Information and Computation 208 (2010) 341–350

Contents lists available at ScienceDirect

Information and Computation

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

9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class☆

Selçuk Kavut*, Melek Diker Yücel

Department of Electrical Engineering and Institute of Applied Mathematics, Middle East Technical University – ODTÜ, 06531 Ankara, Turkey

ARTICLE INFO

Article history:
Received 12 December 2008
Revised 5 August 2009
Available online 4 January 2010

Keywords:
Boolean functions
Combinatorial problems
Cryptography
Dihedral symmetry
Nonlinearity
Rotational symmetry

ABSTRACT

We give a new lower bound to the covering radius of the first order Reed–Muller code $RM(1,n)$, where $n \in \{9, 11, 13\}$. Equivalently, we present the n-variable Boolean functions for $n \in \{9, 11, 13\}$ with maximum nonlinearity found till now. In 2006, 9-variable Boolean functions having nonlinearity 241, which is strictly greater than the bent concatenation bound of 240, have been discovered in the class of Rotation Symmetric Boolean Functions (RSBFs) by Kavut, Maitra and Yücel. To improve this nonlinearity result, we have firstly defined some subsets of the n-variable Boolean functions as the generalized classes of "k-RSBFs and k-DSBFs (k-Dihedral Symmetric Boolean Functions)", where k is a positive integer dividing n. Secondly, utilizing a steepest-descent like iterative heuristic search algorithm, we have found 9-variable Boolean functions with nonlinearity 242 within the classes of both 3-RSBFs and 3-DSBFs. Thirdly, motivated by the fact that RSBFs are invariant under a special permutation of the input vector, we have classified all possible permutations up to the linear equivalence of Boolean functions that are invariant under those permutations.

1. Introduction

On odd number of input variables n, constructing Boolean functions with maximum possible nonlinearity is an open problem in the area of cryptography and combinatorics. The problem is also related to the upper bound $\lfloor 2^{n-1} - 2^{\frac{n}{2}-1} \rfloor$ on the covering radius of the first order Reed–Muller code [3], which is later improved [4] as $2\lfloor 2^{n-2} - 2^{\frac{n}{2}-2} \rfloor$. Boolean functions on even number of input variables n, attaining the maximum nonlinearity of $\left(2^{n-1} - 2^{\frac{n}{2}-1}\right)$ are called the bent functions [5]. For odd n, the nonlinearity value $\left(2^{n-1} - 2^{\frac{n-1}{2}}\right)$ is known as the *bent concatenation bound*. In Table 1, we present the bent concatenation bound for $7 \leqslant n \leqslant 15$, together with recent nonlinearity results [4,6–9].

For odd $n \leqslant 7$, it is known that the maximum nonlinearity is equal to the bent concatenation bound [10,11]. However, in 1983, using combinatorial techniques and search methods, Patterson and Wiedemann [9] constructed 15-variable Boolean functions with nonlinearity 16,276, exceeding the bent concatenation bound by 20. Utilizing those 15-variable functions it is possible to obtain functions with nonlinearity $\left(2^{n-1} - 2^{\frac{n-1}{2}} + 20 \times 2^{\frac{n-15}{2}}\right)$ for odd $n \geqslant 15$. Astoundingly, for the cases of $n = 9, 11, 13$, the maximum nonlinearity known until 2006 was still equal to the bent concatenation bound.

☆ This work is partially presented in [1,2].

* Corresponding author.
E-mail addresses: skavut@gyte.edu.tr (S. Kavut), melekdy@metu.edu.tr (M. Diker Yücel).

0890-5401/$ - see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.ic.2009.12.002

Table 1
Summary of nonlinearity results for $n = 7, 9, 11, 13, 15$.

n	7	9	11	13	15
Bent concatenation bound: $2^{n-1} - 2^{\frac{n-1}{2}}$	56	240	992	4032	16,256
Nonlinearity results in [6]	–	241	994	4036	16,264
Balanced function nonlinearities in [7,8]	–	–	–	4036	16,272
Our nonlinearity results	–	242	996	4040	16,272
Patterson–Wiedemann construction [9]	–	–	–	–	16,276
Upper bound [4]	56	244	1000	4050	16,292

In 2006, 9-variable Rotation Symmetric Boolean Functions (RSBFs) with nonlinearity 241 $\left(= 2^{9-1} - 2^{\frac{9-1}{2}} + 1\right)$ were discovered [6], which led to the construction of functions with nonlinearity exceeding the bent concatenation bound by $2^{\frac{n-9}{2}}$, for odd $n \geqslant 9$. Such functions were attained utilizing the steepest-descent like iterative algorithm that first appeared in [12] and then was suitably modified in [6] for a search in the class of RSBFs.

