Results on Bent Functions

Xiang-dong Hou

Department of Mathematics and Statistics, Wright State University, Dayton, Ohio 45435

and

Philippe Langevin

G.E.C.T., Université de Toulon, 83130 La Garde, France

Communicated by Vera Pless

Received November 15, 1996

In this paper, we present three results on bent functions: a construction, a restriction, and a characterization. Starting with a single bent function, in a simple but very effective way, the construction produces a large number of new bent functions in the same number of variables. The restriction imposes new conditions on the directional derivatives of bent functions. Certain non-existence results that were previously obtained through computer search follow easily from these conditions. The characterization describes bent functions as certain solutions of a system of quadratic equations. Interesting new properties of bent functions are obtained using the characterization. © 1997 Academic Press

1. INTRODUCTION

Bent functions are a fascinating topic in combinatorics. From a design theoretic point of view, these functions are precisely the non-trivial difference sets in elementary abelian 2-groups; from a coding theoretic point of view, they are the vectors that are farthest away from the first order Reed-Muller codes. Dillon's thesis [7] is an excellent source of results on bent functions up to the mid 1970's. For recent work on the topic, see [1–5] by Carlet, [6] by Carlet and Guillot, [8] by Dobbertin, [10] by Kumar, Scholtz, Welch, and [11] by Langevin on constructions, characterizations, and generalizations of bent functions. Also see [9] by Hou on cubic bent functions. Despite extensive study, many questions about bent functions remain open. The ultimate goal of classifying bent functions under the action of the general affine group seems to be out of reach for
the time being. Even with cubic bent functions, our knowledge is very limited.

The purpose of this paper is to introduce several new ideas to the study of bent functions. As result of these ideas, we found a new construction of bent functions, a new restriction on bent functions, and a new characterization of bent functions.

Constructions of bent functions are important, especially when our knowledge of them is so limited. One needs abundant examples to discover properties of bent functions or to disprove conjectures about them. Most of the known constructions of bent functions gather around the idea of partial spreads of GF(2)^m. Roughly speaking, these constructions only cover the bent functions with nice geometric structures. Other known constructions usually combine bent functions in fewer variables to produce a bent function in more variables. Since the number of variables goes up, iteration is not available among bent functions on the same space. Our construction works in a totally different way. Starting with a single bent function with few restrictions, the construction produces a large number of new bent functions in the same number of variables. In some special cases of this construction, the results are explicit. The construction is very effective in the sense that the results it produces are unpredictable as shown by examples. Cubic bent functions are of particular importance in this construction.

A Boolean function of degree 3 in 6 variables whose cubic part is \(X_1X_2X_3 + X_4X_5X_6\) can not be bent. This was the result of a computer search [13]. However, the real reason behind this phenomenon is a restriction on bent functions previously not known. Let \(f\) be a bent function in \(2t\) variables written in the form \(f = g(X_1, ..., X_{2t-1}) + X_{2t}h(X_1, ..., X_{2t-1})\). Then \(|gh| = (1/2)|h| + 2^{t-2} (\varepsilon = 0, \pm 1)\) for every linear function \(\alpha\) in \(X_1, ..., X_{2t-1}\). An immediate consequence of this restriction is that the degree of \(gh\) is at most \(2t - 2\) for \(t > 3\). This simple condition disqualifies a large family of functions as candidates for bent functions, including the function at the beginning of this paragraph. The restriction opens a door to a series of new properties of bent functions and eliminates many unnecessary searches in computer experiments.

Recently, Carlet and Guillot [6] found a characterization for bent functions viewed as complex valued functions rather than GF(2) valued functions. They characterize bent functions as the extended version of the generalized partial spreads class. Let \(\mathcal{A}_m\) be the set of all functions \(g : GF(2)^m \rightarrow \mathbb{C}\) such that both \(g\) and its Fourier transform are integer valued. Then a Boolean function on GF(2)^2t, viewed as a complex valued function, is bent if and only if \(f + 2^{t-1}1_{\{0\}} \in \mathcal{A}_{2t}\), where \(1_{\{0\}}\) is the characteristic function of \(\{0\}\). \(\mathcal{A}_{2t}\) is a finitely generated free abelian group. With respect to every set of generators of \(\mathcal{A}_{2t}\), one has a characterization for bent functions. We determine a basis of \(\mathcal{A}_{2t}\). Using this basis, we characterize
bent functions as certain solutions of a system of quadratic equations. Interesting new properties of bent functions follow from the characterization.

Section 2 is the background of bent functions. Sections 3–5 are devoted to the new construction of bent functions. Section 6 is on the new restriction on bent functions. Section 7 is on the new characterization of bent functions.

