# Multidimensional Bent Functions

Laurent POINSOT

Université du Sud Toulon-Var
Institut des Sciences de l'Ingénieur de Toulon et du Var
Avenue G. Pompidou
BP 56
83162 La Valette du Var cédex, France
poinsot@univ-tln.fr

**Abstract.** The concept of bent functions, originally introduced by Dillon and Rothaus, is very relevant in cryptography because this kind of functions represents the maximal resistance against the so-called linear cryptanalysis. In 1997, Logachev, Salnikov and Yashchenko described a fundamental notion of bentness for functions defined on a finite Abelian group $G$ with values in the unit circle of the complex field. In this paper, by replacing this unit circle by the unit hypersphere $\mathcal{S}_{\mathcal{H}}(0_{\mathcal{H}}, 1)$ of an arbitrary finite-dimensional Hermitian space $\mathcal{H}$, we develop a generalization of the concept of bentness for $\mathcal{S}_{\mathcal{H}}(0_{\mathcal{H}}, 1)$-valued functions defined on $G$, called *multidimensional bent functions.*

**Keywords :** Bent functions, Hermitian spaces and multidimensional Fourier transform.

## 1 Introduction

Independently introduced by Dillon [Dil74] and Rothaus [Rot76], Boolean bent functions are those $\mathbb{F}_2$-valued functions with an even number $m$ of (Boolean) variables such that for all $\alpha \in \mathbb{F}_2^m$, $\widehat{\chi \circ f}(\alpha) = \pm 2^{\frac{m}{2}}$, where $\widehat{F}$ is the Fourier transform of a function $F : \mathbb{F}_2^m \to \mathbb{C}$, $\chi : \mathbb{F}_2^m \to \mathbb{C}$ such that $\chi(x) = (-1)^x$ and the symbol "$\circ$" denotes the composition of functions. Such functions are very relevant in cryptography since they exhibit the best resistance against the well-known Matsui's linear cryptanalysis [Mat94] and are also closely related to the differential attack of Biham and Shamir [BS91].
While noticing that for $f : \mathbb{F}_2^m \to \mathbb{F}_2$, $\chi \circ f$ is $\mathbb{U}$-valued, where $\mathbb{U}$ is the unit circle in the complex field, Logachev, Salnikov and Yashchenko [LSY97] adapted the concept of bentness to a more general context. Following their approach, a $\mathbb{U}$-valued function $f$ defined on a finite Abelian group $G$ is *bent* if for all $\alpha \in G$,

$$|\widehat{f}(\alpha)|^2 = |G| \tag{1}$$

where $|z|$ is the complex-modulus of the complex number $z$ and $|G|$ is the cardinality of the group $G$.

In this paper, we present a natural way to extend this last concept. First note that $\mathbb{U}$ is the unit sphere of the most simple Hermitian space $\mathbb{C}$. Then we can naturally consider functions defined on a finite Abelian group $G$ but with values in an higher-dimensional unit hypersphere rather than $\mathbb{U}$-valued. So let $f : G \to \mathcal{S}_{\mathcal{H}}(0_{\mathcal{H}}, 1)$ where $\mathcal{S}_{\mathcal{H}}(0_{\mathcal{H}}, 1)$ is the unit hypersphere of the Hermitian space $\mathcal{H}$ with center at the zero of $\mathcal{H}$. Then the equation (1) can be naturally re-written in this context

$$\| \widehat{f}(\alpha) \|^2_{\mathcal{H}} = |G| \tag{2}$$

where $\| u \|_{\mathcal{H}}$ is the norm (that comes from an inner product) of $u \in \mathcal{H}$ and the Fourier transform used is called *multidimensional*. This kind of functions will be called in this paper *multidimensional bent functions*.

## 2 Hermitian spaces

Let us begin with some general notations used in this paper. If $S$ is a finite set, we denote by "$|S|$" its cardinality. When $z \in \mathbb{C}$, $\overline{z}$ is its (complex) conjugate and $|z|$ is its complex-modulus ($|z|^2 = \overline{z}z$).
In this paper, $G$ always represents a finite Abelian group (in an additive representation), $e_G$ is its neutral element and $G^* = G \setminus \{e_G\}$.
If $V$ is a complex vector space, $0_V$ is the zero of $V$.
In this paper, each time we say that $\mathcal{H}$ is an *Hermitian space*, we mean that $\mathcal{H}$ is a finite dimensional complex vector space (non reduced to $\{0_{\mathcal{H}}\}$) equipped with an inner product, denoted $\langle u, v\rangle_{\mathcal{H}}$ with $(u, v) \in \mathcal{H}^2$, which is Hermitian (linear in $u$ and anti-linear in $v$) and positive definite ($\forall u \in \mathcal{H}$, $\langle u, u\rangle_{\mathcal{H}} \geq 0$ and if $\langle u, u\rangle_{\mathcal{H}} = 0$ then $u = 0_{\mathcal{H}}$). Two Hermitian spaces with the same dimension are isomorphic. In particular $\mathbb{C}^n$ with the usual inner product is a canonical representative for $n$-dimensional Hermitian spaces. For $u \in \mathcal{H}$, we define its *norm* (associated with the inner product) as $\| u \|^2_{\mathcal{H}} = \langle u, u\rangle_{\mathcal{H}}$.
Let $B_{\mathcal{H}}$ be an orthonormal basis of $\mathcal{H}$. By properties of such basis, we have for each $u \in \mathcal{H}$, $u = \sum_{e \in B_{\mathcal{H}}} \langle u, e\rangle_{\mathcal{H}} e$. We defined the complex number $u_e$ as $\langle u, e\rangle_{\mathcal{H}}$, then $u = \sum_{e \in B_{\mathcal{H}}} u_e e$. Moreover we have

