JOURNAL OF COMBINATORIAL THEORY, Series A **76**, 328–335 (1996)
ARTICLE NO. 0110

NOTE

A Characterization of Binary Bent Functions

Claude Carlet

INRIA Project CODES, Domaine de Voluceau, BP 105, 78153 Le Chesnay Cedex, France; and GREYC, Université de Caen, France

and

Philippe Guillot

Communicated by V. Pless

Received April 20, 1995

A recent paper by Carlet introduces a general class of binary bent functions on $(GF(2))^n$ (n even) whose elements are expressed by means of characteristic functions (indicators) of $(n/2)$-dimensional vector-subspaces of $(GF(2))^n$. An extended version of this class is introduced in the same paper; it is conjectured that this version is equal to the whole class of bent functions. In the present paper, we prove that this conjecture is true. © 1996 Academic Press, Inc.

1. INTRODUCTION

Let $n = 2p$ be a positive even integer. Let V_n be the set of all binary words of length n. V_n is a n-dimensional vector-space over the field $GF(2)$. In this paper, we are interested in bent functions over V_n. These functions refer to both algebraic and combinatorial problems. They can be defined as the functions that reach the maximum Hamming distance to the set of affine functions defined on V_n.

Some algebraic properties of bent functions are well known. For instance, the degree of such a function cannot exceed p (see [9]). Another definition of bent functions is based on combinatorial properties of their support: a function is bent if and only if its support is a Hadamard *difference set*, i.e., a set E with the property that for any nonzero element a in V_n, the equation $x - y = a$ (that is, $x + y = a$, since the characteristic

0097-3165/96 $18.00

of the field is 2) with unknown x and y ranging in E has always the same number $|E|-2^{n-2}$ of solutions (see [3, 4]).

In this paper, we give a proof of a conjecture stated in [2] which leads to a characterization in terms of linear combinations modulo 2^p of characteristic functions of p-dimensional vector-subspaces of V_n. This refers to both combinatorial and algebraic properties of V_n.

In next sections we introduce the necessary background on *Möbius function* over V_n that will be needed for the proofs and which is not classical in this context.

2. PRELIMINARIES

We will denote by **0** and **1** the vectors (0, ..., 0) and (1, ..., 1). There exists on the vector-space V_n a natural dot product, denoted by "$\cdot$" and defined by

$$\forall u=(u_1, ..., u_n),\ \forall v=(v_1, ..., v_n), \quad u\cdot v=u_1v_1+\cdots+u_nv_n,$$

the addition being computed in GF(2).

For any vector-subspace E of V_n, we shall denote by ϕ_E the characteristic function (i.e., the indicator) of E in V_n, and by $E^\perp$ the orthogonal of E: $E^\perp=\{y\in V_n \mid \forall x\in E, x\cdot y=0\}$.

V_n is a lattice. The partial order relation is the direct product n times of the order relation defined over $\{0, 1\}$ by $1\geqslant 0$:

$$u=(u_1, ..., u_n)\geqslant v=(v_1, ..., v_n)\Leftrightarrow \forall i\in\{1, ..., n\}, u_i\geqslant v_i.$$

A Möbius function (cf. [8, 10]) relative to this lattice structure can be defined as follows:

For any elements u and v of V_n, let $\mu^+(u, v)$ denote the number of paths of even length from u to v in this lattice and $\mu^-(u, v)$ the number of odd length paths (recall that a k-length path from u to v is a sequence $u_0, u_1, ..., u_k$ such that $u_0=u$, $u_k=v$ and for any i, $u_i>u_{i+1}$).

The Möbius function μ is equal to

$$\mu(u, v)=\mu^+(u, v)-\mu^-(u, v), \qquad u, v\in V_n.$$

This definition is a general one. In the particular framework which is ours, we have

$$\mu(u, v)=(-1)^{w(u+v)} \qquad \text{if} \quad u\geqslant v \quad \text{and} \quad 0 \text{ otherwise},$$

where $w(u+v)$ denotes the Hamming weight of the word $u+v$.

