# A lot of bent functions

Jacques Wolfmann

SUBMITTED

# A LOT OF BENT FUNCTIONS

J.WOLFMANN

Abstract. We introduce an infinite sequence $(F_i)_{i\in\mathbb{N}}$ of boolean functions whose terms all are bent functions. Furhermore we present a constrution of a lot of distinct bent function.

## 1. Introduction

$\mathbb{F}_2$ is the finite field of order 2 and a $m$-boolean function is a map from $\mathbb{F}_2^m$ to $\mathbb{F}_2$. As usual, in order to benefit from the properties of a finite field we identify the $\mathbb{F}_2$-vector space $\mathbb{F}_2^m$ with the finite field $\mathbb{F}_{2^m}$.

The Fourier transform (or Walsh transform) $\hat{F}$ of a m-boolean function $F$ is the map from $\mathbb{F}_{2^m}$ into $\mathbb{Z}$ defined by:
$\hat{F}(v) = \sum_{x\in\mathbb{F}_2^m}(-1)^{f(x)+Tr(vx)}$ where $Tr$ is the trace of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$.
$\hat{F}(v)$ is called the Fourier coefficient of $v$.
Notation: If $e \in \mathbb{F}_{2^m}$ then $T_e(x) = Tr(ex)$ where $Tr$ is the trace of $\mathbb{F}_{2^m}$.
It is easy to prove that:

(1) $\hat{F}(v) = 2^m - 2w(F + T_v)$

two where $w$ denotes the weight of a boolean function.

$F$ is bent if all its Fourier coefficients are in $\{-2^{m/2}, 2^{m/2}\}$.
$F$ is near-bent if all its Fourier coefficients are in $\{-2^{(m+1)/2}, 0, 2^{(m+1)/2}\}$
Since the Fourier coefficients are in $\mathbb{Z}$, bent functions exist only when $m$ is even and near-bent functions exist only when $m$ is odd.
If $m = 2t$ and if $F$ is a bent function then the dual $\tilde{F}$ of $F$ is the $(2t)$-boolean function defined by: $\hat{F}(v) = (-1)^{\tilde{F}(v)}2^t$ where $\hat{F}$ is the Fourier transform of $F$. It is well-known and easy to proof that the dual $\tilde{F}$ of a bent function $F$ is a bent function and that the dual of $\tilde{F}$ is $F$.

Bent functions were introduced by Rothaus in [6] .They are interesting for Coding Theory, Cryptology and Sequences and were the topic of a lot of works. See for instance [2], [5] Chap. 14, [7], [1].

The main results of this work are the introduction of infinite sequences of bent functions (section 5) and a construction of a set of distinct bent functions (section 6).

*Key words and phrases.* Bent Functions, Near-Bent Functions.

## 2. special representation of $\mathbb{F}_2^{2t}$

In this paper we describe every $(2t)$-bent function by means of two $(2t-1)$-near-bent functions. This approach was already used in [4] [8],[9],[10] and for the construction of the famous Kerdock codes (see [3] and [5] Chap.15).
We describe every $2t$-boolean function $F$ by means of two $(2t-1)$-boolean functions as follows:
we identified the finite field $\mathbb{F}_{2^{2t}}$ with:

$\mathbb{F}_{2^{2t-1}} \times \mathbb{F}_2 = \{X = (x, \nu) \mid x \in \mathbb{F}_{2^{2t-1}}, \nu \in \mathbb{F}_2\}$.

In this way a $(2t)$-boolean function $F$ is now defined by:

$(*) \quad F(x, \nu) = (\nu + 1)f(x) + \nu g(x)$

We are now able to introduce an infinite sequence of bolean functions whose terms all are bent functions. where $f$ and $g$ are the two $(2t-1)$-boolean functions such that

$f(x) = F(x, 0)$ and $g(x) = F(x, 1)$.

