Journal of Computational and Applied Mathematics 259 (2014) 522–528

Contents lists available at ScienceDirect

Journal of Computational and Applied Mathematics

journal homepage: www.elsevier.com/locate/cam

Counting Boolean functions with specified values in their Walsh spectrum

Erdener Uyan [a,*], Çağdaş Çalık [a], Ali Doğanaksoy [a,b]

[a] Institute of Applied Mathematics, Middle East Technical University, Turkey

[b] Department of Mathematics, Middle East Technical University, Turkey

ARTICLE INFO

Article history:
Received 15 February 2013
Received in revised form 15 June 2013

Keywords:
Boolean functions
Walsh spectrum
Counting

ABSTRACT

The problem of counting Boolean functions with specified number s of Walsh coefficients ω in their Walsh spectrum is discussed in this paper. Strategies to solve this problem shall help solving many more problems related to desired cryptographic features of Boolean functions such as nonlinearity, resiliency, algebraic immunity, etc. In an attempt to study this problem, we present a new framework of solutions. We give results for $|\omega| \geq 2^{n-1}$ and for all s, in line with a previous work of Wu (1998) [12]. We also provide various results such as existence and construction for some s when $\omega = 0$, multiplicities for all ω and naive bounds on s for $\omega > 2^{n/2}$.

1. Introduction

The theory of Boolean functions is a wide area of research in cryptography, coding theory and combinatorics. There are various open problems regarding the construction and enumeration of Boolean functions possessing certain cryptographic features (cf. [1]). Most of the enumeration problems are still unsolved today. The foremost reason is that they require huge amount of computational resources, exceeding the capability of today's computers when the number of input variables (n) gets higher. This study is mainly devoted to determining the existence and enumeration of functions having an arbitrary value appearing a certain number of times in their Walsh spectrum.

Exploring new properties of Walsh spectrum can be employed to solve problems of constructing, verifying and enumerating Boolean functions having properties such as correlation immunity and resiliency, as studied in [2,3], or algebraic immunity as studied in [4]. It can also help to obtain new higher bounds on perfectly balanced Boolean functions as shown in [5]. All mentioned works promote and emphasize the importance of finding relations among the Walsh coefficients of Boolean functions.

The paper is organized as follows. We first provide a background in Section 2, and explain the problem of interest and the proposed framework for the solution in Section 3. Section 4 contains the previous results in the literature related to the problem as well as the results obtained in this study. Conclusion is given in Section 5.

2. Preliminaries

A Boolean function is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. There are 2^n possible inputs of length n; hence the set of n-variable Boolean functions, denoted by $\mathcal{B}_n$, has cardinality 2^{2^n}. The main tool to study the nonlinearity of Boolean functions is the

* Corresponding author. Tel.: +90 3122103148.
E-mail address: uerdener@metu.edu.tr (E. Uyan).

0377-0427/$ – see front matter
http://dx.doi.org/10.1016/j.cam.2013.06.035

Walsh–Hadamard transform, which is defined for an n-variable Boolean function f as

$$W_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus a \cdot x}, \quad a \in \mathbb{F}_2^n. \tag{1}$$

The vectors $[f(a_0), f(a_1), \ldots, f(a_{2^n-1})]$ and $[W_f(a_0), W_f(a_1), \ldots, W_f(a_{2^n-1})]$ are called the *truth table* (*TT*) and the *Walsh spectrum* (*WS*) of a Boolean function f, respectively. The transformation between these vectors can be done with the *Fast Walsh transform* (FWT) with $\mathcal{O}(n2^n)$ complexity [6].

Each component $W_f(a)$ of *WS* is called a *Walsh coefficient*. Its magnitude indicates the correlation between f and the corresponding linear function $a \cdot x = a_1x_1 + a_2x_2 + \cdots + a_nx_n$ for $a, x \in \mathbb{F}_2^n$. The nonlinearity of f is computed from the Walsh spectrum by

$$\mathcal{N}_f = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \left| W_f(a) \right|. \tag{2}$$

The *support* of f is the set $\Omega_f = \{a \in \mathbb{F}_2^n | f(a) = 1\}$ and the *weight* of f, $wt(f)$, is the cardinality of the support, i.e. $wt(f) = |\Omega_f|$.

