The Rayleigh quotient of bent functions

Lars Eirik Danielsen[1], Matthew G. Parker[1], and Patrick Solé[2]

[1] The Selmer Center, Department of Informatics, University of Bergen, PB 7803, N-5020 Bergen, Norway
larsed@ii.uib.no, matthew@ii.uib.no
[2] CNRS LTCI, TelecomParisTech, Dept Comelec, Paris, France
patrick.sole@telecom-paristech.fr

Abstract. The Rayleigh quotient of a bent function is an invariant under the action of the orthogonal group, and it measures the distance of the function to its dual. An efficient algorithm is derived that generates all bent functions of given Rayleigh quotient. The Rayleigh quotient of some bent functions obtained by primary (Maiorana McFarland, Dillon) or secondary (direct and indirect sum) constructions is computed.

Keywords: Boolean functions, bent functions, Walsh Hadamard transform, Rayleigh quotient, plateaued functions

1 Introduction

Ever since its introduction by Rothaus, the main problem with the class of Boolean functions known as bent has been the classification. In this article we study a parameter that measures the distance between a function and its dual and this parameter is invariant under the action of the extended orthogonal group, a subgroup of the affine group. We introduced this parameter in [4] and called it the Rayleigh quotient as it is proportional to the Rayleigh quotient (in the sense of numerical analysis) of the matrix of the Walsh Hadamard transform. For a bent function in n variables this quantity in the normalization used here, is an even integer in the range $[-2^n, 2^n]$. It was proved in [4] that a bent function is equal to its dual iff its Rayleigh quotient is 2^n, in which case the function is called *self dual*. Likewise a bent function is the complement of its dual iff its Rayleigh quotient is -2^n, in which case the function is called *anti self dual*. [4] then tabulated the Rayleigh quotient values for all self dual bent Boolean functions in ≤ 6 variables and all quadratic such functions in 8 variables, up to the action of the extended orthogonal group.

This article builds on the results of [4], by tabulating the Rayleigh quotient of all bent Boolean functions of ≤ 6 variables, up to equivalence with respect to the extended orthogonal group, and is organized as follows. Section 2 contains the necessary notation. Section 3 develops the linear algebra needed to study the Rayleigh quotient. Section 4 exploits these ideas to derive an algorithm, more effective than exhaustive search, to construct all bent functions with prescribed Rayleigh quotient - this algorithm is a variant on that used in [4]. Along the

In *Cryptography and Coding*, *Lecture Notes in Comput. Sci.*, volume 5921, pp. 418–432, Springer-Verlag, Berlin, 2009.

way a connection with plateaued functions is pointed out. Section 5 presents computational results, tabulating the Rayleigh quotients of all bent functions up to 6 variables. Section 6 studies some properties and symmetries of the Rayleigh quotient. Section 7 gives evaluations of the Rayleigh quotient for some special constructions of bent functions: Maiorana McFarland and Dillon, as well as for secondary constructions like the direct and indirect sum.

We are not aware of much work in the literature pertaining to the Rayleigh quotient. However, [6] has considered the respective algebraic degree of a Boolean function and its dual. Moreover, the decompositions of bent functions have been studied in [1], where a link is made between the Walsh Hadamard spectra of the restrictions of a function and the decompositions of its dual.

2 Definitions and notation

A *Boolean function* f in n variables is any map from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Its *Walsh Hadamard Transform* (WHT), namely $\hat{F} \in \mathbb{R}^{2^n}$, can be defined as

$$\hat{F}(x) := \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y)+x\cdot y},$$

where $x \cdot y$ denotes the dot product of x with y. The *sign function* of f is defined by $F := (-1)^f$. The Boolean function, f, is said to be *bent* iff $|\hat{F}(x)| = 2^{n/2}$, $\forall x$, which is only possible if n is even. If f is bent then its *dual* with respect to the WHT, $\tilde{f}$, is also a bent Boolean function. Let $\tilde{F}$ be the sign function of $\tilde{f}$ for the case that f is bent. Then the duality of $\tilde{f}$ to f is defined by

$$\tilde{F}(x) := 2^{-n/2}\hat{F}(x) \quad \Leftrightarrow \quad (-1)^{\tilde{f}(x)} := 2^{-n/2} \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y)+x\cdot y}, \;\; f \text{ bent}.$$

The matrix of the WHT is the Hadamard matrix H_n of Sylvester type, which we now define by tensor products. Let

$$H := \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Let $H_n := H^{\otimes n}$ be the n-fold tensor product of H with itself. Thus $H_n = H_{n-1} \otimes \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{smallmatrix}\right)$, where $H_1 = H$. Let $\mathcal{H}_n := 2^{-n/2}H_n$, be its normalized version. Recall the Hadamard property

$$H_n H_n^T = 2^n I_{2^n},$$

where we denote by I_M the M by M identity matrix. View F as a vector $F = (F_{0\ldots00}, F_{0\ldots01}, \ldots, F_{1\ldots11}) \in \mathbb{F}_2^n$, whose elements, F_x, are ordered lexicographically in x. Let $\hat{F}$ have a similar vector interpretation. Then we can express the WHT in matrix-vector form as

$$\hat{F} = FH_n.$$

For example, when $n = 2$ and $f(y_1, y_2) = y_1 y_2$, we have $F = (1, 1, 1, -1)$ and

$$\hat{F} = FH_2 = \begin{pmatrix} 1 & 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 2 & -2 \end{pmatrix}.$$

In this case $|\hat{F}_x| = 2$, $\forall x$, so f is bent and its dual is $\tilde{f}(x_1, x_2) = x_1 x_2$, where $\tilde{F} = (-1)^{\tilde{f}} = 2^{-1}\hat{F} = (1, 1, 1, -1)$.

