Information Sciences 259 (2014) 192–211

Contents lists available at ScienceDirect

Information Sciences

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

# Affine equivalence of quartic homogeneous rotation symmetric Boolean functions

Thomas W. Cusick [a,*], Younhwan Cheon [b]

[a] University at Buffalo, Department of Mathematics, 244 Mathematics Building, Buffalo, NY 14260, USA
[b] Korea Army Academy at YeongCheon, Department of Mathematics, ChangHa GoGyung, YeongCheon, KyungBuk 770-849, Republic of Korea

ARTICLE INFO

*Article history:*
Received 30 August 2012
Received in revised form 30 July 2013
Accepted 1 September 2013
Available online 10 September 2013

*Keywords:*
Boolean functions
Rotation symmetry
Quartic function
Affine equivalence
Patterns

ABSTRACT

Homogeneous rotation symmetric Boolean functions have been extensively studied in recent years because of their applications in cryptography. Little is known about the basic question of when two such functions in $n$ variables are affine equivalent. The simplest case of quadratic rotation symmetric functions which are generated by cyclic permutations of the variables in a single monomial was only settled in 2009, and the first substantial progress on the much more complicated cubic case came in 2010. In this paper, we show that much of the work on the cubic case can be extended to the quartic case. We also prove an exact formula for the number and sizes of the affine equivalence classes when $n$ is a prime.


## 1. Affine equivalence of quartic rotation symmetric Boolean functions

Boolean functions have many applications in coding theory and cryptography. A detailed account of the latter applications can be found in the book [7]. If we define $V_n$ to be the vector space of dimension $n$ over the finite field $GF(2) = \{0, 1\}$, then an $n$ variable Boolean function $f(x_1, x_2, \ldots, x_n) = f(\mathbf{x})$ is a map from $V_n$ to $GF(2)$. Every Boolean function $f(\mathbf{x})$ has a unique polynomial representation (usually called the *algebraic normal form* [7, p. 6]), and the degree of $f$ is the degree of this polynomial. A function of degree $\leqslant 1$ is called affine, and if the constant term is 0 such a function is called linear. If every term in the algebraic normal form of $f$ has the same degree, then the function is *homogeneous*. All functions studied in this paper will be homogeneous. We let $B_n$ denote the set of all Boolean functions in $n$ variables, with addition and multiplication done mod 2.

We say a Boolean function $f(\mathbf{x})$ in $B_n$ is *rotation symmetric* if the algebraic normal form of the function is unchanged by any cyclic permutation of the variables $x_1, x_2, \ldots, x_n$. In recent years, rotation symmetric functions have proven to be very useful in several areas of cryptography [7, pp. 108–118]. This has led to many papers which study different aspects of the theory of rotation symmetric functions (see, for example, the references in [7, pp. 108–118] and the recent papers [3,5,6,9,10,13,14].

We say that two Boolean functions $f(\mathbf{x})$ and $g(\mathbf{x})$ in $B_n$ are *affine equivalent* if $g(\mathbf{x}) = f(A\mathbf{x} + \mathbf{b})$, where $A$ is an $n$ by $n$ nonsingular matrix over the finite field $GF(2)$ and $b$ is an $n$-vector over $GF(2)$. We say $f(A\mathbf{x} + \mathbf{b})$ is a *nonsingular affine transformation* of $f(\mathbf{x})$.

An important basic question is to decide when two Boolean functions are affine equivalent. Early work on the coding theory interpretation of this question used *ad hoc* methods to settle the problem for small numbers of variables (see [1,12]), but our concern is analyzing the case of fixed degree and an arbitrary number $n$ of variables. There is some more

* Corresponding author. Tel.: +1 716 645 8801; fax: +1 716 645 5039.
*E-mail addresses:* cusick@buffalo.edu (T.W. Cusick), yhcrypt@gmail.com (Y. Cheon).

0020-0255/$ - see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.ins.2013.09.001

recent work on testing affine equivalence (for example, [2,8]), but this gives very little progress on the general problem. The general problem seems extremely difficult, so current research is devoted to studying special cases, in particular the rotation symmetric functions. The simplest case of quadratic rotation symmetric functions in $n$ variables which are generated by cyclic permutations of the variables in a single monomial was only settled in 2009 (see [11]). Affine equivalence for cubic rotation symmetric Boolean functions was recently studied by the first author [4], and further progress was made in [3]. In this paper we extend the work of [4] to affine equivalence for quartic rotation symmetric Boolean functions, concerning which there is almost nothing in the literature. We shall consider the simplest of such functions $f$, namely those generated by cyclic permutations of the variables in a single monomial. We call these the *quartic monomial rotation symmetric (MRS)* functions. Thus for some $j$, $k$ and $l$, $1 < j < k < l$, we have

$$f(\mathbf{x}) = x_1x_jx_kx_l + x_2x_{j+1}x_{k+1}x_{l+1} + \cdots + x_nx_{j-1}x_{k-1}x_{l-1}. \tag{1}$$