RSBFs seem to be *rich* in terms of highly nonlinear functions and there is a close relation between RSBFs and idempotents [13,14]. Considering a Boolean function f as a mapping from $GF(2^n) \to GF(2)$, the functions for which $f(\alpha^2) = f(\alpha)$ for any $\alpha \in GF(2^n)$, are referred to as idempotents. As pointed out in [13,14], the idempotents can be regarded as RSBFs with proper choice of basis. In [9], 15-variable Patterson–Wiedemann functions having nonlinearity 16,276 are also identified in the idempotent class.

As the size of the RSBF class is much smaller $\left(\approx 2^{\frac{2^n}{n}}\right)$ than the total size of n-variable Boolean functions $\left(2^{2^n}\right)$, an exhaustive search is possible for 9-variable RSBFs. In [15], such a search has shown that there is no 9-variable RSBF having nonlinearity greater than 241. So, we feel like increasing the search space of the heuristic in order to find functions with higher nonlinearity.

Motivated by this fact, we firstly propose the generalized k-RSBFs, as functions which satisfy $f(\alpha^{2^k}) = f(\alpha)$, where $1 \leqslant k|n$. Note that if $k = 1$, the resulting class corresponds to conventional RSBFs, and for $k = n$, generalized k-RSBFs cover the entire space. In the space of k-RSBFs, we also define the generalized class of k-DSBFs (k-Dihedral Symmetric Boolean Functions) as a subset of k-RSBFs by imposing the condition of invariance under the action of dihedral group.

Secondly, we have used the steepest-descent like iterative algorithm in [6] for a search in the generalized 3-RSBF and 3-DSBF classes. This search has successfully ended up with 9-variable functions in both of these classes, having nonlinearity 242, and absolute indicator values of 32, 40 and 56. This result shows that the covering radius of the first order Reed–Muller code $RM(1, 9)$ is at least 242. This result is also important for $n = 11$ and $n = 13$, since the bent concatenation of 9-variable functions with nonlinearity 242 leads to the construction of 11-variable and 13-variable functions with nonlinearities exceeding the bent concatenation bound by $2 \times 2^{\frac{n-9}{2}}$.

Thirdly, knowing the fact that k-RSBFs and k-DSBFs are invariant under some special types of permutations on input vectors, we have considered the possibility of other rich classes that are invariant under some permutations. Linearly equivalent Boolean functions [16] f and g, where $f = g(Ax)$ and A is an invertible matrix, have the same nonlinearity; therefore, while searching for highly nonlinear functions, it is quite logical to classify all $n!$ permutations up to the linear equivalence of Boolean functions that are invariant under them. More specifically, for 9-variable Boolean functions, we classify 9! many permutations into 30 classes, which are different up to the linear equivalence of Boolean functions that are invariant under them. Then for each class, by picking up a representative permutation arbitrarily, we have searched the corresponding set of Boolean functions. In some of these sets, we have consequently obtained 9-variable Boolean functions with nonlinearity 242 and absolute indicator values of 40, 48 and 56. So, our aim of defining other rich classes is accomplished. We note, however, that the presented functions do not contain any zero in their Walsh spectra; therefore, they cannot be linearly transformed to balanced functions.

In the following section, after reviewing some basic definitions related to Boolean functions, we present preliminaries of permutation group actions. In Section 3, we introduce the generalized rotation symmetric and dihedral symmetric Boolean functions. Classification of permutations on inputs of 9-variable Boolean functions, with respect to the linear equivalence of Boolean functions that are invariant under them, is presented in Section 4. Different results related to 9-variable Boolean functions with nonlinearity 242 are presented in Sections 3 and 4.

2. Preliminaries

2.1. Boolean functions

An n-variable Boolean function $f(x)$ produces a single-bit result for each n-bit input vector $x = (x_0, \ldots, x_{n-1})$, which may be considered as a mapping from $\{0, 1\}^n$ into $\{0, 1\}$. $f(x)$ is basically represented by its *truth table*, that is, a binary vector of length 2^n,