$$\begin{aligned}
\| u \|^2_{\mathcal{H}} &= \langle u, u\rangle_{\mathcal{H}} \\
&= \langle \sum_{e \in B_{\mathcal{H}}} u_e e, \sum_{e' \in B_{\mathcal{H}}} u_{e'} e'\rangle_{\mathcal{H}} \\
&= \sum_{e \in B_{\mathcal{H}}} u_e \sum_{e' \in B_{\mathcal{H}}} \overline{u_{e'}} \langle e, e'\rangle_{\mathcal{H}} \\
&= \sum_{e \in B_{\mathcal{H}}} u_e \overline{u_e} \\
&\quad \text{(since } \langle e, e'\rangle_{\mathcal{H}} \text{ is equal to 0 if } e \neq e' \text{ and to 1 if } e = e'\text{)} \\
&= \sum_{e \in B_{\mathcal{H}}} |u_e|^2 \ .
\end{aligned} \tag{3}$$

For $u \in \mathcal{H}$ and $\rho \in \mathbb{R}$ such that $\rho > 0$, we define the *hypersphere* in $\mathcal{H}$ with center at $u$ and radius $\rho$ as

$$\begin{aligned} \mathcal{S}_{\mathcal{H}}(u, r) &= \{v \in \mathcal{H} | \parallel v - u \parallel_{\mathcal{H}} = \rho\} \\ &= \{v \in \mathcal{H} | \sum_{e \in B_{\mathcal{H}}} |v_e - u_e|^2 = \rho^2\} \ . \end{aligned} \tag{4}$$

Finally the *unit hypersphere* of $\mathcal{H}$ is simply defined as $\mathcal{S}_{\mathcal{H}}(0_{\mathcal{H}}, 1)$.

# 3 Bent functions of Logachev, Salnikov and Yashchenko

## 3.1 Fourier transform over finite Abelian groups

Let $G$ be a finite Abelian group (in an additive representation). The *dual group* $\widehat{G}$ of $G$ is defined as the group of all homomorphisms from $G$ to $\mathcal{S}_{\mathbb{C}}(0,1)$ (this last set has a group structure). Its elements are called *characters* and it is isomorphic to $G$. We fix some isomorphism and assume that all characters $\chi_G^{\alpha} \in \widehat{G}$ are indexed by the elements $\alpha \in G$ (in particular $\forall x \in G,\ \chi_G^{e_G}(x) = 1$). For instance if $G = \mathbb{F}_2^m$ (where $\mathbb{F}_2$ is the Galois field with two elements 0 and 1), $\chi_{\mathbb{F}_2^m}^{\alpha}(x) = (-1)^{\alpha . x}$ for all $(\alpha, x) \in (\mathbb{F}_2^m)^2$ where the symbol "." denotes the canonical dot product of $\mathbb{F}_2^m$. Note that for all $(\alpha, x) \in G^2$, $\chi_G^{\alpha}(x) = \chi_G^{x}(\alpha)$.
The characters satisfy the important following relation

$$\sum_{x \in G} \chi_G^{\alpha}(x) = \begin{cases} |G| & \text{if } \alpha = e_G \ , \\ 0 & \text{if } \alpha \in G^* \ . \end{cases} \tag{5}$$

Let $f : G \to \mathbb{C}$. The *Fourier transform* of $f$ is the function $\widehat{f} : G \to \mathbb{U}$ defined for $\alpha \in G$ by

$$\widehat{f}(\alpha) = \sum_{x \in G} f(x) \chi_G^{\alpha}(x) \ . \tag{6}$$

This transform satisfies the well-known *Parseval's relation* given below.

$$\sum_{x \in G} |f(x)|^2 = \frac{1}{|G|} \sum_{\alpha \in G} |\widehat{f}(\alpha)|^2 \ . \tag{7}$$

We have also the following convenient relation

$$\forall \alpha \in G,\ \widehat{\widehat{f}}(\alpha) = |G| f(-\alpha) \ . \tag{8}$$

## 3.2 Classical bent functions

Boolean bent functions [Rot76] are those functions $f$ from $\mathbb{F}_2^m$ to $\mathbb{F}_2$ such that for all $\alpha \in \mathbb{F}_2^m$, $\widehat{\chi_{\mathbb{F}_2}^1 \circ f}(\alpha) = \pm 2^{\frac{m}{2}}$. They are very relevant in cryptography since they also exhibit the best resistance against the so-called *linear cryptanalysis* [Mat94].
In [LSY97], Logachev, Salnikov and Yashchenko introduced a general notion of bentness for $\mathcal{S}_{\mathbb{C}}(0,1)$-valued functions defined on a finite Abelian group (note that the values of $\chi_{\mathbb{F}_2}^1 \circ f$ belong to $\{\pm 1\} \subset \mathcal{S}_{\mathbb{C}}(0,1)$).

