Information Sciences 314 (2015) 212–224

Contents lists available at ScienceDirect

Information Sciences

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

Affine equivalence of quartic monomial rotation symmetric Boolean functions in prime power dimension

Pantelimon Stănică

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

ARTICLE INFO

Article history:
Received 10 February 2014
Received in revised form 28 January 2015
Accepted 30 March 2015
Available online 3 April 2015

Mathematics Subject Classification [2010]:
94A60
94C10
06E30

Keywords:
Boolean functions
Circulant matrices
Affine equivalence
Permutations
Prime powers

ABSTRACT

In this paper we analyze and exactly compute the number of affine equivalence classes under permutations for quartic monomial rotation symmetric functions in prime and prime power dimensions.

Published by Elsevier Inc.

1. Introduction

An n-variable Boolean function f is a map from the n dimensional vector space $\mathbb{F}_2^n = \{0,1\}^n$ into the two-element field $\mathbb{F}_2$, that is, an n-variable Boolean function f is a multivariate polynomial over $\mathbb{F}_2$. Denoting the addition operator over $\mathbb{F}_2$ by '+', a Boolean function can be thought as a multivariate polynomial, called the *algebraic normal form* (ANF)

$$f(x_1,\ldots,x_n) = a_0 + \sum_{1\leqslant i\leqslant n} a_i x_i + \sum_{1\leqslant i<j\leqslant n} a_{ij} x_i x_j + \ldots + a_{12\ldots n} x_1 x_2 \ldots x_n,$$

where the coefficients $a_0, a_{ij}, \ldots, a_{12\ldots n} \in \mathbb{F}_2$. The maximum number of variables in a monomial is called the (*algebraic*) *degree*, and it is denoted by $deg(f)$. If all monomials in its ANF have the same degree, the Boolean function is said to be *homogeneous*.

Functions of degree at most one are called *affine* functions. An affine function with constant term equal to zero is called a *linear* function. Define the scalar product of $\mathbf{x} = (x_1,\ldots,x_n)$, $\mathbf{y} = (y_1,\ldots,y_n)$ both in $\mathbb{F}_2^n$, by $\mathbf{x}\cdot\mathbf{y} = \sum_{i=1}^n x_i y_i$. The *(Hamming) weight*, denoted by $wt(\mathbf{x})$, of a binary string $\mathbf{x}$ is the number of ones in $\mathbf{x}$, and the *Hamming distance* $d(\mathbf{x},\mathbf{y})$ between $\mathbf{x}$ and

E-mail address: pstanica@nps.edu

http://dx.doi.org/10.1016/j.ins.2015.03.071
0020-0255/Published by Elsevier Inc.

$\mathbf{y}$ is the number of positions where $\mathbf{x}$, $\mathbf{y}$ differ. An n-variable function f is said to be *balanced* if its output column in the truth table contains equal number of 0s and 1s (i.e., $wt(f) = 2^{n-1}$). The nonlinearity of an n-variable function f is the minimum distance to the entire set of affine functions, which is 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* [10] 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 $1 \leqslant k \leqslant n$. That is, the rotation symmetric Boolean functions (RSBF) are invariant under cyclic rotation of inputs. A partition of some cardinality g_n is generated by $G_n(x_1, \ldots, x_n) = \{\rho_n^k(x_1, \ldots, x_n) | 1 \leqslant k \leqslant n\}$, and so, the number of n-variable RSBFs is 2^{g_n}. It was shown [11] that $g_n = \frac{1}{n}\sum_{k|n} \phi(k) 2^{\frac{n}{k}}$, where ϕ is Euler's totient function. We refer to [8,9,11] for the formula on how to calculate the number of partitions with weight w, say $g_{n,w}$, for arbitrary n and w.

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

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

where $a_0, a_1, a_{1j}, \ldots, a_{12\ldots n} \in \mathbb{F}_2$, 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 [11]).

We say that two Boolean functions $f(\mathbf{x})$ and $g(\mathbf{x})$ in $\mathscr{B}_n$ 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*).

