Available online at www.sciencedirect.com

ScienceDirect

Mathematics and Computers in Simulation 143 (2018) 57–64

MATHEMATICS AND COMPUTERS IN SIMULATION

www.elsevier.com/locate/matcom

Original articles

A secondary construction of bent functions, octal gbent functions and their duals

Wilfried Meidl

Austrian Academy of Sciences, Altenbergerstrasse 69, 4040-Linz, Austria

Received 4 January 2016; received in revised form 8 February 2016; accepted 15 February 2016
Available online 7 March 2016

Abstract

We observe that every octal gbent function in even dimension is essentially equivalent to a bent function obtained with Carlet's secondary construction of bent functions from three bent functions with certain properties. We use this strong connection to completely describe octal gbent functions in even dimension and their duals. This is also the first comprehensive treatment of duality for gbent functions. Implementations of this construction of bent functions also enable us to construct infinite classes of octal gbent functions and their duals. We present some examples.

Keywords: Bent function; Gbent function; Duality; Boolean function; Walsh–Hadamard transform; Sequence generation

1. Introduction

Let $\mathbb{V}_n$ be an n-dimensional vector space over $\mathbb{F}_2$. For a Boolean function f from $\mathbb{V}_n$ to $\mathbb{F}_2$ the *Walsh–Hadamard transform* is the complex valued function

$$\mathcal{W}_f(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{V}_n} (-1)^{f(\mathbf{x})}(-1)^{\langle\mathbf{u},\mathbf{x}\rangle},$$

where $\langle , \rangle$ denotes a nondegenerate inner product on $\mathbb{V}_n$. If $\mathbb{V}_n$ is $\mathbb{F}_2^n$, we can take the dot product $\mathbf{u}\cdot\mathbf{x}$ for $\langle\mathbf{u},\mathbf{x}\rangle$, the standard inner product for $\mathbb{V}_n = \mathbb{F}_{2^n}$ is $\langle\mathbf{u},\mathbf{x}\rangle = \mathrm{Tr}_n(\mathbf{ux})$, where $\mathrm{Tr}_n(\mathbf{z})$ denotes the absolute trace of $\mathbf{z}\in\mathbb{F}_{2^n}$. A function f for which $|\mathcal{W}_f(\mathbf{u})| = 2^{n/2}$ for all $\mathbf{u}\in\mathbb{V}_n$ is called a *bent* function [4,12]. Obviously bent functions only exist if n is even, and then $\mathcal{W}_f(\mathbf{u}) = 2^{n/2}(-1)^{f^*(\mathbf{x})}$ for a Boolean function $f^*(\mathbf{x})$, called the *dual* of f. As is well known, the dual f^* is also a bent function.

For an integer q let $\mathbb{Z}_q$ be the ring of integers modulo q. For a *generalized Boolean function* f from $\mathbb{V}_n$ to $\mathbb{Z}_{2^k}$, $k\ge 1$, the *generalized Walsh–Hadamard transform* is the complex valued function

$$\mathcal{H}_f^{(k)}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{V}_n} \zeta_{2^k}^{f(\mathbf{x})}(-1)^{\langle\mathbf{u},\mathbf{x}\rangle}, \quad \zeta_{2^k} = e^{\frac{2\pi i}{2^k}}.$$

E-mail address: meidlwilfried@gmail.com.

http://dx.doi.org/10.1016/j.matcom.2016.02.003
0378-4754/

Note that $\mathcal{H}_f^{(1)}(\mathbf{u}) = \mathcal{W}_f(\mathbf{u})$. We shall use ζ, respectively, $\mathcal{H}_f$, instead of ζ_{2^k}, respectively, $\mathcal{H}_f^{(k)}$, when k is fixed. If we identify $\mathbb{V}_n$ with $\mathbb{F}_{2^n}$, we will write z rather than $\mathbf{z}$ for elements in $\mathbb{F}_{2^n} = \mathbb{V}_n$. We denote the set of all generalized Boolean functions from $\mathbb{V}_n$ to $\mathbb{Z}_{2^k}$ by $\mathcal{GB}_n^{2^k}$ and when $k = 1$, by $\mathcal{B}_n$. A function $f \in \mathcal{GB}_n^{2^k}$ is called *generalized bent* (*gbent*) if $|\mathcal{H}_f(\mathbf{u})| = 2^{n/2}$ for all $\mathbf{u} \in \mathbb{V}_n$. Differently to the case $k = 1$, gbent functions also exist for odd n when $k > 1$. As shown in [6], if f is gbent (and $k \neq 2$ if n is odd), then for every $\mathbf{u} \in \mathbb{V}_n$, we have $\mathcal{H}_f(\mathbf{u}) = 2^{n/2}\zeta_{2^k}^{f^*(\mathbf{u})}$ for some $f^* \in \mathcal{GB}_n^{2^k}$, which is again gbent, see [7]. In consistence with the case $k = 1$, we may call f^* the dual of f.

