Self-Dual Bent Functions

Claude Carlet

LAGA, Universities of Paris 8 and Paris 13 and CNRS
Department of Mathematics, University of Paris 8
2, rue de la liberté, 93526 Saint-Denis Cedex, France
Email: claude.carlet@inria.fr

Lars Eirik Danielsen

Department of Informatics
University of Bergen
PO Box 7803, N-5020 Bergen, Norway
Email: larsed@ii.uib.no

Matthew G. Parker

Department of Informatics
University of Bergen
PO Box 7803, N-5020 Bergen, Norway
Email: matthew@ii.uib.no

Patrick Solé

Telecom ParisTech
Dept Comelec
46, rue Barrault, 75013 Paris France
Email: sole@telecom-paristech.fr

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. Bounds on the Rayleigh quotient are given for Boolean functions in an odd number of variables. 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 affine equivalence.

Keywords: Boolean functions; bent functions; Walsh-Hadamard transform; self-dual codes

In *Int. J. Inform. and Coding Theory* 1(4), 384–399, 2010.

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 (Dobbertin, 1995), they can be used as an ingredient to build balanced filtering functions. While 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 (Dillon, 1974) 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-McFarland and Dillon'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-McFarland 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.

When the number of variables is odd and bent functions cannot exist maximizing the Rayleigh quotient still makes sense. We give an iterative construction to build Boolean functions with Rayleigh quotient converging to some asymptote.

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 Rayleigh 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

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

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

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

Theorem 3.1: *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

$$\left| \sum_{x,y} (-1)^{f(x)+f(y)+x\cdot y} \right| \le \sum_{x} \left| \sum_{y} (-1)^{f(x)+f(y)+x\cdot y} \right|.$$

By the Cauchy Schwarz inequality the latter sum is at most

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

which, by Parseval's 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 Rayleigh 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 5.2 below, $2^{n/2}$ (resp. $-2^{n/2}$). See for instance (Demmel, 1997, 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 5.2 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 3.2: *The Hamming distance between a self-dual bent function f_1 and an anti-self-dual 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 $\{\pm 1\}^{2^n}$. In that direction we have

Theorem 3.3: *The maximum Rayleigh quotient of a Boolean function g in an odd number of variables n is at least $S_g \geq 2^{(3n-1)/2}$.*

Table 1 Boolean Functions with Maximum Rayleigh Quotient Found by Experiment

n	$\mathcal{S}_{f\max}$	Examples
3	0.883883	$123 + 13 + 23$
5	0.883883	$12345 + 1235 + 2345 + 124 + 125 + 234 + 245 + 12 + 14 + 34 + 1$
7	0.883883	$123456 + 123457 + 12345 + 12346 + 12347 + 13456 + 13457 + 23456 + 23457 + 1234 + 1236 + 1237 + 1246 + 1247 + 1345 + 1456 + 1457 + 2356 + 2357 + 2456 + 2457 + 123 + 126 + 127 + 134 + 136 + 2456 + 2457 + 123 + 126 + 127 + 134 + 136 + 137 + 145 + 236 + 237 + 246 + 247 + 346 + 347 + 356 + 357 + 456 + 457 + 16 + 17 + 25 + 26 + 27 + 35 + 36 + 37 + 46 + 47 + 56 + 57 + 67 + 3 + 5$
9	0.883883	algebraic degree 7, number of monomials is 110
11	0.905981	algebraic degree 8, number of monomials is 524
13	0.919791	algebraic degree 9, number of monomials is 1767
15	0.926697	algebraic degree 10, number of monomials is 5494
17	0.930149	algebraic degree 11, number of monomials is 16673
19	0.931876	algebraic degree 12, number of monomials is 50208
21	0.932739	algebraic degree 13, number of monomials is 150811
23	0.933170	algebraic degree 14, number of monomials is 452618
25	0.933386	algebraic degree 15, number of monomials is 1358037

