Journal of Combinatorial Theory, Series A **93**, 242–260 (2001)
doi:10.1006/jcta.2000.3076, available online at http://www.idealibrary.com on IDEAL®

Completed $\mathscr{GPS}$ Covers All Bent Functions

Philippe Guillot

Thomson-CSF Comsys, 66 Rue du Fossé Blanc, 92231 Gennevilliers CEDEX, France
E-mail: Philippe.Guillot@tcc.thomson-csf.com

Communicated by the Managing Editors

Received April 30, 1998

In a recent paper, the so-called "generalized partial spread" ($\mathscr{GPS}$) class which unifies almost all the known classes of bent functions is introduced. A necessary condition for a bent function to belong to $\mathscr{GPS}$ is that it takes the same value as its dual at the zero vector. In this paper, it is shown that the necessary condition above is sufficient. This proves that the completed class by composition with translations covers all the binary bent functions. Moreover, the elements of $\mathscr{GPS}$ are characterized in term of solutions of a quadratic Diophantine equation which may lead to count all bent functions. These results are presented in the general framework of partial bent functions which unify bent functions and r-dimensional vector space indicators.

Key Words: Bent functions; Möbius function; generalized partial spread.

1. INTRODUCTION

Let $n = 2r$ be an even integer and V_n be the n-dimensional vector space over $GF(2)$ of all binary words of length n. We are interested in Boolean (i.e., $\{0, 1\}$-valued) functions on V_n. These functions are considered here as real valued functions. So, the set of Boolean functions can be viewed as the 2^n-dimensional real vector space of the real valued functions on V_n denoted by $\mathscr{F}_n$. This article is devoted to the study of some properties of bent functions. Given that they achieve the property of perfect nonlinearity, bent functions on V_n play an important role in different topics such as coding theory and cryptology (see [8, 13]). They can be equivalently defined as the Boolean functions which reach the maximum Hamming distance to the set of affine functions on V_n and as the Boolean functions f such that the function $x \mapsto (-1)^{f(x)+f(x+a)}$ is balanced for every nonzero vector $a \in V_n$ (see [8]).

There exist several constructions of bent functions due to Maiorana-McFarland, Dillon, Carlet, and Dobbertin (see [4, 8, 9]), but the problem of the complete enumeration of all bent functions remains open.

0097-3165/01 $35.00

Let us first recall some preliminaries. The all zero vector is simply denoted by 0 and the all one vector by 1. The usual dot product on V_n is defined for all $x=(x_1, ..., x_n)$ and $y=(y_1, ..., y_n)\in V_n$ by $x\cdot y=x_1y_1+\cdots+x_ny_n$ (modulo 2). For any subset E of V_n, the *dual* of E, denoted by $E^\perp$, is the vector subspace equal to $\{x\in V_n \mid \forall y\in E x\cdot y=0\}$. The Walsh transform of a function $f\in\mathscr{F}_n$ is the element of $\mathscr{F}_n$ denoted by $\hat{f}$ and defined by

$$\forall y\in V_n, \qquad \hat{f}(y)=\sum_{x\in V_n} f(x)(-1)^{x\cdot y}.$$

The Walsh transformation is a linear invertible mapping on $\mathscr{F}_n$. It satisfies $\hat{\hat{f}}=2^n f$. The Parseval's equality holds:

$$\forall f\in\mathscr{F}_n, \qquad \sum_{y\in V_n}\hat{f}^2(y)=2^n\sum_{x\in V_n} f^2(x).$$

For any subset S of V_n, let ϕ_S denote the indicator of S, i.e., the element of $\mathscr{F}_n$ which takes value 1 on S and 0 elsewhere. It is well known that the Walsh transform of the indicator of a d-dimensional vector subspace E of V_n is equal to

$$\widehat{\phi_E}=2^d\phi_{E^\perp} \tag{1}$$

Conversely, if the Walsh transform of a Boolean function f takes only two values 0 and M, then it is necessarily the indicator of a d-dimensional vector space and then $M=2^d$.

A Boolean function $f\in\mathscr{F}_n$ is called *bent* if the Walsh transform of the function $f_\chi: x\mapsto(-1)^{f(x)}$ has constant magnitude 2^r, i.e., if

$$\forall y\in V_n, \qquad \widehat{f_\chi}(y)=\pm 2^r.$$

Thus, if a function f is bent, there exists another Boolean function denoted by $\tilde{f}$ and called the *dual* function of f defined by $\widehat{f_\chi}=2^r(-1)^{\tilde{f}}$ (see [8, 9]).

For any element x of V_n, let $\mathrm{w}(x)$ denote the Hamming weight of x defined as the number of nonzero components of x and $\bar{x}=x+1$, the componentwise complementary of x.

2. GENERALIZED PARTIAL SPREADS

In [4], Carlet shows that, up to a translation, almost all the known bent functions are elements of a new class called the *generalized partial spreads* class and denoted $\mathscr{GPS}$. We show here that $\mathscr{GPS}$ contains almost all the

bent functions and presents a suitable framework for their study. In this section, we recall the definition and the main property of this class which are stated and proved in [4].

DEFINITION 1. A Boolean function f on V_n, $n = 2r \geqslant 4$, belongs to $\mathscr{GPS}$ if there exists r-dimensional vector spaces $E_1, ..., E_k$ and integers $m_1, ..., m_k$ such that

$$f = -2^{r-1}\phi_{\{0\}} + \sum_{i=1}^{k} m_i \phi_{E_i} \tag{2}$$

Such a decomposition of a Boolean function f is called a *geometric form* of f. An example of explicit construction is given by the $\mathscr{PS}$ class (see [8]), where the E_i's are pairwise in direct sum. The following proposition states the main properties of $\mathscr{GPS}$.

PROPOSITION 1 [4]. *Let $f = -2^{r-1}\phi_{\{0\}} + \sum_{i=1}^{k} m_i \phi_{E_i}$ be a Boolean function which belongs to $\mathscr{GPS}$, the following properties hold*:

(1) *f is bent*;

(2) *the complementary function $\bar{f} = 1 - f$ belongs to $\mathscr{GPS}$*;

(3) *for any linear invertible mapping A on V_n, the function $f \circ A$ belongs to $\mathscr{GPS}$*;

(4) *$\tilde{f}$ belongs to $\mathscr{GPS}$ and $\tilde{f} = -2^{r-1}\phi_{\{0\}} + \sum_{i=1}^{k} m_i \phi_{E_i^{\perp}}$*;

(5) $f(0) = \tilde{f}(0)$

As noticed in [4], a consequence of the latter property is that $\mathscr{GPS}$ does not cover the whole set of bent functions. Indeed, let f be a bent function and $a \in V_n$ such that $f(a) \neq f(0)$, then the function $f_a : x \mapsto f(x + a)$ is bent and satisfies $f_a(0) = f(a) \neq \tilde{f}(0) = \tilde{f}_a(0)$. In Section 8, it is shown that property (5) characterizes $\mathscr{GPS}$.

