SELF DUAL BENT FUNCTIONS

Claude Carlet[1], Lars Eirik Danielsen[2], Matthew Geoffrey Parker[2] and Patrick Solé[3]

Abstract. A bent function is called self dual if it is equal to its dual. It is called anti self dual if it is equal to the complement of its dual. A spectral characterization in terms of the Rayleigh quotient of the Sylvester Hadamard matrix is derived. An efficient search algorithm based on the spectrum of the Sylvester matrix is derived. Primary and Secondary constructions are given. All self dual bent Boolean functions in ≤ 6 variables and all quadratic such functions in 8 variables are given, up to a restricted form of linear equivalence.

Keywords: Boolean functions, bent functions, Walsh Hadamard transform, self dual codes

1. Introduction

Bent functions form a remarkable class of Boolean functions with applications in many domains, such as difference sets, spreading sequences for CDMA, error correcting codes and cryptology. In symmetric cryptography, these functions can be used as building blocks of stream ciphers. They will not, in general, be used directly as combining functions or as filtering functions, because they are not balanced, but as Dobbertin showed in [6], they can be used as an ingredient to build balanced filtering functions. While

[1] Department of Mathematics, University of Paris VIII, 2, rue de la Liberté; 93526 - Saint-Denis cedex 02, France,claude.carlet@inria.fr
[2] The Selmer Center, Department of Informatics, University of Bergen, PB 7800, N-5020 Bergen, Norway, larsed@ii.uib.no
[3] CNRS-I3S, Les Algorithmes, Euclide B, 2000 route des Lucioles, BP 121, 06 903 Sophia Antipolis, France, sole@unice.fr.

this class of Boolean functions is very small compared to the class of all Boolean functions it is still large enough to make enumeration and classification impossible if the number of variables is ≥ 10. It is therefore desirable to look for subclasses that are more amenable to generation, enumeration and classification.

A subclass that has received little attention since Dillon's seminal thesis [6] is the subclass of those Boolean functions that are equal to their dual (or Fourier transform in Dillon's terminology). We call these **self dual bent functions**. Of related interest are those bent functions whose dual is the complement of the function. We call these **anti self dual bent functions**. In this work we characterize the sign functions of these two class of functions as the directions where extrema of the **Rayleigh quotient** of the Sylvester type Hadamard matrix occur, or, equivalently, as eigenvectors of that matrix. This spectral characterization allows us to give a very simple and efficient search algorithm, that makes it possible to enumerate and classify all self dual bent function for ≤ 6 variables and all quadratic such functions in 8 variables. The computational saving on the exhaustive search is doubly exponential in n. We derive primary constructions (Maiorana MacFarland and Dillons's partial spreads), secondary constructions (going from bent function in n variables to self dual or anti self dual bent functions in $n+m$ variables) and class symmetries (operations on Boolean functions that preserve self duality or anti self duality). The subclass of the Maiorana MacFarland class of bent functions exhibits interesting connections with **self-dual codes**, a fact which was our original motivation at the start of the study: to connect the duality of codes with the duality of Boolean functions. This appears also in the section on class symmetries.

The material is organized as follows. Section 2 collects the notation and definitions that we need for the rest of the paper. Section 3 contains the characterization in terms of Rayleygh quotient and the bounds on that quantity for an odd number of variables. Section 4 looks into constructions, first primary then secondary. Section 5 describes the search algorithm and establishes the symmetry between self dual and anti self dual bent functions. The numerical results are listed in section 6.

2. Definitions and Notation

A **Boolean function** f in n variables is any map from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Its **sign function** is $F := (-1)^f$, and its **Walsh Hadamard transform** (WHT) can be defined as

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

When F is viewed as a column vector 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 and $\mathcal{H}_n := H^{\otimes n}/2^{n/2}$, 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. A Boolean function in n variables is said to be **bent** if and only if $\mathcal{H}_n F$ is the sign function of some other Boolean function. That function is then called the **dual** of f and denoted by $\tilde{f}$. The sign function of $\tilde{f}$ is henceforth denoted by $\tilde{F}$. If, furthermore, $f = \tilde{f}$, then f is **self dual bent**. This means that its sign function 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**. This means that its sign function is an eigenvector of $\mathcal{H}_n$ attached to the eigenvalue -1.

