Discrete Mathematics 338 (2015) 2197–2211

Contents lists available at ScienceDirect

Discrete Mathematics

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

Circulant matrices and affine equivalence of monomial rotation symmetric Boolean functions

David Canright, Jong H. Chung [1], Pantelimon Stănică *

Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943-5216, USA

ARTICLE INFO

Article history:
Received 30 April 2014
Received in revised form 15 October 2014
Accepted 17 May 2015
Available online 19 June 2015

Keywords:
Boolean functions
Circulant matrices
Affine equivalence
Permutations

ABSTRACT

The goal of this paper is two-fold. We first focus on the problem of deciding whether two monomial rotation symmetric (MRS) Boolean functions are affine equivalent via a permutation. Using a correspondence between such functions and circulant matrices, we give a simple necessary and sufficient condition. We connect this problem with the well known Ádám's conjecture from graph theory. As applications, we reprove easily several main results of Cusick et al. on the number of equivalence classes under permutations for MRS in prime power dimensions, as well as give a count for the number of classes in pq number of variables, where p, q are prime numbers with $p < q < p^2$. Also, we find a connection between the generalized inverse of a circulant matrix and the invertibility of its generating polynomial over $\mathbb{F}_2$, modulo a product of cyclotomic polynomials, thus generalizing a known result on nonsingular circulant matrices.

Published by Elsevier B.V.

1. Introduction

The class of rotation symmetric Boolean functions (RSBFs) has received some attention from a combinatorial and cryptographic perspective. The initial study on the nonlinearity of these functions (called idempotents there) was done by Filiol and Fontaine [19]. Later on, the nonlinearity and correlation immunity of such functions have been studied in detail in [9,23,31,30,37,38]. Applications of such functions in hashing has also been investigated by Pieprzyk and Qu [35]. We want to mention also several papers [15–17,19,36] dealing with some other properties of RSBF, as well as their involvement in S-boxes. These functions are interesting to look into, since their space is much smaller ($\approx 2^{\frac{2^n}{n}}$) than the total space of Boolean functions (2^{2^n}) and the set contains functions with good cryptographic properties. It has been experimentally demonstrated that there are functions in this class which are good in terms of balancedness, nonlinearity, correlation immunity, algebraic degree and algebraic immunity (resistance against algebraic attack) [16].

It is interesting to note that the famous Patterson–Wiedemann functions [33] that achieve nonlinearity 16,276 (strictly greater than nonlinearity $2^{15-1} - 2^{(15-1)/2}$ obtained by bent functions concatenation) in 15 variables are in fact rotation symmetric. Moreover, Kavut et al. [25–27] proved that there exist rotation symmetric functions in 9 variables having nonlinearity 241 and 242 (which is also strictly greater than the bent concatenation nonlinearity $2^{9-1} - 2^{(9-1)/2}$), which was rather surprising and gives further motivation for the investigation of rotation symmetric Boolean functions.

Recently, there is some sustained effort to investigate the affine equivalence of some classes of Boolean functions, in particular the rotation symmetric Boolean functions (RSBF). In spite of their simplicity, the problem proves to be quite challenging. We mention here the papers [3,7,10–13] (and the references therein), which deal with low degrees (two to four) of

* Corresponding author.
E-mail addresses: dcanright@nps.edu (D. Canright), jong.chung@usma.edu (J.H. Chung), pstanica@nps.edu (P. Stănică).
[1] Current address: Department of Mathematical Sciences, United States Military Academy, West Point, NY 10996, USA.

http://dx.doi.org/10.1016/j.disc.2015.05.017
0012-365X/Published by Elsevier B.V.

monomial RSBFs, or some particular cases of the dimension where the functions are defined. Here, we propose a more elegant (we believe) approach for equivalence, which works for any degree, and apply it to count some cubic equivalence classes.

Here is an outline of this work. Section 2 gives basic definitions, including monomial rotation symmetric (MRS) Boolean functions and affine equivalence, and a known result for such quadratic functions. Section 3 discusses computational complexity of determining affine equivalence. Section 4 gives several useful facts about circulant matrices. In Section 5, we define S-equivalence (affine-equivalent by permutation matrix) and show in detail the connection between MRS functions and circulant matrices, resulting in our Theorem 5.2 that S-equivalence of the functions is the same as P-Q equivalence of the matrices. In Section 6 we use this connection, along with a powerful result of Wiedemann and Zieve [40], to give new proofs for counting the number of equivalence classes for cubic MRS functions, in three cases: degree $n = p$ prime (our Theorem 6.3), $n = p^k$ prime power (Theorem 6.5), and $n = pq$ product of two primes (Theorem 6.6). In Section 7, we explore how a circulant matrix inverse, pseudoinverse, or generalized inverse might relate to function equivalence. First, Theorem 7.3 generalizes a previous result, to give a condition on the factors of the generating polynomial that guarantee the circulant matrix has a circulant reflexive generalized inverse. Then Theorem 7.8 gives a necessary condition on weights when functions are S-equivalent with invertible circulant matrices. Also, Theorem 7.12 gives some facts about the case when the matrix has a pseudoinverse.

2. Preliminaries

A Boolean function f on n variables may be viewed as a mapping from $\mathbb{F}_2^n = \{0, 1\}^n$ into the two-element field $\mathbb{F}_2$; it can also be interpreted as the output column of its *truth table* f, that is, a binary string of length 2^n, $f = [f(0, 0, \ldots, 0), f(1, 0, \ldots, 0), \ldots, f(1, 1, \ldots, 1)]$. The set of all Boolean functions is denoted by $\mathcal{B}_n$.

