent functions constructed from chain rings", Finite Fields and Applications 4, pp. 55–61.

[3] Hou, X. D., 2000, "Bent functions, partial difference sets and quasi-Frobenius rings", Designs, Codes and Cryptography 20, pp. 251–268.

[4] Hou, X., 2004, "p-ary and q-ary versions of certain results about bent functions and resilient functions", Finite Fields and Applications 10, pp. 566–582.

[5] Kumar,P.V., Scholtz, R.A., and Welch, L.R., 1985 "Generalized bent functions and their properties", Journal of Combinatirial Theory, Ser. A 1(40), pp. 90–107.

[6] Rothaus, O.S., 1976, "On Bent functions" Journal of Combinatorial Theory 20, pp. 300–305.

[7] Sarkar, P., and Maitra, S., 2000, Constructions of nonlinear Boolean functions with important cryptographic properties. In Advances in Cryptology-Eurocrypt 2000, LNCS 1807, pages 485–506.

[8] Sarkar, P., and Maitra, S., "Cross-correlation analysis of cryptographically useful Boolean functions", Theory of Computing Systems 35 (2002), pp. 39–57.

[9] Schmidt, K., U., 2009, Quaternary constant-amplitude codes for multicode CDMA. IEEE Transactions on Information Theory 55(4), pp. 1824–1832.

[10] Singh, D., Bhaintwal M., and Singh, B. K., 2013, "Some results on q-ary bent functions, International Journal of Computer Mathematics", 90(9), pp. 1761–1773.

[11] Solé, P., Tokareva, N., Connections between quaternary and binary bent functions. Cryptology ePrint Archives (2009), http://www.eprint.iacr.org/2009/544.

[12] Tokareva N., Generalizations of bent functions: A survey. Cryptology ePrint Archives (2009), http://eprint.iacr.org/2011/111.pdf

[13] Zhuo, Z., Chong, J., Cao, H., and Xiao, G., 2011, Spectral analysis of two Boolean functions and their derivatives, Chinese Journal of Electronics 20(4), pp. 747–749.

[14] Zhou, Y., Xie, M., and Xiao, G., 2010, On the global avalanche characteristics between two Boolean functions and the higher order nonlinearity, Information Sciences 180, pp. 256–265.

[15] Xiao, G. Z., and Messey, J. L., 1988, "A Spectral Characterization of Correlation-Immune Combing Functions", IEEE Transactions on Information Theory, 34(3): 569–571.