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

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

Taking dot product on the left by G yields

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

□

Define the *normalised Rayleigh quotient magnitude* of a Boolean function, f, of n variables, to be

$$\mathcal{S}_f = \frac{|S_f|}{2^{3n/2}}.$$

When n is even then the maximum achievable $\mathcal{S}_f$ is exactly one. When n is odd then the bent concatenation construction contained in the proof of Theorem 3.3 gives $\mathcal{S}_f = 2^{-\frac{1}{2}}$. We call this latter figure the *bent-concatenation bound* for $\mathcal{S}_f$. We are interested in finding Boolean functions that achieve $\mathcal{S}_f > 2^{-\frac{1}{2}} = 0.707$ for n odd. It turns out that such functions do exist. Table 1 shows the maximum $\mathcal{S}_f$ found so far by some initial computations, for different n, by the iterative method we now describe. Note that the search for $n = 3$ is exhaustive, while searches for $n \geq 5$ are non-exhaustive.

For lack of bent functions—and therefore dual bent functions—in odd number of variables, we need to introduce the following notion of duality. For any Boolean function f in n variables, with n odd, let

$$\hat{F} = F^m F^p,$$

with $F^m \geq 0$, and F^p with values in $\{\pm 1\}$. If $F^m(x) = 0$, we take the convention that $F^p(x) = 1$. (Mnemonic: m for magnitude and p for phase). Let F_0 denote an arbitrary sign function in n variables. Define for $k \geq 1$, a sequence of sign functions in $n + 2k$ variables that, at each step, satisfy one of the following two recursions:

$$F_k = (F_{k-1}, F_{k-1}^p, F_{k-1}^p, -F_{k-1})^t \quad \text{or} \quad F_k = (F_{k-1}^p, F_{k-1}, F_{k-1}, -F_{k-1}^p)^t.$$

The attached Boolean function is f_k such that $F_k = (-1)^{f_k}$.

Theorem 3.4: *The sequence of normalized Rayleigh quotients of f_k is nondecreasing.*

Proof: Note that $H_{n+2k} = H_2 \otimes H_{n+2k-2}$. Write, for simplicity $M = H_{n+2k-2}$, and S_k for S_{f_k}. We evaluate S_k as a function of S_{k-1}. Using the expression for H_{n+2k-2}, we get, depending on the choice of F_k,

$$H_{n+2k} F_k = H_2(MF_{k-1}, MF_{k-1}^p, MF_{k-1}^p, -MF_{k-1})^t,$$

or

$$H_{n+2k} F_k = H_2(MF_{k-1}^p, MF_{k-1}, MF_{k-1}, -MF_{k-1}^p)^t.$$

Multiplying on the left by F_k^t (regarded as a length 4 row vector) we get, for either choice of F_k,

$$S_k = 4\langle F_{k-1}, MF_{k-1}^p \rangle + 4\langle F_{k-1}^p, MF_{k-1} \rangle,$$

and, by self-adjunctness of M,

$$S_k = 8\langle MF_{k-1}, F_{k-1}^p \rangle.$$

By definition of the phase part, $MF_{k-1} = F_{k-1}^p F_{k-1}^m$. Plugging back in yields

$$|S_k| = 8 \sum_x F_{k-1}^m(x).$$

By definition of the Rayleigh quotient,

$$S_{k-1} = \sum_x F_{k-1}(x) F_{k-1}^p(x) F_{k-1}^m(x),$$

from which it follows that $|S_{k-1}| \leq \sum_x F_{k-1}^m(x)$ and, therefore, that