The addition operator over $\mathbb{F}_2$ is denoted by $+$. An n-variable Boolean function f can be considered to be a multivariate polynomial over $\mathbb{F}_2$. This polynomial can be expressed as a sum of products representation of all distinct kth order products $(0 \le k \le n)$ of the variables. More precisely, $f(x_1, \ldots, x_n)$ can be written as

$$a_0 + \bigoplus_{1\le i\le n} a_i x_i + \bigoplus_{1\le i<j\le n} a_{ij} x_i x_j + \cdots + a_{12\ldots n} x_1 x_2 \ldots x_n,$$

where the coefficients $a_0, a_{ij}, \ldots, a_{12\ldots n} \in \{0, 1\}$. This representation of f is called the *algebraic normal form* (ANF) of f. The number of variables in the highest order product term with nonzero coefficient is called the *algebraic degree*, or simply the degree of f and denoted by $deg(f)$. A Boolean function is said to be *homogeneous* if its ANF contains terms of the same degree only.

Functions of degree at most one are called *affine* functions. An affine function with constant term equal to zero is called a *linear* function. Let $\mathbf{x} = (x_1, \ldots, x_n)$ and $\boldsymbol{\omega} = (\omega_1, \ldots, \omega_n)$ both belong to $\mathbb{F}_2^n$ and $\mathbf{x}\cdot\omega = x_1\omega_1 + \cdots + x_n\omega_n$. The *Hamming distance* between $\mathbf{x}$ and ω, denoted by $d(\mathbf{x}, \boldsymbol{\omega})$, is the number of positions where $\mathbf{x}$, ω differ. Also the *(Hamming) weight*, denoted by $wt(\mathbf{x})$, of a binary string $\mathbf{x}$ is the number of ones in $\mathbf{x}$. An n-variable function f is said to be *balanced* if its output column in the truth table contains equal number of 0's and 1's (i.e., $wt(f) = 2^{n-1}$). The nonlinearity of an n-variable function f is the minimum distance to the entire set of all affine functions, distance known to be bounded from above by $2^{n-1} - 2^{n/2-1}$. We define the (right) rotation operator ρ_n on a vector $(x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$ by $\rho_n(x_1, x_2, \ldots, x_n) = (x_n, x_1, x_2, \ldots, x_{n-1})$. Hence, ρ_n^k acts as a k-cyclic rotation on an n-bit vector. A Boolean function f is called *rotation symmetric* if for each input $(x_1, \ldots, x_n)$ in $\mathbb{F}_2^n$, $f(\rho_n^k(x_1, \ldots, x_n)) = f(x_1, \ldots, x_n)$, for $1 \le k \le n$. That is, the rotation symmetric Boolean functions are invariant under cyclic rotation of inputs. The inputs of a rotation symmetric Boolean function can be divided into partitions so that each partition consists of all cyclic shifts of one input. A partition is generated by $G_n(x_1, x_2, \ldots, x_n) = \{\rho_n^k(x_1, x_2, \ldots, x_n) | 1 \le k \le n\}$ and the number of sets in this partition is denoted by g_n. Thus the number of n-variable RSBFs is 2^{g_n}. Let $\phi(k)$ be Euler's *phi*-function, then Stănică and Maitra [37] give $g_n = \frac{1}{n}\sum_{k|n} \phi(k)\, 2^{\frac{n}{k}}$. We refer to [37,31,30] for the formula on how to calculate the number of partitions with weight w, for arbitrary n and w, as well as the number h_n of full length n classes (Ref. [28] corrects the count of [37] for h_n, when n is not a prime power).

A rotation symmetric function $f(x_1, \ldots, x_n)$ can be (for short) written as

$$a_0 + a_1 x_1 + \sum a_{1j} x_1 x_j + \cdots + a_{12\ldots n} x_1 x_2 \ldots x_n,$$

where the coefficients $a_0, a_1, a_{1j}, \ldots, a_{12\ldots n} \in \{0, 1\}$, and the existence of a representative term $x_1 x_{i_2} \ldots x_{i_l}$ implies the existence of all the terms from $G_n(x_1 x_{i_2} \ldots x_{i_l})$ in the ANF. This representation of f (not unique, since one can choose any representative in $G_n(x_1 x_{i_2} \ldots x_{i_l})$) is called the *short algebraic normal form* (SANF) of f. If the SANF of f contains only one term, we call such a function a *monomial rotation symmetric* (MRS) function. Certainly, the number of terms in the ANF of a monomial rotation symmetric function is a divisor of n (see [37]). If that divisor is in fact n, we call the function a *full-cycle MRS*, otherwise a *short-cycle MRS*.

We say that two Boolean functions $f(\mathbf{x})$ and $g(\mathbf{x})$ in $\mathcal{B}_n$ are *affine equivalent* if $g(\mathbf{x}) = f(\mathbf{x}A + \mathbf{b})$, where $A \in GL_n(\mathbb{F}_2)$ ($n \times n$ nonsingular matrices over the finite field $\mathbb{F}_2$ with the usual operations) and $\mathbf{b}$ is an n-vector over $\mathbb{F}_2$. We say $f(\mathbf{x}A + \mathbf{b})$ is a *nonsingular affine transformation* of $f(\mathbf{x})$. It is easy to see that if f and g are affine equivalent, then they have the same weight and nonlinearity: $wt(f) = wt(g)$ and $N_f = N_g$ (these are examples of *affine invariants*).

The relevance of these two invariants can be inferred by recalling the well-known result (see [10], for example).