If f is not only bent but, furthermore, $f = \tilde{f}$, then f is *self dual bent* - such is the case for the example just given. This means that the sign function of f is an eigenvector of $\mathcal{H}_n$ attached to the eigenvalue 1. Similarly, if $f = \tilde{f} + 1$ then f is *anti self dual bent*. For example, $f(y_1, y_2) = y_1 y_2 + y_1 + y_2$ is anti self dual bent. This means that its sign function is an eigenvector of $\mathcal{H}_n$ attached to the eigenvalue -1. Define the *Rayleigh quotient* S_f of a Boolean function f in n variables by the character sum

$$S_f := \sum_{x,y \in \mathbb{F}_2^n} (-1)^{f(x)+f(y)+x\cdot y} = \sum_{x \in \mathbb{F}_2^n} F(x)\hat{F}(x).$$

Define the *normalized Rayleigh quotient* N_f of a bent Boolean function f in n variables by the character sum

$$N_f := \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\tilde{f}(x)} = 2^{-n/2} S_f.$$

We see that $N_f = 2^n$ if f is self dual bent and $N_f = -2^n$ if f is anti self dual bent.

3 Linear algebra

We now establish an orthogonal eigen-decomposition of the sign function of a Boolean function and use it to obtain expressions for the Rayleigh quotient of a bent Boolean function in terms of this eigen-decomposition. Recall the following elementary Lemma from [4].

Lemma 1. *The spectrum of $\mathcal{H}_n$ consists of the two eigenvalues ± 1, each with multiplicity 2^{n-1}. A basis of the eigenspace attached to the eigenvalues 1 (resp. -1) is formed from the rows of the $2^{n-1} \times 2^n$ matrix $(H_{n-1} + 2^{n/2} I_{2^{n-1}}, H_{n-1})$ (resp. $(H_{n-1} - 2^{n/2} I_{2^{n-1}}, H_{n-1})$). An orthogonal decomposition of $\mathbb{R}^{2^n}$ in eigenspaces of H_n is*

$$\mathbb{R}^{2^n} = Ker(H_n + 2^{n/2} I_{2^n}) \oplus Ker(H_n - 2^{n/2} I_{2^n}).$$

Proof. The basis characterization follows because

$$\begin{aligned} &(H_{n-1} + 2^{n/2} I_{2^{n-1}}, H_{n-1})\mathcal{H}_n \\ &\quad = (H_{n-1} + 2^{n/2} I_{2^{n-1}}, H_{n-1}) 2^{-n/2} (H_{n-1} \otimes H_1) \\ &\quad = 2^{-n/2} (2H_{n-1} + 2^{n/2} I_{2^{n-1}}, 2^{n/2} I_{2^{n-1}})(H_{n-1} \otimes I_2) \\ &\quad = (2^{n/2} I_{2^{n-1}} + H_{n-1}, H_{n-1}). \end{aligned}$$

Similar arguments show that

$$(H_{n-1} - 2^{n/2} I_{2^{n-1}}, H_{n-1})\mathcal{H}_n = -(H_{n-1} + 2^{n/2} I_{2^{n-1}}, H_{n-1}).$$

The kernel (i.e. nullspace) of $H_n + 2^{n/2} I_{2^n}$ is the row space of a matrix, say M^+, such that $(H_n + 2^{n/2} I_{2^n}) M^+ = 0$. From the above basis characterization we see that one choice is $M^+ = (H_{n-1} - 2^{n/2} I_{2^{n-1}}, H_{n-1})$. Similarly, $Ker(H_n - 2^{n/2} I_{2^n})$ is the row space of $M^- = (H_{n-1} + 2^{n/2} I_{2^{n-1}}, H_{n-1})$. The orthogonal decomposition of $\mathbb{R}^{2^n}$ follows because the two kernels are orthogonal, i.e. because $M^+ M^{-T} = 0$. □