There are cases, when it is known that these invariants are also sufficient (two quadratic functions are affine equivalent if and only if their weights and nonlinearity are the same – see [3], for example). However, in general, for higher degrees, that it is not the case, but there are attempts to solve the equivalence problem (see [1] and the references therein).

2. Background on *S*-equivalence

In [2] the authors introduced the notion of *S-equivalence* $f \stackrel{S}{\sim} g$, which is the affine equivalence of monomial rotation symmetric (MRS) functions f, g under permutation of variables (we will write here $f \sim g$, for easy displaying).

An $n \times n$ matrix C is *circulant*, denoted by $C(c_1, c_2, \ldots, c_n)$, if all its rows are successive circular rotations of the first row, that is,

$$C = \begin{pmatrix} c_1 & c_2 & \ldots & c_n \\ c_n & c_1 & \ldots & c_{n-1} \\ \ldots & \ldots & \ldots & \ldots \\ c_2 & c_3 & \ldots & c_1 \end{pmatrix}.$$

On the set $\mathscr{C}_n$ of circulant matrices an equivalence relation was introduced in [2]: for $A_1 = C(a_1, \ldots, a_n), A_2 = C(b_1, \ldots, b_n)$, then $A_1 \approx A_2$ if and only if $(a_1, \ldots, a_n) = \rho_n^k(b_1, \ldots, b_n)$, for some $0 \leqslant k \leqslant n-1$. It was shown that the set of equivalence classes (the equivalence class of $C(a_1, a_2, \ldots, a_n)$ is denoted by $C\langle a_1, a_2, \ldots, a_n\rangle$, or $\langle C(a_1, a_2, \ldots, a_n)\rangle$) form a commutative monoid (under the natural operation $\langle A\rangle \cdot \langle B\rangle := \langle AB\rangle$). Moreover, the previous operation partitions the invertible $n \times n$ circulant matrices into equivalence classes, say $\mathscr{C}_n^*/_{\approx}$, and consequently, $(\mathscr{C}_n^*/_{\approx}, \cdot)$ becomes a group.

Let $f = x_1 x_{j_2} \ldots x_{j_d} + x_2 x_{j_2+1} \ldots x_{j_d+1} + \ldots + x_n x_{j_2-1} \ldots x_{j_d-1}$ be an MRS function of degree d, with the SANF $x_1 x_{j_2} \ldots x_{j_d}$. We associate to f the following (unique) circulant matrix equivalence class

$$A_f = \langle \mathrm{C}(\overset{\overset{1}{\downarrow}}{1}, 0, \ldots, \overset{\overset{j_2}{\downarrow}}{1}, 0, \ldots, 0, \overset{\overset{j_3}{\downarrow}}{1}, \ldots, 0, \overset{\overset{j_d}{\downarrow}}{1}, \ldots, 0)\rangle, \tag{1}$$

where the 1 bits (indicated above) appear in positions given by the indices in the SANF monomial of f.

For a binary (row) vector $(a_1, a_2, \ldots, a_n)$ of dimension n, we let $\Delta(a_1, a_2, \ldots, a_n) \equiv \{i | a_i = 1\}$, and by abuse of notation, $\Delta(C(\mathbf{a})) = \Delta(\mathbf{a})$. Similarly, for a single monomial term $x_{i_1} x_{i_2} \ldots x_{i_d}$ of degree d in n variables, we define $\Delta(x_{i_1} x_{i_2} \ldots x_{i_d}) \equiv \{i_j | j = 1, 2, \ldots, d\}$. We can also extend this to the MRS function with this SANF, $f = x_{i_1} x_{i_2} \ldots x_{i_d}$, as $\Delta(f) = \Delta(x_{i_1} x_{i_2} \ldots x_{i_d})$, which is not unique, but we prefer (so not to complicate the notation) to consider all such sets equal under a cyclic rotation permutation of the indices. That is, for A_f as in (1), then