It is easy to check that for every $(x, \nu)$ the rigth member of $(*)$ is equal to $F(x, \nu)$.
Conversely, if $f$ and $g$ are any two $(2t-1)$-boolean functions then $(*)$ define a $(2t)$-boolean function $F$ and $f$ and $g$ are the restriction of $F$ respectively to $\mathbb{F}_{2^{2t-1}} \times \{0\}$ and $\mathbb{F}_{2^{2t-1}} \times \{1\}$.

We denote such a function by $F = [f, g]$.

. We now characterize the $(2t-1)$-boolean functions $f$ and $g$ such that $F = [f, g]$ is a bent function. The next proposition is a special version of a well-known result on the hyperplane section of a support of a bent function. A proof is given in [9].

**Proposition 1.**
*Let $f$ an $g$ be two $(2t-1)$-boolean functions and let $\hat{f}$ and $\hat{g}$ be respectively their Fourier Transforms. $F = [f, g]$ is a bent function if and only if:*

*(a) $f$ and $g$ are near-bent.*
*(b) $\forall a \in \mathbb{F}_{2^{2t-1}} \mid \hat{f}(a) \mid + \mid \hat{g}(a) \mid = 2^t$.*

*Proof.*
See [9], Proposition 14. □

Remark: (b) means that one of $\mid \hat{f}(a) \mid$ and $\mid \hat{g}(a) \mid$ is equal to $2^t$ and the other one is equal to 0.

## 3. The machinery

**Definition 2.** *If $f$ is a $(2t-1)$-boolean function then::*
*$\hat{I}_f^0$ is the indicator of the set $\{x \in \mathbb{F}_{2^{2t-1}} \mid \hat{f}(x) = 0\}$*
*$\hat{I}_f^-$ is the indicator of the set $\{x \in \mathbb{F}_{2^{2t-1}} \mid \hat{f}(x) = -2^t\}$*
*deduce $\hat{I}_f^+$ is the indicator of the set $\{x \in \mathbb{F}_{2^{2t-1}} \mid \hat{f}(x) = 2^t\}$*

*In other words:* $\hat{I}_f^0(x) = 1$ *if and only if* $\hat{f}(x) = 0$, $\hat{I}_f^-(x) = 1$ *if and only if* $\hat{f}(x) = -2^t$ *and* $\hat{I}_f^+(x) = 1$ *if and only if* $\hat{f}(x) = 2^t$.

**Definition 3.**
*If* $f$ *is a* $m$*-boolean function and if* $\omega \in \mathbb{F}_{2^m}$ *the derivative of* $f$ *relatively to* $\omega$*, denoted by* $D_\omega(f)$*, is the* $m$*-boolean function defined by* $D_\omega(f)(x) = f(x) + f(x + \omega)$.

Now we need some preliminary results.

**Lemma 4.**
*Let* $F = [f, g]$ *be a* $(2t)$*-bent function and let* $\hat{F}$ *be the Fourier transform of* $F$.

*a)* $\hat{F}(u, 0) = \hat{f}(u) + \hat{g}(u)$.

*b)* $\hat{F}(u, 1) = \hat{f}(u) - \hat{g}(u)$.

*c) If* $f + g = t_u$ *then* $\hat{g}(a) = \hat{f}(a + u)$

*Proof.*
See [9], Lemma 13. □

We now introduce a connexion between the dual of a bent function $[f_0, f_1]$ and the indicators $\hat{I}_f^0$, $\hat{I}_f^-$ and $\hat{I}_f^+$ .

**Theorem 5.**
*Let* $F = [f, g]$ *be a* $(2t)$*-bent function and let* $\tilde{F} = [\tilde{f}, \tilde{g}]$ *be its dual function. Then:*

*a)* $\tilde{f} = \hat{I}_f^- + \hat{I}_g^-$
*b)* $\tilde{f} + \tilde{g} = \hat{I}_f^0$.
*c)* $\hat{I}_f^0 + \hat{I}_g^0 = 1$
*d) If* $f + g = t_u$ *then:*

$\tilde{f}(x) = \hat{I}_f^-(x) + \hat{I}_f^-(x + u)$ *(in other words* $\tilde{f} = D_u(\hat{I}_f^-)$*).*
$\tilde{g}(x) = \hat{I}_f^-(x) + \hat{I}_f^+(x + u)$.