By Lemma 1, the orthogonal decomposition in eigenspaces of H_n yields the following decomposition for the sign function F of a Boolean function, $F = F^+ + F^-$, with $F^\pm \in Ker(H_n \pm 2^{n/2} I_{2^n})$, and $\langle F, F \rangle = \langle F^+, F^+ \rangle + \langle F^-, F^- \rangle$, where $\langle A, B \rangle$ is the inner product of real vectors A and B. By observing that $\hat{F} = 2^{n/2}(F^+ - F^-)$, and that $S_f = \langle F, \hat{F} \rangle$, we obtain

$$N_f = \langle F^+, F^+ \rangle - \langle F^-, F^- \rangle,$$

and by the triangle inequality, $|N_f| \leq 2^n$, with equality if and only if $F = F^+$ or $F = F^-$. If f is bent then the sign function, $\tilde{F}$, of its dual exists, and

$$\tilde{F} = F^+ - F^-.$$

Thus $F \pm \tilde{F} = 2F^\pm$ has entries in $\{0, \pm 2\}$, so both F^+ and F^- have entries in $\{0, \pm 1\}$. Denote by S_+ (resp. S_-) the set of $x \in \mathbb{F}_2^n$ such that $F_x^+ = 0$ (resp. $F_x^- = 0$). Because $F = F^+ + F^-$ has entries in $\{\pm 1\}$, it follows that the sets S_+ and S_- partition $\mathbb{F}_2^n$. Conversely, given a pair of eigenvectors of $\mathcal{H}_n$, F^+ and F^-, with entries in $\{0, \pm 1\}$, and with corresponding sets S_+ and S_-, such that $S_+ \cup S_- = \mathbb{F}_2^n$, then the sum of F^+ and F^- is the sign function of a bent function. In summary

Proposition 1. *Let F be the sign function of a bent Boolean function of n variables. Then there exist two vectors F^+ and F^-, and two subsets, S_+ and S_-, with the following properties.*

1. $F = F^+ + F^-$
2. *F^+ and F^- have entries in $\{0, \pm 1\}$.*
3. *the sets S_+ and S_- partition $\mathbb{F}_2^n$.*
4. *$F_x^\pm = 0$ iff $x \in S_\pm$.*

Conversely, given eigenvectors, $F^\pm$, of $\mathcal{H}_n$, and sets $S_\pm$ with the last three properties, the sum $F^+ + F^-$ is the sign function of a bent function with normalized Rayleigh quotient

$$N_f = |S_-| - |S_+| = 2^n - 2|S_+| = 2|S_-| - 2^n.$$

Moreover, $|S_+| = d_H(f, \tilde{f})$, where $d_H(\,,\,)$ denotes the Hamming distance.

Example: Let $n = 4$ and $f = x_1x_3 + x_2x_3 + x_2x_4 + x_2$. Then $F = (1, 1, 1, 1, -1, 1, 1, -1, 1, 1, -1, -1, -1, 1, -1, 1)$. As f is a bent function it has a dual. By computation, $\tilde{f} = x_1x_3 + x_1x_4 + x_2x_4 + x_4$ and $\tilde{F} = (1, -1, 1, -1, 1, 1, 1, 1, 1, 1, -1, -1, 1, -1, -1, 1)$. It follows that $F^+ = (F + \tilde{F})/2 = (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, -1, -1, 0, 0, -1, 1)$, giving $S_+ = \{0010, 0011, 1000, 1011, 1100, 1110\}$. Therefore the normalized Rayleigh quotient of f is $N_f = 2^n - 2|S_+| = 4$.

4 Search algorithm

We now describe an algorithm where we construct all bent Boolean functions, F, of n variables, given a specified zero set, S_+, for F^+, where $F = F^+ + F^-$. For an arbitrary n-variable function, $A(x_1, x_2, \ldots, x_n)$, with domain $\mathbb{F}_2^n$, let $A_{|_{x_1=0}}$ (resp. $A_{|_{x_1=1}}$) be the restrictions of A to $x_1 = 0$ and $x_1 = 1$ respectively, such that $A(x) = (A_{|_{x_1=0}}, A_{|_{x_1=1}})$.

Let $F^+ := (Y, Z)$, where $Y, Z \in \mathbb{R}^{2^{n-1}}$, such that $Y := F^+_{|_{x_1=0}}$, and $Z := F^+_{|_{x_1=1}}$, i.e. F^+ is the concatenation of Y with Z. Let $S_+ \subset \mathbb{F}_2^n$ similarly be decomposed into S_+^Y and S_+^Z, where

$$S_+^Y := \{s_{|_{x_1=0}} \mid s \in S_+\} \subset \mathbb{F}_2^{n-1}, \qquad S_+^Z := \{s_{|_{x_1=1}} \mid s \in S_+\} \subset \mathbb{F}_2^{n-1}.$$

We want to construct an F^+ with zero set S_+.