3. PARTIAL BENT FUNCTIONS

This work will be presented for a more general family of Boolean functions which unifies bent functions and r-dimensional vector spaces. We call call them *partial bent functions.*

Bent functions are those whose support is in fact a *difference set* (see [8]). Similarly the support of *partial* bent functions defined below is a *partial* difference set (see [12]). This notion is related with strongly regular graphs and two weight projective codes (see [2]).

Remark. Partial bent function defined here is a notion totally different from the notion of *partially bent functions* defined in [6].

DEFINITION 2. A Boolean function on V_n is called *partial bent* if it has even weight and if its Walsh transform takes exactly two values on $V_n \backslash \{0\}$ which differ of 2^r.

It is not a restriction to consider only even weight function because from $\widehat{\phi_{\{0\}}} = 1$, changing the value at 0 does not change the second condition on the Walsh transform.

If f is partial bent, then by definition, there exist two real numbers m and $\tilde{m}$ and a Boolean function $\tilde{f}$, called the *dual* of f, which can be choosen of even weight and such that

$$\hat{f} = m + 2^r \tilde{f} - 2^r \tilde{m} \phi_{\{0\}}. \tag{3}$$

This relation characterizes partial bent function. Notice that m is the lowest value of $\hat{f}$ on $V_n \backslash \{0\}$ and thus is an integer. Applying the Walsh transformation to equality (3) yields

$$\hat{\tilde{f}} = \tilde{m} + 2^r f - 2^r m \phi_{\{0\}}$$

which proves that $\tilde{f}$ is also a partial bent function; its dual is f itself and that $\tilde{m}$ is an integer.

Notice that, f and $\tilde{f}$ being of even weight, the integers m and $\tilde{m}$ are even.

EXAMPLES.

- Bent functions are partial bent bunctions with parameter $m = -2^{r-1}$;
- r-dimensional vector space indicators are partial bent functions with parameter $m = 0$.

The following proposition states the stability properties of the family of partial bent functions.

PROPOSITION 2. *If f is a partial bent function on V_n then*

(1) *the complementary function $\bar{f} = 1 - f$ is also a partial bent function and $\tilde{\bar{f}} = \bar{\tilde{f}}$;*

(2) *for all invertible linear mapping A on V_n, the function $f \circ A$ is also a partial bent function and $\widetilde{f \circ A} = \tilde{f} \circ ({}^t A)^{-1}$.*

Proof. From relation (3), we deduce

$$\widehat{1-f} = 2^n \phi_{\{0\}} - \hat{f} = (-2^r - m) + 2^r(1-\tilde{f}) - 2^r(-2^r - \tilde{m})\,\phi_{\{0\}}.$$

This proves the first part of the proposition. The second part is a direct consequence of the well known property of the Walsh transform: $\widehat{f \circ A} = \hat{f} \circ ({}^tA)^{-1}$. ∎

Note that the composition of a partial bent function with a translation is not in general a partial bent function.

The parameters m and $\tilde{m}$ of relation (3) are necessarily related one to the other as shown by the following proposition.

PROPOSITION 3. *Let f be a partial bent function on V_n and $\tilde{f}$ its dual. If $f(0) = \tilde{f}(0)$ then $\tilde{m} = m$. If $f(0) \neq \tilde{f}(0)$ then $\tilde{m} = -m - 2^r$.*

Proof. Suppose that $f(0) = \tilde{f}(0)$. We can assume without a loss of generality that $f(0) = \tilde{f}(0) = 0$. Otherwise, consider the complementary functions. For all nonzero vector u, we have $\hat{f}(u) = m + 2^r \tilde{f}(u)$ and $\hat{f}(0) = m - 2^r \tilde{m}$. By squaring these relations and noticing, $\tilde{f}$ being Boolean, that $\tilde{f}(u) = \tilde{f}^2(u)$, for all nonzero vector u, we have $\hat{f}^2(u) = m^2 + (2^n + 2^{r+1})\tilde{f}(u)$ and $\hat{f}^2(0) = m^2 - 2^{r+1} m\tilde{m} + 2^n \tilde{m}^2$. By summing these relations on u, using Parseval's equality and noticing that $\sum_{u \neq 0} \tilde{f}(u) = \hat{\tilde{f}}(0)$, we get

$$2^n m^2 + (2^n + 2^{r+1} m)\hat{\tilde{f}}(0) - 2^{r+1} m\tilde{m} + 2^n \tilde{m}^2 = 2^n \hat{f}(0).$$

By using $\hat{\tilde{f}}(0) = \tilde{m} - 2^r m$ and $\hat{f}(0) = m - 2^r \tilde{m}$ in this equality, we yield, after elementary calculations

$$(\tilde{m} - m)(\tilde{m} + m + 2^r + 1) = 0.$$

The integers m and $\tilde{m}$ being even, the second factor cannot be null and thus, $\tilde{m} = m$.

A very similar proof assuming $f(0) \neq \tilde{f}(0)$ leads to the second part of the proposition. ∎

4. EXTENDED $\mathcal{GPS}$

$\mathcal{GPS}$ is a subclass of the bent functions. We define here a generalization which is a subclass of the partial bent functions.

DEFINITION 3. A Boolean function on V_n belongs to *extended* $\mathscr{GPS}$, denoted $\mathscr{EGPS}$, if there exist integers $m_0, m_1, ..., m_k$ and r-dimensional vector spaces $E_1, ..., E_k$ such that f is expressed as

$$f = m_0 \phi_{\{0\}} + \sum_{i=1}^{k} m_i \phi_{E_i}. \tag{4}$$

The difference with $\mathscr{GPS}$ is that we allow the $\phi_{\{0\}}$-coefficient to be different from -2^{r-1}.

PROPOSITION 4. *Let f be a Boolean function expressed as in relation* (4). *Then the function g defined by*

$$g = m_0 \phi_{\{0\}} + \sum_{i=1}^{k} m_i \phi_{E_i^\perp}$$

is also a Boolean function.

Proof (*Summary*). Apply the Walsh transform to relation (4) and use Parseval's equality to prove that

$$\sum_{x \in V_n} g(x) = \sum_{x \in V_n} g^2(x),$$

the function g being integer valued. This proves that it is a Boolean function. ∎

If $m_0 = 0$ it corresponds to the class of r-dimensional vector spaces indicators and the function g is the indicator of the dual.