3. Problem

The starting point of this study is stated as problem C3 in [1]. It asks whether there exists a Boolean function whose Walsh spectrum contains a specified number of zeros, technically termed as follows.

Problem 3.1 (*C3 [1]*)**.** Given an integer s, is there a function $f \in \mathcal{B}_n$ such that $\#\{a \in \mathbb{F}_n^2 \mid W_f(a) = 0\} = s$?

This problem can be generalized by introducing a variable ω denoting a Walsh coefficient value and transforming the decision problem to a counting problem by asking the number of n-variable Boolean functions, whose Walsh spectrum contains a specified number s of a specified Walsh coefficient ω, exist in $\mathcal{B}_n$.

Problem 3.2. Given integers s and ω, how many functions f exist in $\mathcal{B}_n$ such that $\#\{a \in \mathbb{F}_2^n | \, |W_f(a)| = \omega\} = s$?

It should be noted that ω is the absolute value of a Walsh coefficient. This assumption has been made because the nonlinearity of a Boolean function is directly related to the magnitude of the coefficients in its Walsh spectrum. Thus, the sign of $W_f(a)$ is omitted, and Walsh coefficients are considered with their absolute values throughout the rest of the paper.

Problem 3.2 is important in the sense that it contains the distribution problem of the nonlinearities, or equivalently the weight distribution of first-order Reed–Muller codes. It is also related to the open problem of determining the number of bent functions in general and provides the classification and enumeration of Boolean functions in $\mathcal{B}_n$ with respect to their Walsh spectrum values. In order to follow a systematic approach, we first form a precise mathematical framework.

3.1. Proposed framework

The variables involved in solution instances of Problem 3.2 are n,s and ω. Hence, the solutions are parametrized with respect to the 3-tuple (n,s,ω).

Definition 3.3. Let n,s and ω be nonnegative integers with $n \geq 1$ and $\omega, s \leq 2^n$. We denote the set of Boolean functions such that $\#\{a \in \mathbb{F}_2^n | \, |W_f(a)| = \omega\} = s$ with $\mathcal{S}(n, s, \omega)$.

Definition 3.4. A *function distribution table* of $\mathcal{B}_n$ (FDT_n) is a table whose entry at sth row and ωth column denotes the number of n-variable Boolean functions having Walsh coefficient ω appearing exactly s times in their Walsh spectrum.

The column headers of an FDT are the Walsh coefficients $|W_f(a)|$ considered as absolute values, whereas rows correspond to the number s of times a Walsh coefficient ω is observed in the Walsh spectrum of a function $f \in \mathcal{B}_n$. The template for FDT_n is given in Table 1.

Example 3.5. $\mathcal{S}(n, 2^n - 1, 0) = \mathcal{S}(n, 1, 2^n) = \mathcal{A}_n$ is the set of affine functions in $\mathcal{B}_n$. So $\Upsilon = |\mathcal{A}_n| = 2^{n+1}$ in Table 1.

Example 3.6. $\mathcal{S}(n, 2^n, 2^{n/2})$ is defined for even values of n and corresponds to the set of bent functions in $\mathcal{B}_n$. The cardinality ψ of this set is known only up to $n = 8$ [7,8].

Remark 3.7. A function $f \in \mathcal{B}_n$ is counted in exactly one entry of each column of FDT_n. Thus, the sum of each column corresponds to $|\mathcal{B}_n| = 2^{2^n}$.

Remark 3.8. Let FDT_n^+ be FDT_n without the row $s = 0$. Then, a function $f \in \mathcal{B}_n$ is counted in r different entries of FDT_n^+, where r is the number of distinct Walsh coefficients (up to absolute values) in its spectrum.