**Definition 1.** Let $G$ be a finite Abelian group. A function $f : G \to \mathcal{S}_{\mathbb{C}}(0,1)$ is called *bent* if for all $\alpha \in G$,

$$|\widehat{f}(\alpha)|^2 = |G| \ . \tag{9}$$

$\mathcal{B}(G)$ is the set of such bent functions.

Several properties similar to the boolean case remain true in this context. We can recall two of them, summarized in the result below.

**Proposition 1.** *Let $G$ be a finite Abelian group (in an additive representation) and $f : G \to \mathcal{S}_{\mathbb{C}}(0,1)$. We define the* derivative *of $f$ in direction $\alpha \in G$ by*

$$\begin{array}{rcl} d_\alpha f : G & \to & G \\ x & \mapsto & \overline{f(x)} f(x+\alpha) \ . \end{array} \tag{10}$$

*We have the following properties.*

1. *$f$ is bent if and only if $\forall \alpha \in G^*$, $\widehat{d_\alpha f}(e_G) = 0$.*
2. *If $f$ is bent then the function $\tilde{f} : G \to \mathcal{S}_{\mathbb{C}}(0,1)$, called* dual *of $f$ and defined by $\tilde{f} = \dfrac{1}{\sqrt{|G|}} \widehat{f}$, is also bent.*

## 4 Multidimensional Fourier transform

In this section, $G$ is a finite Abelian group in an additive representation and $\mathcal{H}$ is an Hermitian space. We fix some orthonormal basis $B_{\mathcal{H}}$ of $\mathcal{H}$. Our objective is here to introduce some Fourier's tools in order to treat the case of $\mathcal{S}_{\mathcal{H}}(0_{\mathcal{H}},1)$-valued functions in the same way as the $\mathcal{S}_{\mathbb{C}}(0,1)$-valued functions are exploited in the theory of bent functions by Logachev, Salnikov and Yashchenko.

**Definition 2.** Let $\phi : G \to \mathcal{H}$. The *multidimensional Fourier transform* of $\phi$ is the function $\widehat{\phi}^{MD}$ defined by

$$\begin{array}{rcl} \widehat{\phi}^{MD} : G & \to & \mathcal{H} \\ \alpha & \mapsto & \displaystyle\sum_{x \in G} \chi_G^\alpha(x) \phi(x) \ . \end{array} \tag{11}$$

We have also

$$\widehat{\phi}(\alpha) = \sum_{x \in G} \sum_{e \in B_{\mathcal{H}}} \langle \phi(x), \overline{\chi_G^\alpha(x)} e \rangle_{\mathcal{H}} e = \sum_{x \in G} \sum_{e \in B_{\mathcal{H}}} \langle \phi(x), e \rangle_{\mathcal{H}} \chi_G^\alpha(x) e \ . \tag{12}$$

If $\mathcal{H} = \mathbb{C}$, it is easy to see that the multidimensional Fourier transform coincides with the classical one.
Let $\phi : G \to \mathcal{H}$. Let $e \in B_{\mathcal{H}}$. We define the *coordinate function* $\phi_e$ of $\phi$ on $e$ as

$$\begin{array}{rcl} \phi_e : G & \to & \mathbb{C} \\ x & \mapsto & \langle \phi(x), e \rangle_{\mathcal{H}} \ . \end{array} \tag{13}$$

According to the properties of orthonormal basis, we can easily observe that $\forall x \in G$,

$$\phi(x) = \sum_{e \in B_{\mathcal{H}}} \phi_e(x) e \ . \tag{14}$$

We use these coordinate functions in order to establish a connection between the classical and multidimensional versions of the Fourier transform.

**Lemma 1.** *Let $\phi : G \to \mathcal{H}$. Then we have for all $\alpha \in G$,*

$$\widehat{\phi}^{MD}(\alpha) = \sum_{e \in B_{\mathcal{H}}} \widehat{\phi_e}(\alpha) e \ . \tag{15}$$

*Proof.* Let $\alpha \in G$.

$$\begin{aligned}
\widehat{\phi}^{MD}(\alpha) &= \sum_{x \in G} \chi_G^\alpha \phi(x) \\
&= \sum_{x \in G} \sum_{e \in B_{\mathcal{H}}} \chi_G^\alpha(x) \phi_e(x) e \\
&= \sum_{e \in B_{\mathcal{H}}} \left( \sum_{x \in G} \phi_e(x) \chi_G^\alpha(x) \right) e \\
&= \sum_{e \in B_{\mathcal{H}}} \widehat{\phi_e}(\alpha) e \ .
\end{aligned}$$

□

In the sequel of this subsection, we establish some properties about the multidimensional Fourier transform, similar to classical ones, for a function $\phi : G \to \mathcal{H}$. Let us compute the Fourier transform of $\widehat{\phi}^{MD}$. Let $\alpha \in G$.

