Journal of Combinatorial Theory, Series A 127 (2014) 161–175

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

A secondary construction and a transformation on rotation symmetric functions, and their action on bent and semi-bent functions [☆]

Claude Carlet [a], Guangpu Gao [b,c], Wenfen Liu [b,c]

[a] *LAGA, (UMR 7539), University of Paris 8, University of Paris 13, CNRS, 2 rue de la Liberté, F-93526 Saint-Denis Cedex, France*
[b] *State Key Laboratory of Mathematical Engineering and Advanced Computing, China*
[c] *State Key Laboratory of Networking and Switching Technology (Beijing University of Posts and Telecommunications), China*

ARTICLE INFO

Article history:
Received 29 May 2013
Available online 24 June 2014

Keywords:
Rotation symmetric Boolean function
Bent function
Idempotent

ABSTRACT

We study more in detail the relationship between rotation symmetric (RS) functions and idempotents, in univariate and bivariate representations, and deduce a construction of bent RS functions from semi-bent RS functions. We deduce the first infinite classes found of idempotent and RS bent functions of algebraic degree more than 3. We introduce a transformation from any RS Boolean function f over $GF(2)^n$ into the idempotent Boolean function $f'(z) = f(z, z^2, \dots, z^{2^{n-1}})$ over $GF(2^n)$, leading to another RS Boolean function. The trace representation of f' is directly deduced from the algebraic normal form of f, but we show that f and f', which have the same algebraic degree, are in general not affinely equivalent to each other. We exhibit infinite classes of functions f such that (1) f is bent and f' is not (2) f' is bent and f is not (3) f and f' are both bent (we show that this is always the case for quadratic functions and we also investigate cubic functions).

[☆] The work of G. Gao, and W. Liu is supported in part by National Basic Research Program under Grant No. 2012CB315905 and Open Foundation of State Key Laboratory of Networking and Switching Technology (Beijing University of Posts and Telecommunications) (SKLNST-2013-1-06).

E-mail addresses: claude.carlet@univ-paris8.fr (C. Carlet), guangpu.gao@gmai.com (G. Gao).

http://dx.doi.org/10.1016/j.jcta.2014.05.008
0097-3165/© 2014 Elsevier Inc. All rights reserved.

1. Introduction

Rotation symmetric (RS) Boolean functions $f(x_0, x_1, \dots, x_{n-1})$, invariant under circular permutations of the coordinates, have been originally introduced by Filiol and Fontaine in [8,9] under the name of idempotent functions and soon after studied by Pieprzyk and Qu [20] under their final name. They allowed obtaining Boolean functions in odd numbers of variables beating the best known nonlinearities [12], and new bent functions (in even numbers of variables) [5,10,22,23]. They need less space to be stored and allow faster computation of the Walsh transform. Idempotents are Boolean functions f over $\mathrm{GF}(2^n)$ such that $f(z^2) = f(z)$, for every $z \in \mathrm{GF}(2^n)$. There is a bijective correspondence between idempotent functions and RS functions, by decomposing z over a normal basis (see Remark 3.2). By abuse of language, we shall sometimes use the term of RS function for idempotent function. The original motivation for the study of these functions is that the rotation symmetry seems to increase the probability of finding interesting functions by random search and gives nice structure which can be used for the study.

Bent functions are extremal combinatorial objects [21]. They lie at maximal Hamming distance from affine functions and provide then an optimal resistance against attacks by affine approximations, such as the fast correlation cryptanalysis. They are weak against other attacks like the Siegenthaler correlation attack and the fast algebraic attack, but their study is nevertheless useful for cryptographic purposes (they are involved in several block ciphers, for instance). They are also related to (Hadamard) difference sets, designs, sequences for telecommunications and optimal error correcting codes (such as the Kerdock codes). Semi-bent functions are similar (but weaker) objects, which can be balanced (that is, have output uniformly distributed over $\mathrm{GF}(2)$), contrary to bent functions. For more details on bent and semi-bent functions, see [1,3,4,18] and the references therein.

After recalling in Section 2 the main definitions, we investigate in Section 3 the relationship between the representation of Boolean functions by the algebraic normal form (and the related notion of RS function), and the univariate representation (and the related notion of idempotent function). We also study RS functions in bivariate representation; we show that, in this framework, a proper relationship is between weak RS functions (invariant under circular permutation of indices by two positions) and weak idempotents (a natural notion that we introduce). We deduce a way of constructing a new RS n-variable function, where $n \equiv 2 \pmod 4$, from two known semi-bent RS functions in $n/2$ variables, by using the indirect sum. Then an infinite class of quartic RS bent functions is exhibited (the first infinite class found of RS bent functions of algebraic degree more than 3). In Section 4, we study a new transformation: given an RS Boolean function f, we consider the function $f'(z)$, $z \in \mathrm{GF}(2^n)$, expressed in univariate representation (leading to the trace representation) and obtained from the algebraic normal form of $f(x_0, x_1, \dots, x_{n-1})$ by replacing x_i by z^{2^i}; this function f' is a Boolean idempotent function. The trace representation of f' is directly deduced from the algebraic