2. BACKGROUND

The algebra of Boolean functions on \( \text{GF}(2)^m \) is denoted by \( \mathcal{P}_m \). Actually, \( \mathcal{P}_m = \text{GF}(2)[X_1, \ldots, X_m]/(X_1^2 - X_1, \ldots, X_m^2 - X_m) \). For \( 0 \leq r \leq m \), the \( r \)th order Reed–Muller code of length \( 2^m \) is \( R(r, m) = \{ F \in \mathcal{P}_m; \deg F \leq r \} \). Let \( g: \text{GF}(2)^m \rightarrow \mathbb{C} \) be any function. Its Fourier transform is a function \( \mathcal{F}g: \text{GF}(2)^m \rightarrow \mathbb{C} \) defined by

\[
\mathcal{F}g(s) = \frac{1}{2^{m/2}} \sum_{x \in \text{GF}(2)^m} g(x)(-1)^{\langle s, x \rangle}, \quad s \in \text{GF}(2)^m,
\]

where \( \langle s, x \rangle = s_1x_1 + \cdots + s_mx_m \) for \( s = (s_1, \ldots, s_m) \), \( x = (x_1, \ldots, x_m) \). (Note that the Fourier transformation in this paper is normalized.) One has \( \mathcal{F}^2g = g \). The Hamming weight and distance in \( \mathcal{P}_m \) are denoted by \( | \cdot | \) and \( d( \cdot, \cdot ) \). Bent functions only exist in \( \mathcal{P}_2 \). A function \( f \in \mathcal{P}_2 \) is called bent if and only if

\[
|f + x| = 2^{2^{l-1}} + 2^{l-1} \quad \text{for all} \quad x \in R(1, 2^l).
\]

There are many equivalent definitions for \( f \) to be bent. We list a few that are relevant in this paper.

(i) \( d(f, R(1, 2^l)) = 2^{2^{l-1}} - 2^{l-1} \), the covering radius of \( R(1, 2^l) \), i.e., \( f \) is the farthest from \( R(1, 2^l) \);

(ii) \( |f(X + a) + f(X)| = 2^{2^{l-1}} \) for all \( 0 \neq a \in \text{GF}(2)^{2^l} \), where \( X = (X_1, \ldots, X_{2^l}) \);

(iii) \( \mathcal{F} [(-1) f](s) = \pm 1 \) for all \( s \in \text{GF}(2)^{2^l} \).

If \( f \) is bent, then by (ii), \( \mathcal{F} [(-1) f] = (-1)^f \) for some Boolean function \( f \). \( \tilde{f} \) is also bent and is called the dual of \( f \). A bent function \( f \) is linked to Hadamard matrices in two ways: Both \( [f(x + y)]_{x,y \in \text{GF}(2)^{2^l}} \) and \( [f(x) + \tilde{f}(y) + \langle x, y \rangle]_{x,y \in \text{GF}(2)^{2^l}} \) are \((0,1)\)-Hadamard matrices with constant row and column sums, i.e., regular Hadamard matrices. Bent functions in \( \mathcal{P}_2 \) (\( t \geq 2 \)) have degree at most \( t [13] \).
3. A CONSTRUCTION OF BENT FUNCTIONS, THE BASIC VERSION

For any \( f \in \mathcal{P}_2 \), define

\[
    l(f) = \{ x \in \mathcal{P}_2 : |f + x| = 2^{2t-1} \pm 2^{t-1} \}.
\]

(3.1)

Thus \( f \) is bent if and only if \( l(f) \supseteq R(1, 2t) \).

**Lemma 3.1 (The Basic Construction).** Let \( f \in \mathcal{P}_2 \) and let \( \sigma = (\sigma_1, ..., \sigma_{2t}) : \mathbb{GF}(2)^{2t} \rightarrow \mathbb{GF}(2)^{2t} \) be a bijection. Then \( f \circ \sigma^{-1} \) is a bent function if and only if the linear span \( \text{span}(\sigma_1, ..., \sigma_{2t}) \subseteq l(f) \).

**Proof.** One only has to note that \( \text{span}(\sigma_1, ..., \sigma_{2t}) \subseteq l(f) \) if and only if \( \alpha \cdot \sigma \in l(f) \) for all \( \alpha \in R(1, 2t) \) and that \( |F \circ \sigma^{-1} + x| = |F + \alpha \cdot \sigma| \) for all \( \alpha \in R(1, 2t) \).

The idea in Lemma 3.1 is simple. However, in order for the construction to work, one has to find the bijection \( \sigma \). This is the interesting part of the construction. Before exploring any further, we provide an example to show the effectiveness of the construction.