3. A characterization

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

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

Theorem 1. *Let n denote an* even *integer and f be a Boolean function in n variables. The modulus of the character sum S_f is at most $2^{3n/2}$ with equality if and only if f is self dual bent or anti self dual bent.*

Proof. The triangle inequality yields

$$|\sum_{x,y}(-1)^{f(x)+f(y)+x.y}| \leq \sum_{x}|\sum_{y}(-1)^{f(x)+f(y)+x.y}|$$

By Cauchy Schwarz inequality the latter sum is at most

$$\sqrt{2^n \sum_{x}(\sum_{y}(-1)^{f(x)+f(y)+x.y})^2}$$

which, by Parseval identity ($\sum_x(\hat{F}(x))^2 = 2^{2n}$) equals $2^{3n/2}$. So, $S_f \leq 2^{3n/2}$, with equality only if there is equality in these two inequalities. Equality holds in the Cauchy Schwarz inequality if and only if $|F(x)\hat{F}(x)| = |\hat{F}(x)|$ is a constant function of x that is if and only if f is bent. Equality in the triangle inequality holds then if and only if the sign of $F(x)\hat{F}(x) = 2^{n/2}F(x)\tilde{F}(x)$ is a constant function of x that is if and only if, furthermore, f is self dual (+ sign) or anti self dual (− sign). □

By using the sign function F of f we can write

$$S_f = \sum_{x\in\mathbb{F}_2^n} F(x)\hat{F}(x) = \langle F, H_n F\rangle.$$

The standard properties of the **Rayleygh quotient** attached to the real symmetric matrix H_n show that the maximum (resp. minimum) of S_f are obtained for F an eigenvector of H_n attached to a maximum (resp. minimum) eigenvalue of H_n, which are, by Lemma 1 below, $2^{n/2}$ (resp. $-2^{n/2}$). See for instance [4, p.198] or any textbook in Numerical Analysis for basic definition and properties of the Rayleigh quotient of an hermitian matrix. Alternatively, by using Lemma 1 below, the orthogonal decomposition in eigenspaces of H_n yields $F = F^+ + F^-$, with $F^\pm \in Ker(H_n \pm 2^{n/2}I_{2^n})$, and $\langle F, F\rangle = \langle F^+, F^+\rangle + \langle F^-, F^-\rangle$. Plugging this decomposition into S_f gives

$$S_f = 2^{n/2}\langle F^+, F^+\rangle - 2^{n/2}\langle F^-, F^-\rangle,$$

and by the triangle inequality, $|S_f| \leq 2^{3n/2}$, with equality if and only if $F = F^+$ or $F = F^-$.

Proposition 1. *The Hamming distance between a self dual bent function f_1 and an antiselfdual bent function f_2, both of n variables, is 2^{n-1}.*

Proof. Let F_1 (resp; F_2) denote the sign function of f_1 (resp; f_2.). On the one hand

$$\langle F_1, H_n F_2\rangle = -2^{n/2}\langle F_1, F_2\rangle,$$

by anti self duality of f_2. On the other hand by self adjunctness of H_n, we have

$$\langle F_1, H_n F_2\rangle = \langle H_n F_1, F_2\rangle,$$

which equals $2^{n/2}\langle F_1, F_2\rangle$, by self duality of f_1. Since

$$\langle F_1, F_2\rangle = -\langle F_1, F_2\rangle = 0,$$

the result follows. □

An interesting open problem is to consider the maximum of S_f for n odd, when the eigenvectors of H_n cannot be in $\{\pm 1\}^n$. In that direction we have

Theorem 2. *The maximum Rayleygh quotient of a Boolean function g in an odd number of variables n is at least $S_g \geq 2^{(3n-1)/2}$.*

Proof. Let F be the sign function of a self dual bent function in $n-1$ variables, so that $H_{n-1}F = 2^{(n-1)/2}F$. Define a Boolean function in n variables by its sign function $G = (F, F)$. Write $H_n = H \otimes H_{n-1}$, to derive

$$H_n G = (2H_{n-1}F, 0)^t = (2^{(n+1)/2}F, 0)^t.$$

Taking dot product on the left by G yields

$$S_g = 2^{(n+1)/2}F^t F = 2^{(n+1)/2}2^{n-1} = 2^{(3n-1)/2}.$$

□

4. Constructions

4.1. Primary Constructions

4.1.1. 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 dimension $n/2$ variable vectors, $\phi \in GL(n/2, 2)$ and g arbitrary Boolean. In the following theorem L^t denote the transpose of L.

