Contents lists available at ScienceDirect

Discrete Applied Mathematics

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

# Modular periodicity of exponential sums of symmetric Boolean functions

Francis N. Castro, Luis A. Medina [*]

*Department of Mathematics, University of Puerto Rico, San Juan, PR 00931, Puerto Rico*

A R T I C L E I N F O

*Article history:*
Received 1 March 2016
Accepted 7 October 2016
Available online xxxx

*Keywords:*
Symmetric Boolean functions
Exponential sums
Recurrences
Pisano periods

A B S T R A C T

This work brings techniques from the theory of recurrent integer sequences to the problem of balancedness of symmetric Boolean functions. In particular, the periodicity modulo $p$ ($p$ odd prime) of exponential sums of symmetric Boolean functions is considered. Periods modulo $p$, bounds for periods and relations between them are obtained for these exponential sums. The concept of avoiding primes is also introduced. This concept and the bounds presented in this work are used to show that some classes of symmetric Boolean functions are not balanced. In particular, every elementary symmetric Boolean function of degree not a power of 2 and less than 2048 is not balanced. For instance, the elementary symmetric Boolean function in $n$ variables of degree 1292 is not balanced because the prime $p = 176129$ does not divide its exponential sum for any positive integer $n$. It is showed that for some symmetric Boolean functions, the set of primes avoided by the sequence of exponential sums contains a subset that has positive density within the set of primes. Finally, in the last section, a brief study for the set of primes that divide some term of the sequence of exponential sums is presented.

## 1. Introduction

Boolean functions are beautiful combinatorial objects with applications to many areas of mathematics as well as outside the field. Some examples include combinatorics, electrical engineering, game theory, the theory of error-correcting codes, and cryptography. In the modern era, efficient implementation of Boolean functions with many variables is a challenging problem due to memory restrictions of current technology. Because of this, symmetric Boolean functions are good candidates for efficient implementations.

In many applications, especially ones related to cryptography, it is important for Boolean functions to be balanced. Every symmetric function is a combination of elementary symmetric polynomials, thus an important step should be to understand the balancedness of them. In [10], Cusick, Li and Stănică proposed a conjecture that explicitly states when an elementary symmetric function is balanced:

*There are no nonlinear balanced elementary symmetric Boolean functions except for degree* $k = 2^l$ *and* $2^{l+1}D - 1$*-variables, where* $l, D$ *are positive integers.* Surprisingly, this conjecture is still open, but some advances have been made. For some history of the problem, as well as its current state, the reader is invited to read [5–7,10,11,13,14,26].

The subject of Boolean functions can be studied from the point of view of complexity theory or from the algebraic point of view as it is done in this article, where the periodicity of exponential sums of symmetric Boolean functions modulo a prime is exploited. The study of divisibility properties of Boolean functions is not new. In fact, it is an active area of research

[*] Corresponding author.
*E-mail addresses:* franciscastr@gmail.com (F.N. Castro), luis.medina17@upr.edu (L.A. Medina).

http://dx.doi.org/10.1016/j.dam.2016.10.005

[1,2,20–23]. However, the authors believe that the modular periodicity of these functions has not been studied in detail nor its possible connections to Cusick–Li–Stănică's conjecture.

In [6], the authors viewed exponential sums of symmetric Boolean functions as integer sequences. As part of their study, they showed that these sequences satisfy homogeneous linear recurrences with integer coefficients. Moreover, in the case of one elementary symmetric function, they were able to provide the minimal homogeneous linear recurrence. It is a well-established result in number theory that recurrent integer sequences are periodic or eventually periodic modulo an integer $m$, with the first serious study being done by Lucas [17]. Some of the results available on this topic are used in this manuscript to find bounds for the periods of these sequences. These bounds and the periodicity of exponential sums of symmetric Boolean functions are used to show that some families are not balanced. For example, every elementary symmetric Boolean function of degree not a power of 2 and less than 2048 is not balanced. In particular, the elementary symmetric Boolean function in $n$ variables of degree 1292 is not balanced because the prime $p = 176129$ does not divide its exponential sum for any positive integer $n$. One of the main goals of this manuscript is to provide some insights about the $p$-divisibility ($p$ prime) of the exponential sum of symmetric Boolean functions.