$$\begin{aligned}
\widehat{\widehat{\phi}^{MD}}^{MD}(\alpha) &= \sum_{x \in G} \chi_G^\alpha(x) \widehat{\phi}^{MD}(x) \text{ (by definition)} \\
&= \sum_{x \in G} \sum_{e \in B_{\mathcal{H}}} \widehat{\phi_e}(x) \chi_G^\alpha(x) e \text{ (according to lemma 1)} \\
&= \sum_{E \in B_{\mathcal{H}}} \left( \sum_{x \in G} \widehat{\phi_e}(x) \chi_G^\alpha(x) \right) e \\
&= \sum_{e \in B_{\mathcal{H}}} \widehat{\widehat{\phi_e}}(\alpha) e \\
&= |G| \sum_{e \in B_{\mathcal{H}}} \phi_e(-\alpha) e \text{ (according to relation (8))} \\
&= |G| \phi(-\alpha) \text{ (according to formula (14))} \ .
\end{aligned}$$

Keep in mind the equality $\widehat{\widehat{\phi}^{MD}}^{MD}(\alpha) = |G| \phi(-\alpha)$ which will be useful in the sequel. Moreover we have proved the *inversion formula* :

$$\forall \alpha \in G, \ \phi(\alpha) = \frac{1}{|G|} \sum_{x \in G} \overline{\chi_G^\alpha(x)} \widehat{\phi}^{MD}(x) \ . \tag{16}$$

Now we present a certain kind of Parseval's equation in this context.

**Theorem 1.** *(Parseval's equation) Let $\phi : G \to \mathcal{H}$ then*

$$\sum_{x \in G} \| \phi(x) \|^2_{\mathcal{H}} = \frac{1}{|G|} \sum_{\alpha \in G} \| \widehat{\phi}^{MD}(\alpha) \|^2_{\mathcal{H}} \ . \tag{17}$$

*If $\phi : G \to \mathcal{S}_{\mathcal{H}}(0_{\mathcal{H}}, 1)$ then*

$$\sum_{\alpha \in G} \| \widehat{\phi}^{MD}(\alpha) \|_{\mathcal{H}} = |G|^2 \ . \tag{18}$$

*Proof.*

$$\begin{aligned}
\sum_{x \in G} \| \phi(x) \|^2_{\mathcal{H}} &= \sum_{x \in G} \sum_{e \in B_{\mathcal{H}}} |\phi_e(x)|^2 \\
&= \sum_{e \in B_{\mathcal{H}}} \sum_{x \in G} |\phi_e(x)|^2 \\
&= \frac{1}{|G|} \sum_{e \in B_{\mathcal{H}}} \sum_{\alpha \in G} |\widehat{\phi_e}(\alpha)|^2 \\
&\quad \text{(according to the Parseval's equation applied on } \phi_e) \\
&= \frac{1}{|G|} \sum_{\alpha \in G} \sum_{e \in B_{\mathcal{H}}} |\widehat{\phi_e}(\alpha)|^2 \\
&= \frac{1}{|G|} \sum_{\alpha \in G} \| \widehat{\phi}^{MD}(\alpha) \|^2_{\mathcal{H}}
\end{aligned} \tag{19}$$

The second assertion is obvious. □

It is possible and even more interesting to obtain this Parseval's equation by an alternative way. Let $(\phi, \psi) \in (\mathcal{H}^G)^2$ and $\alpha \in G$. By replacing the multiplication by the inner product, we define their *convolutional product* as follows

$$(\phi * \psi)(\alpha) = \sum_{x \in G} \langle \psi(\alpha + x), \phi(x) \rangle_{\mathcal{H}} \ . \tag{20}$$

Since $\phi * \psi : G \to \mathbb{C}$, we can compute its classical discrete Fourier transform

$$\begin{aligned}
\widehat{(\phi * \psi)}(\alpha) &= \sum_{x \in G} (\phi * \psi)(x) \chi^{\alpha}_G(x) \\
&= \sum_{x \in G} \sum_{y \in G} \chi^{\alpha}_G(x) \langle \psi(x + y), \phi(y) \rangle_{\mathcal{H}} \\
&= \sum_{x \in G} \sum_{y \in G} \chi^{\alpha}_G(x + y) \overline{\chi^{\alpha}_G(y)} \langle \psi(x + y), \phi(y) \rangle_{\mathcal{H}} \\
&= \sum_{x \in G} \sum_{y \in G} \langle \chi^{\alpha}_G(x + y) \psi(x + y), \chi^{\alpha}_G(y) \phi(y) \rangle_{\mathcal{H}} \\
&= \sum_{y \in G} \langle \sum_{x \in G} \chi^{\alpha}_G(x + y) \psi(x + y), \chi^{\alpha}_G(y) \phi(y) \rangle_{\mathcal{H}} \\
&= \sum_{y \in G} \langle \widehat{\psi}^{MD}(\alpha), \chi^{\alpha}_G(y) \phi(y) \rangle_{\mathcal{H}} \\
&= \langle \widehat{\psi}^{MD}(\alpha), \sum_{y \in G} \chi^{\alpha}_G(y) \phi(y) \rangle_{\mathcal{H}} \\
&= \langle \widehat{\psi}^{MD}(\alpha), \widehat{\phi}^{MD}(\alpha) \rangle_{\mathcal{H}} \ .
\end{aligned} \tag{21}$$