**Example 3.2.** Let \( X = (X_1, ..., X_t), Y = (X_{t+1}, ..., X_{2t}) \) Then

\[
    f = \langle X, Y \rangle + Q(X_1, ..., X_t)
\]

(3.2)

is bent for all \( Q \). Consider \( \sigma : \mathbb{GF}(2)^{2t} \rightarrow \mathbb{GF}(2)^{2t} \), \( (X, Y) \mapsto (\pi(X), Y) \), where \( \pi : \mathbb{GF}(2)^{t} \rightarrow \mathbb{GF}(2)^{t} \) is a bijection. Then \( \sigma \) is a bijection with \( \sigma^{-1}(X, Y) = (\pi^{-1}(X), Y) \), and \( \alpha \cdot \sigma \in l(f) \) for all \( \alpha \in R(1, 2t) \). By Lemma 3.1,

\[
    f \circ \sigma^{-1} = \langle \pi^{-1}(X), Y \rangle + Q \circ \pi^{-1}(X)
\]

(3.3)

is bent. This is the Maiorana–McFarland family of bent functions.

4. A SPECIAL CASE OF THE CONSTRUCTION

**Theorem 4.1.** Let \( f = X_1 f_1 + X_2 f_2 + X_1 X_2 \alpha + g \in \mathcal{P}_2 \) be a bent function, where \( f_1, f_2, \alpha, g \) are functions of \( X_3, ..., X_{2t} \), and \( \deg \alpha \leq 1 \). Then

\[
    (\alpha + 1) f_1 f_2 + (X_1 + 1) f_1 + (X_1 + X_2 + \alpha + 1) f_2 + \alpha(X_1 + 1) X_2 + g \in \mathcal{P}_2\,
\]

(4.1)

is a bent function.
Proof. (1) We claim that span\( (R(1, 2t), f_1 + X_2 x, f_2 + X_1 x) \subseteq l(f) \).
(Note that \( f_1 + X_2 x \) and \( f_2 + X_1 x \) are the derivatives of \( f \) with respect to \( x_1 \) and \( x_2 \).) Let \( \beta \in \text{span}(R(1, 2t), f_1 + X_2 x, f_2 + X_1 x) \). Then for some \( \varepsilon_1, \varepsilon_2 \in \text{GF}(2) \) and \( \gamma \in R(1, 2t) \),

\[
\beta = \varepsilon_1 (f_1 + X_2 x) + \varepsilon_2 (f_2 + X_1 x) + \gamma
\]

(4.2)

Note that \( \varepsilon_1, \varepsilon_2, \gamma \in R(1, 2t) \). Thus we have

\[
|f + \beta| = |f(x_1 + \varepsilon_1, x_2 + \varepsilon_2, x_3, ..., x_{2t}) + \varepsilon_1 \varepsilon_2 x + \gamma| = 2^{2^{t-1}} + 2^{t-1}, \tag{4.3}
\]

i.e. \( \beta \in l(f) \).

(2) Let

\[
\sigma(x_1, ..., x_{2t}) = \left( (f_1, f_2) + (X_1, X_2) \begin{bmatrix} 1 & x + 1 \\ x & 1 \end{bmatrix}, x_3, ..., x_{2t} \right) \tag{4.4}
\]

\[
\tau(x_1, ..., x_{2t}) = \left[ (f_1, f_2) + (X_1, X_2) \begin{bmatrix} 1 & x + 1 \\ x & 1 \end{bmatrix}, x_3, ..., x_{2t} \right] \tag{4.5}
\]

Then \( \tau \circ \sigma = \text{id} \). Hence \( \sigma \) is a bijection of \( \text{GF}(2)^{2t} \). Also note that the coordinate functions of \( \sigma \) are in \( \text{span}(R(1, 2t), f_1 + X_2 x, f_2 + X_1 x) \). By Lemma 3.1, \( f \circ \sigma^{-1} = f \circ \tau \) is a bent function.

(3) Direct computation shows that \( f \circ \tau \) is the function in (4.1).

Remark. The function in (4.1) is obtained from \( f \) through a transformation. The square of this transformation applied to \( f \) yields \( f(x_1, x_2 + x, x_3, ..., x_{2t}) \).

Corollary 4.2. Let \( f \) be the bent function in Theorem 4.1. Then

\[
\text{deg} \left( (x + 1) f_1 f_2 \right) \leq t. \tag{4.6}
\]

Proof. The conclusion needs no proof when \( t = 1 \). If \( t \geq 2 \), then \( \text{deg} f \leq t \). Thus all the terms except the first one in (4.1) have degree \( \leq t \). Since the function (4.1) also has degree \( \leq t \), we have (4.6).