It is well known that μ satisfies the following orthogonality relation:

$$\sum_{u \geqslant t \geqslant v} \mu(t, v) = \begin{cases} 1, & \text{if} \quad u = v \\ 0, & \text{otherwise.} \end{cases}$$

This relation leads to an inversion formula: for any function g from V_n to $\mathbf{Z}$, let g° be the function expressed on V_n as

$$g^\circ(u) = \sum_{x \in V_n} \mu(x, u)\, g(x); \tag{1}$$

then g can be recovered from g° by the relation

$$g(x) = \sum_{u \geqslant x} g^\circ(u). \tag{2}$$

This means that function g can be expressed as a sum in $\mathbf{Z}$ of characteristic functions of subspaces of V_n. Indeed, according to equality (2), we have

$$g(x) = \sum_{u \in V_n} g^\circ(u)\, \phi_{F_u}(x), \tag{3}$$

where F_u denotes the subspace of V_n that is equal to the set $\{x \in V_n \mid x \leqslant u\}$. Moreover, this decomposition is unique according to relation (1) (that gives its coefficients).

Note that the dimension of F_u is $w(u)$. The function g° is the so-called *Möbius transform of* g.

Note. In this paper, operations take place in the ring of integers. It is also possible to operate in the field $GF(2)$. In this context, relation (3) means that functions ϕ_{F_u}, $u \in V_n$, form a basis of the vector-space of all boolean functions over V_n. The Möbius transform of g gives the decomposition of g in this basis.

Note that the restriction of this basis to those elements whose Hamming weight is greater or equal to an integer r leads to the so-called *Jennings basis* of the Reed–Muller code of order $n - r$, relative to the canonical basis of V_n (see [1]). Note, also, that modulo 2, the Möbius transform relative to the *dual* order relation $\leqslant$ leads to the *algebraic normal form* of function g.

3. A NEW CHARACTERIZATION OF BENT FUNCTIONS

We are now able to prove the conjecture on bent functions stated in [2]. Let us first recall what is this conjecture.

A Boolean function f on V_n is *bent* if its distance to the Reed–Muller code of order 1 is maximum. Translated in terms of Walsh transform, this condition is equivalent to the fact that the values of the Walsh transform of the real-valued function $f_\chi = (-1)^f$ are all equal to $\pm 2^p$. So, a function f is called bent if, for any element s of V_n, we have (cf. [3, 6, 9]):

$$\widehat{f_\chi}(s) = \sum_{x \in V_n} (-1)^{f(x) + s \cdot x} = \pm 2^p.$$

If f is a bent function, then there exists a Boolean function, that we shall denote by $\tilde{f}$, such that, for any s in V_n:

$$\widehat{f_\chi}(s) = 2^p (-1)^{\tilde{f}(s)},$$

or equivalently,

$$= 2^p \tilde{f}_\chi.$$

This function $\tilde{f}$ is bent too. We will call it the *dual* of f (Dillon calls it the "Fourier" transform of f in [3]). Its dual is f itself (cf. [3, 9]).

In next theorem, δ_0 denotes the Dirac symbol on V_n ($\delta_0(x)$ equals 1 if $x = \mathbf{0}$, and 0 otherwise).

Note that δ_0 is also equal to the function $\phi_{\{\mathbf{0}\}} = \phi_{F_0}$.

We shall also use the following well-known property: let E be any d-dimensional vector-subspace of V_n. Then the characteristic function ϕ_E of E in V_n, satisfies the following relation:

$$\widehat{\phi_E} = 2^d \phi_{E^\perp}. \tag{4}$$

What is conjectured in [2] is stated in the following theorem, whose proof is the purpose of the present paper.