$$|S_{k-1}| \leq \frac{|S_k|}{8}.$$

By the identity $2^{3(n+2k)/2} = 8 \cdot 2^{3(n+2k-2)/2}$, the result follows. □

Since a bounded nondecreasing sequence of reals converge we can define the *asymptote* of a Boolean function f by the limit of the normalized Rayleigh quotients of f_k with initial condition $f_0 = f$ for k large. In Table 2 we give some lower bounds on asymptotes for $\mathcal{S}_{f_k}$ as $k \to \infty$, for n small, by iterating just the construction $F_k = (F_{k-1}, F_{k-1}^p, F_{k-1}^p, -F_{k-1})^t$. For instance, for $n = 3$, experiments show that applying the construction to the Boolean functions in 3 variables partitions the input space into four classes depending on the asymptote of $\mathcal{S}_{f_k}$ for k large. We see, for $n = 3$, that the four lower bounds are $\mathcal{S}_{f_{10}} = 0.507629$, 0.882848, 0.883538, and 0.883883, which appear to be tight to within two or three decimal places. Observe that the f_{10} are Boolean functions of $3 + (10 \times 2) = 23$ variables. One could, of course, get tighter bounds by computing, in each case, e.g. $\mathcal{S}_{f_{11}}$ and higher, but computational demands then become prohibitive. The lowest two classes for $n = 2, 3$, and the lowest class for $n = 4$ are for f_0 taken from the set of affine functions. Observe that, for n even, we appear to obtain a construction for functions which are '*asymptotically self-dual*'.

At each iteration step, we could either choose construction

$$F_k = (F_{k-1}, F_{k-1}^p, F_{k-1}^p, -F_{k-1})^t$$

or

$$F_k = (F_{k-1}^p, F_{k-1}, F_{k-1}, -F_{k-1}^p)^t,$$

and, although not shown in Table 2, this extra freedom appears, experimentally, to yield a much larger set of asymptotic bounds.

To demonstrate that the above recursive construction is effective, we need to consider what the average Rayleigh quotient of a Boolean function is when picked at random. Computer experiments give the following:

- For $n = 2$, $\mathcal{S}_{f_{\mathrm{av}}} = 0.5$.
- For $n = 3$, $\mathcal{S}_{f_{\mathrm{av}}} = 0.398$.
- For $n = 4$, $\mathcal{S}_{f_{\mathrm{av}}} = 0.281$.
- For $n = 5$, $\mathcal{S}_{f_{\mathrm{av}}} \approx 0.199$.
- For $n = 6$, $\mathcal{S}_{f_{\mathrm{av}}} \approx 0.141$.
- For $n = 7$, $\mathcal{S}_{f_{\mathrm{av}}} \approx 0.100$.
- For $n = 8$, $\mathcal{S}_{f_{\mathrm{av}}} \approx 0.070$.

From these experimental results we propose the following conjecture.

Conjecture 3.5: *The expected absolute Rayleigh quotient of a random Boolean function is* $\sim 9/2^{\frac{n}{2}+3}$ *for large* n.

Table 2 Lower Bounds, $\mathcal{S}_{f_k}$, on the Normalised Asymptotic Rayleigh Quotient Magnitude of f_k for f_0 an n-Variable Boolean Function

n	k	Lower bound on asymptote
1	11	0.883883
2	0	1.0
	12	0.999756
	12	0.687317
3	10	0.883883
	10	0.883538
	10	0.882848
	10	0.507629
4	0	1.0
	10	0.999756
	10	0.999512
	6	0.871582
	6	0.840820
	6	0.831810
	6	0.828461
	6	0.813049
	6	0.812500
	6	0.811523
	6	0.809570
	6	0.807617
	6	0.687500
	6	0.686523
	6	0.684570
	6	0.680664
	10	0.366730
5		Highest class sampled
	10	0.933386
		Lowest class sampled
	10	0.508104

4 Constructions

4.1 Primary Constructions

4.1.1 Quadratic Functions

Recall that a matrix over $\mathbb{F}_2$ is called *symplectic* (see (MacWilliams and Sloane, 1977, Chap. 15, sec. 2, p. 435)) if it is symmetric with zero diagonal. Let f be a quadratic function, and let $\varphi_f(x,x') = f(0) + f(x) + f(x') + f(x+x')$ its associated symplectic form. We have (see (MacWilliams and Sloane, 1977, Chap. 15)) $\varphi_f(x,x') = x' \cdot L_f(x)$, where L_f is a linear endomorphism whose matrix is symplectic (conversely, for every symplectic matrix, denoting by L the linear function admitting it as a matrix, the set of functions f such that $\varphi_f(x,x') = x' \cdot L(x)$ is a coset of the Reed-Muller code of order 1 in the Reed-Muller code of order 2).

