From near-bent to bent: A special case

J Wolfmann

FROM NEAR-BENT TO BENT: A SPECIAL CASE

J.WOLFMANN

Abstract. We consider the construction of $(2t)$-bent functions from two $(2t-1)$-near-bent functions in a special case. We deduce new families of bent-functions.

1. Introduction

$\mathbb{F}_2$ is the finite field of order 2. A m-Boolean function (or Boolean function in m dimensions) is a map F from $\mathbb{F}_2^m$ to $\mathbb{F}_2$. Bent functions are the Boolean functions whose Fourier coefficients have constant magnitude and were introduced by Rothaus in [6]. It means that a m-Boolean function F is bent if all its Fourier coefficients are in $\{-2^{m/2}, 2^{m/2}\}$. Since Fourier coefficient are in $\mathbb{Z}$ then bent functions in m dimensions exist only when m is even.

Bent functions are of interest for Coding Theory, Cryptology and well-correlated binary sequences. For example, they have the maximum Hamming distance to the set of affine Boolean functions.
It is easy to prove that the set $\mathcal{B}(m)$ of m-bent functions is invariant under the action of the product of the affine linear group of $\mathbb{F}_2^m$ with the group of translations of affine Boolean functions. The corresponding partition of $\mathcal{B}(m)$ under the action of this group defines an equivalence.

Two main infinite families of bent functions are known (see [7]) but in general it is very difficult to decide if any bent function is equivalent to a member of these families.

Bent functions have been the topic of a lot of works but the complete classification of bent functions is still open.
In order to improve the knowledge on bent functions, it is convenient to find new properties and constructions. This is the goal of this work.
By definition, a m-Boolean function F is near-bent (sometimes called semi-bent [4]) if all its Fourier coefficients are in $\{-2^{(m+1)/2}, 0, 2^{(m+1)/2}\}$
Near-bent functions exist only when m is odd.

It is known that the restrictions of a $(2t)$-bent function to any hyperplan and to the complement of this hyperplan (view as $(2t-1)$-Booleans functions) are near-bent. Properties of these near-bent functions are investigated in [8] in connexion with the theory of cyclic codes.
In the present paper we consider the question of the construction of

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

$(2t)$-bent functions from two $(2t-1)$-near-bent functions. A first approach of this problem appears in [5].

We restrict the problem to the special situation where the sum of the two $(2t-1)$-near-bent functions is an affine linear form of $\mathbb{F}_2^{2t-1}$. The study in this case was initiated by Leander and McGuire in [5] where they present several properties and constructions. One of their results is Theorem 14 of the present paper. In particular they obtain a non-weakly-normal bent function proving that this special point of view could produce new classes of bent functions.
In this work we introduce new properties of the $(2t-1)$-near-bent functions involved in the construction of bent functions and we deduce new infinite families of bent functions.

This paper is a continuation and a generalisation of [9]. Lemma 5, Lemma 6 and Theorem 7 are already in [9] and are recalled for convenience, Theorem 14 is in [5] while all the other Theorem, Proposition, Corollary, Lemma and the entire subsection 3.5 are new.

2. Preliminaries

2.1. **Classical definitions and results.**

We gather here some definition and well-known results that we will use in the paper. Properties (P_1) to (P_5) are classical and follow immediately from the definitions or from straightforward calculations.
The distribution given in (P_6) is a special cases of Proposition 4 in [2]. See [1],[2],[3],[7] for details.

2.1.1. *Boolean functions.*

$\mathbb{F}_{2^m}$ is the finite field of order 2^m.
A **m-Boolean function** is a map F from $\mathbb{F}_2^m$ to $\mathbb{F}_2$.
Its **weight** is the number of X in $\mathbb{F}_2^m$ such that $F(X)=1$ and is denoted by $w(F)$.

If $e \in \mathbb{F}_2^m$ then the **Derivative** of F with respect to e is the m-Boolean function D_eF defined by: $D_eF(X) = F(X) + F(X+e)$

The **Fourier transform** (or Walsh transform) $\hat{F}$ of F is the map from $\mathbb{F}_2^m$ into $\mathbb{Z}$ defined by:

$$\hat{F}(v) = \sum_{X \in \mathbb{F}_{2^m}} (-1)^{F(X)+<v,X>}$$

where $<,>$ denotes any inner product of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$.
$\hat{F}(v)$ is called the Fourier coefficient of v.
Notation: T_v is the Boolean function defined by $T_v(X) =< v, X >$.
It comes immediately:

$(P_1) : \hat{F}(v) = 2^m - 2w(F+T_v)$.

Remark: the set of $\hat{F}(v)$ when v runs through $\mathbb{F}_{2^m}$ is independent of the choice of the inner product $<,>$.

2.1.2. *Bent functions.*
A $(2t)$-Boolean function is **"bent"** if all its Fourier coefficients are in $\{-2^t, 2^t\}$ A well-known characterisation of a bent function is the following.
(P_2): A $(2t)$-Boolean function F is bent if and only if for every $e \in \mathbb{F}_2^{2t}$ the derivative D_eF is balanced:

$$\sharp\{X \mid D_eF(X) = 1\} = \sharp\{X \mid D_eF(X) = 0\}.$$

In other words F is bent if and only if the weight of D_eF is 2^{2t-1} for every e.

(P_3) Let F be a $(2t)$-boolean function and let L be an affine linear form of $\mathbb{F}_2^{2t}$.

F is a bent function if and only if $F + L$ is a bent function.

The **dual** $\tilde{F}$ of a $(2t)$-bent function F is the $(2t)$-Boolean function $\tilde{F}$ defined by: $\hat{F}(v) = (-1)^{\tilde{F}(v)}2^t$ where $\hat{F}$ is the Fourier transform of F. It is easy to prove that $\tilde{F}$ is bent and that the dual of $\tilde{F}$ is F.