If $m_0 = -2^{r-1}$, it corresponds to the $\mathscr{GPS}$ class and g is the dual of f.

Notice that we have

$$\hat{f} = m_0 + 2^r \sum_{i=1}^{k} m_i \phi_{E_i} = m_0 + 2^r (g - m_0 \phi_{\{0\}})$$

and thus the function f is partial bent and its dual is g. In particular, the function g and the coefficient m_0 do not depend on the choice of the vector spaces E_i which define f.

Applying the previous relations to the zero vector shows that any element of $\mathscr{EGPS}$ and its dual take the same value at the zero vector.

5. MOBIUS DECOMPOSITION OF FUNCTIONS

In the following sections, the Möbius transform tool will be used as in [5, 7], and a brief summary of this follows. The set V_n is a lattice with the

Lucas partial order relation defined for all $x=(x_1, ..., x_n)$ and $y=(y_1, ..., y_n) \in V_n$ by

$$x \succcurlyeq y \Leftrightarrow \forall i \in \{1, ..., n\}\ x_i \geqslant y_i.$$

Let $x \vee y$ and $x \wedge y$ denote respectively the least upper bound and the greatest lower bound of the two vectors x and y, and $x \backslash y = x \wedge \bar{y}$ denote the vector z such that for all index i, $z_i = 1$ if and only if $x_i = 1$ and $y_i = 0$. For any $a, b \in V_n$, interval $[a, b]$ is defined to be equal to the set $\{x \in V_n \mid a \preccurlyeq x \preccurlyeq b\}$. Note that if $a \not\preccurlyeq b$ then $[a, b]$ is equal to the empty set. Likewise, half open intervals $]a, b]$ and $[a, b[$ are respectively equal to the sets $\{x \in V_n \mid a \prec x \preccurlyeq b\}$ and $\{x \in V_n \mid a \preccurlyeq x \prec b\}$.

For each vector y, the interval $[0, y]$ is a vector space of dimension $\mathrm{w}(y)$. Its dual is the interval $[0, \bar{y}]$.

The Lucas partial order relation satisfies the following orthogonality relation (see [14]):

LEMMA 1. *For any a and $b \in V_n$, $\sum_{t \in [a, b]} (-1)^{\mathrm{w}(b) - \mathrm{w}(t)} = 1$ if $a = b$ and 0 otherwise.*

This relation leads to the classical Möbius inversion formula. For any element f of $\mathscr{F}_n$, the Möbius transform of f with respect to $\succcurlyeq$ is the element of $\mathscr{F}_n$ denoted by $\mathring{f}$ and defined by

$$\forall y \in V_n, \qquad \mathring{f}(y) = \sum_{x \succcurlyeq y} (-1)^{\mathrm{w}(x) - \mathrm{w}(y)} f(x).$$

The Möbius transformation is a linear invertible mapping on $\mathscr{F}_n$. The function f can be recovered from $\mathring{f}$ by the Möbius inversion formula,

$$\forall x \in V_n, \qquad f(x) = \sum_{y \succcurlyeq x} \mathring{f}(y) \tag{5}$$

Note that this Möbius transformation is not the one defined in [8] with the usual Lucas order $\preccurlyeq$ which leads to the *algebraic normal form* of Boolean functions. The transformation used here is defined with the *dual* order $\succcurlyeq$. But these two transforms have very similar properties. The reason for using order $\succcurlyeq$ is that the relation (5) can be rewritten as

$$f = \sum_{y \in V_n} \mathring{f}(y)\, \phi_{[0, y]},$$

which is a decomposition of f into vector subspaces of V_n indicators. We call it the *Möbius decomposition* of f. By the inversion formula, this decomposition is unique. In other words, the set $\{\phi_{[0, y]}\}_{y \in V_n}$ is a basis of the vector space $\mathscr{F}_n$.

The following proposition states the relationship between the Möbius decomposition of a partial bent function and that of its dual.

PROPOSITION 5. *Let f be a partial bent function on V_n and $\tilde{f}$ be its dual,*

$$\forall y \in V_n, \qquad y \neq 0, 1, \qquad \mathring{f} = 2^{r-\mathrm{w}(y)} \mathring{\tilde{f}}(y) \tag{6}$$

$$\mathring{f}(1) = 2^{-r}(\mathring{\tilde{f}}(0) - m) \tag{7}$$

$$\mathring{f}(0) = m + 2^r \mathring{\tilde{f}}(1). \tag{8}$$

Proof. From Proposition 3, f satisfies $\hat{\tilde{f}} = m + 2^r f - 2^r m \phi_{\{0\}}$ for some integer m. Thus $f = m\phi_{\{0\}} + 2^{-r}\hat{\tilde{f}} - 2^{-r}m$. On the other hand, by applying the Walsh transform to the Möbius decomposition of $\tilde{f}$, we yield

$$\hat{\tilde{f}} = \sum_{y \in V_n} 2^{\mathrm{w}(y)} \mathring{\tilde{f}}(y)\, \phi_{[0, \bar{y}]} = \sum_{y \in V_n} 2^{n-\mathrm{w}(y)} \mathring{\tilde{f}}(\bar{y})\, \phi_{[0, y]}.$$

We deduce the following decomposition of f:

$$f = (m + 2^r \mathring{\tilde{f}}(1))\, \phi_{\{0\}} + \sum_{y \neq 0, 1} 2^{r-\mathrm{w}(y)} \mathring{\tilde{f}}(\bar{y})\, \phi_{[0, y]} + 2^{-r}(\mathring{\tilde{f}}(0) - m).$$

This is the unique Möbius decomposition of f. The result holds by terms identification. ∎

6. SOME PRELIMINARIES

The central result of this article is a decomposition theorem of functions by mean of r-dimensional vector space indicators. The proof will be constructive. In this section, we define the vector spaces we use.

6.1. *Spaces $G_{m, y}$*

For any m and $y \in V_m$ such that $m \preccurlyeq y$, let $G_{m, y}$ be the vector space equal to the direct sum of the interval $[0, m]$ and of the line generated by the vector $y \backslash m$. It $y \succ m$ then $\dim(G_{m, y}) = \mathrm{w}(m) + 1$ and if $y = m$ then $G_{m, y} = [0, m]$ and so $\dim(G_{m, y}) = \mathrm{w}(m)$.

The following lemma expresses the indicator of $[0, y]$ by mean of indicators of some spaces $G_{m, y}$.