It is a kind of simplification of the convolutional product by the Fourier transform. Now let us compute $(\phi * \psi)(e_G)$. There are two ways to do this. The first one is given by definition : $(\phi * \psi)(e_G) = \sum_{x \in G} \langle \psi(x), \phi(x) \rangle_{\mathcal{H}}$. The second one is given by the inversion formula of the usual Fourier transform.

$$\begin{aligned}(\phi * \psi)(e_G) &= \frac{1}{|G|} \sum_{\alpha \in G} \widehat{(\phi * \psi)}(\alpha) \overline{\chi_G^{e_G}(\alpha)} \\ &= \frac{1}{|G|} \sum_{\alpha \in G} \widehat{(\phi * \psi)}(\alpha) \\ &= \frac{1}{|G|} \sum_{\alpha \in G} \langle \widehat{\psi}^{MD}(\alpha), \widehat{\phi}^{MD}(\alpha) \rangle_{\mathcal{H}} \ .\end{aligned} \tag{22}$$

Then we have $\sum_{x \in G} \langle \psi(x), \phi(x) \rangle_{\mathcal{H}} = \frac{1}{|G|} \sum_{\alpha \in G} \langle \widehat{\psi}^{MD}(\alpha), \widehat{\phi}^{MD}(\alpha) \rangle_{\mathcal{H}}$.
Now let $\phi = \psi$, then

$$\sum_{x \in G} \langle \phi(x), \phi(x) \rangle_{\mathcal{H}} = \frac{1}{|G|} \sum_{\alpha \in G} \langle \widehat{\phi}(\alpha), \widehat{\phi}(\alpha) \rangle_{\mathcal{H}} \tag{23}$$

*i.e.*

$$\sum_{x \in G} \| \phi(x) \|_{\mathcal{H}}^2 = \frac{1}{|G|} \sum_{\alpha \in G} \| \widehat{\phi}(\alpha) \|_{\mathcal{H}}^2 \ . \tag{24}$$

## 5 Multidimensional bent functions

**Definition 3.** Let $\phi : G \to \mathcal{S}_{\mathcal{H}}(0_{\mathcal{H}}, 1)$. $\phi$ is said *multidimensional bent* if $\forall \alpha \in G$, $\| \widehat{\phi}^{MD}(\alpha) \|_{\mathcal{H}}^2 = |G|$ (*i.e.* $\widehat{\phi}^{MD} : G \to \mathcal{S}_{\mathcal{H}}(0_{\mathcal{H}}, \sqrt{|G|})$).

**Lemma 2.** *Let $\phi : G \to \mathcal{H}$. Then $\phi(x) = 0_{\mathcal{H}}$ $\forall x \in G^*$ if and only if $\widehat{\phi}^{MD}(\alpha) = \phi(e_G)$ $\forall \alpha \in G$.*

*Proof.* $\Rightarrow$) $\widehat{\phi}^{MD}(\alpha) = \sum_{x \in G} \chi^{\alpha}(x) \phi(x) = \phi(e_G)$ $\forall \alpha \in G$.

$\Leftarrow$) $\phi(x) = \frac{1}{|G|} \sum_{\alpha \in G} \overline{\chi_G^{\alpha}(x)} \widehat{\phi}^{MD}(\alpha)$ (by the inversion formula of the multidimensional Fourier transform). Then by hypothesis, $\phi(x) = \frac{\phi(e_G)}{|G|} \sum_{\alpha \in G} \chi_G^{\alpha}(x) = 0_{\mathcal{H}}$ if $x \in G^*$ and $\phi(e_G)$ otherwise. □

Note that this lemma is in particular true for $\mathcal{H} = \mathbb{C}$ and then for the usual Fourier transform.
We now define a kind of derivative for $\mathcal{H}$-valued functions. Another time we use the natural "multiplication" of $\mathcal{H}$ which is its inner product.

**Definition 4.** Let $\phi : G \to \mathcal{H}$ and $\alpha \in G$. The *derivative of $\phi$ in direction $\alpha$* is defined by

$$\begin{aligned} d_\alpha\phi : G &\to \mathbb{C} \\ x &\mapsto \langle \phi(\alpha + x), \phi(x) \rangle_{\mathcal{H}} \end{aligned} \tag{25}$$

This derivative measures the default of orthogonality between $\phi(x)$ and $\phi(\alpha+x)$.