(P_4): Let $\tilde{F}$ be the dual of a $(2t)$-bent function F. Then:

$$\tilde{F}(v) = 1 \text{ if and only if } \hat{F}(v) = -2^t.$$

2.1.3. *Near-bent functions.*
A $(2t-1)$-Boolean function is **"near-bent"** if all its Fourier coefficients are in $\{-2^t, 0, 2^t\}$.

In the litterature, near-bent functions are sometimes called semi-bent functions (see [4]).

(P_5) Let f be a $(2t-1)$-boolean function and let l be an affine linear form of $\mathbb{F}_2^{2t-1}$.

f is a near-bent function if and only if $f + l$ is a near-bent function.

(P_6): The distribution of the Fourier coefficients of a $(2t-1)$-near bent function f is well known (see Proposition 4 in [2]).

$$\hat{f}(v) = 2^t \quad \text{number of } v\text{: } 2^{2t-3} + (-1)^{f(0)}2^{t-2}$$
$$\hat{f}(v) = 0 \quad \text{number of } v\text{: } 2^{2t-2}$$
$$\hat{f}(v) = -2^t \quad \text{number of } v\text{: } 2^{2t-3} - (-1)^{f(0)}2^{t-2}.$$

2.2. **A two-variable representation.**

2.2.1. *Special description of* $\mathbb{F}_2^{2t}$.
We identify $\mathbb{F}_2^{2t}$ with the finite field $\mathbb{F}_{2^{2t}}$ and $\mathbb{F}_{2^{2t}}$ with:

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

If $m = 2t-1$ the inner product used to calculate the Fourier coefficients is defined by $< a, x >= tr(ax)$ where tr is the trace function of $\mathbb{F}_{2^{2t-1}}$.
Notation: For every $a \in \mathbb{F}_{2^{2t-1}}$ the $(2t-1)$-Boolean function t_a is defined by $t_a(x) = tr(ax)$.

If $m = 2t$, a special inner product adapted to the above special description of $\mathbb{F}_2^{2t}$ will be defined in 2.2.3.

2.2.2. *Special representation of* $(2t)$*-Boolean functions.*
Using the description of $\mathbb{F}_{2^{2t}}$ as $\mathbb{F}_{2^{2t-1}} \times \mathbb{F}_2$ then a $(2t)$- Boolean function F now is a map from $\mathbb{F}_{2^{2t-1}} \times \mathbb{F}_2$ to $\mathbb{F}_2$.

$$\forall (u, \nu) \in \mathbb{F}_{2^{2t-1}} \times \mathbb{F}_2 : F(u, \nu) = 0 \text{ or } 1$$

Let F be such a function. Define two $(2t-1)$-Boolean functions f_0 and f_1 by $f_0(u) = F(u, 0)$ and $f_1(u) = F(u, 1)$.
Now let ϕ be the $(2t)$-Boolean function defined by:
$\phi(x, y) = (y + 1)f_0(x) + yf_1(x)$.
If $\nu = 0$ then $\phi(u, 0) = f_0(u) = F(u, 0)$.
If $\nu = 1$ then $\phi(u, 1) = f_1(u) = F(u, 1)$.
Therefore, for all (u, ν) then $F(u, \nu) = \phi(u, \nu)$ whence $\phi = F$.

$$F(x, y) = (y + 1)f_0(x) + yf_1(x)$$

This is the **two-variable representation** of F.
The $(2t)$-Boolean function F is completely defined by the two $(2t - 1)$-Boolean functions f_0 and f_1.

Notation:
F is denoted by $[f_0, f_1]$
f_0 and f_1 are called the **components** of F.

From the definitions of f_0 and f_1 we have:

$(P_7) : w(F) = w(f_0) + w(f_1)$

2.2.3. *Representation of* $(2t)$*-linear forms.*
The purpose of this part is to express $(2t)$-linear forms and the inner product $<,>$ over $\mathbb{F}_{2^{2t}}$ used in the calculation of the Fourier coefficients in such a way which is consistent with the identification of $\mathbb{F}_{2^{2t}}$ as $\mathbb{F}_{2^{2t-1}} \times \mathbb{F}_2$.
With this identification it is easy to check that $<,>$ defined by $< (a, \eta), (x, \nu) >= tr(ax)+\eta\nu$ is an inner product of $\mathbb{F}_{2^{2t}}$ (non-degenerate symmetric bilinear form). We use it to calculate the Fourier coefficients.

Definition 1.
The inner product T_v *of* $\mathbb{F}_{2^{2t}}$ *such that* $T_v(X) =< v, X >$ *is now defined by*

$$T_{(a,\eta)}(x, \nu) = tr(ax) + \eta\nu.$$

Consequently, every affine linear form of $\mathbb{F}_{2^{2t}}$ is of the kind $T_{(a,\eta)} + \omega$ with $(a, \eta) \in \mathbb{F}_{2^{2t}}$ and $\omega \in \mathbb{F}_2$. We immediately obtain :

Proposition 2.
(*) $\quad T_{(a,\eta)} = [t_a, t_a + \eta]$.
Let $F = [f_0, f_1]$ *be a* $(2t)$*-boolean function.*

(**) $F + T_{(a,\eta)} = [f_0 + t_a, f_1 + t_a + \eta]$.

2.3. **Representation of bent functions.**
The next proposition is a special version of a well known result which appears in several papers ([2],[7],...). A proof is given in [9].

