Finite Fields and Their Applications 50 (2018) 66–83

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Explicit evaluation of Walsh transforms of a class of Gold type functions ☆

Ayhan Coşgun

Department of Mathematics, Middle East Technical University, Dumlupınar Bul., No:1, 06800, Ankara, Turkey

ARTICLE INFO

Article history:
Received 22 April 2017
Received in revised form 22 September 2017
Accepted 10 November 2017
Available online xxxx
Communicated by Gary McGuire

MSC:
06E30
11D09
11T24
12E20

Keywords:
Finite fields
Quadratic forms
Gold type functions
Walsh transform

ABSTRACT

Let $K = \mathbb{F}_{2^k}$ denote the finite field of 2^k elements. The Walsh transform of a class of Gold type functions $f(x) = \mathrm{Tr}_K\left(x^{2^a+1} + x^{2^b+1}\right)$, $0 \le a < b$ at $\alpha \in K$ is determined in recent results of Lahtonen et al. (2007) [7], Roy (2012) [10] and Coşgun et al. (2016) [2] under some restrictions on k, a, b and α. In this paper, we give explicit evaluation of the Walsh transforms of f without any restriction on k, a, b and α. Therefore we improve and generalize the related results in literature. Furthermore, we evaluate the Walsh transform of a more general Gold type function $f_\gamma(x) = \mathrm{Tr}_K\left(\gamma x^{2^a+1} + \gamma x^{2^b+1}\right)$, $0 \le a < b$ at $\alpha \in K$ for any $\gamma \in \mathbb{F}_{2^k} \cap \mathbb{F}_{2^{b-a}}$ without any restriction on k, a, b and α.

☆ This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

E-mail address: ayhan.cosg@gmail.com.

https://doi.org/10.1016/j.ffa.2017.11.005
1071-5797/

1. Introduction

Let f be a Boolean function $f : V_k \longrightarrow \mathbb{F}_2$, where V_k is a k-dimensional vector space over $\mathbb{F}_2$. The *Walsh transform* (or *Walsh–Hadamard transform*) of f at α is the function $f^W : V_k \longrightarrow \mathbb{Z}$ defined by

$$f^W(\alpha) = \sum_{x \in V_k} (-1)^{f(x)+\langle \alpha, x \rangle} \tag{1}$$

where $\langle \alpha, x \rangle$ denotes an (non-degenerate) inner product on V_k. We refer, for example, to [1] for more details on Walsh transform for Boolean functions.

Let $V_k = K$ where $K = \mathbb{F}_{2^k}$ denotes the finite field of 2^k elements and let Tr_K denote the absolute trace map from K to $\mathbb{F}_2$. Then a natural choice for $\langle \alpha, x \rangle$ is $\mathrm{Tr}_K(\alpha x)$ and equation (1) becomes

$$f^W(\alpha) = \sum_{x \in K} (-1)^{f(x)+\mathrm{Tr}_K(\alpha x)}. \tag{2}$$

The *Walsh spectrum* of a Boolean function $f : K \longrightarrow \mathbb{F}_2$ is defined to be the set

$$\left\{ f^W(\alpha) : \alpha \in K \right\}.$$

When the spectrum is precisely $\left\{ \pm 2^{\frac{k}{2}} \right\}$, f is called *bent function*. For an integer $0 \le r \le k$, a function $f : K \longrightarrow \mathbb{F}_2$ is called *r-plateaued* if its Walsh spectrum is $\left\{ 0, \pm 2^{\frac{1}{2}(k+r)} \right\}$. Bent functions have significance due to their applications in cryptography and r-plateaued functions gain interest as they can be used to construct bent functions (see [7,10] for instance).

Gold functions

$$f(x) = \mathrm{Tr}_K\left(x^{2^a+1} \right), \text{ with } \gcd(a,k) = 1 \text{ and } k \text{ is odd},$$

are introduced in [4] and this family is a famous example of functions having 3-valued Walsh spectrum. Gold [4] determined $f^W(\alpha)$ in terms of $f^W(1)$ and $f^W(1)$ is evaluated first in [3] and then in [7]. Furthermore, more general Gold functions are studied in the appendix of [3]. With the hypothesis that a is relatively prime to k and k is odd, Gold functions have the spectrum $\left\{ 0, \pm 2^{\frac{(k+1)}{2}} \right\}$ (i.e. they are 1-plateaued).

In this paper we deal with the Walsh transforms of Gold type functions. Without loss of generality we assume $0 \le a < b$ ($a = b$ is a trivial case) and by a Gold type function we mean

$$f(x) = \mathrm{Tr}_K\left(x^{2^a+1} + x^{2^b+1} \right).$$

Gold type functions were studied by various authors in literature. For instance, in [7], Lahtonen, McGuire and Ward give $f^W(0)$ for