Inequality (4.6) is a restriction on bent functions. In Section 6, we will see another strong restriction of similar nature on bent functions. We now turn to concrete examples of Theorem 4.1.
Example 4.3. The function
\[ F = X_1 X_2 X_3 + X_2 X_4 X_5 + X_4 X_7 + X_2 X_7 + X_3 X_6 + X_4 X_8 + X_5 X_6 \in \mathcal{B} \]  
(4.7)
is bent. (See [9].) Write \( F \) in the form
\[ F = X_1 X_2 (X_3) + X_1 (X_4 X_5 + X_7) + (X_4 X_8 + X_5 X_6) + X_5 X_6 \]  
(4.8)
Then Theorem 4.1 produces the bent function
\[ G = (X_1 + 1) X_6 (X_4 X_5 + X_7) + (X_1 + 1) X_8 \]
\[ + (X_1 + X_2 + X_3 + 1) (X_4 X_5 + X_7) + X_5 (X_1 + 1) X_2 \]
\[ + X_4 X_5 + X_3 X_6 + X_4 X_8 + X_5 X_6 \]
\[ = X_3 X_4 X_5 X_8 + X_1 X_2 X_3 + X_1 X_4 X_5 + X_2 X_4 X_5 \]
\[ + X_3 X_5 X_6 + X_4 X_5 X_8 + X_2 X_5 X_8 \]
\[ + X_7 X_3 X_7 X_8 + X_7 X_8 \]  
(4.9)
Note that \( \deg F = 3 \) but \( \deg G = 4 \).

Example 4.4. Let \( G \in \mathcal{B} \) be the bent function constructed in Example 4.3, and write it in the form
\[ G = X_2 X_3 (X_1 + 1) + X_3 (X_4 X_5 + X_7) \]
\[ + X_3 (X_4 X_5 X_8 + X_4 X_8 + X_5 X_6 + X_8) \]
\[ + (X_1 X_4 X_5 + X_4 X_5 X_8 + X_4 X_5 X_8 + X_5) \]
\[ + X_1 X_2 X_3 + X_1 X_4 X_5 + X_1 X_7 + X_1 X_8 \]
\[ + X_3 X_4 X_5 + X_5 X_6 + X_7 X_8 + X_7 + X_8 \].  
(4.10)
Then Theorem 4.1 produces the bent function
\[ H = X_1 X_2 X_3 X_6 + X_2 X_4 X_5 X_8 + X_3 X_4 X_5 X_8 \]
\[ + X_4 X_5 X_6 + X_5 X_6 + X_7 X_8 + X_3 X_8 + X_3 X_8 \]
\[ + X_4 X_5 + X_5 X_6 + X_2 X_5 + X_3 X_6 + X_3 X_6 + X_3 X_7 \]
\[ + X_4 X_5 + X_4 X_6 + X_5 X_6 + X_7 X_8 + X_3 X_8 \].  
(4.11)
Although $G$ and $H$ are both of degree 4, they are not equivalent (by an affine transformation of coordinates followed by an addition of a linear function). (See [9]. The fourth ranks of $G$ and $H$ are different: $r_4(G) = 4$, $r_4(H) = 6$.)

Remark. If $f$ is a cubic bent function, then the condition $\deg \sigma \leq 1$ in Theorem 4.1 is always satisfied and Theorem 4.1 always applies. Actually, we will see that Theorem 4.1 can be made much more general if $f$ is cubic.

5. A CONSTRUCTION FROM CUBIC BENT FUNCTIONS

For any $f \in \mathcal{P}_m$, define

$$D_a f = f(X + a) + f(X), \quad a \in \text{GF}(2)^m, \tag{5.1}$$

$$D_f = \{ D_a f : a \in \text{GF}(2)^m \}. \tag{5.2}$$

Lemma 5.1. If $f \in R(3, 2t)$ is a cubic bent function, then $\text{span}(D_f, R(1, 2t)) \subset \text{GF}(2)^m$.

Proof. For any $\sigma \in \text{span}(D_f, R(1, 2t))$, $\sigma \equiv D_a f + \cdots + D_{a_k} f \pmod{R(1, 2t)}$ for some $a_i, \ldots, a_k \in \text{GF}(2)^2$. Since $f \in R(3, 2t)$, one has $D_{a_k+\beta} f \equiv D_{a_k} f + D_{f} f \pmod{R(1, 2t)}$ for all $a, \beta \in \text{GF}(2)^2$. Hence $\sigma \equiv D_{a_k} f \pmod{R(1, 2t)}$, where $a = a_1 + \cdots + a_k$. Thus $\sigma = D_{a_k} f + \beta$ for some $\beta \in R(1, 2t)$ and

$$|f + \sigma| = |f + D_{a_k} f + \beta| = |f(X + a) + \beta| = 2^{2t-1} \pm 2^{t-1}. \tag{5.3}$$

Theorem 5.2. Let $f \in R(3, 2t)$ be a bent function. If $\sigma_i \in \text{span}(D_f, R(1, 2t))$ (1 $\leq i \leq 2t$) such that $\sigma = (\sigma_1, \ldots, \sigma_{2t})$ is a bijection of $\text{GF}(2)^2$, then $f \circ \sigma^{-1}$ is a bent function.

Proof. It follows immediately from Lemmas 3.1 and 5.1.

The following is a criterion for $\sigma : \text{GF}(2)^m \rightarrow \text{GF}(2)^m$ to be a bijection.