Theorem 3. *A Maiorana McFarland function is self dual bent (resp. anti self dual bent) if and only if $g(y) = b \cdot y + \epsilon$ and $\phi(y) = L(y) + a$ where L is a linear automorphism satisfying $L \times L^t = I_{n/2}$, $a = L(b)$, and a has even (resp. odd) Hamming weight. In both cases the code of parity check matrix $(I_{n/2}, L)$ is self dual and (a, b) one of its codewords. Conversely, to the ordered pair (H, c) of a parity check matrix H of a self dual code of length n and one of its codewords c can be attached such a Boolean function.*

Proof. The dual of a Maiorana-McFarland bent function $x \cdot \phi(y) + g(y)$ is equal to $\phi^{-1}(x) \cdot y + g(\phi^{-1}(x))$ [1]. If the function f is self-dual then g and ϕ must be affine, that is, $g(y) = b \cdot y + \epsilon$ and $\phi(y) = L(y) + a$ (where L is a linear automorphism). Then f is self-dual if and only if, for every $x, y \in \mathbb{F}_2^{n/2}$: $x \cdot (L(y)+a) + b \cdot y + \epsilon = y \cdot L^{-1}(x + a) + L^{-1}(x + a) \cdot b + \epsilon$, that is, for every $x, y \in F_2^{n/2}$, $x \cdot L(y) = y \cdot L^{-1}(x)$ (i.e. $L \times L^t = I_n$), $a = L(b)$ and b has even weight. □

Any self-dual code of length n gives rise to K parity check matrices, and each such distinct parity check matrix gives rise to $2^{n/2-1}$ self-dual bent functions, and $2^{n/2-1}$ anti self-dual bent functions. Thus, any self-dual code of length n gives rise to $K \times 2^{n/2-1}$ self-dual bent functions, and the same number of anti self-dual bent functions, to within variable re-labelling. All such functions are quadratic. It is possible to both classify and/or enumerate this class given a classification and/or enumeration of all self-dual codes, coupled with a method to classify and/or enumerate all distinct parity check matrices for each code. One way of performing this last task is to generate all *edge-local complementation* (ELC) orbits [3], to within re-labelling of vertices, for the bipartite graph associated with each distinct self-dual code of size n. For each of self-dual and nega self-dual, enumeration would then be realised by summing the orbit sizes and then multiplying the result by $2^{n/2-1}$, and classification would be realised by listing each member in the union of orbits. Each member of such a list would then be a $\mathrm{RM}(2, n)$ coset leader for a coset of $2^{n/2-1}$ self-dual and $2^{n/2-1}$ nega self-dual quadratic Boolean functions.

4.1.2. Dillon's partial spreads

Let $x, y \in \mathbb{F}_{2^{n/2}}$. The class denoted by $\mathcal{PS}_{ap}$ in [1] 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 balanced and $g(0) = 0$.

Theorem 4. *A Dillon function is self dual bent if g satisfies $g(1) = 0$, and, for all $u \neq 0$ the relation $g(u) = g(1/u)$. There are exactly $\binom{2^{n/2-1}-1}{2^{n/2-2}}$ such functions.*

Proof. By [1] the dual of a Dillon function is obtained by exchanging the roles of x and y. Define g by its values on pairs $u, 1/u$ for u different from zero and one. Counting and balancedness implies then that $g(1) = 0$ and that the number of such pairs where g takes the value one is $\binom{2^{n/2-1}-1}{2^{n/2-2}}$. The result follows. □

By complementing functions one may go beyond the $\mathcal{PS}_{ap}$ class.

Corollary 1. *Let g be a function from $\mathbb{F}_{2^{n/2}}$ down to $\mathbb{F}_2$, that satisfies $g(1) = g(0)$, and, for all $u \neq 0$ the relation $g(u) = g(1/u)$. If g is balanced then with the same convention as above the function $f(x, y) = g(x/y)$ is self dual bent.*

4.2. Secondary Constructions

4.2.1. Class symmetries

In this section we give class symmetries that is operations on boolean functions that leave the self dual bent class invariant as a whole. Define, following [7], the orthogonal group of index n over $\mathbb{F}_2$ as

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

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 5. *Let f denote a self dual bent function in n variables. If $L \in \mathcal{O}_n$ and $c \in \{0, 1\}$ then $f(Lx) + c$ is self dual bent.*

Proof. Set $g(x) := f(Lx) + c$. The Walsh Hadamard transform of that function is

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

where the first equality holds by a change of variable involving $L^{-1} = L^T$, and the last before last by self duality of f. □

Recall that a function is I-bent if it has flat spectrum wrt some unitary transform U obtained by tensoring m matrices I_2 and $n-m$ matrices $\mathcal{H}_1$ in any order [8], for some $m \leq n$.