*Proof.*

Proposition 1 says that one of $\mid \hat{f}(a) \mid$ and $\mid \hat{g}(a) \mid$ is equal to $2^t$ and the other one is equal to 0.
It follows that every $a$ in $\mathbb{F}_{2^{2t-1}}$ belongs to one of the following sets:

$\mathcal{A}_1 = \{a \in \mathbb{F}_{2^{2t-1}} \mid \hat{f}(a) = -2^t \text{ and } \hat{g}(a) = 0\}$
$\mathcal{A}_2 = \{a \in \mathbb{F}_{2^{2t-1}} \mid \hat{f}(a) = 0 \text{ and } \hat{g}(a) = -2^t\}$
$\mathcal{A}_3 = \{a \in \mathbb{F}_{2^{2t-1}} \mid \hat{f}(a) = 2^t \text{ and } \hat{g}(a) = 0\}$
$\mathcal{A}_4 = \{a \in \mathbb{F}_{2^{2t-1}} \mid \hat{f}(a) = 0 \text{ and } \hat{g}(a) = 2^t\}$

Remark that $\mathcal{A}_1$ is the set of elements $a$ of $\mathbb{F}_{2^{2t-1}}$ such that $\hat{f}(a) = -2^t$. In other words $\mathcal{A}_1$ is the support of $\hat{I}_f^-$.

Similarly:
$\mathcal{A}_2$ is the support of $\hat{I}_g^-$, $\mathcal{A}_3$ is the support of $\hat{I}_f^+$,
$\mathcal{A}_4$ is the support of $\hat{I}_g^+$
The distribution of the Fourier coefficients of a near bent function is well known (see for instance Prop. 4 in [1]). This means that $\mathcal{A}_i$ is non empty for $i = 1, 2, 3, 4$. Furthermore, obviously:
$\mathcal{A}_i \cap \mathcal{A}_j = \emptyset$ if $i \neq j$ and only if $\mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{A}_3 \cup \mathcal{A}_4 = \mathbb{F}_{2^{2t-1}}$.

Proof of a)
The definition of the dual of $F$ induces that $(a, \eta)$ is in the support of $\tilde{F}$ if and only if $\hat{F}(a, \eta) = -2^t$.
Since $\hat{F}(a, 0) = \hat{f}(a) + \hat{g}(a)$ (Theorem 5) then:
$\hat{F}(a, 0) = -2^t$ if $a \in \mathcal{A}_1$ or $a \in \mathcal{A}_2$. In other words: $\tilde{f}(a) = 1$ if and only if $a \in \mathcal{A}_1 \cup \mathcal{A}_2$. Therefore $\mathcal{A}_1 \cup \mathcal{A}_2$ is the support of $\tilde{f}$.
Since $\mathcal{A}_1$ is the support of $\hat{I}_f^-$ and $\mathcal{A}_2$ is the support of $\hat{I}_g^-$ and because these two sets are disjoint then $\mathcal{A}_1 \cup \mathcal{A}_2$ is the support of $\hat{I}_f^- + \hat{I}_f^-$. This means $\tilde{f} = \hat{I}_f^- + \hat{I}_f^-$.

Proof of b)
$\hat{I}_f^0$ is the indicator of the set $\{x \in \mathbb{F}_{2^{2t-1}} \mid \hat{f}(x) = 0\}$.
We know that $(a, 0)$ is in the support of $\tilde{F}$ if and only if $a \in \mathcal{A}_1 \cup \mathcal{A}_2$. and $(a, 1)$ is in the support of $\tilde{F}$ if and only if $a \in \mathcal{A}_1 \cup \mathcal{A}_4$.
Hence the support of $\tilde{f}$ is $\mathcal{A}_1 \cup \mathcal{A}_2$ and the support of $\tilde{g}$ is $\mathcal{A}_1 \cup \mathcal{A}_4$.
Consequently the support of $\tilde{f} + \tilde{g}$ is $\mathcal{A}_2 \cup \mathcal{A}_4$. This set is also the support of $\hat{I}_f^0$, this means $\tilde{f} + \tilde{g} = \hat{I}_f^0$.