THEOREM 1. *Let f be a Boolean function on V_n. Then f is bent if and only if there exist p-dimensional subspaces $E_1, ..., E_k$ of V_n and integers $m_1, ..., m_k$ (positive or negative) such that for any element x of V_n:*

$$\sum_{i=1}^{k} m_i \phi_{E_i}(x) = 2^{p-1} \delta_0(x) + f(x) \qquad [\text{mod } 2^p]. \tag{5}$$

The fact that condition (5) implies that f is bent has been already proved in [2]. To prove that any bent function f satisfies condition (5), we need a few lemmas.

LEMMA 1. *If f is a bent function and f° is its Möbius transform, then for every non-zero word u of weight smaller than p, $f^\circ(u)$ is divisible by $2^{p-w(u)}$.*

Proof. Let g be the dual of f and g° the Möbius transform of g. According to equalities (3) and (4), we have

$$\hat{g}(x)=\sum_{u\in V_n} g^{\circ}(u)\,2^{w(u)}\phi_{(F_u)^{\perp}}(x).$$

It is a simple matter to check that $(F_u)^{\perp}$ is equal to $F_{\bar{u}}$ (where $\bar{u}=\mathbf{1}+u$ is the componentwise complement of vector u). We deduce

$$\hat{g}(x)=\sum_{u\in V_n} g^{\circ}(u)\,2^{w(u)}\phi_{F_{\bar{u}}}(x)=\sum_{u\in V_n} g^{\circ}(\bar{u})\,2^{n-w(u)}\phi_{F_u}(x). \tag{6}$$

Since f is the dual of g, we have $\widehat{g_\chi}=2^p f_\chi$. Equality $g_\chi=1-2g$ implies $\widehat{g_\chi}=\hat{1}-2\hat{g}=2^n\delta_0-2\hat{g}$, and since $f_\chi=1-2f$, we deduce

$$2^p(1-2f)=2^n\,\delta_0-2\hat{g}.$$

Therefore, we have for all x in V_n:

$$f(x)=2^{-p}\hat{g}(x)-2^{p-1}\delta_0(x)+\tfrac{1}{2}. \tag{7}$$

So, from relations (6) and (7), we obtain

$$\begin{aligned} f(x)&=\sum_{u\in V_n} g^{\circ}(\bar{u})\,2^{p-w(u)}\phi_{F_u}(x)-2^{p-1}\,\delta_0(x)+\tfrac{1}{2}\\ &=\sum_{u\in V_n} g^{\circ}(\bar{u})\,2^{p-w(u)}\phi_{F_u}(x)-2^{p-1}\phi_{F_\mathbf{0}}(x)+\tfrac{1}{2}\phi_{F_\mathbf{1}}(x). \end{aligned}$$

This last equality expresses f as a linear combination of characteristic functions of spaces F_u. So, according to the unicity of the function f°, we deduce that for any nonzero word u of weight smaller than p, $f^{\circ}(u)$ is divisible by $2^{p-w(u)}$. If the word u has weight greater than p, then we know only that $f^{\circ}(u)$ is an integer. ∎

LEMMA 2. *Let F be any d-dimensional subspace of V_n, $d>p$. There exist p-dimensional subspaces $E_1, ..., E_k$ of V_n and integers $m_1, ..., m_k$ such that for any element x of V_n:*

$$\phi_F(x)=\sum_{i=1}^{k} m_i\phi_{E_i}(x) \qquad [\text{mod } 2^p].$$

Proof. We prove by induction on j that for all integer j in $\{1 \cdots d-p\}$, there exist $(d-j)$-dimensional subspaces $E_1, ..., E_k$ of V_n and integers $m_1, ..., m_k$ such that $\phi_F=\sum_{i=1}^{k} m_i\phi_{E_i}$ [mod 2^p]. The proof of the lemma is obtained by applying this property with $j=d-p$.

