Discrete Applied Mathematics 238 (2018) 14–23

Contents lists available at ScienceDirect

Discrete Applied Mathematics

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

# Construction methods for generalized bent functions

S. Hodžić [a,*], E. Pasalic [b]

[a] University of Primorska, FAMNIT, Glagoljaska 6, 6000 Koper, Slovenia
[b] University of Primorska, FAMNIT & IAM, Glagoljaska 6, 6000 Koper, Slovenia

ARTICLE INFO

*Article history:*
Received 24 March 2017
Received in revised form 23 November 2017
Accepted 27 November 2017
Available online 19 December 2017

*Keywords:*
Generalized bent functions
Walsh–Hadamard transform
(Generalized) Maiorana–McFarland class
Gray maps

ABSTRACT

Generalized bent (gbent) functions is a class of functions $f : \mathbb{Z}_2^n \to \mathbb{Z}_q$, where $q \geq 2$ is a positive integer, that generalizes a concept of classical bent functions through their co-domain extension. A lot of research has recently been devoted towards derivation of the necessary and sufficient conditions when $f$ is represented as a collection of Boolean functions. Nevertheless, apart from the necessary conditions that these component functions are bent when $n$ is even (respectively semi-bent when $n$ is odd), no general construction method has been proposed yet for $n$ odd case. In this article, based on the use of the well-known Maiorana–McFarland (MM) class of functions, we give an explicit construction method of gbent functions, for any even $q > 2$ when $n$ is even and for any $q$ of the form $q = 2^r$ (for $r > 1$) when $n$ is odd. Thus, a long-term open problem of providing a general construction method of gbent functions, for odd $n$, has been solved. The method for odd $n$ employs a large class of disjoint spectra semi-bent functions with certain additional properties which may be useful in other cryptographic applications.

## 1. Introduction

A generalization of Boolean functions was introduced in [6] for considering a much larger class of mappings from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$ which naturally induced generalized concepts of the well known class of *bent Boolean functions* introduced by Rothaus [12]. Nevertheless, due to a more natural connection to cyclic codes over rings, functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_q$, where $q \geq 2$ is a positive integer, have drawn even more attention [15]. This class of mappings $\mathbb{Z}_2^n$ to $\mathbb{Z}_q$ will be called *generalized Boolean functions* throughout this article and in particular its subclass possessing similar properties as standard bent functions will be named *generalized bent (gbent) functions*. The relations between generalized bent functions, constant amplitude codes and $\mathbb{Z}_4$-linear codes ($q = 4$) were studied in [15]. There are also other generalizations of bent functions such as bent functions over finite Abelian groups for instance [19]. A nice survey on different generalizations of bent functions can be found in [23].

There are several reasons for studying generalized bent functions. In the first place there is a close connection of these objects to classical bent functions when $n$ is even. Indeed, using a suitable representation of $f : \mathbb{Z}_2^n \to \mathbb{Z}_q$ as a collection of its component Boolean functions (whose number depends on 2-adic representation of $q$), it turns out that the necessary condition for these component functions is that some of their linear combinations are bent if $f$ is supposed to be gbent. The quaternary $q = 4$ and octal case $q = 8$ were investigated in [18] and [20], respectively. Also, in many other recent works [16,17,21] the authors mainly considered the case $q = 2^h$ and the bent properties of the component functions for a given prescribed form of a gbent function. On the other hand, when $n$ is odd and $q = 2^h$, the necessary (but not sufficient)

[*] Corresponding author.
*E-mail addresses:* samir.hodzic@famnit.upr.si (S. Hodžić), enes.pasalic@upr.si (E. Pasalic).

https://doi.org/10.1016/j.dam.2017.11.027

condition that $f$ is gbent is that some linear combinations of the component functions are semi-bent Boolean functions with the three valued Walsh spectra $\{0, \pm 2^{\frac{n+1}{2}}\}$.

The main reason, from an applicative point of view, for the interest in these objects is a close relationship between certain objects used in the design of orthogonal frequency-division multiplexing (OFDM) modulation technique, which in certain cases suffers from relatively high peak-to-mean envelope power ratio (PMEPR), and gbent functions. To overcome the issues of having large PMEPR, the $q$-ary sequences lying in complementary pairs [2] (also called Golay sequences) having a low PMEPR can be easily determined from the gbent function associated with this sequence, see [14] and the references therein. Another motivation for studying these objects comes from the fact that Gray maps of gbent functions are plateaued functions, see [3, Propositions 6-7]. The possibility of obtaining plateaued functions from gbent functions through Gray maps has an independent cryptographic significance. Thus, a generic construction of gbent functions also provides a generic method for designing plateaued functions by using the results in [3].