**Proposition 2.** *Let $\phi : G \to \mathcal{S}_{\mathcal{H}}(0_{\mathcal{H}}, 1)$. Then $\phi$ is bent if and only if $\forall \alpha \in G^*$, $\widehat{d_\alpha\phi}(e_G) = 0$.*

*Proof.* Let define the following auto-correlation function

$$\begin{aligned} AC_\phi : G &\to \mathbb{C} \\ \alpha &\mapsto \widehat{d_\alpha\phi}(e_G) \ . \end{aligned} \tag{26}$$

We have

$$\begin{aligned} \widehat{d_\alpha f}(e_G) &= \sum_{x \in G} d_\alpha\phi(x)\chi_G^{e_G}(x) \\ &= \sum_{x \in G} d_\alpha\phi(x) \\ &= \sum_{x \in G} \langle \phi(\alpha + x), \phi(x) \rangle_{\mathcal{H}} \\ &= (\phi * \phi)(\alpha) \ . \end{aligned} \tag{27}$$

Let us compute $\widehat{AC_\phi}(\alpha)$.

$$\begin{aligned} \widehat{AC_\phi}(\alpha) &= \sum_{x \in G} AC_\phi(x)\chi_G^\alpha(x) \\ &= \sum_{x \in G} (\phi * \phi)(x)\chi_G^\alpha(x) \\ &= \widehat{(\phi * \phi)}(\alpha) \\ &= \langle \widehat{\phi}^{MD}(\alpha), \widehat{\phi}^{MD}(\alpha) \rangle_{\mathcal{H}} \text{ (by the formula (21))} \\ &= \| \ \widehat{\phi}^{MD}(\alpha) \ \|_{\mathcal{H}}^2 \ . \end{aligned} \tag{28}$$

Then we have $\forall \alpha \in G^*$, $\widehat{d_\alpha\phi}(e_G) = 0 \Leftrightarrow \forall \alpha \in G^*$, $AC_\phi(\alpha) = 0$
$\Leftrightarrow \forall \alpha \in G$, $\widehat{AC_\phi}(\alpha) = AC_\phi(e_G)$ (according to lemma 2)
$\Leftrightarrow \forall \alpha \in G$, $\| \ \widehat{\phi}^{MD}(\alpha) \ \|_{\mathcal{H}}^2 = AC_\phi(e_G)$.
As $AC_\phi(e_G) = (\phi * \phi)(e_G) = \sum_{x \in G} \langle \phi(x), \phi(x) \rangle_{\mathcal{H}} = \sum_{x \in G} \| \ \phi(x) \ \|_{\mathcal{H}}^2 = |G|$ (since $\phi$ is $\mathcal{S}_{\mathcal{H}}(0_{\mathcal{H}}, 1)$-valued), we conclude the expected result. □

Let us also see a notion of dual function for multidimensional bentness similar to the traditional one.

**Proposition 3.** *Let $\phi : G \to \mathcal{S}_{\mathcal{H}}(0_{\mathcal{H}}, 1)$ be a multidimensional bent function. Then the function $\tilde{\phi} : G \to \mathcal{S}_{\mathcal{H}}(0_{\mathcal{H}}, 1)$, defined by $\tilde{\phi} = \frac{1}{\sqrt{|G|}}\widehat{\phi}^{MD}$ and called* dual of $\phi$, *is also multidimensional bent.*

*Proof.* Let first check that $\tilde{\phi}(\alpha) \in \mathcal{S}_{\mathcal{H}}(0_{\mathcal{H}}, 1)$ for all $\alpha \in G$. We have $\| \tilde{\phi}(\alpha) \|^2_{\mathcal{H}} = \frac{1}{|G|} \| \widehat{\phi}^{MD}(\alpha) \|^2_{\mathcal{H}} = 1$ (since $\phi$ is multidimensional bent). Now let compute $\widehat{\tilde{\phi}}^{MD}(\alpha) = \frac{1}{\sqrt{|G|}} \widehat{\widehat{\phi}^{MD}}(\alpha) = \frac{|G|}{\sqrt{|G|}} \phi(-\alpha) = \sqrt{|G|}\phi(-\alpha)$. Then we have that $\| \widehat{\tilde{\phi}}^{MD}(\alpha) \|^2_{\mathcal{H}} = |G| \| \phi(-\alpha) \|^2_{\mathcal{H}} = |G|$ (by hypothesis). □

## 6 Some constructions of multidimensional bent functions

### 6.1 Concatenation construction

Let $\rho = \sum_{e \in B_{\mathcal{H}}} \rho_e e \in \mathcal{S}_{\mathcal{H}}(0_{\mathcal{H}}, 1)$ and $\psi : G \to \mathcal{S}_{\mathcal{H}}(0_{\mathcal{H}}, 1)$ such that for each $e \in B_{\mathcal{H}}$, $\psi_e$ is defined as $\rho_e \phi_e$ where $\phi_e : G \to \mathcal{S}_{\mathbb{C}}(0, 1)$ is an element of $\mathcal{B}(G)$ (*i.e.* $\phi_e$ is classical bent). Then $\psi$ is a multidimensional bent function.
First let us check that for all $x \in G$, $\psi(x) \in \mathcal{S}_{\mathcal{H}}(0_{\mathcal{H}}, 1)$. We have $\| \psi(x) \|^2_{\mathcal{H}} = \sum_{e \in B_{\mathcal{H}}} |\psi_e(x)|^2 = \sum_{e \in B_{\mathcal{H}}} |\rho_e \phi_e(x)|^2 = 1$.
Now let show that $\psi$ is bent. We have $\widehat{\psi}^{MD}(\alpha) = \sum_{e \in B_{\mathcal{H}}} \rho_e \widehat{\phi_e}(\alpha) e$. Then we have $\| \widehat{\psi}^{MD}(\alpha) \|^2_{\mathcal{H}} = \sum_{e \in B_{\mathcal{H}}} |\rho_e \widehat{\phi_e}(\alpha)|^2 = |G| \sum_{e \in B_{\mathcal{H}}} |\rho_e|^2 = |G|$.
This construction is a kind of concatenation of usual bent functions. We can generalized it as follows.