Proposition 3.
F is a bent function if and only if:
(a) f_0 and f_1 are near-bent.
(b) $\forall a \in \mathbb{F}_{2^{2t-1}} \mid \hat{f}_0(a) \mid + \mid \hat{f}_1(a) \mid = 2^t$

Remark: (b) means that one of $\mid \hat{f}_0(a) \mid$ *and* $\mid \hat{f}_1(a) \mid$ *is equal to* 2^t *and the other one is equal to 0.*

Problem:

The previous proposition leads to the following problem: construction of $(2t)$-bent-functions by means of $(2t-1)$-near-bent functions f_0 and f_1 satisfying (b).
In order to study this point we have an additional information on f_0 and f_1.

Proposition 4.
If $[f_0, f_1]$ is bent then $f_0 + f_1$ is balanced (considered as a Boolean function on $\mathbb{F}_{2^{2t-1}}$).

Proof.
$D_{0,1}(F)(u,\nu) = F(u,\nu) + F(u,\nu+1)$.
The two-variable representation of F is:
$F(x,y) = (y+1)f_0(x) + yf_1(x)$. Hence
$F(u,\nu) = (\nu+1)f_0(u) + \nu f_1(u)$
$F(u,\nu+1) = (\nu+1+1)f_0(u) + (\nu+1)f_1(u)$.
Finally $D_{0,1}(F)(u,\nu) = f_0(u) + f_1(u)$.
On the other hand, we know from (P_2) that $D_{0,1}(F)$ is balanced which means that the number of (u,ν) such that $D_{0,1}(F)(u,\nu) = 1$ is 2^{2t-1}.
Now, note that $D_{(0,1)}(F)(u,1) = f_0(u) + f_1(u) = D_{(0,1)}(F)(u,0)$. Since for a given u such that $f_0(u) + f_1(u) = 1$ there are two (u,ν) such that $D_{(0,1)}(F)(u,\nu) = 1$ then the number of u such that $f_0(u) + f_1(u) = 1$ is $\frac{1}{2}2^{2t-1} = 2^{2t-2}$ and this proves that $f_0 + f_1$ is balanced. □

Special case:
Because of the above proposition, a possible approach to attack our problem is to search f_0 and f_1 such that $f_0 + f_1$ is balanced.
For every $\epsilon \in \mathbb{F}_2$ the Boolean function $tr + \epsilon$ where tr is the trace function of $\mathbb{F}_{2^{2t-1}}$ over of $\mathbb{F}_2$, is balanced and is therefore a good candidate for $f_0 + f_1$.

This leads us to focus in this work on the case $f_1 + f_0 = tr + \epsilon$.

Results in this case are given by McGuire and Leander in [5].

3. Results

3.1. **Previous results.**

The three next results have already been published in [9] with their proofs. We need them for the rest of the paper.

Lemma 5.
Let $F = [f_0, f_1]$ be a $(2t)$-Boolean function. Then:

a) $\hat{F}(u, 0) = \hat{f}_0(u) + \hat{f}_1(u)$.

b) $\hat{F}(u, 1) = \hat{f}_0(u) - \hat{f}_1(u)$.

Proof. see [9], Lemma 13. □

Lemma 6.
If f_0 and f_1 are the components of a bent function F. and $\omega \in \mathbb{F}_2$ then: $D_1 f_0 = \omega$ if and only if $D_1 f_1 = \omega + 1$.

Proof. see [9], Proposition 16. □

The next theorem is a fundamental result.

Theorem 7.
Let f_0 be a $(2t-1)$-near-bent function. If the derivative $D_1 f_0$ is a constant function then the $(2t)$-Boolean function $F = [f_0, f_0 + tr]$ is bent.

Proof. see [9], Theorem 1. □

3.2. **New results.**

3.2.1. *Results on near-bent functions.*

Definition 8.
If f is a $(2t-1)$-near-bent function then $\hat{I}_f$ is the indicator of the set $\{x \in \mathbb{F}_{2^{2t-1}} \mid \hat{f}(x) = 0\}$ where $\hat{f}$ is the Fourier transform of f.
(In other words, $\hat{I}_f(x) = 1$ if and only if $\hat{f}(x) = 0$).

Lemma 9.
Let f be a $(2t-1)$-near-bent function and $\epsilon \in \mathbb{F}_2$.
If $D_1 f = \epsilon$ then $\hat{I}_f = tr + \epsilon$

Remark: According to the definition of $\hat{I}_f$ this lemma means that if $D_1 f = \epsilon$ then $\hat{f}(x) = 0$ if and only if $tr(x) + \epsilon = 1$.

Proof. $D_1 f = \epsilon$ means that $f(x+1) = f(x) + \epsilon$. The transform $\tau : x \to x + 1$ is a permutation of $\mathbb{F}_{2^{2t-1}}$ and then preserves the weight of every $(2t-1)$-Boolean function. Thus:

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

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

If $tr(u) + \epsilon = 1$ 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 $w(f + t_u) = 2^{2t-1} - w(f + t_u)$ and thus:
If $tr(u) + \epsilon = 1$ then $w(f + t_u) = 2^{2t-2}$ which is equivalent to $\hat{f}(u) = 0$.
For every ϵ the number of u such that $tr(u) + \epsilon = 1$ is 2^{2t-2} and this is also the number of u such that $\hat{f}(u) = 0$ (see (P_6)). Then, immediately: $\hat{f}(u) = 0$ if and only if $tr(u) + \epsilon = 1$. This means $\hat{I}_{f_0} = tr + \epsilon$ □

3.2.2. *Results on bent functions.*
The next theorem is a key point of this work.