As mentioned above, general construction methods of gbent functions are not known apart from a few special cases for some particular (small) valued $q$. When $q = 4$ and $n$ is even, from [18] we have that a function $f : \mathbb{Z}_2^n \to \mathbb{Z}_4$, given in the form $f(x) = a_0(x) + 2a_1(x)$, is gbent if and only if $a_1$ and $a_1 \oplus a_0$ are Boolean bent functions. Several other results related to the case $q = 4$ and $n$ even are given in [15], where some of them involve the trace forms of Galois rings whose employment is also discussed in [24]. For the octal case $q = 8$ both necessary and sufficient conditions for the component functions of $f : \mathbb{Z}_2^n \to \mathbb{Z}_8$, representing uniquely $f$ as $f(x) = a_0(x) + 2a_1(x) + 2^2a_2(x)$ where $a_0, a_1, a_2$ are Boolean functions, were given in [21]. Some recent results on gbent functions related to the case $q = 8$ can be found in [20,10]. Once again, it is necessary (but not sufficient) that certain linear combinations of these Boolean functions are bent when $n$ is even, respectively semi-bent when $n$ is odd. In addition, the Walsh spectra of these functions must satisfy certain conditions related to Hadamard matrices which make the design methods rather involved, cf. Theorem 1.

Several other more general classes of gbent functions were described in [21], such as generalized Maiorana–McFarland class (GMMF) [21, Theorem 8], generalized Dillon class (GD) [21, Theorem 9], partial spread class (PS) [9] and generalized spread class (GS) [21, Theorem 10]. It has been shown that the GD and GMMF classes are both contained in the GS class [21, Theorem 12]. The construction of these gbent functions was also considered in [17] though from the cross-correlation point of view. Apart from the generic construction method of gbent functions inherent to the GMMF class though only for even $n$, the other classes only provide sufficient gbent conditions which are not easy to satisfy in an efficient manner. Gbent functions of the form $g(x) = \frac{q}{2}a(x) + kb(x)$, $k \in \{\frac{q}{4}, \frac{3q}{4}\}$, $q = 4s$ $(s \in \mathbb{N})$, were analyzed in [4], where it has been shown that certain constructions of gbent functions for $q \in \{4, 8\}$ [17,20,21] belong to this class of functions (see [4, Section 5]). One may notice that many coordinate functions of the function $g$, when $g$ is written in the form (2), are equal to each other or possibly are zero functions. Different from this approach our construction method can generate gbent functions for any even $q$ whose pairwise coordinate functions are different (see Remark 4), which implies that many gbent functions which are not of the form $\frac{q}{2}a(x) + kb(x)$ can be generated.

However, the first general characterization of gbent functions, in terms of the choice of component functions for any even $q$ and regardless of the parity of $n$, was given in [5, Theorem 4.1]. Based on the necessary and sufficient conditions, which are derived in [3], in this article we present the first generic method for construction of gbent functions for any even $q$ when $n$ is even and for $q = 2^r$ when $n$ is odd. The method is based on the use of the Maiorana–McFarland (MM) class of functions which contains both semi-bent and bent functions. Nevertheless, the difficulty lies in the fact that the component functions (more precisely certain linear combinations of them) apart from being bent or semi-bent (depending on the parity of $n$) must satisfy additional constraints. More precisely, when $n$ is odd certain linear combinations of the component functions must be disjoint spectra semi-bent functions and apart from that the signs of their Walsh coefficients are supposed to satisfy certain Hadamard recursion, for more details see Section 3. Therefore, the selection of component functions turns out to be a rather nontrivial task. We efficiently solve this problem by using suitable permutations for deriving disjoint spectra semi-bent functions from the MM class that satisfy the gbent conditions. The question of finding another generic methods for the same purpose is left as an interesting open problem. We emphasize that the case $n$ even which is also briefly discussed is of minor importance (due to the generic method provided through the GMMF class) and the main contribution is a novel and efficient method of satisfying rather demanding gbent conditions when $n$ is odd.

The rest of this article is organized as follows. Some basic definitions and notions related to gbent functions are given in Section 2. In Section 3 we describe the problem of constructing gbent functions in terms of the sufficient conditions imposed on their component functions. A method of deriving disjoint spectra semi-bent functions from the MM class, needed in the design of gbent functions for odd $n$, is given in Section 4, where the case $n$ even is also briefly discussed. In Section 5, we illustrate construction details for $n$ odd case. Some concluding remarks are found in Section 6.

## 2. Preliminaries

The set of all Boolean functions in $n$ variables, that is the mappings from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2$ is denoted by $\mathcal{B}_n$. Especially, the set of affine functions in $n$ variables we define as $\mathcal{A}_n = \{a \cdot x \oplus b \mid a \in \mathbb{Z}_2^n,\ b \in \{0, 1\}\}$, where "·" stands for the standard inner (dot) product of two vectors. A function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is commonly represented using its associated algebraic normal form (ANF) as

$$f(x_1, \ldots, x_n) = \sum_{u \in \mathbb{Z}_2^n} \lambda_u \prod_{i=1}^{n} {x_i}^{u_i}, \tag{1}$$