Proof of c)
$\hat{I}_f^0$ is the indicator of the set $\{a \in \mathbb{F}_{2^{2t-1}} \mid \hat{f}(a) = 0\}$.
Then $\mathcal{A}_2 \cup \mathcal{A}_4$ is the support of $\hat{I}_f^0$,
$\hat{I}_g^0$ is the indicator of the set $\{a \in \mathbb{F}_{2^{2t-1}} \mid \hat{g}(a) = 0\}$. We see that $\mathcal{A}_1 \cup \mathcal{A}_3$ is the support of $\hat{I}_g^0$.
Since $\mathcal{A}_2 \cup \mathcal{A}_4$ and $\mathcal{A}_1 \cup \mathcal{A}_3$ are disjoint then $\mathcal{A}_2 \cup \mathcal{A}_4 \cup \mathcal{A}_1 \cup \mathcal{A}_3$ is the support of $\hat{I}_f^0 + \hat{I}_g^0$. We know that $\mathcal{A}_2 \cup \mathcal{A}_4 \cup \mathcal{A}_1 \cup \mathcal{A}_3 = \mathbb{F}_{2^{2t-1}}$ and this proves that $\hat{I}_f^0 + \hat{I}_g^0 = 1$.

Proof of d)
$\hat{I}_f^0$ is the indicator of the set $\{x \in \mathbb{F}_{2^{2t-1}} \mid \hat{f}(x) = 0\}$
Now assume $f + g = t_u$. From the descriptions of $\mathcal{A}_1$ and $\mathcal{A}_2$, if $a \in \mathcal{A}_1$ then $a + u \in \mathcal{A}_2$ and if $b \in \mathcal{A}_2$ then $b = a + u$ with $a = b + u \in \mathcal{A}_1$.
Hence $\mathcal{A}_2 = \{a + u \mid a \in \mathcal{A}_1\}$. We know that the support of $\tilde{f}$ is $\mathcal{A}_1 \cup \mathcal{A}_2$ and that $\mathcal{A}_1$ is the support of $\hat{I}_f^-$. It follows that:
$\tilde{f}(x) = \hat{I}_f^-(x) + \hat{I}_f^-(x + u) = D_u \hat{I}_f^-(x)$ □

## 4. Preliminary results

The next results are important tools for the proof of the main Theorems.

**Theorem 6.** *(McGuire and Leander)*
*Let $f$ be a near-bent function.*
*$[f, f + t_e]$ is a bent-function if and only if $D_e(\hat{I}_f^0) = 1$.*

*Proof.*
See [4], Theorem 3. □

**Theorem 7.** *(W)*
*Let $f$ be a $(2t-1)$-near-bent function.*
*let $\omega$ be in $\mathbb{F}_{2^{2t-1}}$ and let $\epsilon$ be in $\mathbb{F}_2$.*

$$\textit{If } D_\omega f = \epsilon \textit{ then } \hat{I}_f = t_\omega + \epsilon$$

Remark: According to the definition of $\hat{I}_f$ this lemma means that if $D_\omega f = \epsilon$ then $\hat{f}(x) = 0$ if and only if $t_\omega(x) = 1 + \epsilon$.