Theorem 4.1: *If f is self-dual bent or anti-self-dual bent quadratic Boolean function then the symplectic matrix attached to its symplectic form L_f is an involution, and $f(x) + f(L_f(x))$ is constant.*

Proof: It is well-known (see e.g. (Carlet, 2009)) that

$$\left(\sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)}\right)^2 = 2^n|\mathcal{E}_f|,$$

where $\mathcal{E}_f$ is the kernel of L_f, if the restriction of f to $\mathcal{E}_f$ is constant, and if not constant then the squared character sum is 0. By Theorem 3.1 the function f is self-dual bent or anti-self-dual bent if and only if

$$\left(\sum_{x,y\in\mathbb{F}_2^n} (-1)^{f(x)+f(y)+x\cdot y}\right)^2 = 2^{3n}.$$

According to the facts recalled above and applied to the quadratic function f in $2n$ variables $(x,y) \mapsto f(x) + f(y) + x \cdot y$, this is equivalent to the fact that $\mathcal{E}_{\rm f}$ has dimension n and f is constant on $\mathcal{E}_{\rm f}$. So let us calculate the symplectic form associated to f. It is straightforward to see that it equals $x' \cdot L_f(x) + y' \cdot L_f(y) + x \cdot y' + x' \cdot y$. We deduce that

$$\begin{aligned}\mathcal{E}_{\rm f} &= \{(x,y) \in (\mathbb{F}_2^n)^2 \mid L_f(x) + y = L_f(y) + x = 0\}\\ &= \{(x,y) \in (\mathbb{F}_2^n)^2 \mid y = L_f(x), L_f^2(x) + x = 0\}.\end{aligned}$$

Hence, f is self-dual bent or anti-self-dual bent if and only if $L_f^2 = id$ and the function $f(x) + f(L_f(x)) + x \cdot L_f(x)$ is constant. But $x \cdot L_f(x) = \varphi_f(x,x) = f(0) + f(x) + f(x) + f(0) = 0$. □

Example 4.2: Let us take the example of the Gold-like monomial functions $f(x) = tr(ax^{2^i+1})$, $a \in \mathbb{F}_{2^n}$, with the inner product $x \cdot y = tr(xy)$. We have $L_f(x) =$

$ax^{2^i} + (ax)^{2^{n-i}}$. Hence $\mathcal{E}_f$ has dimension n if and only if, for every $x \in \mathbb{F}_{2^n}$, we have $a(ax^{2^i} + (ax)^{2^{n-i}})^{2^i} + (a(ax^{2^i} + (ax)^{2^{n-i}}))^{2^{n-i}} = x$, that is $a^{2^i+1}x^{2^{2i}} + a^2x + a^{2^{n-i+1}}x + a^{2^{n-2i}+2^{n-i}}x^{2^{n-2i}} = x$, that is $a^{2^i+1}x^{2^{2i}} + (a^2 + a^{2^{n-i+1}} + 1)x + a^{2^{n-2i}+2^{n-i}}x^{2^{n-2i}} = 0$. Hence, f is self-dual bent or anti-self-dual bent if and only if:

- either $i = n/2$ and $a^2 + a^{2^{n/2+1}} + 1 = 0$,
- or $i = n/4$, $a^{2^{n/4}+1} + a^{2^{n/2}+2^{3n/4}} = 0$ and $a^2 + a^{2^{3n/4+1}} + 1 = 0$.

Remark 4.3: Classifying all involutory symplectic matrices seem difficult. For instance, taking the adjacency matrix of an undirected graph of girth at least three provides, after reduction modulo 2, many examples.