Lemma 5.3 [7, Remark 6.3.7.]. A map $\sigma = (\sigma_1, \ldots, \sigma_m) : \text{GF}(2)^m \rightarrow \text{GF}(2)^m$ is a bijection if and only if $|\epsilon_1 \sigma_1 + \cdots + \epsilon_m \sigma_m| = 2^{m-1}$ for all $0 \neq (\epsilon_1, \ldots, \epsilon_m) \in \text{GF}(2)^m$.

In Theorem 5.2, span$(D_f, R(1, 2t))$ is of dimension $1 + 2t + r_2(f)$, where $r_2(f)$ is the “cubic rank” of $f$ defined in [9]. In order for Theorem 5.2 to work, the question is how to choose $\sigma_i \in \text{span}(D_f, R(1, 2t))$ such that $\sigma = (\sigma_1, \ldots, \sigma_{2t})$ is a bijection. (One should avoid choosing all $\sigma_i \in R(1, 2t)$, a trivial case where $\sigma$ is an affine transformation.) Lemma 5.3 is not very
helpful here; it is useful for checking bijections, not for finding them. A natural attempt is to let

\[ \sigma = (D_{u_1}f, ..., D_{u_t}f), \]  

where \( u_1, ..., u_t \) are a basis of \( GF(2)^t \). The \( \sigma \) in (5.4) is not always a bijection. But our computer experiments seem to indicate that there are plenty of choices of the basis \( u_1, ..., u_t \) to make the \( \sigma \) a bijection, though we do not have any theoretic proof for this claim. (In our experiments, about one out of two choices of the basis \( u_1, ..., u_t \) is good.) A necessary condition for the map in (5.4) to be bijective is that \( \dim(\text{span}(Df)) \geq 2t \). This condition is always satisfied for bent functions. In fact, if \( f \in \mathcal{P}_m \) cannot be written in fewer than \( m \) variables through a linear transformation, the map \( u \mapsto D_uf \) from \( GF(2)^m \) to \( \mathcal{P}_m \) is one-to-one. Thus \( \|Df\| = 2^m \), implying that \( \dim(\text{span}(Df)) \geq m \).

**Example 5.4.** Let \( F \in R(3, 8) \) be the bent function in Example 4.3. Let \( e_1, ..., e_8 \) be the standard basis of \( GF(2)^8 \). With computer assist, we find that

\[ \sigma = (D_{e_1}F, ..., D_{e_8}F) \]  

is a bijection and

\[ F \circ \sigma^{-1} = X_1X_2X_3 + X_1X_6 + X_2X_7 + X_3X_5 + X_4X_5 + X_5X_6 + X_6X_8. \]  

(5.6)

Note \( F \) and \( F \circ \sigma^{-1} \) are both of degree 3, but not equivalent.

**Example 5.5.** Start with the same \( F \). Let

\[
\begin{align*}
    u_1 &= e_1 + e_2 + e_4 + e_5, \\
    u_2 &= e_1 + e_2 + e_3 + e_6, \\
    u_3 &= e_2 + e_3 + e_4 + e_8, \\
    u_4 &= e_3 + e_5 + e_6 + e_8, \\
    u_5 &= e_5, \\
    u_6 &= e_6, \\
    u_7 &= e_7, \\
    u_8 &= e_8.
\end{align*}
\]

(5.7)
Then
\[ \tau = (D_m F, \ldots, D_m F) \] (5.8)
is a bijection and
\[ F \circ \tau^{-1} = X_1 X_3 + X_1 X_5 + X_1 X_9 + X_2 X_4 + X_2 X_6 + X_2 X_8 + X_3 X_4 \]
\[ + X_3 X_6 + X_3 X_7 + X_4 X_6 + X_4 X_7 + X_5 X_7 + X_1 + X_6 + X_7 \] (5.9)

It is interesting to note that the degree goes down in the construction of this example.

Examples of Theorem 5.2 are abundant. However, the main question, in a slightly more general form, remains.

**Question.** Let \( \sigma_1, \ldots, \sigma_m \in R(2, m) \). When is \((\sigma_1, \ldots, \sigma_m)\) a bijection of GF(2)\(^m\)? (A meaningful answer should be a criterion substantially easier to use than Lemma 5.3.)

### 6. A RESTRICTION ON BENT FUNCTIONS

**Lemma 6.1.** Let \( g, h \in \mathcal{P}_{m-1} \). Then
\[ |gh|_{m-1} = \frac{1}{2}(|g| + X_m(h + 1)|_m - |h + 1|_{m-1}), \] (6.1)
where \(|.|_m\) and \(|.|_{m-1}\) are the Hamming weights in \( \mathcal{P}_m \) and \( \mathcal{P}_{m-1} \) respectively.