Theorem 1. *Let Z have entries in $\{0, \pm 1\}$, with $Z_x = 0$ iff $x \in S_+^Z$. Define $Y := Z + \frac{2H_{n-1}}{2^{n/2}}Z$. If Y has entries in $\{0, \pm 1\}$, with $Y_x = 0$ iff $x \in S_+^Y$, then the vector $F^+ = (Y, Z)$ is in the eigenspace of $\mathcal{H}_n$ attached to 1 with zero set S_+.*

Proof. By Lemma 1, for eigenspace 1, we consider an X such that $F^+ = X(H_{n-1} + 2^{n/2}I_{2^{n-1}}, H_{n-1}) = (Y, Z)$, from which it follows that $Y = Z + \frac{2H_{n-1}}{2^{n/2}}Z$. Moreover, we require that Y and Z both have, by Proposition 1, entries in $\{0, \pm 1\}$. For each arbitrary choice of Z with entries in $\{0, \pm 1\}$, we can then check whether Y has entries in $\{0, \pm 1\}$. □

A similar result holds for F^-, for $F^- := (Y, Z)$, $Y := F^-_{|_{x_1=0}}$ and $Z := F^-_{|_{x_1=1}}$. The proof is analogous and is omitted.

Theorem 2. *Let Z have entries in $\{0, \pm 1\}$, with $Z_x = 0$ iff $x \in S_-^Z$. Define $Y := Z - \frac{2H_{n-1}}{2^{n/2}}Z$. If Y has entries in $\{0, \pm 1\}$, with $Y_x = 0$ iff $x \in S_-^Y$, then the vector $F^- = (Y, Z)$ is in the eigenspace of $\mathcal{H}_n$ attached to -1 with zero set S_-.*

Based on Proposition 1 and the above two theorems we give an algorithm to generate all bent functions with given zero set S_+, and therefore, from Proposition 1, with fixed Rayleigh quotient $2^n - 2|S_+|$.

Algorithm $BWS(n, S_+)$

1. Pick Z with entries in $\{0, \pm 1\}$, and $Z_x = 0$ iff $x \in S_+^Z$

2. Compute all candidate Y as $Y := Z + \frac{2H_{n-1}}{2^{n/2}}Z$.
3. If Y has entries in $\{0, \pm 1\}$ and $Y_x = 0$ iff $x \in S_+^Y$ let $F^+ := (Y, Z)$, else go to next Z.
4. Pick Z with entries in $\{0, \pm 1\}$, and $Z_x = 0$ iff $x \notin S_+^Z$
5. Compute all candidate Y as $Y := Z - \frac{2H_{n-1}}{2^{n/2}}Z$.
6. If Y has entries in $\{0, \pm 1\}$ and $Y_x = 0$ iff $x \notin S_+^Y$ let $F^- := (Y, Z)$, else go to next Z.
7. Output $F = F^+ + F^-$ for all F^+ found in step 3 and all F^- found in step 6.

It should be noted that, compared to brute force exhaustive search of complexity 2^{2^n} this algorithm is of complexity 2^R with $R \leq 2^{n-1}$, depending on the size of S.

We point out a connection with *plateaued functions*. Recall that, according to [9], a Boolean function f in n variables is plateaued of order r if the entries of its WHT, $\hat{F}$, have modulus either zero or $2^{n-r/2}$, where r is even and can range from 0 to n. If $r = n$ then f is bent.

Theorem 3. *Keep the notation of Proposition 1. Write $F^+ = (Y^+, Z^+)$ and $F^- = (Y^-, Z^-)$. If Y^+ and Z^+ (resp. Y^- and Z^-) have the same supports, that is*

$$\{x \mid Y_x^{\pm} = 0\} = \{x \mid Z_x^{\pm} = 0\},$$

then both $Z^+ + Z^-$ and $Z^+ - Z^-$ (resp. $Y^+ + Y^-$ and $Y^+ - Y^-$)are sign functions of plateaued functions of order $n-2$ in $n-1$ variables.

Proof. By Proposition 1 both $Z^+ \pm Z^-$ and $Y^+ \pm Y^-$ have entries in $\{\pm 1\}$ and are thus legitimate sign functions of Boolean functions in $n-1$ variables. By hypothesis, $\frac{Y^+ - Z^+}{2}$ and $\frac{Z^- - Y^-}{2}$ have entries in $\{0, \pm 1\}$. By Proposition 1 their sum and difference still have entries in $\{0, \pm 1\}$. Like in Theorem 1 and 2 we have

$$H_{n-1}Z^+ = 2^{n/2}(\frac{Y^+ - Z^+}{2}) \tag{1}$$

and, symmetrically,

$$H_{n-1}Z^- = 2^{n/2}(\frac{Z^- - Y^-}{2}) \tag{2}$$

The result follows now by adding and subtracting equations 1 and 2. □

Note that this result is different from the construction of bent functions from complementary plateaued functions in [8].

5 Numerical results

In previous work, we have classified self dual bent functions [4]. We here extend this result by calculating the Rayleigh quotient of all bent functions of up to six variables. Tables 1 and 2 list the number of bent functions, where no symmetries

are taken into account, of four and six variables with normalized Rayleigh quotient N_f. Table 3 gives the Rayleigh quotients of all quadratic bent functions of six variables. It follows from Theorem 5 that there will always be the same number of functions with $N_f = -x$ as there are functions with $N_f = x$, so these functions are counted together. (For instance, there are 20 bent functions of four variables with $N_f = 16$, and 20 such functions with $N_f = -16$.)