Theorem 10.
Let $F = [f_0, f_1]$ be a $(2t)$-bent function and let $\tilde{F} = [\tilde{f_0}, \tilde{f_1}]$ be its dual function. Then $\tilde{f_0} + \tilde{f_1} = \hat{I}_{f_0}$

Proof.
From the definitions of bent and near-bent functions, every a in $\mathbb{F}_{2^{2t-1}}$ belongs to one of the following sets:

$\mathcal{A}_1 = \{a \in \mathbb{F}_{2^{2t-1}} \mid \hat{f_0}(a) = -2^t \text{ and } \hat{f_1}(a) = 0\}$
$\mathcal{A}_2 = \{a \in \mathbb{F}_{2^{2t-1}} \mid \hat{f_0}(a) = 0 \text{ and } \hat{f_1}(a) = -2^t\}$
$\mathcal{A}_3 = \{a \in \mathbb{F}_{2^{2t-1}} \mid \hat{f_0}(a) = 2^t \text{ and } \hat{f_1}(a) = 0\}$
$\mathcal{A}_4 = \{a \in \mathbb{F}_{2^{2t-1}} \mid \hat{f_0}(a) = 0 \text{ and } \hat{f_1}(a) = 2^t\}$

The definition of the dual of F induces that (a, η) is in the support of $\tilde{F}$ if and only if $\hat{F}(a, \eta) = -2^t$.
From Lemma 5:
$\hat{F}(u, 0) = \hat{f_0}(u) + \hat{f_1}(u)$ and $\hat{F}(u, 1) = \hat{f_0}(u) - \hat{f_1}(u)$.

Therefore:
$\hat{F}(a, 0) = -2^t$ if and only if $a \in \mathcal{A}_1$ or $a \in \mathcal{A}_2$,
$\hat{F}(a, 1) = -2^t$ if and only if $a \in \mathcal{A}_1$ or $a \in \mathcal{A}_4$,

We deduce 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 $a \in \mathcal{A}_1 \cup \mathcal{A}_4$.
In other words the support of $\tilde{f_0}$ is $\mathcal{A}_1 \cup \mathcal{A}_2$ and the support of $\tilde{f_1}$ is $\mathcal{A}_1 \cup \mathcal{A}_4$.
It follows that the support of $\tilde{f_0} + \tilde{f_1}$ is $\mathcal{A}_2 \cup \mathcal{A}_4$ which is nothing but the set $\{x \in \mathbb{F}_{2^{2t-1}} \mid \hat{f_0}(x) = 0\}$. □

A bent function $F = [f_0, f_1]$ is self-dual if $F = \tilde{F}$ where $\tilde{F}$ is the dual of F.

Corollary 11.
If a $(2t)$-bent function $F = [f_0, f_1]$ is self-dual then $f_1 = f_0 + \hat{I}_{f_0}$.

Proof.
By Theorem 10, $\tilde{f_0} + \tilde{f_1} = \hat{I}_{f_0}$. Since F is self-dual then $\tilde{f_0} + \tilde{f_1} = f_0 + f_1$ which gives the result. □

The converse of Theorem 7 is not true. In other words, it is not true that if $f_0 + f_1 = tr$ then $D_1 f_0$ is a constant function, as it will be seen with several examples. However, we have a pseudo-reciprocoal theorem. The next Theorem is an improvement of a Theorem of [9]

Theorem 12.
Let $F = [f_0, f_1]$ be a bent function and let $\tilde{F} = [\tilde{f_0}, \tilde{f_1}]$ be its dual function. Let ϵ be in $\mathbb{F}_2$.

$f_0 + f_1 = tr + \epsilon$ if and only if $D_1\tilde{f_0} = \epsilon$.

Proof.
Step 1: assume $f_0 + f_1 = tr + \epsilon$ with $\epsilon \in \mathbb{F}_2$.

From (P_1): $\hat{f_0}(u) = 2^{2t-1} - 2w(f_0 + t_u)$. Thus:

$$(R)\ \hat{f_0}(u+1) = 2^{2t-1} - 2w(f_0 + t_{u+1}).$$

• If $\epsilon = 0$:
Since $f_0 + f_1 = tr$ then:
$\hat{f_1}(u) = 2^{2t-1} - 2w(f_0 + t_1 + t_u) = 2^{2t-1} - 2w(f_0 + t_{u+1})$.
By using (R) we have $\hat{f_1}(u) = \hat{f_0}(u+1)$.
We deduce from lemma 5:
$\hat{F}(u,0) = \hat{f_0}(u) + \hat{f_0}(u+1)$ and $\hat{F}(u+1,0) = \hat{f_0}(u+1) + \hat{f_0}(u)$
whence $\hat{F}(u,0) = \hat{F}(u+1,0)$.
According to (P_4): $\tilde{f_0}(u) = \tilde{f_0}(u+1))$ and this means $D_1\tilde{f_0} = 0$.

• If $\epsilon = 1$.
Since $f_0 + f_1 = tr + 1$ then:
$\hat{f_1}(u) = 2^{2t-1} - 2w(f_0 + t_1 + t_u + 1) = 2^{2t-1} - 2w(f_0 + t_{u+1} + 1)$.
Observe that $w(f_0 + t_{u+1} + 1) = 2^{2t-1} - w(f_0 + t_{u+1})$.
This implies:
$\hat{f_1}(u) = 2^{2t-1} - 2[2^{2t-1} - w(f_0 + t_{u+1})] = -2^{2t-1} + 2w(f_0 + t_{u+1})$.
With (R) it follows $\hat{f_1}(u) = -\hat{f_0}(u+1)$.
From lemma 5: $\hat{F}(u,0) = \hat{f_0}(u) - \hat{f_0}(u+1)$ whence
$\hat{F}(u+1,0) = \hat{f_0}(u+1) - \hat{f_0}(u)$ and finally $\hat{F}(u,0) = -\hat{F}(u+1,0)$.
This means that $\hat{F}(u,0)$ and $\hat{F}(u+1,0)$ are not equal to 2^t in the same time. From (P_4): $\tilde{f_0}(u) \neq \tilde{f_0}(u+1))$ which yields $D_1\tilde{f_0} = 1$.