We first prove initial step of the induction ($j=1$). Let $\mathscr{H}$ be the set of all linear hyperplanes of F. Then, for all x, $\sum_{H \in \mathscr{H}} \phi_H(x)$ is equal to $2^d - 1$ if $x=0$; to $2^{d-1}-1$ if $x \in F - \{0\}$; and to 0 otherwise. Indeed, we may without loss of generality assume that F is equal to V_d. The indicators in V_d of the linear hyperplanes of V_d are functions of the form $x \to a \cdot x + 1$, where "$\cdot$" is the usual dot product in V_d and where a ranges over $V_d - \{0\}$. The zero vector belongs to any of these $2^d - 1$ hyperplanes and any nonzero vector u of V_d belongs to those hyperplanes whose indicators are the functions $x \to a \cdot x + 1$, where $a \cdot u = 0$ and $a \neq 0$, whose number is $2^{d-1} - 1$.

So, we have the following equality for all x in V_n:

$$\sum_{H \in \mathscr{H}} \phi_H(x) = 2^{d-1}\delta_0(x) + (2^{d-1}-1)\,\phi_F(x). \tag{8}$$

Thus, modulo 2^p,

$$\sum_{H \in \mathscr{H}} \phi_H(x) = -\phi_F(x) \qquad [\text{mod } 2^p],$$

since $d > p$. Since elements of $\mathscr{H}$ all have dimension $d-1$, this proves the initial step of the induction.

To prove the inductive step, suppose we have, modulo 2^p, a decomposition of ϕ_F into a linear combination (with integral coefficients) of characteristic functions of $(d-j)$-dimensional subspaces ($j < d-p$), then apply the result of initial step to all terms of this combination to obtain the result at rank $j+1$. ∎

Lemma 3. *Let F be any d-dimensional subspace of V_n, $d < p$. There exist p-dimensional subspaces $E_1, ..., E_k$ of V_n and integers $m, m_1, ..., m_k$ such that for any element x of V_n,*

$$2^{p-d}\phi_F(x) = m + \sum_{i=1}^{k} m_i \phi_{E_i}(x) \qquad [\text{mod } 2^p].$$

Proof. The result is obtained by applying for $j = p-d$ the following property: for all integer j in $\{1 \cdots p-d\}$, there exist $(d+j)$-dimensional subspaces $E_1, ..., E_k$ of V_n and integers $m, m_1, ..., m_k$ such that $2^j \phi_F = m + \sum_{i=1}^k m_i \phi_{E_i}$ [mod 2^p]. We prove this property by induction on j.

Let $\mathscr{H}$ be the set of all linear hyperplanes of $F^\perp$. Equality (8) becomes

$$\sum_{H \in \mathscr{H}} \phi_H(x) = 2^{n-d-1}\,\delta_0(x) + (2^{n-d-1}-1)\,\phi_{F^\perp}(x).$$

Taking the Walsh transform of both terms of this equality and using property (4), we deduce

$$2^{n-d-1} \sum_{H \in \mathscr{H}} \phi_{H^{\perp}}(x) = 2^{n-d-1} + (2^{2n-2d-1} - 2^{n-d})\, \phi_F(x)$$

and, therefore,

$$\sum_{H \in \mathscr{H}} \phi_{H^{\perp}}(x) = 1 + (2^{n-d} - 2)\, \phi_F(x).$$

We deduce

$$2\phi_F(x) = 1 - \sum_{H \in \mathscr{H}} \phi_{H^{\perp}}(x) \qquad [\text{mod } 2^p].$$

As, for any element H of $\mathscr{H}$, $H^{\perp}$ has dimension $d+1$, this proves the initial step of the induction.

Suppose now that we have, modulo 2^p, a decomposition of $2^j \phi_F$ ($j < p - d$) into a linear combination (with integral coefficients) of characteristic functions of $(d+j)$-dimensional subspaces of V_n, *plus* an integral constant. Multiplying this equality by 2 and applying the result of initial step to all nonconstant terms of this decomposition (that is possible since $j < p - d$) gives the result at rank $j+1$. This completes the proof. ∎