Bent functions can be used to construct families of binary sequences with pairwise low crosscorrelation, see [11], which has applications in code-division multiple access (CDMA) systems. Attaining highest possible nonlinearity, bent functions play a fundamental role in applications in cryptography, for instance in S-Boxes in block ciphers, or as components for constructing nonlinear Boolean functions in the design of pseudorandom sequences for stream ciphers. For background on Boolean functions in cryptography we refer to [3,10].

Generalized bent functions were introduced in [13] in connection with CDMA systems, and several constructions of quaternary gbent functions were exploited in connection with algebraic codes over $\mathbb{Z}_4$, to design families of quaternary constant-amplitude codes for multicode CDMA systems. Since then one can observe an increasing interest in gbent functions, see [5,8,14,15].

We start recalling some preliminary results in Section 2. In Section 3, after describing the dual of a gbent function in $\mathcal{GB}_n^4$, n even, we reveal a close connection between a secondary construction of bent functions in [2] and octal gbent functions in even dimension n. We use this connection to completely describe gbent functions in $\mathcal{GB}_n^8$, n even, and their duals. Finally we present some infinite classes of gbent functions employing the analysis of the construction of bent functions in [2] by Mesnager in [9]. We close this article with some perspectives in Section 4.

2. Preliminaries

Henceforth we write $\oplus$ for the addition modulo 2 respectively the addition in $\mathbb{F}_2$, and $+$ for the addition in $\mathbb{C}$, V_n, $\mathbb{Z}_q$, $q > 2$. Let f be a function from V_n to $\mathbb{Z}_{2^k}$ given as

$$f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x}) + \cdots + 2^{k-1}a_{k-1}(\mathbf{x}), \quad a_i \in \mathcal{B}_n,\ 0 \le i \le k-1.$$

As one may expect, one can show relations between the generalized Walsh–Hadamard transform of f and the Walsh–Hadamard transforms of the associated Boolean functions. The following lemma is Lemma 3.1 in [14] and Lemma 17 in [15].

Lemma 1. *The following statements are true:*

(i) *Let $f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x}) \in \mathcal{GB}_n^4$ with $a_0, a_1 \in \mathcal{B}_n$. The generalized Walsh–Hadamard transform of f is given by*

$$2\mathcal{H}_f^{(4)}(\mathbf{u}) = \left(\mathcal{W}_{a_1}(\mathbf{u}) + \mathcal{W}_{a_0\oplus a_1}(\mathbf{u})\right) + i\left(\mathcal{W}_{a_1}(\mathbf{u}) - \mathcal{W}_{a_0\oplus a_1}(\mathbf{u})\right).$$

(ii) *Let $f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x}) + 4a_2(\mathbf{x}) \in \mathcal{GB}_n^8$ with $a_0, a_1, a_2 \in \mathcal{B}_n$. The generalized Walsh–Hadamard transform of f is given by*

$$4\mathcal{H}_f^{(8)}(\mathbf{u}) = \alpha_0\mathcal{W}_{a_2}(\mathbf{u}) + \alpha_1\mathcal{W}_{a_0\oplus a_2}(\mathbf{u}) + \alpha_2\mathcal{W}_{a_1\oplus a_2}(\mathbf{u}) + \alpha_{12}\mathcal{W}_{a_0\oplus a_1\oplus a_2}(\mathbf{u}),$$

where $\alpha_0 = 1 + (1+\sqrt{2})i$, $\alpha_1 = 1 + (1-\sqrt{2})i$, $\alpha_2 = 1 + \sqrt{2} - i$, $\alpha_{12} = 1 - \sqrt{2} - i$.

Whether f is gbent or not is hence strongly related to properties of the Walsh–Hadamard transforms of the associated Boolean functions.

Proposition 1. *Let n be an even integer.*

(i) [14, *Theorem 32*] *The function $f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x})$ in $\mathcal{GB}_n^4$ is gbent if and only if a_1 and $a_0 \oplus a_1$ are bent.*

(ii) [15, *Theorem 19*] *The function $f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x}) + 4a_2(\mathbf{x})$ in $\mathcal{GB}_n^8$ is gbent if and only if a_2, $a_0 \oplus a_2$, $a_1 \oplus a_2$ and $a_0 \oplus a_1 \oplus a_2$ are bent functions, and $\mathcal{W}_{a_0\oplus a_2}(\mathbf{u})\mathcal{W}_{a_1\oplus a_2}(\mathbf{u}) = \mathcal{W}_{a_2}(\mathbf{u})\mathcal{W}_{a_0\oplus a_1\oplus a_2}(\mathbf{u})$ for all $\mathbf{u} \in V_n$.*