Conclusion: if $f_0 + f_1 = tr + \epsilon$ then $D_1\tilde{f_0} = \epsilon$.

Step 2: Conversely, assume $D_1\tilde{f_0} = \epsilon$.
Lemma 9 shows that $\hat{I}_{\tilde{f_0}} = tr + \epsilon$. Hence by Theorem 10:
$f_0 + f_1 = tr + \epsilon$. □

Corollary 13.
If a bent function $F = [f_0, f_1]$ is self-dual then $f_1 = f_0 + tr + \epsilon$ if and only if $D_1 f_0 = \epsilon$.

Proof.
This a direct consequence of Theorem 12 since if F is self-dual then $\tilde{f}_0 + \tilde{f}_1 = f_0 + f_1$. □

Another result on $\hat{I}_f$ is given in [5].

Theorem 14. *(McGuire and Leander)*
Let f be a near-bent function.
$D_1(\hat{I}_f) = 1$ if and only if $[f, f + tr]$ is a bent-function.

Proof. see [5]. □

Corollary 15.
Let $F = [f_0, f_1]$ be a bent function and let $\tilde{F} = [\tilde{f}_0, \tilde{f}_1]$ be its dual.
$D_1(f_0 + f_1) = 1$ if and only if $[\tilde{f}_0, \tilde{f}_0 + tr]$ is a bent function.

Proof.
Theorem 10 says that $\hat{I}_{f_0} = \tilde{f}_0 + \tilde{f}_1$ and Theorem 14 proves that $D_1(\tilde{f}_0 + \tilde{f}_1) = 1$ if and only if $[f_0, f_0 + tr]$ is bent. The expected result is obtained by interchanging the roles of F and $\tilde{F}$. □

Example: (obtained by computing)
$t = 4$,
$f_0 = tr(x^{29} + x^{27} + x^{23} + x^{21} + x^5 + x)$, $f_1 = tr(x^{29} + x^{27} + x^{23} + x^{21} + x^9)$
$f_0 + f_1 = tr(x^9 + x^5 + x)$ then $D_1(f_0 + f_1) = 1$.

The dual of $[f_0, f_1]$ is $[tr(x^{13} + x^7), tr(x^{19} + x^{11} + x^7)]$
then $[tr(x^{13} + x^7), tr(x^{13} + x^7 + x)]$ is bent.

3.3. **Pseudo duality.**
The results of the previous theorems lead to introduce a new definition.

Definition 16.
Let $G = [g_0, g_1]$ be a $(2t)$-bent function and let $\tilde{G} = [\tilde{g}_0, \tilde{g}_1]$ be its dual function. The pseudo-duals of G are the two $(2t)$-Boolean functions: $\bar{G}_0 = [\tilde{g}_0, \tilde{g}_0 + tr]$ and $\bar{G}_1 = [\tilde{g}_1, \tilde{g}_1 + tr]$.

The next theorem is the generalisation of a result of [9].

Theorem 17.
Define two conditions on a $(2t)$-Boolean function $G = [g_0, g_1]$:
$(\mathcal{T}) : g_0 + g_1 = tr + \xi$ with $\xi \in \mathbb{F}_2$ and $(\mathcal{C}) : D_1 g_0 = \mu$ with $\mu \in \mathbb{F}_2$

Let F be a bent function. If F meets condition $(\mathcal{T})$ with $\xi = \epsilon$ then:

A) The pseudo-duals $\bar{F}_0$ and $\bar{F}_1$ are bent functions.
$\bar{F}_0$ meets $(\mathcal{T})$ with $\xi = 0$ and $(\mathcal{C})$ with $\mu = \epsilon$.
$\bar{F}_1$ meets $(\mathcal{T})$ with $\xi = 0$ and $(\mathcal{C})$ with $\mu = \epsilon + 1$.

B) The dual $\bar{\tilde{F}}_0$ of $\bar{F}_0$ meets $(\mathcal{T})$ with $\xi = \epsilon$ and $(\mathcal{C})$ with $\mu = 0$.
C) The dual $\bar{\tilde{F}}_1$ of $\bar{F}_1$ meets $(\mathcal{T})$ with $\xi = \epsilon + 1$ and $(\mathcal{C})$ with $\mu = 1$.

Proof.
Notations:

$F = [f_0, f_1]$, dual of F: $\tilde{F} = [\tilde{f}_0, \tilde{f}_1]$,
Pseudo-dual $\bar{F}_0 = [\bar{f}_0^{(0)}, \bar{f}_1^{(0)}]$. Pseudo-dual $\bar{F}_1 = [\bar{f}_0^{(1)}, \bar{f}_1^{(1)}]$.

Dual of $\bar{F}_0$: $\bar{\tilde{F}}_0 = [\bar{\tilde{f}}_0^{(0)}, \bar{\tilde{f}}_1^{(0)}]$. Dual of $\bar{F}_1$: $\bar{\tilde{F}}_1 = [\bar{\tilde{f}}_0^{(1)}, \bar{\tilde{f}}_1^{(1)}]$

Proof of A):
Since $f_0 + f_1 = tr + \epsilon$ then, from Theorem 12 and Lemma 6:
$(\star)$ $D_1\tilde{f}_0 = \epsilon$ and $D_1\tilde{f}_1 = \epsilon + 1$.
By the definition $\bar{F}_0 = [\tilde{f}_0, \tilde{f}_0 + tr]$. That is $\bar{F}_0$ meets $(\mathcal{T})$ with $\xi = 0$. Furthermore, we deduce from Theorem 7 that $\bar{F}_0$ is a bent function and meets $(\mathcal{C})$ with $\mu = \epsilon$. Similarly, again from Theorem 12 and from Theorem 7, $\bar{F}_1$ is a bent function and meets $(\mathcal{T})$ with $\xi = 0$ and $(\mathcal{C})$ with $\mu = \epsilon + 1$.