4.1.2 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, ϕ any permutation in $\mathbb{F}_2^{n/2}$, and g arbitrary Boolean. In the following theorem we consider the case where $\phi \in GL(n/2, 2)$. Let L^t denote the transpose of L.

Theorem 4.4: *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 $\phi^{-1}(x) \cdot y + g(\phi^{-1}(x))$ (Carlet, 2009). 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 a certain number, let's say K, of row-column inequivalent systematic parity check matrices, and each such inequivalent 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 row-column inequivalent systematic parity check matrices for each code. One way of

performing this last task is to generate all *edge-local complementation* (ELC) orbits (Danielsen and Parker, 2008), 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 anti-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 $2^{n/2-1}$ anti-self-dual quadratic Boolean functions.

4.1.3 Dillon's Partial Spreads

Let $x, y \in \mathbb{F}_{2^{n/2}}$. The class denoted by $\mathcal{PS}_{ap}$ in (Carlet, 2009) 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 4.5: *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 (Carlet, 2009) 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. Balancedness means that g evaluates to one $2^{n/2-1}$ times. The enumeration then follows by observing that u is never equal to $1/u$ for $u \neq 1$. □

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

Corollary 4.1: *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.*

4.1.4 Monomial Functions

In general we shall consider functions of the type $f(x) = tr(ax^d)$, $a \in \mathbb{F}_{2^n}$, even n, with the inner product $x \cdot y = tr(xy)$. The *Gold exponent* $d = 2^i + 1$ has been treated in the quadratic function subsection. The *Dillon exponent* $d = 2^i - 1$ follows by (Leander, 2006, Cor. 4). The function is self-dual bent if $K(a) = 0$, where $K(a)$ denotes a Kloosterman sum. It is in fact a special case of the preceding subsection. The *Kasami exponent* $d = 2^{2i} - 2^i - 1$ is treated in (Langevin and Leander, 2008) where it is shown that the dual is not even a monomial function.

4.2 Secondary Constructions

4.2.1 Class Symmetries

In this section we give class symmetries that are operations on Boolean functions that leave the self-dual bent class invariant as a whole. Define, following (Janusz, 2007), 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 the $n \times n$ all-one matrix.

Theorem 4.6: *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

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

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 with respect to some unitary transform U obtained by tensoring m matrices I_2 and $n - m$ matrices $\mathcal{H}_1$ in any order (Riera and Parker, 2006), for some $m \leq n$.

Theorem 4.7: *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, 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. Still it shows that self-dual and anti-self-dual bent functions cannot be considered separately.

Proposition 4.8: *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 (Carlet, 2004). 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 4.9: *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, $\tilde{f}_1$ its dual, and*

$f_2 = \tilde{f}_1 + \epsilon$ 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 (Carlet, 2004). 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 the 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 an 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 us 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 5.1: *Let $n \geq 2$ be an even integer and Z be arbitrary in $\{\pm 1\}^{2^{n-1}}$. Define $Y := Z + \frac{2H_{n-1}}{2^{n/2}} Z$. If Y is in $\{\pm 1\}^{2^{n-1}}$, then the vector (Y, Z) is the sign function of a self-dual bent function in n variables. Moreover all self-dual bent functions respect this decomposition.*

We prepare for the proof by a linear algebra lemma.

Lemma 5.2: *The spectrum of $\mathcal{H}_n$ consists of the two eigenvalues ± 1 with the same multiplicity 2^{n-1}. A basis of the eigenspace attached to 1 is formed from 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 $\mathrm{Tr}(\mathcal{H}_n) = 0$. 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 $Y \in \{\pm 1\}^{2^{n-1}}$ 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 anti-self-dual bent functions.