We shall use the notation $(1, j, k, l)$ for the function $f(\mathbf{x})$ in (1), no matter how the terms on the right-hand side are written (so the order of the terms, and of the 4 variables in each term, does not matter). If $(1, j, k, l)$ is written in the form (1) (so the first subscripts in the $n$ terms are $1, 2, \ldots, n$ in order, and the other three subscripts in order each give cyclic permutations of $1, 2, \ldots, n$, as shown), we say $f$ is written in *standard form*. Note we do not require $j < k < l$, so there are six ways to write $f(\mathbf{x})$ in standard form. If we specify the representation of $f(\mathbf{x})$ ($(1, j, k, l)$, $(1, j, l, k)$, $(1, k, j, l)$, $(1, k, l, j)$, $(1, l, j, k)$, or $(1, l, k, j)$), then the standard form is unique. Clearly each subscript $j$, $1 \leqslant j \leqslant n$, appears in exactly 4 of the terms in any representation of $f(\mathbf{x})$; we shall call these four terms the $j$-terms of $f$. We shall use the notation (see Tables 1–8)

$$[i, j, k, l] = x_ix_jx_kx_l \tag{2}$$

as shorthand for the monomial on the right-hand side; note that the order of the variables matters, so, for example, the 24 permutations of $i, j, k, l$ give 24 different representations of form (2) for the same monomial $x_ix_jx_kx_l$.

**Definition 1.1.** If $n$ is even, it is possible for the representation (1) to contain only $\frac{n}{2}$ or (if $n$ is divisible by 4) $\frac{n}{4}$ distinct terms. If this happens, we modify the definition of the function in (1) so that only the distinct terms are used. We define the "short quartic functions" to be the ones with fewer than $n$ terms (so functions with $\frac{n}{2}$ and $\frac{n}{4}$ terms are both "short") and we define the "very short quartic functions" to be the ones with $\frac{n}{4}$ terms. Thus every very short function is also a short function.

**Lemma 1.2.** *If $n$ is divisible by 2, there are short quartic functions of the form $(1, i, \frac{n}{2}+1, i+\frac{n}{2})$ where $2 \leqslant i \leqslant \left[\frac{n}{4}\right]+1$. If $n$ is divisible by 4 and $i = \frac{n}{4}+1$, we have a very short quartic function. These $\left[\frac{n}{4}\right]$ functions give all the short quartic functions in $n$ variables.*

**Proof.** If $n$ is divisible by 2, then the function $(1, i, \frac{n}{2}+1, i+\frac{n}{2})$ where $2 \leqslant i \leqslant \left[\frac{n}{4}\right]+1$ is exceptional because then the representation (1) has only $\frac{n}{2}$ distinct terms, or only $\frac{n}{4}$ distinct terms if $n$ is divisible by 4 and $i = \frac{n}{4}+1$. Thus in these cases the representation (1) reduces to a sum of only $\frac{n}{2}$ or $\frac{n}{4}$ terms. Also $(1, i, \frac{n}{2}+1, i+\frac{n}{2})$ is the same function as $(1, (\frac{n}{2}+2)-i, \frac{n}{2}+1, n+2-i)$ for any $n$, so there are $\left[\frac{n}{4}\right]$ short quartic functions in $n$ variables. □

Our goal is to study the affine equivalence classes for quartic rotation symmetric functions $(1, j, k, l)$. In order to do this, we need to be able to identify all of the distinct functions $(1, j, k, l)$. We define

$$\begin{aligned} D_n = \{(1,j,k,l) : {} & j < k < l \leqslant n, \text{ every function } (1,j,k,l) \text{ is represented by} \\ & \text{the quadruple } 1,j,k,l \text{ with least } j, \text{ and given that, with least } k, \\ & \text{and given that, with least } l\}. \end{aligned}$$

Every quartic monomial rotation symmetric function $f$ is equal to exactly one function $(1, j, k, l)$ in $D_n$, but of course $f$ is also equal to $(1, p, q, r)$, where $[1, p, q, r]$ is any of the six 1-terms in $(1, j, k, l)$.

Clearly we can determine $D_n$ by making a list of all of the functions $(1, j, k, l)$ with $1 < j < k < l \leqslant n$ in lexicographic order and standard form, and then crossing out any function in the list which has a 1-term appearing in any earlier function in the list. The number of distinct functions which remain after this is given in the following lemma (as usual, $|S|$ denotes the number of elements in the set $S$).

**Lemma 1.3.** *If $n$ is odd, then $|D_n| = (n-1)(n-2)(n-3)/24$; if $n \equiv 2 \bmod 4$, then $|D_n| = (n-2)(n^2-4n+6)/24$; if $n \equiv 0 \bmod 4$, then $|D_n| = n(n^2-6n+14)/24$.*

**Proof.** This counting problem reduces to a well-known counting problem for $n$-bead necklaces with 2 possible colors for the beads. The connection was first noted by Stănică and Maitra [15, p. 1570]. The lemma follows from an explicit computation for our special case with $n = 4$. □

Extending the definition for the cubic case given in [4], we define the notion of *pattern* for any term $[i, j, k, l]$. The pattern of $[i, j, k, l]$ is the integer vector

$$(j-i \bmod n; k-i \bmod n; l-i \bmod n; l-j \bmod n). \tag{3}$$