ARTICLE IN PRESS

Discrete Applied Mathematics ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Discrete Applied Mathematics

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

Communication

On non-existence of bent–negabent rotation symmetric Boolean functions

Bimal Mandal [a], Bhupendra Singh [b], Sugata Gangopadhyay [c], Subhamoy Maitra [a,*], V. Vetrivel [d]

[a] Indian Statistical Institute, 203 B T Road, Kolkata 700 108, India
[b] Secure Systems Division, CAIR, DRDO, Bangalore, India
[c] Department of Computer Science and Engineering, Indian Institute of Technology Roorkee, India
[d] Department of Mathematics, Indian Institute of Technology Madras, India

ARTICLE INFO

Article history:
Received 31 October 2017
Accepted 1 November 2017
Available online xxxx
Communicated by Pantelimon Stanica

Keywords:
Rotation symmetric Boolean function
Autocorrelation
Bent–negabent function

ABSTRACT

In this communication, we present a characterization of bent–negabent functions, which is related to the autocorrelation spectra. A special case of this characterization is then exploited to prove that there is no rotation symmetric Boolean function in $n = 2p^k$ variables which is bent–negabent when p is an odd prime and k is any positive integer.

1. Introduction

In 1976, Rothaus [7] introduced a class of Boolean functions with provably maximum possible distance from the affine functions, called the bent functions. Bent functions exist only in even number of variables and the degree of an n-variable bent function is at most $\frac{n}{2}$. A Boolean function is said to be negabent if its nega-Hadamard spectrum is flat [6,9,4]. Riera and Parker [6] initiated the problem of constructing Boolean functions that are bent as well as negabent at the same time. For subsequent results on bent–negabent functions, one may refer to [9,4,10]. Here, for the first time, we present a characterization of bent–negabent functions that relates to the autocorrelation spectra. It is well known that all the autocorrelation spectrum values of a bent function at non-zero point are zero. Naturally, we should obtain more stringent conditions when a function is bent–negabent. We show that an n-variable (n even) function is bent–negabent if and only if for all non-zero $\mathbf{a} \in \mathbb{F}_2^n$,

$$\sum_{\mathbf{x}\in\mathbb{F}_2^n:\ \mathbf{a}\cdot\mathbf{x}=0} (-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{a})} = \sum_{\mathbf{x}\in\mathbb{F}_2^n:\ \mathbf{a}\cdot\mathbf{x}=1} (-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{a})} = 0$$

when $wt(\mathbf{a})$ is even, and when $wt(\mathbf{a})$ is odd

$$\sum_{\mathbf{x}\in\mathbb{F}_2^n:\ \bar{\mathbf{a}}\cdot\mathbf{x}=0} (-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{a})} = \sum_{\mathbf{x}\in\mathbb{F}_2^n:\ \bar{\mathbf{a}}\cdot\mathbf{x}=1} (-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{a})} = 0.$$

* Corresponding author.
E-mail addresses: bimalmandal90@gmail.com (B. Mandal), bhusingh21@yahoo.co.in (B. Singh), sugatfma@iitr.ac.in (S. Gangopadhyay), subho@isical.ac.in (S. Maitra), vetri@iitm.ac.in (V. Vetrivel).

https://doi.org/10.1016/j.dam.2017.11.001
0166-218X/

Please cite this article in press as: B. Mandal, et al., On non-existence of bent–negabent rotation symmetric Boolean functions, Discrete Applied Mathematics (2017), https://doi.org/10.1016/j.dam.2017.11.001.

Naturally, this provides $2^n - 1$ additional constraints (corresponding to different non-zero $\mathbf{a}$'s) over the bent function by considering the partial sums when the autocorrelation spectrum of a bent–negabent function is studied. Consequently, this leads to non-existence of certain classes of bent–negabent functions that we discuss next.

Rotation symmetric (RotS) Boolean functions are those functions that return the same output if the input bit-patterns are rotated. These functions have more efficient implementation than the general Boolean functions and therefore these are of practical interest in construction of cryptographic primitives. Pieprzyk and Qu [5] studied the rotation symmetric Boolean functions as components in the rounds of a hashing algorithm. For interesting combinatorial results related to RotS Boolean functions, we refer to [11,2,1]. Very recently, Sarkar and Cusick [8] have noted that there does not exist any quadratic rotation symmetric Boolean function which is bent–negabent and further they have checked that for $n \leq 8$ there is no rotation symmetric bent–negabent function. The existence (or non-existence) of a rotation symmetric bent–negabent function with even number of variables is thus an important open question. We partially solve this for $n = 2p^k$, where p is an odd prime and k is any positive integer. One can see that the density of prime powers is of the order of density of the prime numbers [3]. Hence, we may note that for integers till n, the estimated count of even numbers of the form $2p^k$ is $O(\frac{n}{\log n})$. Thus, our result covers a considerable number of even integers.