LEMMA 2. *For any pair of vectors m and $y \in V_n$ such that $m \preccurlyeq y$,*

$$\phi_{[0, y]} = (2 - 2^{\mathrm{w}(y) - \mathrm{w}(m)})\, \phi_{[0, m]} + \sum_{u \in\,]m, y]} \phi_{G_{m, u}} \tag{9}$$

Proof. For any pair m, u of elements of V_n such that $m \prec u$, the space $G_{m,u}$ is the disjoint union of $[0, m]$ and of $[u \backslash m, u]$, then $\phi_{G_{m,u}} = \phi_{[0,m]} + \phi_{[u\backslash m, u]}$. By linearity of Möbius transform, $\mathring{\phi}_{G_{m,u}} = \mathring{\phi}_{[0,m]} + \mathring{\phi}_{[u\backslash m,u]} = \phi_{\{m\}} + \mathring{\phi}_{[u\backslash m,u]}$. Let us compute the second term. For all $x \in V_n$,

$$\mathring{\phi}_{[u\backslash m,u]}(x) = \sum_{y \geqslant x} (-1)^{w(y)-w(x)} \phi_{[u\backslash m,u]}(y) = \sum_{y \in [x \vee (u\backslash m),\, u]} (-1)^{w(y)-w(x)}.$$

From Lemma 1, the latter sum is nonzero only if $u = x \vee (u \backslash m)$, i.e. if $x \in [m, u]$. In the latter case, the sum is equal to $(-1)^{w(u)-w(x)}$, thus $\mathring{\phi}_{[u\backslash m,u]}(x) = (-1)^{w(u)-w(x)} \phi_{[m,u]}(x)$. Finally, $\mathring{\phi}_{G_{m,u}}(x) = \phi_{\{m\}}(x) + (-1)^{w(u)-w(x)} \phi_{[m,u]}(x)$. If $u \succ m$ we have $\phi_{G_{m,u}} = \mathring{\phi}_{[0,m]} + \sum_{y \in [m,u]} (-1)^{w(u)-w(y)} \phi_{[0,y]}$ by Möbius inversion formula. If $u = m$, then $\phi_{G_{m,u}} = \phi_{[0,m]}$. From the Möbius inversion formula applied for all $x \in V_n$ to the function $y \mapsto \phi_{[0,y]}(x)$ on the interval $[m, u]$ (which is isomorphic to the lattice $V_{w(u)-w(m)}$), we obtain, for all $y, m \in V_n$ such that $m \leqslant y$:

$$\phi_{[0,y]} = \phi_{[0,m]} + \sum_{u \in\,]m,\, y]} (\phi_{G_{m,u}} - \phi_{[0,m]}).$$

Relation (9) follows from this equality. ∎

6.2. *Spaces $K_{M,y}$*

Let $K_{M,y}$ be the vector space equal to the sum of the interval $[0, y]$ and the vector space of even weight vectors which are less than or equal to $M \backslash y$. These spaces are the duals of those defined in the previous section. Precisely, $K_{M,y} = (G_{\bar{M},\bar{y}})^{\perp}$. Thus if $y \prec M$ then $\dim(K_{M,y}) = w(M) - 1$ and if $M = y$ then $\dim(K_{M,y}) = w(M)$. Moreover, if $w(y) = w(M)$ or $w(M) - 1$, then $K_{M,y} = [0, y]$. Notice that if $w(M) - w(y) = 2$, then $K_{M,y} = G_{y,M}$.

The following lemma expresses the indicator of $[0, y]$ by mean of indicators of some spaces $K_{M,y}$.

LEMMA 3. *For any pair of vectors M and $y \in V_n$ such that $y \leqslant M$,*

$$2^{w(M)-1-w(y)} \phi_{[0,y]} = (1 - 2^{w(M)-1-w(y)})\, \phi_{[0,M]} + \sum_{u \in [\,y,\, M[} \phi_{K_{M,u}}. \quad (10)$$

Proof. Let us consider the Walsh transform of each side of equality (9) applied to $\bar{y}$ and with $m = \bar{M}$.

$$2^{n-w(y)} \phi_{[0,y]} = (2 - 2^{w(M)-w(y)})\, 2^{n-w(M)} \phi_{[0,M]} + \sum_{u \in\,]\bar{M},\, \bar{y}]} 2^{n-w(M)+1} \phi_{K_{M,\bar{u}}}.$$

The result is obtained by dividing the two members of this equality by $2^{n-w(M)+1}$ and by replacing u by $\bar{u}$ in the sum. ∎

6.3. *Parameters m_y and M_y*

It remains to define which vectors m and M will be used to define the r-dimensional vector spaces $G_{m,y}$ and $K_{M,y}$.

For each vector y of weight $\geqslant r$, let $m_y \in V_n$ be the first prefix of y of weight $r-1$, completed on the right by 0's. For instance with $n=6$, if $y=101011$ then $m_y=101000$. As $w(m_y)=r-1$, then $\dim(G_{m_y,y})=r$.

For each vector y of weight $\leqslant r$, let $M_y \in V_n$ be the first suffix of y containing $r-1$ zeroes, completed on the left by 1's. For instance with $n=6$, if $y=001010$ then $M_y=111010$. As $w(M_y)=r+1$, then $\dim(K_{M_y,y})=r$.

Let m be the restriction of the mapping $y \mapsto m_y$ to the set of $(r+1)$-weight vectors. Similarly, let M be the restriction of the mapping $y \mapsto M_y$ to the set of $(r-1)$-weight vectors. As the weight of M_y equals $r+1$, the composition $M \circ m$ is well defined and map a $(r+1)$-weight vector to a $(r+1)$-weight vector.

LEMMA 4. *The composition $M \circ m$ is increasing for lexicographic order and the only fixed point is the vector $1^{r+1}0^{r-1}$.*

Proof. Let y be any $(r+1)$-weight vector. The effect of the mapping m is to replace the two last 1's by 0's. The effect of M on $m(y)$ is to replace the two first 0's by 1's. Finally, the composition exchanges the two last 1's of y with the two first 0's of m_y. This transformation always moves ones from right to left. Thus, $M \circ m(y)$ is greater than y for the lexicographic order. Moreover, $M \circ m(y)=y$ if and only if the two last 1's of y are on the positions of the two first 0's of m_y. This happens only if $y=1^{r+1}0^{r-1}$ which is the only fixed point of $M \circ m$. ∎

6.4. *Another Lemma*

LEMMA 5. *Let $\mu=1^{r+1}0^{r-1}$ be the maximal $(r+1)$-weight vector for lexicographic order. Then*

$$\sum_{y \preccurlyeq \mu} \phi_{K_{M_y,y}} = 2^r \phi_{\{0\}} + 2^r \phi_{[0,\mu]}.$$

Proof. If $y \preccurlyeq \mu$ then y ends with at least $(r-1)$ zero components, thus $M_y=\mu$. For all $y \preccurlyeq \mu$, we have $K_{[M_y,y]} \subset [0,\mu]$. Let $x \in V_n$ be any vector and let us consider three cases to achieve the proof.