This work is divided in various parts. It starts with some preliminaries (Section 2) about symmetric Boolean functions. It follows with a review of the periodicity modulo $m$ of linear recurrences (Section 3). This is done because, to the knowledge of the authors, it is not common to find the subjects of Boolean functions and periodicity modulo $m$ of recurrent sequences together in a manuscript. Section 3 also contains Theorem 3.2 (Vince [28]), which is an important tool for finding upper bounds for the periods of the sequences considered in this article. After that, in Section 4, the periodicity modulo $p$ ($p$ an odd prime) of exponential sums of symmetric Boolean functions is studied in more detail. In particular, the reader can find bounds and relations for these periods. In Section 5, the concept of avoiding primes is introduced. This concept and the bounds presented in Section 4 are used to show that some of these families are not balanced. Moreover, it is showed that for some symmetric Boolean functions, the set of primes avoided by the sequence of exponential sums has positive density within the set of primes. Finally, in Section 6, a small study for the set of primes that divide some term of the sequence of exponential sums is presented.

## 2. Preliminaries

Let $\mathbb{F}_2$ be the binary field, $\mathbb{F}_2^n = \{(x_1, \dots, x_n) | x_i \in \mathbb{F}_2, i = 1, \dots, n\}$, and $F(\mathbf{X}) = F(X_1, \dots, X_n)$ be a polynomial in $n$ variables over $\mathbb{F}_2$. The exponential sum associated to $F$ over $\mathbb{F}_2$ is

$$S(F) = \sum_{x_1,\dots,x_n \in \mathbb{F}_2} (-1)^{F(x_1,\dots,x_n)}. \tag{2.1}$$

A Boolean function $F$ is called balanced if $S(F) = 0$, i.e. the number of zeros and the number of ones are equal in the truth table of $F$. This property is important for some applications in cryptography.

Any symmetric Boolean function is a linear combination of elementary symmetric polynomials. Let $\sigma_{n,k}$ be the elementary symmetric polynomial in $n$ variables of degree $k$. For example,

$$\sigma_{4,3} = X_1X_2X_3 + X_1X_4X_3 + X_2X_4X_3 + X_1X_2X_4. \tag{2.2}$$

Then, every symmetric Boolean function can be identified with an expression of the form

$$\sigma_{n,k_1} + \sigma_{n,k_2} + \cdots + \sigma_{n,k_s}, \tag{2.3}$$

where $1 \le k_1 < k_2 < \cdots < k_s$ are integers. For the sake of simplicity, the notation $\sigma_{n,[k_1,\dots,k_s]}$ is used to denote (2.3). For example,

$$\begin{aligned} \sigma_{3,[2,1]} &= \sigma_{3,2} + \sigma_{3,1} \\ &= X_1X_2 + X_3X_2 + X_1X_3 + X_1 + X_2 + X_3. \end{aligned} \tag{2.4}$$

It is not hard to show that if $1 \le k_1 < k_2 < \cdots < k_s$ are fixed integers, then

$$S(\sigma_{n,[k_1,k_2,\dots,k_s]}) = \sum_{j=0}^{n} (-1)^{\binom{j}{k_1}+\binom{j}{k_2}+\cdots+\binom{j}{k_s}} \binom{n}{j}. \tag{2.5}$$

**Remark 2.1.** Observe that the right hand side of (2.5) makes sense for $n \ge 1$, while the left hand side exists for $n \ge k_s$. Throughout the rest of the article, $S(\sigma_{n,[k_1,k_2,\dots,k_s]})$ should be interpreted as the expression on the right hand side, so it makes sense to talk about "exponential sums" of symmetric Boolean functions with less variables than their degrees.

Eq. (2.5) links the problem of balancedness of $\sigma_{n,[k_1,\dots,k_s]}$ to the problem of bisecting binomial coefficients (this was first discussed by Mitchell [19]). A solution $(\delta_0, \delta_1, \dots, \delta_n)$ to the equation

$$\sum_{j=0}^{n} x_j \binom{n}{j} = 0, \quad x_j \in \{-1, 1\}, \tag{2.6}$$