Proof of Theorem 1. Consider the decomposition of f given by relation (3) applied to f:

$$f(x) = \sum_{u \in V_n} f^{\circ}(u)\, \phi_{F_u}(x).$$

According to lemma 1, the terms of this sum where $0 < w(u) < p$ have coefficients all divisible by $2^{p - w(u)}$. So, we can apply Lemma 3 to all these terms. We deduce

$$f(x) = f^{\circ}(\mathbf{0})\, \delta_0(x) + m + \sum_{i=1}^{k} m_i \phi_{E_i}(x) + \sum_{w(u) \geqslant p} f^{\circ}(u)\, \phi_{F_u}(x) \quad [\text{mod } 2^p].$$

Constant m is equal to $m\phi_{F_1}$. We apply now Lemma 2 to those terms of the sum where $w(u) > p$ (including $m\phi_{F_1}$). We deduce

$$f(x) = f^{\circ}(\mathbf{0})\, \delta_0(x) + \sum_{i=1}^{k'} m'_i \phi_{E_i}(x) \qquad [\text{mod } 2^p].$$

The last thing that we must check is that the coefficient of δ_0 is congruent to 2^{p-1} modulo 2^p. Note that

$$f^\circ(\mathbf{0}) = \sum_{x \geqslant \mathbf{0}} f(x)(-1)^{w(x)} = \hat{f}(\mathbf{1}),$$

since, modulo 2, $w(x) = \mathbf{1} \cdot x$. $\hat{f}(\mathbf{1})$ is equal to $\hat{\frac{1}{2}}(\mathbf{1}) - \frac{1}{2}\widehat{f_\chi}(\mathbf{1}) = 2^{n-1}\,\delta_0(\mathbf{1}) - \frac{1}{2}\widehat{f_\chi}(\mathbf{1}) = \pm 2^{p-1}$ (f being bent). This completes the proof. ∎

Note. According to the proof of the theorem, we have also a converse of Lemma 1: let f be a Boolean function and f° its Möbius transform. If $f^\circ(\mathbf{0}) = 2^{p-1}$ [mod 2^p] and if, for every nonzero word u of weight smaller than p, $f^\circ(u)$ is divisible by $2^{p-w(u)}$, then f is bent.

CONCLUSION

We have proved that the extended version of generalized partial spreads class $\mathcal{GPS}$ (cf. [2]) is equal to the whole set of binary bent functions (in even dimensions).

The question is now: Does this new way to look at bent functions lead to a classification?

In any case, it would be interesting to characterize the elements of class $\mathcal{GPS}$ itself.

REFERENCES

1. E. F. Assmus and J. D. Key, "Codes and Finite Geometries," Rapport de Recherche INRIA n° 2027 (1993); also *in* "Handbook of Coding Theory" (Brualdy, Huffman, and Pless, Eds.), Elsevier, Amsterdam, to appear.
2. C. Carlet, Generalized partial spreads, *IEEE Trans. Inform. Theory* **41** (1995), 1482–1487.
3. J. F. Dillon, "Elementary Hadamard Difference Sets," Ph.D. thesis, University of Maryland, 1974.
4. J. F. Dillon, Elementary Hadamard difference sets, *in* "Proceedings, Sixth S-E. Conf. Combin. Graph Theory and Comp." (F. Hoffman *et al.*, Eds.), pp. 237–249, Utilitas Math., Winnipeg, 1975.
5. J. P. S. Kung, "Source Book in Matroïd Theory," Birkhäuser, Basel, 1986.
6. F. J. MacWilliams and N. J. Sloane, "The Theory of Error-Correcting Codes," North Holland, Amsterdam, 1977.
7. W. Meier and O. Staffelbach, Nonlinearity criteria for cryptographic functions, *in* "Advances in Cryptology, EUROCRYPT' 89," Lecture Notes in Computer Science, Vol. 434, pp. 549–562, Springer-Verlag, New York/Berlin, 1990.
8. Gian-Carlo Rota, "On the Foundations of Combinatorial Theory," Springer-Verlag, New York/Berlin, 1964; reprint in [5].
9. O. S. Rothaus, On bent functions, *J. Combin. Theory Ser. A* **20** (1976), 300–305.
10. J. H. Van Lint, "Coding Theory," Springer-Verlag, New York/Berlin, 1988.