(1) If $x \not\preccurlyeq \mu$ then x does not belong to any space $K_{M_y,y}$.

(2) If $x=0$ then x belongs to all the $K_{M_y,y}$ for $y \preccurlyeq \mu$. There exist 2^{r+1} such spaces.

(3) if $0 \prec x \preccurlyeq \mu$ and $y \preccurlyeq \mu$ then $x \in K_{M_y,y}$ if and only if vector $x \backslash y$ has an even number of nonzero components. There exist 2^r such spaces. ∎

7. REGULAR DECOMPOSITION

We prove in this section a decomposition theorem of the elements of $\mathscr{F}_n$ by mean of $\phi_{\{0\}}$ and r-dimensional vector space indicators, called *regular decomposition*. We also find a sufficient condition on f which guarantees that its regular decomposition has integer coefficients.

THEOREM 1. *Let $n=2r$ be an even integer greater than or equal to 4 and f be a real valued function on V_n. There exist 2^n-1 vector spaces $F_1, ..., F_{2^n-1}$ of dimension r such that the set $\{\phi_{\{0\}}, \phi_{F_1}, ..., \phi_{F_{2^n-1}}\}$ is a basis of $\mathscr{F}_n$.*

Moreover, if f is integer valued and if for each nonzero $y \in V_n$ of Hamming weight $\leqslant r$, the value of $\mathring{f}(y)$ is multiple of $2^{r-w(y)}$, and if the quantity $d=\sum_{y\succ 0} \mathring{f}(y)(2^{w(y)-r}-1)$ is a multiple of 2^r-1, then the coefficients of f in this basis are integers.

Proof. The starting point of the proof is the Möbius decomposition of $f: f=\sum_{y\in V_n} \mathring{f}(y)\,\phi_{[0,\,y]}$. The principle is to substitute, for $w(y)\neq 0, r$, the $\phi_{[0,\,y]}$'s of this decomposition with expressions given by mean of the r-dimensional vector spaces indicators previously defined. We proceed in five steps.

Step 1. The first step consists in expressing the $\phi_{[0,\,y]}$'s, for $w(y)\geqslant r+1$, by mean of the $\phi_{G_{m_y,\,y}}$'s using Lemma 2.

$$f=\sum_{w(y)\leqslant r} \mathring{f}(y)\,\phi_{[0,\,y]} + \sum_{w(y)\geqslant r+1} \mathring{f}(y)\left((2-2^{w(y)-r+1})\,\phi_{[0,\,m_y]} + \sum_{u\in\,]m_y,\,y]} \phi_{G_{m_y,\,u}}\right).$$

For all y such that $w(y)\geqslant r+1$ and all $u\in\,]m_y, y]$, we have $m_u=m_y$. This allows us to reverse the order of the summations when expanding the second term of the above expression,

$$f=\sum_{w(y)\leqslant r} \mathring{f}(y)\,\phi_{[0,\,y]} + \sum_{w(y)\geqslant r+1} \mathring{f}(y)(2-2^{w(y)-r+1})\,\phi_{[0,\,m_y]} + \sum_{u\in V_n} \sum_{\substack{w(y)\geqslant r+1 \\ u\in\,]m_y,\,y]}} \mathring{f}(y)\,\phi_{G_{m_u,\,u}}.$$

The vector m_y being of weight $r-1$, we have necessarily $\mathrm{w}(u) \geqslant r$ in the last term above. Note that if $\mathrm{w}(u) = r$, then $G_{m_u, u} = [0, u]$. We gather now the terms of this sum corresponding to vector space indicators. These spaces are $[0, y]$ for $\mathrm{w}(y) \leqslant r$ and $G_{m_y, y}$ for $\mathrm{w}(y) > r$. Let a_y be the coefficients of this decomposition,

$$f = \sum_{\mathrm{w}(y) \leqslant r} a_y \phi_{[0, y]} + \sum_{\mathrm{w}(y) > r} a_y \phi_{G_{m_y, y}}. \tag{11}$$

The result of the calculation of the a_y's is

$$a_y = \begin{cases} \mathring{f}(y) & \text{if} \quad \mathrm{w}(y) < r-1; \\ \displaystyle\sum_{u \mid m_u = y} (2 - 2^{\mathrm{w}(u)-r+1})\, \mathring{f}(u) & \text{if} \quad \mathrm{w}(y) = r-1; \\ \displaystyle\sum_{u \mid y \in\,]m_u, u]} \mathring{f}(u) & \text{if} \quad \mathrm{w}(y) \geqslant r. \end{cases} \tag{12}$$

Step 2. The second step consists in replacing the $G_{m_y, y}$ indicators in relation (11) by mean of $[0, y]$ indicators for $\mathrm{w}(y) = r+1$. For any such y, the open interval $]m_y, y[$ contains two elements, say y_1 and y_2. From Lemma 2, we have

$$\phi_{G_{m_y, y}} = 2\phi_{[0, m_y]} - \phi_{[0, y_1]} - \phi_{[0, y_2]} + \phi_{[0, y]}.$$

Using this result in relation (11) leads to an expression of f by mean of $[0, y]$ indicators for $\mathrm{w}(y) \leqslant r+1$ and of $G_{m_y, y}$ indicators for $\mathrm{w}(y) > r+1$. Let b_y be the coefficients of this decomposition.

$$f = \sum_{\mathrm{w}(y) \leqslant r+1} b_y \phi_{[0, y]} + \sum_{\mathrm{w}(y) > r+1} b_y \phi_{G_{m_y, y}}. \tag{13}$$

The computation of the coefficients b_y yields

$$b_y = \begin{cases} a_y & \text{if} \quad \mathrm{w}(y) < r-1 \quad \text{or} \quad \mathrm{w}(y) \geqslant r+1; \\ a_y + 2 \displaystyle\sum_{\substack{\mathrm{w}(u) = r+1 \\ y \in [m_u, u]}} a_u & \text{if} \quad \mathrm{w}(y) = r-1; \\ a_y - \displaystyle\sum_{\substack{\mathrm{w}(u) = r+1 \\ y \in [m_u, u]}} a_u & \text{if} \quad \mathrm{w}(y) = r. \end{cases} \tag{14}$$