Proof of B) and C):
From the definition of the duals:
$(\star\star)$ $\bar{f}_0^{(0)} = \tilde{f}_0$, $\bar{f}_0^{(1)} = \tilde{f}_1$ and $\bar{f}_0^{(0)} + \bar{f}_1^{(0)} = tr$, $\bar{f}_0^{(1)} + \bar{f}_1^{(1)} = tr$.
Now with $(\star)$: $D_1\bar{f}_0^{(0)} = D_1\tilde{f}_0 = \epsilon$ and $D_1\bar{f}_0^{(1)} = D_1\tilde{f}_1 = \epsilon + 1$.
Now, by Theorem 12:
$\bar{\tilde{f}}_0^{(0)} + \bar{\tilde{f}}_1^{(0)} = tr + \epsilon$ and $\bar{\tilde{f}}_0^{(1)} + \bar{\tilde{f}}_1^{(1)} = tr + \epsilon + 1$
Hence $\bar{\tilde{F}}_0$ meets $(\mathcal{T})$ with $\xi = \epsilon$ and $\bar{\tilde{F}}_1$ meets $(\mathcal{T})$ with $\xi = \epsilon + 1$. From $(\star)$ and again by Theorem 12: $D_1\bar{\tilde{f}}_0^{(0)} = 0$ and $D_1\bar{\tilde{f}}_0^{(1)} = 1$ and thus $\bar{\tilde{F}}_0$ meet $(\mathcal{C})$ with $\mu = 0$ and $\bar{\tilde{F}}_1$ meet $(\mathcal{C})$ with $\mu = 1$.

□

Starting from a bent function $F = [f_0, f_1]$ such that $f_0 + f_1 = tr + \epsilon$, Theorem 17 provides new bent functions. The question now is:
are $F, \tilde{F}, \bar{F}_0, \bar{F}_1, \bar{\tilde{F}}_0, \bar{\tilde{F}}_1$ distinct functions or not ?
A first answer is given by the next proposition.

Proposition 18.
Let $F = [f_0, f_1]$ be a bent function and let $\tilde{F} = [\tilde{f}_0, \tilde{f}_1]$ be its dual function. If $f_0 + f_1 = tr$ then:
1) $\bar{F}_0 = \tilde{F}$ if and only if $D_1 f_0 = 0$.
2) If $D_1 f_0 = 0$ then $\bar{F}_1 = \tilde{F} + [tr, tr]$.

Proof.
1) From the definition of $\bar{F}_0$: $\bar{f}_0^{(0)} + \bar{f}_1^{(0)} = tr$. If $\bar{F}_0 = \tilde{F}$ then
$\tilde{f}_0 + \tilde{f}_1 = \bar{f}_0^{(0)} + \bar{f}_1^{(0)} = tr$ and Theorem 12 says that $D_1 f_0 = 0$.
Now if $D_1 f_0 = 0$ then Theorem 7 proves that $\tilde{f}_0 + \tilde{f}_1 = tr$ which means $\bar{F}_0 = \tilde{F}$.

2) If $D_1 f_0 = 0$ then 1) shows that $\bar{F}_0 = \tilde{F}$ whence $\tilde{f}_0 + \tilde{f}_1 = tr$.
Thus $\bar{F}_1 = [\tilde{f}_1, \tilde{f}_1 + tr] = [\tilde{f}_0 + tr, \tilde{f}_0 + tr + tr] = [\tilde{f}_0 + tr, \tilde{f}_0]$
$= [\tilde{f}_0, \tilde{f}_0 + tr] + [tr, tr]$.
Finally $\bar{F}_1 = \bar{F}_0 + [tr, tr] = \tilde{F} + [tr, tr]$. □

Remark: We deduce from the previous result that if $D_1 f_0$ is not a constant function then $\bar{F}_0$ and $\tilde{F}$ are distinct.

The following examples are obtained with computer assist.

Example 1: $t = 4$, $D_1 f_0 = 0$.

F : $f_0(x) = tr(x + x^3 + x^7 + x^{11} + x^{19} + x^{21})$, .
$f_1(x) = f_0(x) + tr(x)$

$\tilde{F}$: $\tilde{f}_0(x) = tr(x^7 + x^{11} + x^{19} + x^{21})$
$\tilde{f}_1(x) = \tilde{f}_0(x) + tr(x)$

$\bar{F}_0 = \tilde{F}$ and $\tilde{\bar{F}}_0 = F$ $\bar{F}_1 = \tilde{F} + [tr, tr]$.

Example 2: $t = 4$, $D_1 f_0 \neq 0, 1$.

F : $f_0(x) = tr(x^7 + x^{13})$.
$f_1(x) = f_0(x) + tr(x)$

$\tilde{F}$: $\tilde{f}_0(x) = tr(x^5 + x^7 + x^9 + x^{13} + x^{19} + x^{21})$
$\tilde{f}_1(x) = \tilde{f}_0(x) + tr(x + x^5 + x^9)$

$\bar{F}_0$: $\bar{f}_0^{(0)}(x) = \tilde{f}_0(x)$, $\bar{f}_1^{(0)}(x) = \tilde{f}_0(x) + tr(x)$

$\bar{F}_1$: $\bar{f}_0^{(1)}(x) = \tilde{f}_1(x)$, $\bar{f}_1^{(1)}(x) = \tilde{f}_1(x) + tr(x)$