*Proof.* $\hat{f}(u) = \sum_{x \in \mathbb{F}_{2^{2t-1}}} (-1)^{f(x)+tr(ux)} = 2^{2t-1} - 2w(f + tr(ux)$.
$\hat{f}(u) = 0$ if and only if $w(f + t_u) = 2^{2t-2}$.
$D_\omega f = \epsilon$ means that $f(x + \omega) = f(x) + \epsilon$.
The transform $\tau : x \to x + \omega$ is a permutation of $\mathbb{F}_{2^{2t-1}}$ and then preserves the weight of every $(2t-1)$-Boolean function. Thus:

$$\sharp\{x \mid f(x) + tr(ux) = 1\} = \sharp\{x \mid f(x + \omega) + tr(u(x + \omega)) = 1\}.$$

$(E)\ \sharp\{x \mid f(x) + tr(ux) = 1\} = \sharp\{x \mid f(x) + \epsilon + tr(ux) + tr(u\omega) = 1\}$.
If $tr(u\omega) + \epsilon = 1$ the right hand member of $(E)$ is:

$$\sharp\{x \mid f(x) + tr(ux) = 0\} = 2^{2t-1} - \sharp\{x \mid f(x) + tr(ux) = 1\}$$

Hence $(E)$ becomes:

$$\sharp\{x \mid f(x) + tr(ux) = 1\} = 2^{2t-1} - \sharp\{x \mid f(x) + tr(ux) = 1\}$$

In other words $w(f + t_u) = 2^{2t-1} - w(f + t_u)$ .

Conclusion:
$\bar{f}_i$ is a near-bent function for every $i \in \mathbb{N}$.
If $tr(u\omega) + \epsilon = 1$ then $w(f + t_u) = 2^{2t-2}$ which is equivalent to $\hat{f}(u) = 0$.

For every $\epsilon$ the number of $u$ such that $tr(u\omega) + \epsilon = 1$ is $2^{2t-2}$ and this is also the number of $u$ such that $\hat{f}(u) = 0$ (see Prop. 4 in [1]). Then, immediately: $\hat{f}(u) = 0$ if and only if $tr(u\omega) + \epsilon = 1$. This means $\hat{I}_f = t_\omega + \epsilon$ □

**Theorem 8.**
*Let $F = [f_0, f_0 + t_u]$ be a bent function with $u$ be in $\mathbb{F}_{2^{2t-1}}$ and let $\tilde{F} = [\tilde{f}_0, \tilde{f}_1]$ be its dual. Let $r$ be in in $\mathbb{F}_{2^{2t-1}}$.*
*$[\tilde{f}_0, \tilde{f}_0 + t_r]$ is a bent function if and only if $tr(ur) = 1$.*

*Proof.*
1) Since the dual of $\tilde{F}$ is $F$ then, according to Theorem 5, b):
$f_0 + f_0 + t_u = \hat{I}^0_{\tilde{f}_0}$ that is $\hat{I}^0_{\tilde{f}_0} = t_u$
Now we know from McGuire and Leander that $[\tilde{f}_0, \tilde{f}_0 + t_r]$ is a bent-function. if and only if $D_r(\hat{I}^0_{\tilde{f}_0}) = 1$.
$D_r(\hat{I}^0_{\tilde{f}_0})(x) = D_r(t_u)(x) = t_u(x) + t_u(x+r) = tr(ux) + tr(u(x+r))$
$= tr(ur)$.
It follows that $[\tilde{f}_0, \tilde{f}_0 + t_r]$ is a bent function if and only if $tr(ur) = 1$.
2) According to Theorem 5,c),: $\hat{I}^0_{\tilde{f}_0} + \hat{I}^0_{\tilde{f}_1} = 1$. We deduce that
$D_r(\hat{I}^0_{\tilde{f}_0}) = D_r(\hat{I}^0_{\tilde{f}_1})$ whence $D_r(\hat{I}^0_{\tilde{f}_1})(x) = tr(ur)$. As previously it comes:
$[\tilde{f}_1, \tilde{f}_1 + t_r]$ is a bent function if and only if $tr(ur) = 1$. □

**Corollary 9.**
*From a bent function $F = [f_0, f_0 + t_u]$ with $u$ in $\mathbb{F}_{2^{2t-1}}$,*
*we obtain $2^{2t-2}$ distinct bent functions $[\tilde{f}_0, \tilde{f}_0 + t_r]$ such that $tr(ur) = 1$*
.