Theorem 6. *Let f denote a self dual bent function in n variables, that is furthermore I-bent. Its I-bent dual is self dual bent.*

Proof. By definition, there is an unitary matrix U and a Boolean function g such that $U(-1)^f = (-1)^g$. The result then follows from the fact that U commutes with $\mathcal{H}_n$.

$$\mathcal{H}_n(-1)^g = \mathcal{H}_n U(-1)^f = U\mathcal{H}_n(-1)^f = U(-1)^f$$

where the last equality comes from the self duality of f. □

4.2.2. $n+m$ variables from n variables and m variables

For this subsection define the **duality** of a bent function to be 0 if it is self dual bent and 1 if it is anti self dual bent. If f and g are Boolean functions in n and m variables, repectively, 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. Still it shows that self dual and anti self dual bent functions cannot be considered separately.

Proposition 2. *If f and g are bent functions of dualities ϵ and ν their direct sum is bent of duality $\epsilon + \nu$.*

A more general construction involving four functions can be found in [2]. If f_1, f_2 and g_1, g_2 are a pair of Boolean functions in n and m variables, respectively, define the **indirect sum** of these four functions by

$$h(x,y) := f_1(x) + g_1(y) + (f_1 + f_2(x))(g_1 + g_2(y)).$$

Theorem 7. *If f_1, f_2 (resp. g_1, g_2) are bent functions of dualities both ϵ (resp. both ν) their indirect sum is bent of duality $\epsilon + \nu$. If f_1 is bent and $f_2 = f_1^{\perp} + \epsilon$ for some $\epsilon \in \{0,1\}$, and g_1 is self dual bent and g_2 is anti self dual bent, then the indirect sum of the four functions is self dual bent of duality ϵ.*

Proof. The proof of the first assertion comes from the fact that the indirect sum is bent if all four functions are bent and in this case the dual function is obtained as the indirect sum of the duals of the four functions [2]. Writing $f_i = f_i + \epsilon$, and $g_i = g_i + \nu$ for $i = 1, 2$, the result follows. The proof of the second assertion is similar and is omitted. □

As an example of construction take $g_1(y_1, y_2) = y_1 y_2$ which is self dual bent and $g_2(y_1, y_2) = y_1 y_2 + y_1 + y_2$ which is anti self dual bent. Let f be a bent function in n variables and put F (resp. $\tilde{F}$) its sign function (resp. the sign function of its dual). The vector $(F, \tilde{F}, \tilde{F}, -F)$ is the sign function of a self dual bent function in $n + 2$ variables. The vector $(F, -\tilde{F}, -\tilde{F}, -F)$ is the sign function of a anti self dual bent function in $n + 2$ variables. The observant reader will notice that the sign pattern of the above construction is the same as that of self dual bent and anti self dual bent functions in 2 variables. This leads to conjecture the existence of 20 different constructions of self dual bent functions in $n + 4$ variables from bent functions in n variables.

5. A search algorithm

Theorem 8. *Let $n \geq 2$ be an even integer and Z be arbitrary in $\{\pm 1\}^{n-1}$. Define $Y := Z + \frac{2H_{n-1}}{2^{n/2}} Z$. If Y is in $\{\pm 1\}^{n-1}$, then the vector (Y, Z) is the sign function of a self dual bent function in n variables.*

We prepare for the proof by a linear algebra lemma.