$\tilde{\bar{F}}_0$: $\tilde{\bar{f}}_0^{(0)}(x) = tr(x + x^7 + x^9 + x^{13} + x^{19} + x^{21})$,
$\tilde{\bar{f}}_1^{(0)}(x) = \tilde{\bar{f}}_0^{(0)}(x) + tr(x)$

$\tilde{\bar{F}}_1$: $\tilde{\bar{f}}_0^{(1)}(x) = tr(x + x^3 + x^7 + x^{13} + x^{19} + x^{21})$
$\tilde{\bar{f}}_1^{(1)}(x) = \tilde{\bar{f}}_0^{(1)}(x) + tr(x + 1)$

3.4. **New infinite families of bent functions.**

Proposition 19.
If f_0 meets one of the two following cases and if $F = [f_0, f_0 + tr]$ then $F, \tilde{F}, \bar{F}_0, \bar{F}_1, \tilde{\bar{F}}_0, \tilde{\bar{F}}_1$ are bent functions and they satisfy condition $(\mathcal{T})$.

(1) Kasami-Welch case
f_0 is a $(2t-1)$-Boolean function such that:

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

(2) Quadratic case

f_0 is a $(2t-1)$-near-bent function such that:
$f_0(x) = \sum_{j=1}^{t-1} c_j tr(x^{2^j+1})$ *with* $c_j \in \mathbb{F}_2$.

Proof. In order to apply Theorem 17, we have to check in every case that F is bent and meets $(\mathcal{T})$ with $\xi = 0$.
• In case (1), the derivative $D_1 f_0$ is not a constant function but it was proved (McGuire, Leander, [5]) that $[f_0, f_0 + tr]$ is bent.
• In case (2) it is easy to prove that $D_1 f_0$ is a constant function and then $[f_0, f_0 + tr]$ is bent. □

Remark: Several examples of near-bent functions in case (2) are given in [4].

3.5. **Adding new functions.**
Let $F = [f_0, f_1]$ be bent with $f_0 + f_1 = tr$.

Question: find g such that $[f_0 + g, f_1 + g]$ is bent.

Remark : In this case, $f_1 + g = f_0 + g + tr$.
Recall that if $u \in \mathbb{F}_{2^{2t-1}}$ then t_u is the $(2t-1)$-function defined by $t_u(x) = tr(ux)$.

Theorem 20.
Let v be in $\mathbb{F}_{2^{2t-1}}$.
If one of the following conditions is satisfied:
(i) f_0 is a $(2t-1)$-near-bent function such that the derivative $D_1 f_0$ is a constant function
(ii) $F = [f_0, f_1]$ is a bent function such that $f_0 + f_1 = tr$.
then the Boolean function $F^\dagger = [f_0^\dagger, f_1^\dagger]$ with $f_0^\dagger = f_0 + t_1 t_v$ and $f_1^\dagger = f_0^\dagger + tr$ is bent.

In order to prove Theorem 20 we need the two following lemmas. The second one is due to Canteaut and Charpin ([2], Theorem 8).

Recall that the inner product $<,>$ which is used for the calculation of the Fourier coefficients is now defined by:
$T_{(a,\eta)}(x,\nu) =< (a,\eta),(x,\nu) >= tr(ax) + \eta\nu$.

Lemma 21.
(L_1): *The indicator of $\langle (u,0),(v,0)\rangle^\perp$ is:*

$$[t_u t_v, t_u t_v] + [t_u + t_v + 1, t_u + t_v + 1].$$

(L_2): *If $G = [g_0, g_1]$ then:*

$$D_{(b,0)} D_{(a,0)} G = [D_b D_a g_0, D_b D_a g_1].$$

(L_3): *If the derivative $D_1 g$ is a constant function then for every u:*

$$D_1 D_u g = D_{u+1} D_u g = 0$$

Proof.
Proof of (L_1):
Let I be the indicator $\langle (u,0),(v,0)\rangle^\perp$.
(x,ν) is othogonal to $(u,0)$ if and only if $< (u,0),(x,\nu) >= tr(ux) = 0$.
In other words the indicator of $\langle (u,0)\rangle^\perp$ is t_u+1. Similarly, the indicator

of $\langle(v,0)\rangle^{\perp}$ is t_v+1. This means that $I(x,\nu)=1$ if and only if: $(tr(ux)+1)(tr(vx)+1)=1$. This result is independent of ν and $f_0(u)=I(u,0)=f_1(u)=I(u,1)=(t_u+1)(t_v+1)$ that is $I=[(t_u+1)(t_v+1),(t_u+1)(t_v+1)]$. Since $(t_u+1)(t_v+1)=t_ut_v+t_u+t_v+1$ then $I=[t_ut_v,t_ut_v]+[t_u+t_v+1,t_u+t_v+1]$.

Proof of (L_2):
$G(x,y)=(y+1)g_0(x)+yg_1(x)$.
$D_{(a,0)}G(x,y)=(y+1)g_0(x+a)+yg_1(x+a)+(y+1)g_0(x)+yg_1(x)$.
$=(y+1)[g_0(x+a)+g_0(x)]+y[g_1(x+a)+g_1(x)]$
$=(y+1)D_ag_0(x)+yD_ag_1(x)$
Then $D_{(a,0)}G=[D_ag_0,D_ag_1]$. By replacing G by $D_{(a,0)}G$ and a by b: $D_{(b,0)}D_{(a,0)}G=[D_bD_ag_0,D_bD_ag_1]$.

