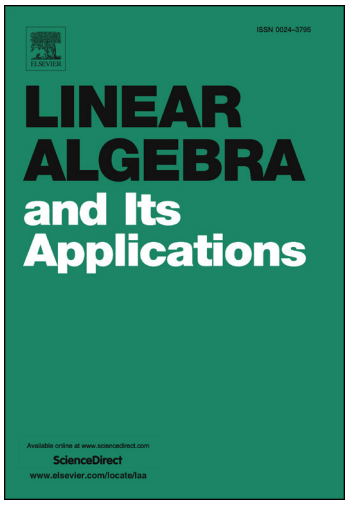
Accepted Manuscript



Hadamard matrices and the spectrum of quadratic symmetric polynomials over finite fields

Francis N. Castro, Luis A. Medina

PII: S0024-3795(18)30123-X
DOI: https://doi.org/10.1016/j.laa.2018.03.013
Reference: LAA 14505

To appear in: *Linear Algebra and its Applications*

Received date: 18 December 2017
Accepted date: 6 March 2018

Please cite this article in press as: F.N. Castro, L.A. Medina, Hadamard matrices and the spectrum of quadratic symmetric polynomials over finite fields, *Linear Algebra Appl.* (2018), https://doi.org/10.1016/j.laa.2018.03.013

HADAMARD MATRICES AND THE SPECTRUM OF QUADRATIC SYMMETRIC POLYNOMIALS OVER FINITE FIELDS

FRANCIS N. CASTRO AND LUIS A. MEDINA

Abstract. In this article, we present a beautiful connection between Hadamard matrices and exponential sums of quadratic symmetric polynomials over Galois fields. This connection appears when the recursive nature of these sequences is analyzed. We calculate the spectrum for the Hadamard matrices that dominate these recurrences. The eigenvalues depend on the Legendre symbol and the quadratic Gauss sum over finite field extensions. In particular, these formulas allow us to calculate closed formulas for the exponential sums over Galois field of quadratic symmetric polynomials. Finally, in the particular case of finite extensions of the binary field, we show that the corresponding Hadamard matrix is a permutation away from a classical construction of these matrices.

1. Introduction

Boolean functions are functions from the vector space $\mathbb{F}_2^n$ to $\mathbb{F}_2$ where $\mathbb{F}_2$ represents the binary field. Applications of these beautiful combinatorial objects to computer science fields such as coding theory, cryptography and information theory have made them a source of active research. Moreover, due to memory restrictions of current technology efficient implementations of these functions is an area of special interest. Efficient implementations, in the most general sense, is a very hard problem. However, some classes like the class of symmetric Boolean functions and the class of rotation symmetric Boolean functions are excellent candidates for efficient implementations. These functions are part of ongoing research.

In some applications related to cryptography it is important for Boolean functions to be balanced. A balanced Boolean function is one for which the number of zeros and the number of ones are equal in its truth table. Let $F(\mathbf{X})$ be a Boolean function. List the elements of $\mathbb{F}_2^n$ in lexicographic order and label them as $\mathbf{x}_0 = (0, 0, \cdots, 0)$, $\mathbf{x}_1 = (0, 0, \cdots, 1)$ and so on. The vector $(F(\mathbf{x}_0), F(\mathbf{x}_1), \cdots, F(\mathbf{x}_{2n-1}))$ is called the *truth table of* F. Balancedness of Boolean functions are usually studied from the point of view of Hamming weights or from the point of view of exponential sums.

The *Hamming weight* of a Boolean function F, usually denoted by $\mathrm{wt}(F)$, is the number of 1's in the truth table of F. Thus, a Boolean function F is balanced if and only if $\mathrm{wt}(F) = 2^{n-1}$. Weights of symmetric Boolean functions are somewhat understood. For instance, it is known since the 90's that weights of symmetric Boolean functions are linear recursive with integer coefficients [4, 7]. On the other hand, the study of weights of rotations symmetric Boolean functions is becoming an active area of research [3, 13, 15, 27, 28]. Similar to the symmetric case, it had been observed that weights of cubic rotation symmetric Boolean functions are linear recursive [3, 13]. This prompted the question if the same holds for any degree. An answer was given by Cusick [12] when he showed that weights of any rotation symmetric Boolean function satisfy linear recurrences with integer coefficients.

The *exponential sum* of an n-variable Boolean function $F(\mathbf{X})$ is defined as

$$S(F) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{F(\mathbf{x})}. \tag{1.1}$$

Observe that a Boolean function $F(\mathbf{X})$ is balanced if and only if $S(F) = 0$. This point of view is also a very active area of research. For some examples, please refer to [6–9, 11, 19, 21, 24]. Moreover, both point of views are equivalent and are linked by the equation

$$\mathrm{wt}(F) = \frac{2^n - S(F)}{2}. \tag{1.2}$$

Date: March 12, 2018.

2010 *Mathematics Subject Classification.* 05B20, 05E05, 11T23.

Key words and phrases. Hadamard matrices, Walsh transform, recurrences, exponential sums.