**Proof.** We have
\[ |g + X_m(h + 1)|_m = |g|_{m-1} + |g + h + 1|_{m-1} \]
\[ = |h + 1|_{m-1} + 2 |g(g + h + 1)|_{m-1} \]
\[ = |h + 1|_{m-1} + 2 |gh|_{m-1}, \] (6.2)
and (6.1) follows.

**Theorem 6.2.** Let \( f = g + X_2 h \in \mathcal{P}_t \) be a bent function, where \( g \in R(t, 2t - 1) \), \( h \in R(t - 1, 2t - 1) \). Then for every \( x \in R(1, 2t - 1) \),
\[ |ghx|_{2t-1} = \frac{1}{2}|hx|_{2t-1} + \varepsilon 2^{t-2}, \quad \varepsilon = 0, \pm 1. \] (6.3)
Proof. From \(|\,(g + \alpha)h|_{2t-1} = |gh|_{2t-1} + |hx|_{2t-1} - 2 |ghx|_{2t-1}, \) one has
\(|ghx|_{2t-1} = \frac{1}{2}|hx|_{2t-1} + \frac{1}{2}(|gh|_{2t-1} - |(g + \alpha)h|_{2t-1})\). \hspace{1cm} (6.4)

By (6.1), \(|gh|_{2t-1} - |(g + \alpha)h|_{2t-1} = \frac{1}{2}(|g + X_2(h + 1)|_{2t} - |g + X_2(h + 1)|_{2t})\). Since \(f\) is bent, one has \(|g + X_2(h + 1)|_{2t} = 2^{2t-1} + 2^{t-1} \) and \(|g + X_2(h + 1)|_{2t} = 2^{2t-1} \). Thus \(|gh|_{2t-1} - |(g + \alpha)h|_{2t-1} = 2^{t-1}, \epsilon = 0, \pm 1, \) and (6.3) follows. \(\square\)

Corollary 6.3. Let \(t \geq 3\) and let \(f = g + X_2h \in \mathcal{B}_2\) be a bent function, where \(g \in R(t, 2t-1), h \in R(t-1, 2t-1)\). Then the following hold.

(i) \(gh \in R(2t - 2, 2t - 1)\).

(ii) If \(h \in R(t - 2, 2t - 1)\), then \(gh \in R(2t - 3, 2t - 1)\).

Proof. (i) Note that \(|h|_{2t-1} = 2^{t-2}\) by the second equivalent definition of bent functions in Section 2. Letting \(\alpha = 1\) in (6.3), we have \(|gh|_{2t-1} \equiv (1/2) |h|_{2t-1} \equiv 0 \pmod{2^{t-2}}\). Thus \(gh \in R(2t - 2, 2t - 1)\).

(ii) Suppose to the contrary that \(\deg gh = 2t - 2\). Then there exists an \(x \in R(1, 2t-1)\) such that \(\deg ghx = 2t - 1\). Since \(hx \in R(t - 1, 2t-1)\), by the McEliece theorem [12, Chap. 15] we have \(|hx|_{2t-1} \equiv 0 \pmod{4}\). Now by (6.3), \(|ghx|_{2t-1} \equiv 0 \pmod{2}\), which is a contradiction. \(\square\)

Remark. For any \(S \subseteq \{1, \ldots, m\}\), denote \(\prod_{x \in S} X_x \in \beta_m^t\) by \(X_S\). Write the bent function in Corollary 6.3 as
\[ f = \sum_{S \subseteq \{1, \ldots, 2t\}} a_S X_S, \hspace{1cm} (6.5) \]
where \(a_S \in GF(2)\). Then in Corollary 6.3, (i) is equivalent to
\[ \sum_{\{S, T\}} a_S a_T = 0, \hspace{1cm} (6.6) \]
and the conclusion of (ii) is equivalent to
\[ \sum_{\{S, T\}} a_S a_T = 0 \text{ for all } W \subseteq \{1, \ldots, 2t - 1\}, |W| = 2t - 2. \hspace{1cm} (6.7) \]
In Section 7, we will see that (6.6) and (6.7) are special cases of a more general identity.
If \( f \in \mathcal{P}_t \) is a bent function written in the form
\[
F = X_{S_1} + \cdots + X_{S_t} + \text{terms of lower degree},
\]  
(6.8)
where \( S_i \subseteq \{1, \ldots, 2t\} \), \( |S_i| = t \), then
\[
f = X_{S'_1} + \cdots + X_{S'_t} + \text{terms of lower degree},
\]  
(6.9)
where \( S'_i = \{1, \ldots, 2t\} \setminus S_i \) [7]. Thus if \( f = \tilde{f} \), the monomials \( X_S \) and \( X_{S'} \) of degree \( t \) must appear in pairs in \( f \), implying that \( f \) has an even number of monomials of degree \( t \). By (6.6), a little more can be said in this situation.

**Corollary 6.4.** Let \( t \geq 3 \) and let \( f \in \mathcal{P}_t \) be a bent function such that \( f = \tilde{f} \). Then the number of monomials of degree \( t \) in \( f \) is \( \equiv 0 \pmod{4} \).