Table 1: Number of Bent Functions of Four Variables with given Rayleigh Quotient

N_f	Functions
± 16	40
± 8	192
± 4	384
0	280
Total	896

Table 2: Number of Bent Functions of Six Variables with given Rayleigh Quotient

N_f	Functions
± 64	85,792
± 48	814,080
± 40	5,225,472
± 36	10,813,440
± 32	33,686,400
± 28	61,931,520
± 24	159,169,536
± 20	327,155,712
± 16	548,066,304
± 12	865,075,200
± 8	1,194,362,880
± 4	1,434,058,752
0	784,985,440
Total	5,425,430,528

According to Prop. 3, $|N_f| \leq 60$ for a bent function of six variables that is neither self dual nor anti self dual. We observe that no function meeting this bound with equality exists. Up to equivalence, where we consider the functions f and g to be in the same equivalence class if $g(x) = f(Lx + d) + d \cdot x + c$, where $LL^T = I$, $d \in \mathbb{Z}_2^n$, $\mathrm{wt}(d)$ even, and $c \in \mathbb{Z}_2$, there are seven bent functions of six variables with $N_f = 48$. Representatives from each equivalence class are listed below. The functions with $N_f = -48$ can be obtained from Theorem 5 (For a

Table 3: Number of Quadratic Bent Functions of Six Variables with given Rayleigh Quotient

N_f	Functions
± 64	1504
± 32	44,160
± 16	503,808
± 8	737,280
0	490,912
Total	1,777,664

classification of the bent functions of six variables with $|N_f| = 64$, we refer to previous work [4].)

1. $x_1x_2x_6 + x_1x_3x_6 + x_1x_4x_5 + x_1x_3x_5 + x_2x_4x_6 + x_3x_4x_6 + x_2x_4x_5 + x_2x_3x_5 + x_1x_2 + x_1x_5 + x_2x_6 + x_3x_4 + x_3x_6 + x_4x_5 + x_5x_6$
2. $x_2x_4x_6 + x_3x_5x_6 + x_1x_4x_5 + x_1x_2x_3 + x_1x_6 + x_2x_5 + x_2x_6 + x_3x_4 + x_3x_5 + x_3x_6 + x_4x_5 + x_4x_6 + x_5x_6 + x_2 + x_3$
3. $x_2x_3x_4 + x_1x_3x_4 + x_2x_3x_6 + x_2x_3x_5 + x_2x_4x_6 + x_2x_4x_5 + x_2x_5x_6 + x_1x_5x_6 + x_1x_2 + x_3x_5 + x_4x_6 + x_5x_6$
4. $x_1x_2x_3 + x_1x_2x_5 + x_1x_3x_4 + x_1x_4x_5 + x_1x_6 + x_2x_4 + x_2x_6 + x_3x_5 + x_3x_6 + x_4x_6 + x_5x_6 + x_1 + x_2 + x_3$
5. $x_1x_2x_3 + x_1x_4x_5 + x_1x_3x_5 + x_3x_5x_6 + x_1x_6 + x_2x_5 + x_3x_4 + x_3x_6 + x_4x_5 + x_5x_6 + x_1 + x_2 + x_3 + x_4$
6. $x_1x_3x_5 + x_1x_2x_5 + x_1x_3x_4 + x_1x_2x_4 + x_1x_6 + x_2x_5 + x_3x_4 + x_4x_6 + x_5x_6 + x_1 + x_2 + x_4$
7. $x_2x_3x_6 + x_2x_4x_6 + x_3x_5x_6 + x_4x_5x_6 + x_1x_6 + x_2x_3 + x_4x_5$

We have also calculated the Rayleigh quotients of all Boolean functions of four and five variables, listed in Tables 4 and 5. For five variables, the non-normalized values S_f are given, since the values N_f are not integer for odd n.

We observe that for Boolean functions of four variables, the highest value of $|N_f| < 16$ is $|N_f| = 13$. Up to equivalence, the following three functions have $N_f = 13$. (For a classification of the functions of four variables with $|N_f| = 16$, we refer to previous work [4].)

1. $x_1x_2x_3x_4 + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 + x_1$
2. $x_1x_2x_3x_4 + x_1x_2 + x_1x_3 + x_2x_4 + x_3x_4$
3. $x_1x_2x_3x_4 + x_1x_2 + x_3x_4$

For Boolean functions of five variables, the highest obtainable Rayleigh quotient is $|S_f| = 160$. Up to equivalence there are four functions with $S_f = 160$, which are listed below. In general, it is not known what the highest possible value of $|S_f|$ for odd n is.