## 5. Sequences of Bent Functions

We are now able to introduce an infinite sequence of bolean functions whose terms all are bent functions.

**Theorem 10.**
*Define sequences $(F_i)_{i\in\mathbb{N}}$ of $(2t)$-boolean functions by:*

*1) $F_0 = [f_0, f_0 + t_{r_0}]$ with $f_0$ a $(2t-1)$-boolean function and $r_0 \in \mathbb{F}_{2^{2t-1}}$, and for $i \geq 1$:*

*$F_i = [f_i, f_i + t_{r_i}]$ with $f_i(x) = D_{r_{i-1}}\hat{I}^-_{f_{i-1}}(x)$ and $tr(r_{i-1}r_i) = 1$.*

*If $F_0$ is a bent function then:*
*$F_i$ is a bent function for every $i \in \mathbb{N}$.*
*$f_i$ is a near-bent function for every $i \in \mathbb{N}$*

*Proof.* We prove the result by induction.
Step 1. For $i = 0$ the boolean function $F_0$ is bent by definition.
Step 2. Assume that for $j \in \mathbb{N}$: $F_j = [f_j, f_j + t_{r_j}]$ is bent.
Let $[\tilde{f}_j, \tilde{g}_j]$ be the dual of $F_j$. Applying Theorem 8 to $F_j$ it comes that $[\tilde{f}_j, \tilde{f}_j + r_{j+1}]$ is bent if and only if $tr(r_j r_{j+1}) = 1$.
According to Theorem 5, d),we know that:
$\tilde{f}_j = D_{r_j}\hat{I}^-_{f_j}(x)$ and then $[\tilde{f}_j, \tilde{f}_j + r_{j+1}]$ is bent. This last function is nothing but $F_{j+1}$ and this proves that $F_{j+1}$ is bent.
Proposition 1 implies that $f_i$ is a near-bent function for every $i \in \mathbb{N}$. □

**Examples:**

1) Kerdock
- $f_0 = Q_u\ Q(x) = \sum_{j=1}^{t-1} tr\left(x^{2^j+1}\right), Q_e(x) = Q(ex)$.
- $r_0 = u$.

This is the initial Kerdock Bent Function (see [3] and [5]).

2) Kasami-Welch
- $f_0(x) = tr(x^{4^s-2^s+1})$ with $2t-1 \not\equiv 0 \mod 3$ and $3s \equiv \pm 1 \mod (2t-1)$, $s < t$,
- $r_0 = 1$.

It is proved in [4] that in this case $[f_0, f_0 + t_1]$ is a bent function.

**Important Remark:**

Of course we whish to find distinct bent functions as terms of $F$. If $F_i = [f_i, f_i + t_{r_i}]$ is equal to $F_l$ with $l < i$ we just have to change $r_i$ by any other $s_i$ such that $tr(r_{i-1}s_i) = 1$. We have $2^{2t-2} - 1$ possibilities.

In this way we can expect to find a lot of bent functions as member of $F$.

**Open question:**

What is the maximum of distinct bent functions as terms of a sequence $F$ ?

## 6. A construction

In the sequence $F$ there are infinitely many terms $F_j$ which are bent functions but they are not distinct since the number of all bent function is limited. Corollary 9 gives $2^{2t-2}$ distinct bent functions. The following constuction improves this result by a specific choice of the $u_i$'s.