### 7. A CHARACTERIZATION OF BENT FUNCTIONS

In most of this section, we view Boolean functions as complex valued functions whose values are 0 and 1.

**Lemma 7.1** (Lemma 1 of [4]). A Boolean function \( f : \text{GF}(2)^{2t} \to \{0, 1\} \subseteq \mathbb{C} \) is bent if and only if \( \mathcal{F}[(-1)^f] \) is integer valued and \( \mathcal{F}[(-1)^f](s) \equiv 1 \pmod{2} \) for all \( s \in \text{GF}(2)^{2t} \).

Let \( \mathcal{A}_t \) be the set of all functions \( g : \text{GF}(2)^{2m} \to \mathbb{C} \) such that both \( g \) and \( \mathcal{F}g \) are integer valued. For every \( S \subseteq \text{GF}(2)^{2m} \), the characteristic function of \( S \) is denoted by \( 1_S \). We have the following characterization for bent functions.

**Lemma 7.2.** A Boolean function \( f : \text{GF}(2)^{2t} \to \{0, 1\} \subseteq \mathbb{C} \) is bent if and only if \( f + 2^{t-1}1_{(0)} \in \mathcal{A}_t \).

**Proof.** Note that
\[
1 - \mathcal{F}[(-1)^f] = 2\mathcal{F}[2^{t-1}1_{(0)} + f] - 2^{t}1_{(0)}.
\]  
(7.1)
Thus Lemma 7.1 completes the proof (since \( t \geq 1 \)).

\( \mathcal{A}_t \) is a finitely generated free abelian group. For every set of generators of \( \mathcal{A}_t \), Lemma 7.2 gives a characterization of bent functions using these generators. The main result of [6] is that \( \mathcal{A}_t \) is generated by \( \{1_E : E \text{ is a } t \text{-dimensional subspace of } \text{GF}(2)^{2t}\} \cup \{g : g \equiv 0 \pmod{2^t}\} \).
Following the line of \[6\], we can find a basis for \(A_t\). For \(x, y \in \text{GF}(2)^m\), we say \(x \leq y\) if \(\text{supp } x \subseteq \text{supp } y\). Define
\[
F_x = \{ y \in \text{GF}(2)^m : y \leq x \}, \quad x \in \text{GF}(2)^m. \tag{7.2}
\]

**Lemma 7.3.** Let
\[
\phi_x = 2^{\max\{0, t - |x|\}} 1_{F_x}, \quad x \in \text{GF}(2)^{2^t}.
\tag{7.3}
\]
Then \(\{ \phi_x : x \in \text{GF}(2)^{2^t} \}\) is a basis of \(A_t\).

**Proof.** That \(\phi_x\) \((x \in \text{GF}(2)^{2^t})\) are linearly independent over \(\mathbb{Z}\) is obvious. That \(\phi_x\) \((x \in \text{GF}(2)^{2^t})\) span \(A_t\) follows from the final note of \([6]\).

**Theorem 7.4** [6]. Let \(f : \text{GF}(2)^{2^t} \to \{0, 1\} \subset \mathbb{C}\) be a Boolean function. Then \(f\) is a bent function if and only if
\[
f = -2^{t-1} 1_{\{0\}} + \sum_{x \in \text{GF}(2)^{2^t}} n_x \phi_x,
\tag{7.4}
\]
for some integers \(n_x\) \((x \in \text{GF}(2)^{2^t})\). In this case
\[
\tilde{f} = -2^{t-1} 1_{\{0\}} + \sum_{x \in \text{GF}(2)^{2^t}} n_x \phi_x.
\tag{7.5}
\]

**Proof.** The first part of the theorem follows immediately from Lemmas 7.2 and 7.3. To see (7.5), note that
\[
1 - 2\tilde{f} = (-1)^7 = \mathcal{F}[(-1)^7] = \mathcal{F}[1 - 2f]
= 2^t 1_{\{0\}} - 2^{t-1} 1_{\{0\}} - \frac{1}{2} + \sum_{x \in \text{GF}(2)^{2^t}} n_x \phi_x. \tag{7.6}
\]
By Theorem 7.4, a function \(f : \text{GF}(2)^{2^t} \to \mathbb{C}\) is bent if and only if
\[
f = -2^{t-1} 1_{\{0\}} + \sum_{x \in \text{GF}(2)^{2^t}} m_x 1_{F_x}\tag{7.7}
\]
with \(m_x \equiv 0 \pmod{2^{\max\{0, t - |x|\}}}\) for all \(x \in \text{GF}(2)^{2^t}\) and \(f^2 = f\). Computation shows that
\[
f^2 - f = \sum_{x} \left[ m_x^2 + 2 \sum_{y \geq x} m_{y-1} m_x + 2 \sum_{\{y, z : y > x, z = x\}} m_y m_z \right] 1_{F_x}
+ \left( 2^{2^t-2} + 2^{t-1} - 2^{t-1} \sum_{x} m_x \right) 1_{F_x}, \tag{7.8}
\]
where $yz = (y_1 z_1, ..., y_2 z_2)$ for $y = (y_1, ..., y_2)$ and $z = (z_1, ..., z_2)$. Therefore, we have proved the following characterization for bent functions.