Theorem 5.3: *Let $n \geq 2$ be an even integer and Z be arbitrary in $\{\pm 1\}^{2^{n-1}}$. Define $Y := Z + \frac{2H_{n-1}}{2^{n/2}}Z$. If Y is in $\{\pm 1\}^{2^{n-1}}$, then the vector $(Z, -Y)$ is the sign function of an anti-self-dual bent function in n variables.*

Proof: Observe the identity

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

From there we see that

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

with $Y' = -Y$. By the analogue of Theorem 3.1 for anti-self-dual bent functions the result follows. □

From this result follows a generation algorithm for anti-self-dual 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 $Y \in \{\pm 1\}^{2^{n-1}}$ 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 $H_n(-1)^f$ have modulus either zero or $2^{n-r/2}$, where r is even and can range from 0 to n.

Theorem 5.4: *Let $n \geq 2$ be an even integer and Z be arbitrary in $\{\pm 1\}^{2^{n-1}}$. Define $Y := Z + \frac{2H_{n-1}}{2^{n/2}}Z$. If Y is in $\{\pm 1\}^{2^{n-1}}$, 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 $H_{n-1}Z$ 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 previously, the entries of $H_{n-1}Y$ 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 3 gives a representative from each equivalence class, and the number of functions in each class. An expression like $12 + 34$ denotes $x_1x_2 + x_3x_4$.

6.3 Eight Variables

We have classified all quadratic self-dual bent functions of 8 variables. Table 4 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 matrix of Sylvester type. We have

Table 3 Self-Dual Bent Functions of 4 and 6 Variables

Representative from equivalence class	Size
12	2
Total number of functions of 2 variables	2
$12 + 34$	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

Table 4 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

determined all self-dual bent functions in at most 6 variables and all quadratic self-dual bent functions for 8 variables. A complete characterization of the class of quadratic self-dual bent functions is a difficult problem that comprises classifying involutory symplectic matrices as a subproblem. The open question is to know if there is more than the Maiorana-McFarland type of Section 4.1. We also have given some symmetries that preserve the self-dual class in Section 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.

Acknowledgement

The authors wish to thank Gregor Leander for helpful discussions.

References

Carlet, C. (2009) 'Boolean functions for cryptography and error correcting codes' in *Boolean Methods and Models*, (to appear), Cambridge University Press, Cambridge.

Carlet, C. (2004) 'On the secondary constructions of resilient and bent functions' in *Coding, Cryptography and Combinatorics, Progr. Comput. Sci. Appl. Logic,* Vol. 23, pp. 3–28, Birkhäuser, Basel.

Danielsen, L.E. and Parker, M.G. (2008) 'Edge local complementation and equivalence of binary linear codes,' *Designs, Codes and Cryptography,* Vol. 49, No. 1–3, pp. 161–170.

Demmel, J.W. (1997) *Applied Numerical Linear Algebra,* SIAM, Philadelphia.

Dillon, J.F. (1974) *Elementary Hadamard Difference Sets*, Ph.D. thesis, Univ. Maryland.

Dobbertin, H. (1995) 'Construction of bent functions and balanced Boolean functions with high nonlinearity,' in *Fast Software Encryption*, *Lecture Notes in Comput. Sci.,* Vol. 1008, pp. 61–74, Springer, Berlin.

Janusz, G.J. (2007) 'Parametrization of self-dual codes by orthogonal matrices,' *Finite Fields Appl.,* Vol. 13, No. 3, pp. 450–491.

Langevin, P. and Leander, G. (2008) 'Monomial bent functions and Stickelberger's theorem,' *Finite Fields Appl.,* Vol. 14, No. 3, pp. 727–742.

Leander G.(2006) 'Monomial bent functions', *IEEE Trans. Inform. Theory,* Vol. 52, No. 2, pp. 738–743.

MacWilliams, F.J. and Sloane, N.J.A. (1977) *The Theory of Error Correcting Codes,* North-Holland, Amsterdam.

Riera, C. and Parker, M.G. (2006) 'Generalized bent criteria for Boolean functions I', *IEEE Trans. Inform. Theory,* Vol. 52, No. 9, pp. 4142–4159.

Zheng, Y. and Zhang, X-M. (2001) 'On plateaued functions,' *IEEE Trans. Inform. Theory*, Vol. 47, No. 3, pp. 1215–1223.