Proof of (L_3):
From $D_ug(x)=g(x+u)+g(x)$:
$D_1D_ug(x)=g(x+1+u)+g(x+1)+g(x+u)+g(x)$,
$D_{u+1}D_ug(x)=g(x+1+u)+g(x+1)+g(x+u)+g(x)$
then $D_1D_ug=D_{u+1}D_ug$.
Note from the above calculation that $D_1D_ug(x)=D_1g(x+u)+D_1g(x)$. Since D_1g is a constant function then $D_1D_ug=0$. □

Lemma 22. *([2],Theorem 8)*
Let F be a $(2t)$-bent function. Let A and B two distinct non-zero elements of $\mathbb{F}_{2^{2t}}$ and $\mathcal{E}=\langle A,B\rangle^{\perp}$. Let $\Phi_{\mathcal{E}}$ be the indicator of $\mathcal{E}$. Then the function $F+\Phi_{\mathcal{E}}$ is bent if and only if the dual function $\tilde{F}$ satisfies $D_BD_A\tilde{F}=0$.

Proof. of Theorem 20.
If $v=0$ or $v=1$ the result is trivial.
If $v\neq 0$ and $v\neq 1$:
From Theorem 7, in case (i) the Boolean function $[f_0,f_0+tr]$ is bent. Consequently, in both cases (i) and (ii) we have to consider the bent function $F=[f_0,f_0+tr]$.
Let $\tilde{F}=[\tilde{f_0},\tilde{f_1}]$ be the dual function of F.
Theorem 12 proves that $D_1\tilde{f_0}=0$ and $D_1\tilde{f_1}=1$. Therefore, from (L_3): $D_1D_v\tilde{f_0}=D_1D_v\tilde{f_1}=0$.
It follows from (L_2) that $D_{(1,0)}D_{(v,0)}\tilde{F}=[0,0]$.
Now, using the notations of Lemma 22 with $A=(1,0)$, $B=(v,0)$, $v\neq 0, v\neq 1$ then from (L_1): $\Phi_{\mathcal{E}}=[t_1t_v,t_1t_v]+[t_1+t_v+1,t_1+t_v+1]$.
Hence, in view of Lemma 22:
$F^{\sharp}=F+[t_1t_v,t_1t_v]+[t_1+t_v+1,t_1+t_v+1]$ is bent.
Since $L=[t_1+t_v+1,t_1+t_v+1]$ is an affine linear form then:
$F^{\natural}=F^{\sharp}+L=[f_0^{\natural},f_1^{\natural}]$ with $f_0^{\natural}=f_0+t_1t_v$ and $f_1^{\natural}=f_1+t_1t_v$ also is bent. □

Remark:
Instead of t_1t_v is it possible to add some other products of two linear

forms. This give rise to bent functions equivalent to those of the kind $[f_0^\natural, f_1^\natural]$ by means of the addition of a linear form.
Example:
$F^{\dagger\dagger} = [f_0^{\dagger\dagger}, f_1^{\dagger\dagger}]$ with $f_0^{\dagger\dagger} = f_0 + t_u t_{u+1}$ and $f_1^{\dagger\dagger} = f_0^{\dagger\dagger} + tr$.
It is easy to check that $t_u t_{u+1} = t_1 t_u + t_u$. Therefore:
$F^{\dagger\dagger} = [f_0 + t_1 t_u + t_u, f_0 + t_1 t_u + t_u + tr] = [f_0 + t_1 t_u, f_0 + t_1 t_u + tr] + [t_u, t_u]$

Corollary 23.
If (i) or (ii) of Theorem 20 is satified then $f_0^\dagger = f_0 + t_1 t_v$ is near-bent.

Proof.
Since $F^\dagger = [f_0^\dagger, f_1^\dagger]$ is bent then according to Proposition 3, (a):
$f_0^\dagger$ and $f_1^\dagger$ are near-bent. □

4. Conclusion

We have introduced a way to construct new bent functions starting from a near-bent functions f such that $D_1 f$ is a constant function or from a bent function such that the sum of the two components is a Boolean function of degree 1. An open question now is to describe explicitely the near-bent functions of the first kind, for example by means of the trace function. Another question is to generalise the study to the case where the degree of the sum of the two components is greater than 1.

5. References

[1] A.Canteaut,C.Carlet,P.Charpin,C.Fontaine, *On Cryptographic Properties of the Cosets of R(1,m)* IEEE Transactions on Information Theory, vol.47, 4, (2001),1494-1513. MR 1830095(2002h:94048)

[2] A.Canteaut,P.Charpin, *Decomposing Bent Functions* IEEE Transactions on Information Theory,49,8, (2003),2004-2019, MR 2004705(2004i:94046)

[3] J.F.Dillon, *Elementary Hadamard Difference Sets* Ph.D. Thesis, University of Maryland(1974), MR 0409221(53 12981)

[4] K.Khoo, G.Gong,D.R. Stinson *A new characterisation of semi-bent and bent functions on finite fields* Des. Codes Crypt.,38,279-295,2006, MR 2197473,11T 71(94A60)

[5] G.Leander, G.McGuire,*Construction of Bent Functions from Near-Bent Functions* Journal of Combinatorial Theory, Series A, 116,4,(2009) 960-970,MR 2513644 94C10(0630 94A60)

[6] O.S.Rothaus, *On Bent Functions* Journal of Combinatorial Theory, series A, 20,(1976),300-305,MR 0403988(53 7797)

[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, 542, Kluwer Academic Publishers (1999) 393-418,MR 1735405 94A55 (11T71 94A60 94B60)

[8] J.Wolfmann, *Cyclic Code Aspects of Bent Functions* in Finite Fields Theory and Applications, Contemporary Mathematics series of the AMS, 518, Amer.Math Soc. Providence, RI, (2010),363-384,MR 2648560 94B15 (06E30 11T71 94C10)

[9] J. Wolfmann *Special Bent and Near-Bent Functions* in Advances in Mathematics of Communication,8, no 1 (2014),21-33,MR 3180712

IMATH(IAA), Université de Toulon, 83957 La Garde Cedex, France
E-mail address: wolfmann@univ-tln.fr