Finite Fields and Their Applications 47 (2017) 94–124

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Bent functions and line ovals

Kanat Abdukhalikov [1]

Department of Mathematical Sciences, UAE University, PO Box 15551, Al Ain, United Arab Emirates

ARTICLE INFO

Article history:
Received 13 September 2016
Received in revised form 7 April 2017
Accepted 18 June 2017
Available online xxxx
Communicated by Pascale Charpin

MSC:
51E15
51E21
51E23
12K10
94A60

Keywords:
Spreads
Ovals
Line ovals
Quasifields
Semifields
Bent functions
Niho bent functions

ABSTRACT

In this paper we study those bent functions which are linear on elements of spreads, their connections with ovals and line ovals, and we give descriptions of their dual bent functions. In particular, we give a geometric characterization of Niho bent functions and of their duals, we give explicit formula for the dual bent function and present direct connections with ovals and line ovals. We also show that bent functions which are linear on elements of inequivalent spreads can be EA-equivalent.

E-mail address: abdukhalik@uaeu.ac.ae.

[1] This work was supported by UAEU grant 31S107.

http://dx.doi.org/10.1016/j.ffa.2017.06.002
1071-5797/

1. Introduction

Bent functions were introduced by Rothaus [33] and then they were studied by Dillon [16] as Hadamard difference sets. A bent function is a Boolean function with an even number of variables which achieves the maximum possible distance from affine functions [7]. Bent functions have relations to coding theory, cryptography, sequences, combinatorics and designs theory [1,7,10].

Dillon [16] introduced bent functions related to partial spreads of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. He constructed bent functions that are constant on the elements of a spread. Dillon also studied a class of bent functions that are linear on the elements of a Desarguesian spread. These functions were throughly studied in [5,6,8,20,17,28] as Niho bent functions. In [2, 9,11,31] these investigations were extended to other types of spreads, and bent functions which are affine on the elements of spreads, were studied.

In this paper we study bent functions which are linear on the elements of spreads and give geometric interpretations of their duals. Carlet and Mesnager showed [8] that any bent function which are linear on the elements of a Desarguesian spread (they are equivalent to Niho bent functions in a bivariate form) determines an o-polynomial (oval polynomial) from finite geometry. Every o-polynomial defines an equivalence class of hyperovals, therefore Carlet and Mesnager revealed a general connection between Niho bent functions and hyperovals in Desarguesian spreads. But there are several inequivalent bent functions for each o-polynomial. We make result of Carlet and Mesnager more precise and show that bent functions linear on elements of a Desarguesian spread are in one-to-one correspondence with line ovals in an affine plane. Points of the line oval completely define the dual bent function. More precisely, the zeros of the dual function of a Niho bent function are exactly the points of the line oval (in other words, the dual function of a Niho bent function is obtained from the characteristic function of the set of points of the line oval by adding all-one constant function). Therefore, we have geometric characterization of Niho bent functions and of their duals. In addition, starting from that line ovals one can construct ovals, but in general they will be in a projective plane, not affine plane. So every Niho bent function uniquely defines a line oval in an affine plane, and conversely, every line oval in an affine plane uniquely defines a Niho bent function. Similarly, each Niho bent function uniquely defines an oval (in general, in a projective plane) with a special property and conversely, such an oval uniquely determines a Niho bent function. Hence, from known Niho bent functions one can get new compact representations of ovals, and conversely from known representations of ovals one can get new examples of Niho bent functions. In particular, Subiaco and Adelaide hyperovals can be written in a very compact way, contrary to the complicated representation when they are written with the help of o-polynomials (Subiaco and Adelaide hyperovals have very complicated o-polynomials). In addition, our investigations allow us to address an open question on duals of Niho bent functions and give explicit straightforward formula for the dual function of any Niho bent function. We also discuss a question on EA-equivalence