Construction:
Let $F_0 = [f, f + t_{u_0}]$ be a bent function.
Let $\tilde{F}_0 = [\tilde{f}_0, \tilde{g}_0]$ be the dual of $F_0$. Define $R_0 = \{v \mid tr(u_0 v) = 1\}$.
We know from Corollary 9 that $B_0 = \{[\tilde{f}_0, \tilde{f}_0 + t_{u_1}] \mid tr(u_0 u_1) = 1\}$ is a set of bent functions.
Now let $u_1$ be in $R_0$ and $u_1 \neq u_0$.
Define $R_1 = \{v \mid tr(u_1 v) = 1, tr(u_0 v) = 0\}$ and
more generally, if $1 \leq j \leq 2t-2$ define
$R_j = \{v \mid tr(u_j v) = 1, tr(u_{j-1} v) = 0, ..., tr(u_0 v) = 0\}$.
with $u_j$ in $R_{j-1}$ and $B_j = \{[\tilde{f}_j, \tilde{f}_j + t_v] \mid v \in R_j\}$.
$B_j$ is a set of bent functions which are not in $B_{j-1}, B_{j-2}, .....B_1, B_0$.

**Theorem 11.**
$(\bigcup B_j)_{j=0}^{2t-2}$ *is a set of distinct bent functions. .*

Question: what is the cardinality of $(\bigcup B_j)_{j=0}^{2t-2}$ ?

**Theorem 12.**
*If* $u_j \in R_{j-1}$ *and* $u_j \notin < u_{j-1}, u_{j-2}, ...u_1, u_0 >$ *(subspace generated by* $u_0, u_1, ..u_{j-1}$*) then* $(\bigcup B_j)_{j=0}^{2t-2}$ *is a set of* $2^{2t-1}-2$ *distinct bent functions.*

*Proof.* First remember that $t_i(x) = tr(u_i x)$.
Step 1:
if $0 \leq j \leq 2t-1$ the linear forms $t_0, t_1, ..t_j$ are linearly independant.
We prove this result by induction.
$t_0$ and $t_1$ are distinct and non zero since $u_1 \neq u_0$ and $tr(u_1 u_0) = 1$. Thus they are linearly independant.
Now assume $t_0, t_1, ..t_{j-1}$ linearly independant. Because of $u_j \notin < u_{j-1}, u_{j-2}, ...u_1, u_0 >$ and by using the vector space isomorphism $u_l \longrightarrow t_l$ then:
$t_j \notin < t_{j-1}, t_{j-2}, ...t_1, t_0 >$. Hence $t_j, t_{j-1}, t_{j-2}, ...t_1, t_0$ are linearly independant.

Step 2: $R_j$ contains $2^{2t-2-j}$ elements.
The $j+1$ linear forms $t_0, t_1 ... t_j$ of $R_j$ are linearly independant then the rank of the system $tr(u_j v) = 1, tr(u_{j-1} v) = 0, ..., tr(u_0 v) = 0$ is $j+1$ and its kernel has dimension $2t-1-(j+1) = 2t-2-j$. Therefore, the cardinality of $R_j$ which the number of solutions of the previous system is $2^{2t-2-j}$.

Step 3: From the definition the cardinality of $(\bigcup B_j)_{j=0}^{2t-2}$ is the cardinality of $(\bigcup R_j)_{j=0}^{2t-2}$ which is $\sum_{j=0}^{2t-2} 2^{2t-2-j} = 2^{2t-1} - 2$. From the construction of $R_j$ and $B_j$, al the member of $(\bigcup B_j)_{j=0}^{2t-2}$ are bent functions. □

**Remark 13.**
*The cardinality of the set of the $u_j$ used in the construction is almost the cardinality of $\mathbb{F}_{2^{2t-1}}$.*

## 7. Existence Problem

*In order to validate Theorem 12 we have to study the existence of $u_j \in R_{j-1}$ and $u_j \notin < u_{j-1}, u_{j-2}, ...u_1, u_0 >$.*

*The following Lemma was proved by Philippe Langevin.*

**Lemma 14.**
*$R_j$ is defined as above. If $0 \leq j < 2t-2$ there exist elements in $R_j$ which are not in in the subspace generated by $u_0$,$u_1$, ..., $u_j$.*

