# On the duality of bent functions


Patrick Solé[1]

CNRS/LTCI, Paris, France


Thurnau April, 2010

[1] joint work with Claude Carlet, Matthew Parker, Lars E. Danielsen

## Motivation

bent functions are important for

- difference sets in abelian groups
- spreading sequences for CDMA
- error correcting codes (Kerdock code . . . )
- symmetric cryptography (stream ciphers . . . )

enumeration and classification is impossible if the number of variables is 10.
$\Rightarrow$ looking for interesting subclasses
study self dual bent functions
hidden agenda : link to self dual codes ?
Leitmotiv Spectrum of Hadamard matrices of Sylvester type.

## 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

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

The matrix of the WHT is the Hadamard matrix $H_n$ of Sylvester type, which we now define by tensor products of 2 by 2 matrices. For one variable we get

$$H_1 := \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

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

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

## Bent functions and their duals

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 $-1$.

## Characterization

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

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

**Satz**

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.

The elementary proof uses Cauchy Schwarz+ Parseval property

## Rayleigh quotient for numerical analysts

If S is a real symmetric n by n matrix and $x \in \mathbb{R}^n$, the Rayleigh quotient $R(S,x)$ is defined as

$$R(S,x) := \frac{\langle Sx, x \rangle}{\langle x, x \rangle}$$

Well known property in literature of eigenvalue computation :

**Satz**

$R(S,x)$ meets its extrema for $x$ eigenvectors attached to the extremal eigenvalues of S.

In this talk : $S = H_n$ and $x = F$ and $Sf = 2^n R(H_n, F)$.

## Sketch of proof

Let $\lambda_i$ be the distinct (real) eigenvalues of $S$.
Put $\lambda = \min_i \lambda_i$ and $\Lambda = \max_i \lambda_i$
Write $x = \sum_i x_i$ an orthogonal decomposition on eigenspaces, so that

$$\langle x, x \rangle = \sum_i \langle x_i, x_i \rangle$$

$$\langle x, Sx \rangle = \sum_i \lambda_i \langle x_i, x_i \rangle$$

and

$$\lambda \langle x, x \rangle \leq \langle x, Sx \rangle \leq \Lambda \langle x, x \rangle.$$

In this talk :$S = H_n$ and $\lambda = -2^{n/2}$ and $\Lambda = +2^{n/2}$
An orthogonal decomposition of $\mathbb{R}^{2^n}$ in eigenspaces of $H_n$ is

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

## Odd number of variables : non bent territory

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

**Satz**

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

The proof uses the concatenation of a self dual bent function in $n-1$ variables with itself.

## Duality for non bent functions

Note that, by definition, the Fourier coefficients of a non bent function are not constant in module.
For lack of bent functions in odd number of variables, we need to introduce a new notion of duality.
For any Boolean function $f$ in n variables, with $n$ odd, let the WHT of its its sign function be decomposed as magnitude and phase

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

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).

## Asymptote of a Boolean function

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 by

$$F_k = (F_{k-1}, F^p_{k-1}, F^p_{k-1}, -F_{k-1}).$$

The attached Boolean function is $f_k$ of sign function $F_k$.

**Satz**

The sequence of normalized Rayleygh quotients of $f_k$ is nondecreasing.

Since a bounded nondecreasing sequence of reals converge we can define the asymptote of a Boolean function f by the limit of the normalized Rayleygh quotients of $f_k$ with initial condition $f_0 = f$ for $k$ large.

## Asymptote : numerics

| $n$ | 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 |

## Constructions

Secondary constructions combine several BF of lower arity
Primary Constructions comprize :

- Maiorana McFarland
- Dillon partial Spreads
- Monomial, Binomial (open problem)

## Maiorana McFarland functions

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, $\phi$ a permutation of $\mathbb{F}_{2^{n/2}}$ and $g$ arbitrary Boolean.
A MMF 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.

## Connection with self dual codes

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.

## Counting issues

**Remark** Any self-dual code of length $n$ gives rise to say $K$ 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.

## Dillon Partial Spreads

Let $x, y \in \mathbb{F}_{2^{n/2}}$. The class denoted by $\mathcal{PS}_{ap}$ consists of so-called Dillon's functions 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 $g(0) = 0$.

**Satz**

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

## Class symmetries

A class symmetry is an operation on Boolean functions that leave the self dual bent class invariant as a whole.
Define, following Janusz, 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 $2n$.

**Satz**

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.

## I-bent functions

Following Riera-Parker, 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, for some $m \leq n$.

**Satz**

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

## Direct sum

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 $f(x)+g(y)$.

**Satz**

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

## Indirect sum

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

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

Some results of Carlet imply.

**Satz**

If $f_1, f_2$ (resp. $g_1, g_2$) are bent functions of dualities both $\epsilon$ (resp. both $\nu$ ) their indirect sum is bent of duality $\epsilon + \nu$. If $f_1$ is bent 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 $\epsilon$.

## Spectrum of $H_n$

**Satz**

The spectrum of $\mathcal{H}_n$ consists of the two eigenvalues $\pm 1$ with the same mutiplicity $2^{n-1}$.
A basis of the eigenspace attached to 1 is formed of the rows of the matrix $(H_{n-1} + 2^{n/2} I_{2^{n-1}}, H_{n-1})$.