For $i = 1, \ldots, n$, $\mathcal{H}_i$ denotes an Hermitian space with a finite dimension (with $\langle ., . \rangle_{\mathcal{H}_i}$ and $\| \, . \, \|_{\mathcal{H}_i}$). We define the product Hermitian space $\mathcal{H} = \prod_{i=1}^{n} \mathcal{H}_i$. Let $((u_1, \ldots, u_n), (v_1, \ldots, v_n)) \in \mathcal{H}^2$, we have

$$\langle (u_1, \ldots, u_n), (v_1, \ldots, v_n) \rangle_{\mathcal{H}} = \sum_{i=1}^{n} \langle u_i, v_i \rangle_{\mathcal{H}_i} \tag{29}$$

and then

$$\| (u_1, \ldots, u_n) \|^2_{\mathcal{H}} = \sum_{i=1}^{n} \| u_i \|^2_{\mathcal{H}_i} \quad . \tag{30}$$

For $i = 1, \ldots, n$, we suppose given $\phi_i : G \to \mathcal{S}_{\mathcal{H}_i}(0_{\mathcal{H}_i}, 1) \subset \mathcal{H}_i$ a multidimensional bent function. Let $\rho = (\rho_1, \ldots, \rho_n) \in \mathcal{S}_{\mathbb{C}^n}(0_{\mathbb{C}^n}, 1) \subset \mathbb{C}^n$. We define

$$\begin{array}{l} \phi : G \to \mathcal{H} \\ \quad x \mapsto (\rho_1 \phi_1(x), \ldots, \rho_n \phi_n(x)) \; . \end{array} \tag{31}$$

Then $\phi$ is a multidimensional bent function.
First let see that $\phi$ is a $\mathcal{S}_{\mathcal{H}}(0_{\mathcal{H}}, 1)$-valued function

$$\| \phi(x) \|^2_{\mathcal{H}} = \sum_{i=1}^{n} |\rho_i|^2 \| \phi_i(x) \|^2_{\mathcal{H}_i} = \sum_{i=1}^{n} |\rho_i|^2 = 1.$$

Let $\alpha \in G$, we have $\widehat{\phi}^{MD}(\alpha) = \sum_{x \in G} \chi^{\alpha}(x)\phi(x) = \sum_{x \in G} (\chi^{\alpha}_G(x)\rho_1\phi_1(x), \ldots, \chi^{\alpha}_G(x)\rho_n \phi_n(x)) = (\rho_1 \widehat{\phi_1}^{MD}(\alpha), \ldots, \rho_n \widehat{\phi_n}^{MD}(\alpha))$.
Then $\| \widehat{\phi}^{MD}(\alpha) \|^2_{\mathcal{H}} = \sum_{i=1}^{n} |\rho_i|^2 \| \widehat{\phi_i}^{MD}(\alpha) \|^2_{\mathcal{H}_i} = |G| \sum_{i=1}^{n} |\rho_i|^2 = |G|$.

### 6.2 Disjoint supports construction

The following constructions are not based anymore on the concatenation of several usual bent functions and so are even more interesting.
Let $G$ be a non trivial ($G$ is not reduced to $e_G$) finite Abelian group. Let $B = \{e_k\}_{k=1}^{|G|}$ be the canonical basis of $\mathbb{C}^{|G|}$ (equipped with the usual inner product). Let $i : G \to \{1, \ldots, |G|\}$ be a bijection. We define the following function

$$\begin{aligned} \phi : G &\to \mathbb{C}^{|G|} \\ x &\mapsto e_{i(x)} \ . \end{aligned} \tag{32}$$