*Proof.* In order to prove the Lemma, we count how many elements $v$ of the space $\langle u_j, \ldots, u_1, u_0 \rangle$ are in $R_j$. A such element decomposes $v = \lambda_j u_j + \cdots + \lambda_1 u_1 + \lambda_0 u_0$ where the scalar $\lambda_i \in \mathbb{F}_2$ satisfy the system:

$$\forall k, \quad 0 \leq k \leq j, \quad \mathrm{tr}(u_k v) = \sum_{i=0}^{j} \lambda_i \mathrm{tr}(u_i u_k) = \begin{cases} medskip 1, & j = k; \\ 0, & k < j. \end{cases}$$

Since $u_i$ belongs to $R_{i-1}$ and $u_k$ belongs to $R_{k-1}$ then $\mathrm{tr}(u_i u_k)$ vanishes whenever the integers $i$ and $k$ are not consecutive. The scalar $\lambda_i$ satisfy

the $j+1$ equations:

$$\begin{aligned}\lambda_{j-1} &= \mathrm{tr}(u_j)\lambda_j + 1;\\ \lambda_{k-1} &= \mathrm{tr}(u_k)\lambda_k + \lambda_{k+1} \quad (1 \le k < j);\\ 0 &= \mathrm{tr}(u_0)\lambda_0 + \lambda_1.\end{aligned}$$

There are precisely two $(j+1)$-tuples that satisfy the first $j$-equations (for $\lambda_0 = 0$ or $\lambda_0 = 1$) . By searching if these solutions are compatible with the equation $(E_j)$ : $\lambda_{j-1} + \lambda_j tr(u_j) = 1$. we see that.
the system may have 0, 1 or 2 solutions.
It is easy to see that the cardinaly of $R_j$ greater or equal to 4 thus at least two of its elements are not in the space $\langle u_j, \ldots, u_1, u_0\rangle$. □

## 8. Conclusion

*Starting from any bent function of the type $[f, f + t_r]$ we have constructed a seqence and a set of boolean functions both containing a large number of bent fuctions. This gives rice to open questions for instance about the maximum number of distinct bent functions as terms of such a sequence.*

## 9. References

*[1] A.Canteault,P.Charpin, Decomposing Bent Functions*
*IEEE Transactions on Information Theory, vol.49, **8**, (2003), 2004-2019.*

*[2] J.F.Dillon, Elementary Hadamard Difference Sets.*
*Ph.D. Thesis, University of Maryland(1974).*

*[3] A. M.Kerdock A class of low-rate non linear codes.*
*Information and Control 20, pp. 182-187, 1972.*

*[4] G. Leander, G. McGuire, Construction of Bent Functions from Near-Bent Functions.*
*Journal of Combinatorial Theory, Series A,vol.116,**4**,(2009),960-970.*

*[5] F.J.Mac Williams, N.J.A.Sloane*
*The Theory of Error Correcting Codes, North-Holland, Amsterdam, 1977.*

*[6] O.S.Rothaus, On Bent Functions.*
*Journal of Combinatorial Theory, series A, 20, (1976), 300-305.*

*[7] J.Wolfmann, Bent Functions and Coding Theory.*
*in Difference Sets, Sequences and their Correlation properties*
*(A. Pott, P.V. Kumar, T. Helleseth, D. Jungnickel, Eds),*
*NATO Sciences Series, Series C, vol.542, Kluwer Academic Publishers (1999) 393-418.*

*[8] J. Wolfmann, Cyclic code aspects of bent functions, in Finite Fields: Theory and Applications, AMS series "Contemporary Mathematics" volume 518, 363-384, 2010*

*[9] J. Wolfmann, Special Bent and Near-Bent Functions in Advances in Mathematics of Cmmunication, vol.8, No 1 (2014), 21-33*

*[10] J. Wolfmann, From Near-Bent to Bent: A special Case. In Topics in Finite Fields, AMS series "Contemporary Mathematics" volume 632, 359-371, 2015*

IMATH(IAA),Université de Toulon, CS 60584,83041 TOULON CEDEX9
*E-mail address:* wolfmann@univ-tln.fr