Step 3. In the third step, by using Lemma 3, we express, for $0 < w(y) < r$, the $[0, y]$ indicators in relation (13) by mean of $K_{M_y, y}$ indicators. We obtain, M_y being of weight $r+1$,

$$f = b_0 \phi_{\{0\}} + \sum_{0 < w(y) < r} \frac{b_y}{2^{r-w(y)}} \left((1 - 2^{r-w(y)}) \, \phi_{[0, M_y]} + \sum_{u \in [y, M_y[} \phi_{K_{M_y, u}} \right)$$

$$+ \sum_{w(y) = r, r+1} b_y \phi_{[0, y]} + \sum_{w(y) > r+1} b_y \phi_{G_{m_y, y}}.$$

For all y such that $w(y) \leqslant r-1$ and all $u \in [y, M_y[$, we have $M_u = M_y$. This allows us to reverse the summations when expanding the above relation,

$$f = b_0 \phi_{\{0\}} + \sum_{0 < w(y) < r} \frac{b_y}{2^{r-w(y)}} (1 - 2^{r-w(y)}) \, \phi_{[0, M_y]}$$

$$+ \sum_{u \in V_n} \sum_{\substack{0 < w(y) < r \\ u \in [y, M_y[}} \frac{b_y}{2^{r-w(y)}} \phi_{K_{M_u, u}}$$

$$+ \sum_{w(y) = r, r+1} b_y \phi_{[0, y]} + \sum_{w(y) > r+1} b_y \phi_{G_{m_y, y}}.$$

We gather now the terms corresponding to the vector space indicators. We get a decomposition of f by mean of $\phi_{\{0\}}$ and of r or $(r+1)$-dimensional vector space indicators. Let c_y be the coefficients of this decomposition,

$$f = c_0 \phi_{\{0\}} + \sum_{0 < w(y) < r} c_y \phi_{K_{M_y, y}} + \sum_{w(y) = r, r+1} c_y \phi_{[0, y]} + \sum_{w(y) > r+1} c_y \phi_{G_{m_y, y}}. \tag{15}$$

The computation of the coefficients c_y yields

$$c_y = \begin{cases} \displaystyle\sum_{\substack{u \neq 0 \\ y \in [u, M_u[}} \frac{b_y}{2^{r-w(u)}} & \text{if} \quad 0 < w(y) \leqslant r \\ \displaystyle\sum_{\substack{u \neq 0 \\ y \in [u, M_u]}} (2^{w(u)-r} - 1) \, b_y & \text{if} \quad w(y) = r, r+1 \\ b_y & \text{if} \quad y = 0 \quad \text{or} \quad w(y) > r+1. \end{cases} \tag{16}$$

Step 4. We minimize now the number of $(r+1)$-dimensional vector space indicators in the expression (15). Let y be a $(r+1)$ weight vector and

let y_1 and y_2 be the two elements of the open interval $]m_y, y[$. Their weight equals r and from Lemma 2, we have

$$\phi_{[0,\,y]} = -2\phi_{[0,\,m_y]} + \phi_{[0,\,y_1]} + \phi_{[0,\,y_2]} + \phi_{G_{m_y,\,y}}.$$

Let now z_1 and z_2 be the two elements of the open interval $]m_y, M_{m_y}[$. Their weight equals r and from Lemma 3, we have

$$2\phi_{[0,\,m_y]} = -\phi_{[0,\,M_{m_y}]} + \phi_{[0,\,z_1]} + \phi_{[0,\,z_2]} + \phi_{K_{M_{m_y},\,m_y}}.$$

Thus, we can express $\phi_{[0,\,y]}$ by mean of $\phi_{[0,\,M_{my}]}$ plus a linear combination of r-dimensional interval indicators:

$$\phi_{[0,\,y]} = \phi_{[0,\,M_{my}]} + \phi_{[0,\,y_1]} + \phi_{[0,\,y_2]} - \phi_{[0,\,z_1]} - \phi_{[0,\,z_2]} + \phi_{G_{m_y,\,y}} - \phi_{K_{M_{m_y},\,m_y}}. \tag{17}$$

We sweep now the y's of weight $r+1$ in the lexicographic order an apply this relation to substitute $\phi_{[0,\,y]}$. From Lemma 5, on each step of this process, the number of $(r+1)$-dimensional vector space indicators invoqued decrease by one until y reach the maximal $(r+1)$-weight vector for lexicographic order. We denote $\mu = 1^{r+1}0^{r-1}$ this element. We have now obtained an expression of f by mean of indicators of $\{0\}$, of $K_{M_y,\,y}$ for $0 < \mathrm{w}(y) < r$, of $[0, y]$ for $\mathrm{w}(y) = r$, of $G_{m_y,\,y}$ for $\mathrm{w}(y) > r$, $y \neq \mu$ and of $[0, \mu]$. These spaces are all r-dimensional except the latter which is $(r+1)$-dimensional. Let d_y denote the coefficients of this decomposition of f,

$$f = d_0\phi_{\{0\}} + \sum_{0 < \mathrm{w}(y) < r} d_y\phi_{K_{M_y},\,y} + \sum_{\mathrm{w}(y) = r} d_y\phi_{[0,\,y]} + \sum_{\substack{y \neq \mu \\ \mathrm{w}(y) > r}} d_y\phi_{G_{m_y,\,y}} + d_\mu\phi_{[0,\,\mu]}. \tag{18}$$

Let us now compute the coefficient d_μ. From relation (17), we have

$$d_\mu = \sum_{\mathrm{w}(y) = r+1} c_y.$$

From relation (16), we have

$$d_\mu = \sum_{0 < \mathrm{w}(y) \leqslant r+1} b_y(2^{\mathrm{w}(y)-r} - 1).$$

Notice that the terms of this sum such that $w(y) = r$ are null and those for which $w(y) = r+1$ are simply equal to b_y. From relation (14), we deduce

$$d_\mu = \sum_{0 < w(y) < r-1} a_y (2^{w(y)-r} - 1) + \tfrac{1}{2} \sum_{w(y) = r-1} a_y.$$

Applying the same principle and using relation (12), we finally yield

$$d_\mu = \sum_{y \neq 0} \mathring{f}(y)(2^{w(y)-r} - 1).$$

Step 5. In the last step of this proof, we use Lemma 5 to substitute the only remaining $(r+1)$-dimensional vector space indicator in the expression (18). From Lemma 5 and $K_{M_\mu, \mu} = [0, \mu]$, we get

$$\phi_{[0,\mu]} = \frac{2^r}{2^r - 1} \phi_{\{0\}} + \sum_{y \prec \mu} \frac{1}{2^r - 1} \phi_{K_{M_y, y}}.$$