1. $x_1x_2x_3x_4 + x_1x_2x_3x_5 + x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + x_1x_4x_5 + x_3x_4x_5 + x_1x_4 + x_1x_5 + x_2x_3$

Table 4: Number of Boolean Functions of 4 Variables with given Rayleigh Quotient

N_f	Functions
± 16	40
± 13	416
± 12	800
± 11	1504
± 10	2560
± 9	2944
± 8	3904
± 7	4992
± 6	5632
± 5	6816
± 4	7264
± 3	7648
± 2	8192
± 1	8448
0	4376
Total	65,536

2. $x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + x_1x_3 + x_1x_4 + x_1x_5 + x_3x_4 + x_3x_5 + x_4x_5 + x_1$
3. $x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + x_3x_4 + x_3x_5 + x_4x_5 + x_1 + x_2 + x_3 + x_4$
4. $x_1x_2x_3 + x_1x_2 + x_1x_3 + x_4x_5$

6 Properties of the Rayleigh quotient

6.1 Elementary properties

The normalized Rayleigh quotient is the sum of 2^n terms ± 1. Therefore

Proposition 2. *The normalized Rayleigh quotient N_f of a bent Boolean function f is an even integer (negative or positive).*

For bent functions that are neither self dual nor anti self dual we can improve on the estimate of N_f over [4].

Proposition 3. *Let f be a bent function in n variables. If f is neither self dual nor anti self dual then $|N_f| \leq 2^n - 4$.*

Proof. By the proof of Theorem 1 we see that if $Z = 0$ then $X = 0$ and $F^+ = 0$ forcing f to be anti self dual. A similar argument for F^- shows that we cannot have $Z = 0$ for F^-. It follows, to avoid either situation, that S_+ cannot have size $2^n - 1$. The result follows. □

Table 5: Number of Boolean Functions of 5 Variables with given Non-Normalized Rayleigh Quotient

S_f	Functions
±160	8960
±155	23,040
±150	50,688
±145	150,528
±140	840,320
±135	1,039,360
±130	1,627,392
±125	2,581,792
±120	9,404,480
±115	7,907,840
±110	10,849,152
±105	14,716,416
±100	44,280,000
±95	31,537,920
±90	38,784,320
±85	47,529,984
±80	125,472,000
±75	79,892,480
±70	92,338,176
±65	105,623,232
±60	254,490,560
±55	149,760,000
±50	164,694,016
±45	180,602,112
±40	404,723,200
±35	224,425,920
±30	236,937,728
±25	249,284,160
±20	529,400,320
±15	277,094,400
±10	284,104,704
±5	288,219,136
0	436,572,960
Total	4,294,967,296

6.2 Symmetries

In this section we give symmetries, that is operations, on Boolean functions that preserve bentness and the Rayleigh quotient. Define, following [7], the *orthogonal group* of index n over $\mathbb{F}_2$ as

$$\mathcal{O}_n := \{L \in GL(n,2) \mid LL^t = I_n\}.$$

Observe that $L \in \mathcal{O}_n$ if and only if (I_n, L) is the generator matrix of a self dual binary code of length $2n$. Thus, for even n, an example is $I_n + J_n$ with $J_n =$all-one matrix.

Theorem 4. *Let f denote a bent function in n variables. If $L \in \mathcal{O}_n$ and $c \in \{0,1\}$ then $g(x) := f(Lx) + c$ is also bent, and $N_g = N_f$.*

Proof. The WHT of g is

$$\hat{G}(x) = (-1)^c \hat{F}(Lx) = 2^{n/2}(-1)^{\tilde{f}(Lx)+c} = 2^{n/2}(-1)^{\tilde{g}(x)},$$

where the first equality holds by observing that $x.y = L(x).L(y)$, and by a change of variable involving $L^{-1} = L^T$, and the last equality by definition of $\tilde{g}$. Computing the normalized Rayleigh quotient of g yields

$$N_g = \langle (-1)^g, (-1)^{\tilde{g}} \rangle = \sum_x (-1)^{f(Lx)}(-1)^{\tilde{f}(Lx)} = N_f. \qquad \square$$

Theorem 5. *Let f denote a bent function in n variables. Define g by $g(x) := f(x+d) + d \cdot x$. If $d \in \mathbb{F}_2^n$ then g is also bent, and $N_g = (-1)^{d \cdot d} N_f$.*

Proof. A change of variables $y = x + d$ in the definition of $\hat{G}$ yields $\hat{G}(y) = (-1)^{d \cdot (y+d)} \times \hat{F}(y+d)$. Therefore g is bent with dual function

$$\tilde{g}(y) = d \cdot (y+d) + \tilde{f}(y+d).$$

Adding up yields

$$g(y) + \tilde{g}(y) = d \cdot d + f(y+d) + \tilde{f}(y+d).$$

The result follows after a change of variables. $\square$

Theorem 5 explains why, for every function, f, with normalized Rayleigh quotient N_f, there exists a family of functions, $\{f_e\}$ each with normalized Rayleigh quotient, N_f, and an equal size family of functions, $\{f_o\}$, each with normalized Rayleigh quotient, $-N_f$, as obtained by evaluating g for even and odd weight values of d, respectively.

We refer, in this and related work, to the combined action of the symmetries of theorems 4 and 5 as the action of the *extended orthogonal group*, being a subgroup of the affine group.