Lemma 1. *The spectrum of $\mathcal{H}_n$ consists of the two eigenvalues ± 1 with the same mutiplicity 2^{n-1}. A basis of the eigenspace attached to 1 is formed of the rows of the matrix $(H_{n-1} + 2^{n/2} I_{2^{n-1}}, H_{n-1})$. 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. (of the Lemma) The minimal polynomial of $\mathcal{H}_n$ is $X^2 - 1$, by symmetry of $\mathcal{H}_n$ and the Hadamard property of H_n. Hence the spectrum. The multiplicity follows by $Tr(\mathcal{H}_n) = 0$. The matrix $\mathcal{H}_n + I_n$ is a projector on the eigenspace attached to the eigenvalue 1. The said basis is, up to scale, the first 2^{n-1} columns of that matrix. The last assertion follows by standard properties of symmetric real matrices. □

Proof. By the Lemma, we need to solve for X with rational coordinates the system

$$\begin{aligned}(H_{n-1} + 2^{n/2} I_{2^{n-1}})X &= 2^{n/2} Y \\ H_{n-1} X &= 2^{n/2} Z\end{aligned}$$

or, equivalently

$$\begin{aligned}Z + X &= Y \\ H_{n-1} X &= 2^{n/2} Z\end{aligned}$$

The result follows by $H_{n-1}^2 = 2^{n-1} I_{n-1}$. □

As an example we treat the case $n = 2$. We get $Y = (2z_1 + z_2, z_1)^T$. The condition $y_1 = \pm 1$ forces $z_1 = -z_2$. We have two self dual bent functions of sign functions $(z_1, z_1, z_1, -z_1)^T$, with $z_1 = \pm 1$. We give an algorithm to generate all self dual bent functions of degree at most k.

Algorithm $SDB(n, k)$

(1) Generate all Z in $RM(k, n-1)$.
(2) Compute all Y as $Y := Z + \frac{2H_{n-1}}{2^{n/2}} Z$.
(3) If $Y \in \{\pm 1\}^{n-1}$ output (Y, Z), else go to next Z.

It should be noted that compared to brute force exhaustive search the computational saving is of order 2^R, with

$$R = 2^n - \sum_{j=0}^{k} \binom{n-1}{j} = 2^{n-1} + \sum_{j=0}^{n-k-1} \binom{n-1}{j}$$

The next result shows that there is a one-to-one correspondence between self-dual and antiselfdual bent functions.

Theorem 9. *Let $n \geq 2$ be an even integer and Z be arbitrary in $\{\pm 1\}^{n-1}$. Define $Y := Z + \frac{2H_{n-1}}{2^{n/2}} Z$. If Y is in $\{\pm 1\}^{n-1}$, then the vector $(Z, -Y)$ is the sign function of a self dual bent function in n variables.*

Proof.

Observe the identity

$$(I_{2^{n-1}} + \frac{2H_{n-1}}{2^{n/2}})(I_{2^{n-1}} - \frac{2H_{n-1}}{2^{n/2}}) = -I_{2^{n-1}}.$$

From there we see that

$$Z = Y' - \frac{2H_{n-1}}{2^{n/2}}Y'$$

with $Y' = -Y$. By the analogue of Theorem 1 for antiselfdual bent functions the result follows. □

From this result follows a generation algorithm for antiselfdual bent functions of degree at most k.

Algorithm $NSDB(n, k)$

(1) Generate all Z in $RM(k, n-1)$.
(2) Compute all Y as $Y := Z - \frac{2H_{n-1}}{2^{n/2}}Z$.
(3) If $Y \in \{\pm 1\}^{n-1}$ output (Y, Z), else go to next Z.

Eventually, we point out a connection with **plateaued functions**. Recall that a Boolean function f on n variables is plateaued of order r if the entries of $H_n(-1)^f$ are in module either zero or $2^{n-r/2}$.

Theorem 10. *Let $n \geq 2$ be an even integer and Z be arbitrary in $\{\pm 1\}^{n-1}$. Define $Y := Z + \frac{2H_{n-1}}{2^{n/2}}Z$. If Y is in $\{\pm 1\}^{n-1}$, then both Y and Z are sign functions of plateaued Boolean functions of order $n-2$ in $n-1$ variables.*

Proof. Observe that the entries of $Y - Z$ take values in the set $\{0, \pm 2\}$, and, therefore the entries of Z in the set $\{0, \pm 2^{n/2}\}$. Similarly, by the proof of the preceding Theorem, $Z := -Y + \frac{2H_{n-1}}{2^{n/2}}Y$. By the same argument as previous, the entries of Y are in the set $\{0, \pm 2^{n/2}\}$. □

6. Numerics

The following results were obtained by using the algorithms $SDB(n, k)$ and $NSDB(n, k)$ for $n \leq 6$ and $k \leq n/2$.. We consider the self-dual bent functions f and g to be equivalent when $g(x) = f(Ax + b) + b \cdot x + c$, where $AA^t = I$, $b \in \mathbb{Z}_2^n$, wt(b) even, and $c \in \mathbb{Z}_2$.