Substituting this expression of $\phi_{[0,\mu]}$ in relation (18) and gathering terms lead to a decomposition of f by means of $\phi_{\{0\}}$ and of r-dimensional vector space indicators only,

$$f = e_0 \phi_{\{0\}} + \sum_{0 < w(y) < r} e_y \phi_{K_{M_y}, y} + \sum_{w(y) = r} e_y \phi_{[0, y]} + \sum_{\substack{y \neq \mu \\ w(y) > r}} e_y \phi_{G_{m_y}, y} + e_\mu \phi_{K_{M_\mu}, 0}.$$

The spaces F_i's of the statement of Theorem 1 are the spaces which appear in the above relation. The values of the e_y's are given by.

$$e_y = \begin{cases} d_0 - \dfrac{2^r}{2^r - 1} d_\mu & \text{if} \quad y = 0 \\ d_y + \dfrac{1}{2^r - 1} d_\mu & \text{if} \quad 0 \prec y \prec \mu \\ d_y & \text{if} \quad y \not\preccurlyeq \mu \\ \dfrac{1}{2^r - 1} d_\mu & \text{if} \quad y = \mu \end{cases} \tag{19}$$

This proves the first part of Theorem 1. It leads to explicit formulas or an algorithm for computing the coefficients of this decomposition (see [11]). During this computation, divisions are performed only on Step 3 and Step 5. If f is integer valued, then $\mathring{f}$ is also integer valued. If for $w(y) \leqslant r$ the value of $\mathring{f}(y)$ is a multiple of $2^{r-w(y)}$, then from relations (16),

the values of the c_y's obtained on Step 3 are integers. Moreover, if d_μ is a multiple of 2^r-1, then from relations (19), the values of the e_y's obtained on Step 5 are all integers. This achieves the proof. ▮

8. CHARACTERIZATION OF $\mathcal{EGPS}$

The regular decomposition theorem provides a very simple characterization of the elements of $\mathcal{EGPS}$.

THEOREM 2. *Let $n=2$ be an even integer $\geqslant 4$ and f be a partial bent function on V_n. Then*

$$f \in \mathcal{EGPS} \Leftrightarrow f(0) = \tilde{f}(0).$$

Proof. The fact that $f \in \mathcal{EGPS}$ implies $f(0)=\tilde{f}(0)$ has already been seen in Section 4. Conversely, let f be any partial bent function such that $f(0)=\tilde{f}(0)$. We show that f satisfies the hypothesis of the second part of theorem 7.1 and the result holds. From relation (6), the Möbius coefficients being integers, for all nonzero vector y of weight $\leqslant r$, the value of $\mathring{f}(y)$ is multiple of $2^{r-\mathrm{w}(y)}$. Moreover, we have now to prove that $d=\sum_{y\succ 0} 2^{\mathrm{w}(y)-r}\mathring{f}(y)-\sum_{y\succ 0}\mathring{f}(y)$ is multiple of 2^r-1. From relations (6) and (7), $d=\sum_{y\neq 0,1}\mathring{\tilde{f}}(y)+2^r\mathring{f}(1)-\sum_{y\succ 0}\mathring{f}(y)$. By Möbius inversion formula, $d=\tilde{f}(0)-\mathring{\tilde{f}}(0)-\mathring{\tilde{f}}(1)+2^r\mathring{f}(1)-f(0)+\mathring{f}(0)$. From relations (7) and (8) and the hypothesis $f(0)=\tilde{f}(0)$, we finally have $d=(2^r-1)\tilde{f}(1)$. ▮

Of course, Theorem 2 is also applicable to bent functions. In this case, it states that for any bent function f we have $f \in \mathcal{GPS} \Leftrightarrow f(0)=\tilde{f}(0)$.

Remark. If we perform the proof of theorem 1 until Step 4 only, we get the existence of a set of r-dimensional vector space indicators, plus one $(r+1)$-vector space indicator in which which any bent function is decomposable with integer coefficients. We retrieve the result proved in [7] and in addition, we get an explicit basis and formulas to compute the coefficients.

We are now able to state and prove the main result of this paper.

COROLLARY 1. *Up to a translation, any bent function is equivalent to an element of $\mathcal{GPS}$.*

Proof. Let f be any bent function. If $f(0)\neq\tilde{f}(0)$, let a be any vector such that $f(0)\neq f(a)$. As seen as above, the function $f_a: x\mapsto f(x+a)$ satisfies $f_a(0)=\tilde{f}_a(0)$ and thus belongs to $\mathcal{GPS}$ according to Theorem 2. ▮

Let us recall that by definition, the elements of $\mathscr{EGPS}$ are Boolean functions which can be expressed as a linear combination, with integer coefficients, of $\phi_{\{0\}}$ and r-dimensional vector space indicators. For a given element of $\mathscr{GPS}$ such an expression is not unique and there may exist several families of suitable vector spaces. But thanks to Theorems 1 and 2, we have shown that there exists a basis $\mathscr{B}_0$ composed of $\phi_{\{0\}}$ plus r-dimensional vector space indicators such that any element of $\mathscr{EGPS}$ can be expressed in this basis with integer coefficients.

This basis is not unique. One can check that any basis $\mathscr{B}$ of $\mathscr{F}_n$ of the same kind, such that the conversion matrix from $\mathscr{B}_0$ to $\mathscr{B}$ is **Z**-invertible (i.e., its determinant equals ± 1) shares the property that the decomposition of any element of $\mathscr{EGPS}$ has integer coefficients.

9. LINEAR ALGEBRA APPROACH

9.1. *$\mathscr{EGPS}$ as Solutions of a Quadratic Diophantine Equation*

Let $\mathscr{F} = \{F_1, ..., F_{2^n-1}\}$ be the set of r dimensional vector spaces defined in Theorem 1. Let f be any real valued function defined on $V_n \backslash \{0\}$ by

$$f = \sum_{i=1}^{2^n-1} e_i \phi_{F_i}, \tag{20}$$

where the e_i's are integers. If f is Boolean on $V_n \backslash \{0\}$ then we can choose $f(0) \in \{0, 1\}$ such that f is of even weight. In this case $f \in \mathscr{EGPS}$ by definition. Conversely, from Theorem 1, any element of $\mathscr{EGPS}$ can be obtained in this way. Thus, $\mathscr{EGPS}$ can be identified with the set of the $2^n - 1$ dimensional integer vectors $e = (e_i)_{i \in \{1, ..., 2^n-1\}}$ which satisfy $\sum_{i=1}^{2^n-1} e_i \phi_{F_i}$ Boolean on $V_n \backslash \{0\}$.