We have $\| \phi(x) \|^2_{\mathbb{C}^{|G|}} = \| e_{i(x)} \|^2_{\mathbb{C}^{|G|}} = 1$ and then $\phi$ is $\mathcal{S}_{\mathbb{C}^{|G|}}(0_{\mathbb{C}^{|G|}}, 1)$-valued.
We have $\widehat{\phi}^{MD}(\alpha) = \sum_{x \in G} \chi^{\alpha}_G e_{i(x)} = \sum_{k=1}^{|G|} \chi^{\alpha}_G(i^{-1}(k)) e_k$ *i.e* we find that $\widehat{\phi}^{MD}(\alpha) = (\chi^{\alpha}_G(i^{-1}(1)), \ldots, \chi^{\alpha}_G(i^{-1}(|G|)))$ and then $\| \widehat{\phi}^{MD}(\alpha) \|^2_{\mathbb{C}^{|G|}} = \sum_{k=1}^{|G|} |\chi^{\alpha}_G(i^{-1}(k)|^2 = |G|$ and so, $\phi$ is multidimensional bent.
We now show that the component functions of $\phi$ can not be, up to a factor, usual bent functions. First of all, none of the component functions (in the canonical basis of $\mathbb{C}^{|G|}$) is usual bent since for $k \in \{1, \ldots, |G|\}$, we have $\phi_k(x) = 0 \forall x \neq i^{-1}(k)$ (it is possible since $|G| > 1$) and then $\phi_k$ can not be $\mathcal{S}_{\mathbb{C}}(0, 1)$-valued. Now suppose that we can find $\rho = (\rho_1, \ldots, \rho_{|G|}) \in \mathcal{S}_{\mathbb{C}^{|G|}}(0_{\mathbb{C}^{|G|}}, 1) \subset \mathbb{C}^{|G|}$ and for $k = 1, \ldots, |G|$, $\psi_k : G \to \mathcal{S}_{\mathbb{C}}(0, 1) \subset \mathbb{C}$ usual bent functions such that $\phi = (\rho_1\psi_1, \ldots, \rho_{|G|}\psi_{|G|})$. As we know that for each $k \in \{1, \ldots, |G|\}$, we have $\forall x \in G$ such that $i(x) \neq k$, $\phi_k(x) = 0$ then $\rho_k\psi_k(x) = 0$ and then $\rho_k = 0$ or $\psi_k(x) = 0$. Since $\psi_k$ must be $\mathcal{S}_{\mathbb{C}}(0, 1)$-valued, $\rho_k = 0$. As it is true for all $k$, we deduce that $\rho = (0, \ldots, 0)$ which is a contradiction with the fact that $\rho \in \mathcal{S}_{\mathbb{C}^{|G|}}(0_{\mathbb{C}^{|G|}}, 1)$.

The previous construction can be generalized as follows. Let $G$ be a non trivial finite Abelian group. Let $A = \{u^{(i)}\}_{i=1}^{|G|}$ be a set of exactly $|G|$ vectors of $\mathbb{C}^{|G|}$ such that for each $i \in \{1, \ldots, |G|\}$ it exists one and only one $k \in \{1, \ldots, |G|\}$, denoted $k(i)$, and $\omega_i \in \mathcal{S}_{\mathbb{C}}(0, 1)$ such that $u^{(i)}_j = \begin{cases} w_i \text{ if } j = k(i) \\ 0 \quad \text{if } j \neq k(i) \end{cases}$. In particular each $u^{(i)}$ is an element of $\mathcal{S}_{\mathbb{C}^{|G|}}(0_{\mathbb{C}^{|G|}}, 1)$. Note that $k : \{1, \ldots, |G|\} \to \{1, \ldots, |G|\}$ is a

bijective map. Let $i : G \to \{1, \ldots, |G|\}$ be a bijection. We define the function

$$\begin{aligned} \phi : G &\to \mathbb{C}^{|G|} \\ x &\mapsto u^{(i(x))} \ . \end{aligned} \tag{33}$$

Then $\phi$ is multidimensional bent.
Let $x \in G$. $\phi(x) \in \mathcal{S}_{\mathbb{C}^{|G|}}(0_{\mathbb{C}^{|G|}}, 1)$ because $\phi(x) = u^{(i(x))} \in \mathcal{S}_{\mathbb{C}^{|G|}}(0_{\mathbb{C}^{|G|}}, 1)$.
Let $\alpha \in G$. We have $\widehat{\phi}^{MD}(\alpha) = \sum_{x \in G} \chi_G^\alpha(x) u^{(i(x))} = \sum_{j=1}^{|G|} \chi_G^\alpha(i^{-1}(j)) u^{(j)}$ which is equal to $(\chi_G^\alpha(i^{-1}(1))\omega_{k^{-1}(1)}, \ldots, \chi_G^\alpha(i^{-1}(|G|))\omega_{k^{-1}(|G|)})$. Then $\| \widehat{\phi}^{MD}(\alpha) \|^2_{\mathbb{C}^{|G|}} = \sum_{j=1}^{|G|} |\chi_G^\alpha(i^{-1}(j))|^2 |\omega_{k^{-1}(j)}|^2 = |G|$.

## References


[BS91] E. Biham, A. Shamir : Differential cryptanalysis of DES-like cryptosystems. In *Journal of Cryptology*, vol. 4, no. 1, p. 3-72, 1991

[Dil74] J. F. Dillon : Elementary Hadamard difference sets. PhD Thesis, University of Maryland, 1974

[LSY97] O. A. Logachev, A. A. Salnikov, V. V. Yashchenko : Bent functions on a finite Abelian group. In *Discrete Math. Appl.*, vol. 7(6), pp. 547-564, 1997

[Mat94] M. Matsui : Linear Cryptanalysis Method for DES Cipher. In *Advances in Cryptology - Eurocrypt '93*, vol. 765 of Lecture Notes in Computer Science, pp. 386-397, 1994

[Rot76] O. S. Rothaus : On bent functions. In *Journal of Combinatorial Theory A*, vol. 20, pp. 300-365, 1976