7 Special constructions

In [4] primary constructions for (anti) self dual bent functions were presented for the case of Maiorana McFarland, Dillon's partial spreads, and monomial power functions. Secondary constructions using both direct and indirect sum were also presented. We now generalise this work, in the cases of Maiorana McFarland and partial spreads, and for direct and indirect sum, to the situation where the Rayleigh quotient can have magnitude less than 2^n.

7.1 Maiorana McFarland

A general class of bent functions is the *Maiorana McFarland* class, that is functions of the form

$$x \cdot \phi(y) + g(y)$$

with $x, y \in \mathbb{F}_2^{n/2}$, $\phi : \mathbb{F}_2^{n/2} \to \mathbb{F}_2^{n/2}$, a permutation, and g arbitrary Boolean.

Theorem 6. *A Maiorana McFarland function $f = x \cdot \phi(y) + g(y)$ with $\phi(x) = L(x) + a$, $L \in GL(n/2, 2)$ and unitary ($L^T = L^{-1}$), and $a \in \mathbb{F}_2^{n/2}$, has normalized Rayleigh quotient*

$$N_f = (-1)^{a \cdot a} \times (\sum_x (-1)^{g(x) + a \cdot L(x)})^2.$$

Proof. The dual of a Maiorana-McFarland bent function $x \cdot \phi(y) + g(y)$ is equal to $\phi^{-1}(x) \cdot y + g(\phi^{-1}(x))$ [5]. Computing the normalized Rayleigh quotient of f yields, after replacing x by $\phi(x)$,

$$N_f = \langle (-1)^f, (-1)^{\tilde{f}} \rangle = \sum_{x,y} (-1)^{\phi(x) \cdot \phi(y) + x \cdot y + g(x) + g(y)},$$

and, since, for L unitary, $L(x) \cdot L(y) = x \cdot y$,

$$N_f = \sum_{x,y} (-1)^{g(x) + a \cdot L(x) + g(y) + a \cdot L(y) + a \cdot a}.$$

The result follows. □

The proof of the following corollary is omitted.

Corollary 1. *If $g(x) + a \cdot L(x)$ is constant, then f is self dual (resp. anti self dual) if a has even (resp. odd) weight, i.e. $N_f = 1$ (resp. $N_f = -1$), and, if $g(x) + a \cdot L(x)$ is balanced then $N_f = 0$.*

7.2 Dillon functions

Let $x, y \in \mathbb{F}_{2^{n/2}}$. The class denoted by $\mathcal{PS}_{ap}$ in [5] consists of so-called Dillon's function of the type

$$f(x, y) = g(x/y)$$

with the convention that $x/y = 0$ if $y = 0$, and where g is a balanced Boolean function and $g(0) = 0$. We introduce the character sum

$$K_g := \sum_u (-1)^{g(u)+g(1/u)}.$$

In particular, if $g = Tr$ then K_g is a *Kloosterman sum.*

Theorem 7. *Let f be a bent function constructed from a Dillon g as above. Its Rayleigh quotient is*

$$N_f = 2^{n/2} + (2^{n/2} - 1)K_g.$$

Proof. The dual of $f = g(x/y)$ is $\tilde{f} = g(y/x)$. Therefore $N_f = \sum_{x,y}(-1)^{g(x/y)+g(y/x)}$. Noting when y vanishes and making the change of variables $u = x/y$ when $y \neq 0$ gives the result. □

7.3 Direct and indirect sums

If f and g are Boolean functions in n and m variables, respectively, define the *direct sum* of f and g as the Boolean function on $n + m$ variables given by $f(x) + g(y)$. The following result is immediate, and its proof is omitted.

Proposition 4. *If f and g are bent functions their direct sum is bent of Rayleigh quotient $N_f N_g$.*

A more general construction involving four functions can be found in [3]. If a, b and c, d are two pairs of Boolean functions in n and m variables, respectively, define the *indirect sum* of these four functions by

$$f(x, y) := a(x) + d(y) + (a(x) + b(x))(c(y) + d(y)).$$

It is shown in [3], and also reviewed in [2], that, if a, b, c, d are bent functions, then f is a bent function, and

Lemma 2.

$$\tilde{f} = \tilde{a} + \tilde{d} + (\tilde{a} + \tilde{b})(\tilde{c} + \tilde{d}).$$

We further show that,

Proposition 5. *If a, b and c, d are two pairs of dual bent functions, i.e. such that $b = \tilde{a}$ and $d = \tilde{c}$, then f and $g = b + c + (a + b)(c + d)$ are also dual bent functions, i.e. $g = \tilde{f}$. Furthermore the Rayleigh quotient of both f and g is*

$$N_f = N_a N_c.$$

Proof. Comes from

$$\tilde{f} = f + (a + b) + (c + d),$$

and the definition of N_a and N_b. The result follows. □

A generalisation on this theme is the following

Proposition 6. *If a, b and c, d are two pairs of bent functions satisfying $b = \tilde{a} + \epsilon$, $d = \tilde{c} + \mu$, for $\epsilon, \mu \in \{0, 1\}$, then $f = a + d + (a + b)(c + d)$ and $g = b + c + (a + b)(c + d)$ are both bent. Furthermore the Rayleigh quotient of both is*