The vector e being with integer components, the function defined by relation (20) is integer valued and thus is Boolean on $V_n \backslash \{0\}$ if and only if it satisfies $\sum_{x \neq 0} f(x) = \sum_{x \neq 0} f^2(x)$. This is equivalent to

$$\begin{gathered} \sum_{x \neq 0} \sum_{i=1}^{2^n-1} e_i \phi_{F_i}(x) = \sum_{x \neq 0} \sum_{i,\, j=1}^{2^n-1} e_i e_j \phi_{F_i} \phi_{F_j} \\ (2^n - 1) \sum_{i=1}^{2^n-1} e_i = \sum_{i,\, j=1}^{2^n-1} e_i e_j (2^{\dim(F_i \cap F_j)} - 1). \end{gathered} \tag{21}$$

This means that the vector $e = (e_i)_{i \in \{1, ..., 2^n-1\}}$ defines an element of $\mathscr{EGPS}$ if and only if it is solution of the quadratic Diophantine equation given by relation (21).

The matrix $Q=(2^{\dim(F_i\cap F_j)}-1)_{i,\,j\in\{1,\ldots,2^n-1\}}$ defines a definite positive quadratic form. Thus, Eq. (21) is the equation of an ellipsoid $\mathscr{E}$.

The function f of relation (20) is defined on $V_n\backslash\{0\}$. It can be defined on V_n by adding a term $m\phi_{\{0\}}$ which is deduced from the e_i's by $m+\sum_{i=1}^{2^n-1} e_i\in\{0,1\}$ and m even. Particular families of $\mathscr{EGPS}$ such as $\mathscr{GPS}$ $(m=-2^{r-1})$ and r-dimensional vector space indicators $(m=0)$, correspond to integer vectors which belong to the intersection of $\mathscr{E}$ and the hyperplane of equation

$$\sum_{i=1}^{2^n-1} e_i = f(0)-m. \tag{22}$$

This intersection is a (2^n-2)-dimensional ellipsoid. In consequence, counting the elements of $\mathscr{GPS}$ is equivalent to counting the integer vectors which belong to the ellipsoid defined by Eqs. (21) and (22) with $m=-2^{r-1}$.

9.2. *The Dual Transform is Linear*

A surprising consequence of this approach is the fact that the dual transform $f\mapsto\tilde{f}$ defined on $\mathscr{EGPS}$ is the restriction of a linear mapping on the real vector space $\mathbf{R}^{2^n-1}$.

Indeed, if $f=\sum_{i=1}^{2^n-1} e_i\phi_{F_i}$ defines the restriction to $V_n\backslash\{0\}$ of an element of $\mathscr{EGPS}$, its dual $\tilde{f}$ is defined on $V_n\backslash\{0\}$ by $f=\sum_{i=1}^{2^n-1} e_i\phi_{F_i^\perp}$. For any $i\in\{1,\ldots,2^n-1\}$, the dual of F_i, is a r-dimensionnal vector space. Thus, the indicator of $F_i^\perp$ can be expressed by mean of the F_i's with integer coefficients,

$$\phi_{F_i\perp}=\sum_{j=1}^{2^n-1} d_{ji}\phi_{F_j}.$$

The restriction of $\tilde{f}$ to $V_n\backslash\{0\}$ of $\tilde{f}$ can be written as

$$\tilde{f}=\sum_{i=1}^{2^n-1}\sum_{j=1}^{2^n-1} d_{ji}e_i\phi_{F_j}$$

Thus, the dual transform $f\mapsto\tilde{f}$ is the restriction to vectors that define element of $\mathscr{EGPS}$ of the linear mapping represented by the matrix $D=(d_{ji})_{i,\,j\in\{1,\ldots,2^n-1\}}$.

The same kind of proof can be applied to transformations $f\mapsto f\circ A$ where A is any invertible linear mapping on V_n. Indeed, the image by A of a r-dimensional vector space is also a r-dimensional vector space.

10. CONCLUSION

We have shown that any bent function either belongs to $\mathcal{GPS}$ or can be deduced from an element of $\mathcal{GPS}$ by the composition with a translation. This establishes the important role played by r-dimensional vector spaces in the study of bent functions. In particular, this approach seems to be suitable to prove or disprove the conjecture stated by H. Dobbertin in [9]: Is any bent function *normal*, i.e., constant on a r-dimensional vector space?

Moreover, the problem of counting the elements of $\mathcal{GPS}$ and thus the number of bent functions is shown to be equivalent to the geometric problem of counting the number of integer vectors of an ellipoid. This is also equivalent to count the number of representations of an integer by the sum of a linear form and a quadratic form. This allows us to use a number theoretic approach in order to solve this problem (see [1]). It is also possible to use an algorithmic approach (see [10]) to enumerate all the elements of $\mathcal{GPS}$. In this case, the symmetry properties of the problem must be used to lower the search complexity.

REFERENCES

1. A. N. Andrianov, "Quadratic Forms and Hecke Operator," Springer-Verlag, Berlin, 1987.
2. P. J. Cameron and J. H. VanLint, "Design, Graphs, Codes and Their Link," Cambridge Univ. Press, Cambridge, UK, 1991.
3. C. Carlet, Two new classes of bent functions, *in* "Proc. EUROCRYPT '93," Lecture Notes in Computer Science, Vol. 765, pp. 386–397, Springer-Verlag, New York/Berlin, 1994.
4. C. Carlet, Generalized partial spread, *IEEE Trans. Inform. Theory* **41** (1995), 1482–1487.
5. C. Carlet and Ph. Guillot, A characterization of binary bent functions, *J. Combin. Theory Ser. A* **76** (1996), 328–335.
6. C. Carlet, Recent results on bent functions, *in* "Proceedings, ICC'97, Portland, 1997," in press.
7. C. Carlet and Ph. Guillot, An alternate characterization of the bentness of binary functions, with uniqueness, *Des. Codes Cryptogr.* **14** (1998), 133–140.
8. J. F. Dillon, "Elementary Hadamard Difference Sets," Ph.D. dissertation, University of Maryland, 1974.
9. H. Dobbertin, Construction of bent functions and balanced boolean functions with high nonlinearity, *in* "Proc. Fast Software Encryption," pp. 61–74, Springer-Verlag, New York/Berlin, 1994.
10. U. Fincke and M. Pohst, Improved methods for calculating vectors of short length in a lattice, including a complexity analysis, *Math. Comp.* **44** (1985), 463–471.
11. P. Guillot, "Fonctions courbes binaires et transformation de Möbius," Thesis, Université de Caen-Basse Normandie, 1999.
12. Ma, A survey of partial difference sets, *Des. Codes Cryptogr.* **4** (1994), 221–261.
13. O. S. Rothaus, On bent functions, *J. Combin. Theory Ser. A* **20** (1976), 300–305.
14. J. H. VanLint, "Coding Theory," Springer-Verlag, New York/Berlin, 1988.