6.1. Two variables

There is one and only one self dual bent function in two variables up to complementation: $(1, 1, 1, -1)$, or x_1x_2. There is one

and only one anti self dual bent function in two variables up to complementation $(1, -1, -1, -1)$.

6.2. Four and Six variables

We have classified all self-dual bent functions of up to 6 variables. Table 1 gives a representative from each equivalence class, and the number of functions in each class. An expression like $12 + 34$ denotes $x_1x_2 + x_3x_4$.

TABLE 1. Self-Dual Bent Functions of 4 and 6 Variables

Representative from equivalence class	Size
12	1
Total number of functions of 2 variables	1
$12 + 34$	12
$12 + 13 + 14 + 23 + 24 + 34 + 1$	8
Total number of functions of 4 variables	20
$12 + 34 + 56$	480
$12 + 34 + 35 + 36 + 45 + 46 + 56 + 3$	240
12+13+14+15+16+23+24+25+26+34+35+36+45+46+56+1+2	32
$134 + 234 + 156 + 256 + 12 + 35 + 46 + 56$	11,520
126+136+125+135+246+346+245+345+12+15+26+34+36+45+56	5760
126+136+145+135+246+236+245+345+12+15+25+34+36+46+56	23,040
$456 + 356 + 145 + 246 + 135 + 236 + 124 + 123 + 15 + 26 + 34 + 35 + 36 + 45 + 46 + 3$	1440
123+124+134+126+125+136+135+234+236+235+146+145+156+246+245+346+345+256+356+456+14+25+36+45+46+56+1+2+3	384
Total number of functions of 6 variables	42,896

6.3. Eight variables

We have classified all quadratic self-dual bent functions of 8 variables. Table 2 gives a representative from each equivalence class, and the number of functions in each class.

7. Conclusion and open problems

In this work we have explored the class of self dual bent functions and characterized it by the Rayleigh quotient of the Hadamard

TABLE 2. Quadratic Self-Dual Bent Functions of 8 Variables

Representative from equivalence class	Size
$12 + 34 + 56 + 78$	30,720
$12 + 34 + 56 + 57 + 58 + 67 + 68 + 78 + 5$	15,360
$13 + 14 + 15 + 26 + 27 + 28 + 34 + 35 + 45 + 67 + 68 + 78 + 1 + 2$	2048
Number of quadratic functions of 8 variables	48,128

matrix of Sylvester type. It would be interesting to obtain lower bounds on the Rayleigh quotient of Boolean functions in an odd number of variables. We have determined all self dual bent functions in at most 6 variables and all quadratic self dual bent functions for 8 variables. In general characterizing the class of quadratic self dual bent functions is a difficult problem. The open question is to know if there is more than the Maiorana MacFarland type of §4.1. We also have given some symmetries that preserve the self dual class in §4.2. It would be interesting to know if there are no more. More connections with the theory of self dual binary codes, for instance weight enumerators, is a goal worth pursuing.

References

[1] C. Carlet, *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.

[2] C. Carlet, *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., pp. 3-28, Progress in Comp. Sc. and Appl. Logic, Birkhäuser Verlag, 2004.

[3] Lars Eirik Danielsen and Matthew G. Parker, *Edge Local Complementation and Equivalence of Binary Linear Codes,* Designs, Codes and Cryptography, to appear in 2008.

[4] James W. Demmel, *Applied Numerical Linear Algebra*, SIAM Philadelphia, PA, 1997.

[5] J.F. Dillon, *Elementary Hadamard Difference Sets*, Ph;D. thesis, Univ. of Maryland, 1974.

[6] H. Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. *Fast Software Encryption, Second International Workshop*, Lecture Notes in Computer Science 1008, pp. 61-74, 1995.

[7] Gerald J. Janusz, *Parametrization of self-dual codes by orthogonal matrices*,Finite Fields and Their Applications Volume 13, Issue 3, July 2007, Pages 450-491

[8] Riera, Constanza; Parker, Matthew G. *Generalized bent criteria for Boolean functions. I*, IEEE Trans. Inform. Theory **IT 52** (2006), no. 9, 4142–4159.
[9] Y. Zheng, X-M. Zhang, *On plateaued functions*, IEEE Trans. Inform. Theory **IT 47** (2001) 1215–1223.

March 4, 2008