1.1. Preliminaries

Let $\mathbb{F}_2$ be the prime field of characteristic 2. Let $\oplus$ denote the addition over $\mathbb{F}_2$. Let $\mathbb{F}_2^n = \{(x_1, x_2, \ldots, x_n) : x_i \in \mathbb{F}_2, 1 \leq i \leq n\}$ be the vector space of dimension n over $\mathbb{F}_2$. For any $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$, we define the vector space addition as $\mathbf{x} \oplus \mathbf{y} = (x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_n \oplus y_n)$ and the inner product as $\mathbf{x} \cdot \mathbf{y} = x_1y_1 \oplus x_2y_2 \oplus \cdots \oplus x_ny_n$. Any function f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is said to be a Boolean function in n variables. The set of all n-variable Boolean functions is denoted by $\mathcal{B}_n$. Any function $f \in \mathcal{B}_n$ can be represented in a unique way as

$$f(x_1, x_2, \ldots, x_n) = \bigoplus_{\mathbf{a}=(a_1,\ldots,a_n)\in\mathbb{F}_2^n} \lambda_{\mathbf{a}}\Big(\prod_{i=1}^{n} x_i^{a_i}\Big),$$

where $\lambda_{\mathbf{a}} \in \mathbb{F}_2$ and $x_1, \ldots, x_n \in \mathbb{F}_2$. This polynomial form is said to be the algebraic normal form (ANF) of $f \in \mathcal{B}_n$. The Hamming weight of $\mathbf{x} \in \mathbb{F}_2^n$, $wt(\mathbf{x})$, is defined as $wt(\mathbf{x}) = \sum_{i=1}^{n} x_i$ where the sum is over the ring of integers. The algebraic degree of $f \in \mathcal{B}_n$, $\deg(f)$, is defined as $\deg(f) = \max_{\mathbf{a}\in\mathbb{F}_2^n}\{wt(\mathbf{a}) : \lambda_{\mathbf{a}} \neq 0\}$. Let $E_k = \{\mathbf{x} \in \mathbb{F}_2^n : wt(\mathbf{x}) = k\}$, $k \in \{0, 1, \ldots, n\}$. Notice that the cardinality of E_k is equal to the cardinality of E_{n-k}, i.e., $|E_k| = |E_{n-k}|$ and $\mathbb{F}_2^n = \cup_{k=0}^{n} E_k$.

The *Walsh–Hadamard transform* of $f \in \mathcal{B}_n$ at $\mathbf{a} \in \mathbb{F}_2^n$, denoted by $W_f(\mathbf{a})$, is defined by

$$W_f(\mathbf{a}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus\mathbf{a}\cdot\mathbf{x}}.$$

The multiset $[W_f(\mathbf{a}) : \mathbf{a} \in \mathbb{F}_2^n]$ is said to be the *Walsh–Hadamard spectrum* of f. Let n be an even positive integer. A function $f \in \mathcal{B}_n$ is said to be bent if and only if $W_f(\mathbf{a}) = \pm 2^{\frac{n}{2}}$, for all $\mathbf{a} \in \mathbb{F}_2^n$. Alternatively, f is bent if and only if

$$\sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{a})} = 0, \text{ for all non-zero } \mathbf{a} \in \mathbb{F}_2^n.$$

The *nega-Hadamard transform* of $f \in \mathbb{F}_2^n$ at $\mathbf{a} \in \mathbb{F}_2^n$, denoted by $\mathcal{N}_f(\mathbf{a})$, is defined by

$$\mathcal{N}_f(\mathbf{a}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus\mathbf{a}\cdot\mathbf{x}} \imath^{wt(\mathbf{x})},$$

where $\imath^2 = -1$. The multiset $[\mathcal{N}_f(\mathbf{a}) : \mathbf{a} \in \mathbb{F}_2^n]$ is said to be the *nega-Hadamard spectrum* of f. An n-variable function f is said to be negabent if the modulus of the complex number $\mathcal{N}_f(\mathbf{a})$ is $|\mathcal{N}_f(\mathbf{a})| = 2^{\frac{n}{2}}$, for all $\mathbf{a} \in \mathbb{F}_2^n$. For an even number of variables, a bent function $f \in \mathcal{B}_n$ is said to be bent–negabent if f is negabent.

Now we describe the rotation symmetric Boolean functions. Let $x_j \in \mathbb{F}_2$ for $j \in \{1, 2, \ldots, n\}$. We define

$$\rho_n^k(x_j) = x_{(j+k) \bmod n} = \begin{cases} x_{j+k}, & \text{if } j + k \leq n; \\ x_{j+k-n}, & \text{if } j + k > n. \end{cases}$$

Let $C_n = \{\rho_n^1, \rho_n^2, \ldots, \rho_n^n\}$ be the permutation group which contains the rotations of n symbols, defined as

$$\rho_n^i(\mathbf{x}) = \rho_n^i(x_1, x_2, \ldots, x_n) = (x_{(1+i) \bmod n}, x_{(2+i) \bmod n}, \ldots, x_{(n+i) \bmod n}). \tag{1}$$

Definition 1. An n-variable Boolean function f is said to be rotation symmetric if and only if for any $\mathbf{x} \in \mathbb{F}_2^n$,

$$f(\rho_n^k(\mathbf{x})) = f(\mathbf{x}), \quad \text{for all } k \in \{1, 2, \ldots, n\}.$$

Please cite this article in press as: B. Mandal, et al., On non-existence of bent–negabent rotation symmetric Boolean functions, Discrete Applied Mathematics (2017), https://doi.org/10.1016/j.dam.2017.11.001.