Finite Fields and Their Applications 46 (2017) 163–178

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Bent and bent$_4$ spectra of Boolean functions over finite fields

Nurdagül Anbar [a,c,*], Wilfried Meidl [b,c]

[a] Technical University of Denmark, Matematiktorvet, Building 303B, DK-2800, Lyngby, Denmark

[b] Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenbergerstrasse 69, 4040-Linz, Austria

[c] Otto-von-Guericke University Magdeburg, Universitätsplatz 2, 39106 Magdeburg, Germany

ARTICLE INFO

Article history:
Received 17 November 2016
Received in revised form 11 March 2017
Accepted 23 March 2017
Available online xxxx
Communicated by Pascale Charpin

MSC:
06E30
11T06
05B10

Keywords:
Bent function
Negabent function
Bent$_4$
Boolean function
Walsh transform
Quadratic functions

ABSTRACT

For $c \in \mathbb{F}_{2^n}$, a c-bent$_4$ function f from the finite field $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is a function with a flat spectrum with respect to the unitary transform $\mathcal{V}_f^c$, which is designed to describe the component functions of modified planar functions. For $c = 0$ the transform $\mathcal{V}_f^c$ reduces to the conventional Walsh transform, and hence a 0-bent$_4$ function is bent. In this article we generalize the concept of partially bent functions to the transforms $\mathcal{V}_f^c$. We show that every quadratic function is partially bent, and hence it is plateaued with respect to any of the transforms $\mathcal{V}_f^c$. In detail we analyse two quadratic monomials. The first has values as small as possible in its spectra with respect to all transforms $\mathcal{V}_f^c$, and the second has a flat spectrum for a large number of c. Moreover, we show that every quadratic function is c-bent$_4$ for at least three distinct c. In the last part we analyse a cubic monomial. We show that it is c-bent$_4$ only for $c = 1$, the function is then called negabent, which shows that non-quadratic functions exhibit a different behaviour.

* Corresponding author.
E-mail addresses: nurdagulanbar2@gmail.com (N. Anbar), meidlwilfried@gmail.com (W. Meidl).

http://dx.doi.org/10.1016/j.ffa.2017.03.008
1071-5797/

1. Introduction

Let f be a function from the finite field $\mathbb{F}_{2^n}$ to its prime field $\mathbb{F}_2$. For an element $c \in \mathbb{F}_{2^n}$, in [1] the unitary transform $\mathcal{V}_f^c$ has been defined as the complex valued function

$$\mathcal{V}_f^c(u) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+\sigma(c,x)} i^{\mathrm{Tr_n}(cx)} (-1)^{\mathrm{Tr_n}(ux)} ,$$

where $i = \sqrt{-1}$, the function $\mathrm{Tr_n}(z)$ denotes the absolute trace of $z \in \mathbb{F}_{2^n}$ and $\sigma(c,x)$ is the Boolean function defined by

$$\sigma(c,x) = \sum_{0\le i<j\le n-1} (cx)^{2^i}(cx)^{2^j} .$$

For $c = 0$, the transform $\mathcal{V}_f^c$ reduces to the conventional Walsh–Hadamard transform

$$\mathcal{V}_f^0(u) = \mathcal{W}_f(u) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr_n}(ux)} .$$

If for some $c \in \mathbb{F}_{2^n}$ we have $|\mathcal{V}_f^c(u)| = 2^{n/2}$ for all $u \in \mathbb{F}_{2^n}$, then we call f a *c-bent$_4$* function. If $c = 0$, then f is a conventional bent function, and a function that satisfies $|\mathcal{V}_f^c(u)| = 2^{n/2}$ for $c = 1$ we call *negabent*. Alternatively, f is c-bent$_4$ if and only if

$$f(x+a) + f(x) + \mathrm{Tr_n}(c^2ax) \tag{1}$$

is balanced for all nonzero $a \in \mathbb{F}_{2^n}$, see [1]. For $c = 0$ we get the alternative definition of bent functions via the derivative, for $c = 1$, Equation (1) has been used in [8] to define negabent functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Recall that a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is called *plateaued* (or also s-plateaued) if $|\mathcal{W}_f(u)| \in \{0, 2^{(n+s)/2}\}$ for some (fixed) integer s (depending only on f). When n is odd and $s = 1$, or n is even and $s = 2$, the function f is also called *semi-bent*. Note that for $c \ne 0$ the value $\mathcal{V}_f^c$ does not have to be integer-valued. In accordance with the above notations, we call f an s-plateaued function with respect to the transform $\mathcal{V}_f^c$ if $|\mathcal{V}_f^c(u)| \in \{0, 2^{(n+s)/2}\}$ for some (fixed) integer s (only depending on f).

The terms bent$_4$ and negabent have been used before for Boolean functions in multivariate form with similar properties, see [4,6,7,9,11,12]. However the multivariate bent$_4$ functions are not obtained by representing univariate bent$_4$ functions in multivariate form (by fixing a basis). For instance, every univariate affine function is c-bent$_4$ for every nonzero c, whereas a multivariate affine function is not c-bent$_4$ for any c different from $(1, 1, \dots, 1)$, see [1] for the details. Hence univariate bent$_4$ functions have to be dealt separately.

The motivation for defining bent$_4$ functions over finite fields with the transforms $\mathcal{V}_f^c$ respectively with Equation (1) comes from modified planar functions, which were recently introduced in [14] as functions F on $\mathbb{F}_{2^n}$ for which