**Proposition 7.5.** Let $f : \mathbb{GF}(2)^t \rightarrow \mathbb{C}$ be written in the form

$$f = -2^{t-1}1_{(0)} + \sum_{x \in \mathbb{GF}(2)^t} m_x 1_{x}.$$  

(7.9)

Then $f$ is a bent function if and only if $m_x (x \in \mathbb{GF}(2)^t)$ are a solution of the system of quadratic equations

$$\begin{cases}
    m_x^2 + \left( 2 \sum_{y > x} m_y - 1 \right) m_x + 2 \sum_{y, z > x, yz = x} m_y m_z = 0, & \text{for } 0 \neq x \in \mathbb{GF}(2)^t, \\
    m_y^2 + \left( 2 \sum_{y > 0} m_y - 2^t - 1 \right) m_0 + 2 \sum_{y, z > 0, yz = 0} m_y m_z = 0, \\
    -2^t \sum_{y > 0} m_y + 2^{2^t-2} + 2^{t-1} = 0
\end{cases}$$

(7.10)

such that $m_x \equiv 0 \pmod{2^{\max(0, t-|x|)}}$ for all $x \in \mathbb{GF}(2)^t$.

Note that all the solutions of (7.10) are integers. They are in one-to-one correspondence with the complex valued Boolean functions on $\mathbb{GF}(2)^t$.

Proposition 7.5 suggests a link between bent functions and the 2-adic number theory. We end this section with another restriction on bent functions that follows from Proposition 7.5.

**Corollary 7.6.** Let $t \geq 3$ and let

$$f = \sum_{S \subseteq \{1, \ldots, 2t\}} a_S \prod_{i \in S} X_i$$

(7.11)

be a bent function where $a_S \in \mathbb{GF}(2)$. Then for each $V \subseteq \{1, \ldots, 2t\}$ with $t + 2 \leq |V| \leq 2t$,

$$\sum_{S : |S \setminus T| = V} a_S a_T = 0.$$  

(7.12)

**Proof.** We may assume $V = \{1, \ldots, k\}$, $t + 2 \leq k \leq 2t$. For each $x \in \mathbb{GF}(2)^t$ and each $S \subseteq \{1, \ldots, 2t\}$, let $s(x) \subseteq \{1, \ldots, 2t\}$ be the support of $x$ and let $v(S)$ be the vector in $\mathbb{GF}(2)^{2t}$ whose support is $S$. The function

$$g = f(X_1 + 1, \ldots, X_{2t} + 1) = \sum_{S \subseteq \{1, \ldots, 2t\}} a_S \prod_{i \in S} (X_i + 1)$$

(7.13)
is also bent. When \( g \) is viewed as a complex valued Boolean function, one has

\[
g = -2^{t-1}1_{\{0\}} + \sum_{S \subseteq \{1, \ldots, 2t\}} \alpha_S 1_{S^c},
\]

(7.14)

where \( \alpha_S \equiv a_S \) (mod 2). Rewrite (7.14) as

\[
g = -2^{t-1}1_{\{0\}} + \sum_{S \subseteq \mathbb{F}_2^t} \alpha_{S} 1_{S^c},
\]

(7.15)

and let \( u = (0, \ldots, 0, 1, \ldots, 1) \). Since \( t - |u| \geq 2 \), it follows from (7.10) that

\[
\sum_{\{y, z\} \ni u, yz = u} \alpha_{S(y)} \alpha_{S(z)} \equiv 0 \pmod{2}.
\]

(7.16)

Thus

\[
0 = \sum_{\{y, z\} \ni u, yz = u} a_{S(y)} a_{S(z)}
\]

\[
= \sum_{S, T \neq \{1, \ldots, k\}, S \cup T = \{1, \ldots, k\}} a_{S} a_{T} = \sum_{S, T \neq \{1, \ldots, k\}, S \cup T = \{1, \ldots, k\}} a_{S} a_{T}.
\]

(7.17)

(Note that \( a_{\{1, \ldots, k\}} = 0 \) since \( \deg f \leq t \).)

Equation (7.12) contains (6.6) and (6.7). Also note that in (6.7), we do not need the condition in Corollary 6.3 (ii) that \( h \in R(t - 2, 2t - 1) \).

ACKNOWLEDGMENT

The first author was supported by a grant from Université de Toulon et du Var during his visit to the university. He is grateful for the hospitality he received there.

REFERENCES