Available online at www.sciencedirect.com
SCIENCE DIRECT
Discrete Applied Mathematics 154 (2006) 202–218
DISCRETE APPLIED MATHEMATICS
www.elsevier.com/locate/dam

Finding nonnormal bent functions

Anne Canteaut[a], Magnus Daum[b], Hans Dobbertin[b], Gregor Leander[b]

[a] *INRIA-Projet CODES, BP 105, 78153 Le Chesnay Cedex, France*
[b] *Ruhr-University Bochum, Postfach 102148, 44780 Bochum, Germany*

Received 12 September 2003; received in revised form 27 April 2004; accepted 21 March 2005
Available online 21 September 2005

Abstract

The question if there exist nonnormal bent functions was an open question for several years. A Boolean function in n variables is called normal if there exists an affine subspace of dimension $n/2$ on which the function is constant. In this paper we give the first nonnormal bent function and even an example for a nonweakly normal bent function. These examples belong to a class of bent functions found in [J.F. Dillon, H. Dobbertin, New cyclic difference sets with Singer parameters, in: Finite Fields and Applications, to appear], namely the Kasami functions. We furthermore give a construction which extends these examples to higher dimensions. Additionally, we present a very efficient algorithm that was used to verify the nonnormality of these functions.

Keywords: Algorithm; Boolean function; Bent function; Normal function

1. Introduction

In cryptography, Boolean functions are used in many different areas, the probably most important being the design of S-Boxes for symmetric encryption. The main *complexity characteristics* for Boolean functions on $\mathbb{F}_2^n$ which are relevant to cryptography are the algebraic degree and the nonlinearity. But other criteria have also been studied. One of them is the question if there exists a space of dimension $n/2$ such that the restriction of a given function is constant (resp. affine) on this space. We call the functions for which such a space exists normal (resp. weakly normal). The notion of normality has been introduced for the first time in [7]. This notion was used to construct balanced functions with high nonlinearities. This construction relies on the fact that if a bent function f is constant on an $(n/2)$-dimensional affine subspace, then f is balanced on each of the other cosets of this affine subspace [2]. Since that time the question if there exist nonnormal bent functions was open. For arbitrary Boolean functions, an easy counting argument shows that there must exist nonnormal functions of n variables for $n \geqslant 10$. It was even shown in [7] that, for increasing dimension, nearly all functions are nonnormal. Asymptotically, there exist Boolean functions of n variables which are not affine on any $\alpha \log_2(n)$-dimensional affine subspace for every $\alpha > 1$ (see [3]). But the question if there exist nonnormal bent functions was an open problem. For a survey on normal Boolean functions see [4].

The question of normality can be generalized to the following combinatorial problem. Given a set of bent functions $\mathscr{B}$, determine the maximal dimension $d(\mathscr{B})$ such that for all functions $f \in \mathscr{B}$ there exists a affine subspace U of dimension $d(\mathscr{B})$ such that f is constant on U.

E-mail address: gregor.leander@rub.de (G. Leander).

0166-218X/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.dam.2005.03.027

Throughout the paper $n = 2m$ be an even number. We recall some definitions:

Definition 1. A *flat* of dimension t is a t-dimensional affine subspace.

Definition 2. Given a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, the function

$$a \in \mathbb{F}_2^n \mapsto f^w(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\langle a,x\rangle}$$

is called the *Walsh transform* of f. Moreover, the $f^w(a)$, $a \in \mathbb{F}_2^n$ are called the Walsh coefficients of f.

Definition 3. A function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called *bent* if for all $a \in \mathbb{F}_2^n$ with $a \neq 0$ the following equation holds:

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+f(x+a)} = 0.$$

This property is equivalent to the fact that all the Walsh coefficients are equal to $\pm 2^m$.

Definition 4. The dual function $\tilde{f}$ of a bent function f of $2m$ variables is the Boolean function defined by

$$f^w(a) = (-1)^{\tilde{f}(a)} 2^m.$$

The dual of a bent function is also bent.

Definition 5. A function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called *normal* if there exists a flat of dimension m such that f is constant on this flat.

As bentness is invariant under addition of affine functions it is natural to consider a generalization of Definition 5.

Definition 6. A function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called *weakly normal* if there exists a flat of dimension m such that the restriction of f to this flat is affine.

A function f is weakly normal if and only if there exists an element $a \in \mathbb{F}_2^n$ such that $f(x) + \langle a, x\rangle$ is normal.

The Hamming weight of a bent function f is $\sum_{x \in \mathbb{F}_2^n} f(x) = 2^{n-1} - (-1)^{\tilde{f}(0)} 2^{m-1}$. It is known that if a bent function is normal with respect to a flat U then it is balanced on all cosets of U. This implies that, if f is constant on a flat of dimension m, the value of the corresponding constant is $\tilde{f}(0)$.

The following section investigates all known families of bent functions and their normality. We prove that most functions in the main classes of bent functions (the Maiorana–McFarland class, the partial spread class and the class $\mathcal{N}$) are normal. We also prove the normality of some modified Maiorana–McFarland bent functions. In Section 3 we present the first nonnormal bent function and even a nonweakly normal bent function. As normality is defined via the *existence* of a flat fulfilling certain criteria, it is very hard to check this property, both in theory and with an algorithm. In order to decide normality of Boolean functions, we present in Section 4 an algorithm which is much faster than a naive approach would be. Finally, Section 5 contains some further applications for this algorithm.

2. Normality of the known families of bent functions

2.1. Direct constructions

Amongst all known constructions for bent functions, there exist three families which can be directly constructed (i.e., which are not derived from other bent functions): the Maiorana–McFarland class, the partial spread class and the class $\mathcal{N}$ which was introduced by Dobbertin [7].

Maiorana–McFarland functions