The first statement comes from the Hadamard property

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

and the fact that $Tr(H_n) = 0$.
The second follows from that equation and from the tensor product $H_n = H \otimes H_{n-1}$.

## Spectral approach to self dual bent functions

The next result follows immediately by the preceding Lemma.

**Satz**

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.
Conversely every self dual bent function can be represented in this way.

## Search Algorithm for self dual bent functions

We give an algorithm to generate all self dual bent functions of degree at most $k$.

**Algorithm** $SDB(n,k)$ For all $Z$ in $RM(k,n-1)$

1. Compute all $Y$ as $Y := Z + \frac{2H_{n-1}}{2^{n/2}}Z$.
2. 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

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

## And anti self dual bent functions ?

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

**Satz**

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 a self dual bent function in $n$ variables.

A direct search algorithm analogue to $SDB(n, k)$ can be easily formulated.

## Connection with plateaued functions

Following Zheng & Zhang 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 $2^{n-r/2}$.

**Satz**

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 $\{\pm 1\}^{n-1}$, then both $Y$ and $Z$ are sign functions of plateaued Boolean functions of order $n-2$ in $n-1$ variables.

## Numerics I

We have classified all self-dual bent functions of up to 6 variables.

TAB.: Self-Dual Bent Functions of 2 and 4 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 |

## Numerics II

TAB.: Self-Dual Bent Functions of 6 Variables

| Representative from equivalence class | Size |
|---|---|
| $12 + 34 + 56$ | 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 |

## Numerics III

We have classified all quadratic self-dual bent functions of 8 variables. Table 3 gives a representative from each equivalence class, and the number of functions in each class.

Tab.: 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 |

## Motivation for NON self dual bent functions

After this study the following questions are natural

- Study the Rayleigh quotient of an unrestricted bent function : may NOT be self dual or anti self dual
- Give an algorithm to construct all bent functions of given Rayleigh quotient
- Rayleigh quotient of some classical primary constructions
- Rayleigh quotient of some classical secondary constructions

Define normalized Rayleigh quotient as

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

## Decomposing the sign function

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 $\langle F, F\rangle = \langle F^+, F^+\rangle + \langle F^-, F^-\rangle$,
with normalized rayleigh quotient

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

. 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 $\{0, \pm 1\}$.

## Decomposing their support

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.

## Characterizing the Rayleigh quotient

By observing that $\hat{F} = 2^{n/2}(F^+ - F^-)$, and that $S_f = \langle F, \hat{F} \rangle$, we obtain

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

or combinatorially

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

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

## Constructing $F^+$ with given support

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 $S_+$.
Same proof as in self dual bent case.

## Constructing $F^-$ with given support

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 $S_-$.

Same proof as in anti self dual bent case.

## Adding up : bent functions with given Rayleigh quotient

we give an algorithm to generate all bent functions with given zero set $S_+$, and therefore, with 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.

Compared to brute force exhaustive search of complexity $2^{2^n}$ this algorithm is of complexity $2^R$ with $R < 2^{n-1}$

## Elementary properties

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

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

## Symmetries

Recall the "orthogonal group" of index $n$ over $\mathbb{F}_2$ as

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

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 $N_g = N_f$.
The next result shows that the distribution of the NRF is symmetric about the origin.
Define $g$ by $g(x) := f(x+d) + d \cdot x$.
If $d \in \mathbb{F}_2^n$ then $g$ is also bent, and $N_g = (-1)^{d \cdot d} N_f$.

# MMF

**Satz**

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

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

The main interest is to exhibit bent functions with zero Rayleigh quotient.

**Satz**

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 $N_f = 0$.

# Dillon

Let $x, y \in \mathbb{F}_{2^{n/2}}$. The class denoted by $\mathcal{PS}_{ap}$ 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**.

**Satz**

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

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

# Indirect sum constructions

There are many possibilities.

**Satz**

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

$$N_f = N_a N_c.$$

**Satz**

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

$$N_f = N_a N_c.$$

## Numerics in 4 variables

TAB.: Number of Bent Functions of Four Variables with given Rayleigh Quotient

| $N_f$ | Functions |
|---|---|
| $\pm 16$ | 40 |
| $\pm 8$ | 192 |
| $\pm 4$ | 384 |
| 0 | 280 |
| Total | 896 |

## Numerics in 6 variables

TAB.: Number of Bent Functions of Six Variables with given Rayleigh Quotient

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

## Open problems

PhD topic : give an algorithm to construct all bent function with prescribed Rayleigh quotient *up to orthogonal equivalence*

The Hadamard Leitmotiv can come back each time there is a new generalization of bent functions, with possibly a different Fourier transform matrix.

- generalized bent functions as per K.U. Schmidt :

  $$f : \mathbb{F}_2^n \longrightarrow \mathbb{Z}_4.$$

  the WHT matrix is the same
- bent functions as per Kumar et al

  $$f : \mathbb{Z}_4^n \longrightarrow \mathbb{Z}_4,$$

  is difficult
- bent functions of the elementary abelian type

  $$f : \mathbb{F}_p^n \longrightarrow \mathbb{F}_p,$$

  for $p$ odd.