$$N_f = N_a N_c.$$

Proof. A direct computation using Lemma 2 shows that

$$f + \tilde{f} = (a + b) + (c + d) + (\epsilon + \mu).$$

The result follows. □

Finally,

Proposition 7. *Let a and b be self dual or anti self dual bent Boolean functions over m variables. Let $d_H(a, b)$ be the Hamming distance between a and b. Let c and d both be bent Boolean functions over n variables. Then, $f = a + d + (a + b)(c + d)$ and $g = b + c + (a + b)(c + d)$ are both bent over $n + m$ variables, and*

$$\begin{aligned}
N_f &= \left(2^m N_d + d_H(a, b)(N_c - N_d)\right)(-1)^{e_a},\ e_a = e_b,\\
N_g &= \left(2^m N_c - d_H(a, b)(N_c - N_d)\right)(-1)^{e_b}, \qquad ''\\
N_g &= \left(2^m N_d + d_H(a, b)(N_c - N_d)\right)(-1)^{e_a},\ e_a \neq e_b,\\
N_f &= \left(2^m N_c - d_H(a, b)(N_c - N_d)\right)(-1)^{e_b}, \qquad ''
\end{aligned}$$

where $e_a, e_b \in \mathbb{F}_2$, $e_a = 0$ (resp. 1) if a is self dual (resp. anti self dual), $e_b = 0$ (resp. 1) if b is self dual (resp. anti self dual).

Proof. From Lemma 2 and the (anti) self dual properties of a and b, we obtain

$$\tilde{f} = a + \tilde{d} + (a + b + e_a + e_b)(\tilde{c} + \tilde{d}) + e_a.$$

Therefore

$$f + \tilde{f} = d + \tilde{d} + (a + b + e_a + e_b)(c + \tilde{c} + d + \tilde{d}) + e_a.$$

Consider the case where $e_a = e_b$. For $x \in \mathbb{F}_2^m$ such that $a(x) + b(x) = 0$ (resp. 1), the previous equation then reduces to $f + \tilde{f} = d + \tilde{d} + e_a$ (resp. $f + \tilde{f} = c + \tilde{c} + e_a$). From Proposition 1. we see that an n-variable bent Boolean function, h, has Rayleigh quotient given by $N_h = 2^n - 2d_H(h, \tilde{h})$. Plugging this back into the previous equations, we obtain

$$(-1)^{e_a} N_f = 2^{n+m} - 2\left((2^m - d_H(a, b))d_H(d, \tilde{d}) + d_H(a, b)d_H(c, \tilde{c})\right)$$

which, after some re-arrangements, gives the expression for N_f when $e_a = e_b$ in the Proposition. Similar arguments can be used to obtain the expression for N_f when $e_a \neq e_b$, and, likewise, one obtains similar expressions for N_g. □

It follows immediately from the proposition that, if $a + b$ is balanced, and $e_a = e_b$, then $N_f = N_g = (-1)^{e_a} 2^{m-1}(N_c + N_d)$. If, further to this, $N_c = -N_d$, e.g. if c is self dual and d is anti self dual, then $N_f = N_g = 0$. Also, from the proposition,

$$N_f + N_g = 2^m(N_c + (-1)^{e_a+e_b} N_d)(-1)^{e_b}.$$

References

1. Canteaut, A., Charpin, P.: Decomposing bent functions. IEEE Trans. Inform. Theory. 49, 2004–2019 (2003)
2. Carlet, C.: *Boolean Functions for Cryptography and Error Correcting Codes*. chapter in *Boolean methods and models* Cambridge University Press (Peter Hammer and Yves Crama eds), (to appear)
3. Carlet, C.: On the secondary constructions of resilient and bent functions. Proceedings of the Workshop on Coding, Cryptography and Combinatorics 2003, K. Feng, H. Niederreiter and C. Xing Eds., Progress in Comp. Sc. and Appl. Logic, Birkhäuser Verlag. 3–28 (2004)
4. Carlet, C, Danielsen, L.E., Parker, M.G., Solé, P.: Self dual bent functions. submitted (2009)
5. Dillon, J.F.: *Elementary Hadamard Difference Sets*. Ph.D. thesis, Univ. of Maryland, (1974)
6. Hou, X.-D.: New constructions of bent functions. J. Combin. Inform. System Sci. 25, no. 1–4, pp. 173–189 (2000)
7. Janusz, G.J.: Parametrization of self-dual codes by orthogonal matrices. Finite Fields and Their Applications. 13, Issue 3, 450–491 (2007)
8. Zheng, Y., Zhang, X. M.: Relationships between bent functions and complementary plateaued functions. Proc. 2nd Int. Conf. Information Security and Cryptology (ICISC'99) (Lecture Notes in Computer Science), ser., Berlin, Heidelberg, New York: Springer-Verlag. 1787, 60–75 (1999)
9. Zheng, Y., Zhang, X-M.: On plateaued functions. IEEE Trans. Inform. Theory. 47, 1215–1223 (2001)