PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 128, Number 4, Pages 987–996
S 0002-9939(99)05146-1
Article electronically published on August 17, 1999

ON THE COEFFICIENTS OF BINARY BENT FUNCTIONS

XIANG-DONG HOU

(Communicated by John R. Stembridge)

ABSTRACT. We prove a 2-adic inequality for the coefficients of binary bent functions in their polynomial representations. The 2-adic inequality implies a family of identities satisfied by the coefficients. The identities also lead to the discovery of some new affine invariants of Boolean functions on $\mathbf{Z}_2^m$.

1. INTRODUCTION

Binary bent functions, referred to in this paper simply as bent functions, were first introduced by Rothaus [19]. A function $f : \mathbf{Z}_2^m \to \mathbf{Z}_2$ is called a bent function if the values of the Fourier transform of $(-1)^f$ are always ± 1. (The Fourier transform of a function $g : \mathbf{Z}_2^m \to \mathbf{C}$ is the function $\hat{g} : \mathbf{Z}_2^m \to \mathbf{C}$ defined by $\hat{g}(x) = (1/\sqrt{2^m}) \sum_{x \in \mathbf{Z}_2^m} g(x)(-1)^{\langle a,x \rangle}$, $a \in \mathbf{Z}_2^m$.) Bent functions on $\mathbf{Z}_2^m$ exist if and only if m is even. These functions play an important role in discrete mathematics through many applications in coding theory, design theory and cryptography. A function $f : \mathbf{Z}_2^{2t} \to \mathbf{Z}_2$ is bent if and only if (i) f is at maximum Hamming distance from the first order Reed-Muller code $R(1, 2t)$; or (ii) the support of f is a Hadamard difference set in $\mathbf{Z}_2^{2t}$; or (iii) $((-1)^{f(x)})_{x \in \mathbf{Z}_2^{2t}}$ is a perfect binary array [7].

Extensive work on bent functions has produced many interesting results regarding constructions, characterizations, generalizations and other aspects of these functions. (See the references.) However, further advances in the area depend on a better understanding of the fundamental structure of bent functions. The present paper is an attempt in this direction. The main result here is a 2-adic inequality satisfied by the coefficients of bent functions in their polynomial representations. The 2-adic inequality implies a family of identities for the coefficients. Our approach is as follows. First, a bent function $f : \mathbf{Z}_2^{2t} \to \mathbf{Z}_2$ is lifted to a function $\bar{f} : \mathbf{Z}_2^{2t} \to \{0, 1\} \subset \mathbf{Z}$. Then the function $\bar{f}$ is analyzed 2-adically using a known characterization of the lifts of bent functions. Finally, the result on $\bar{f}$ is translated back in terms of f. The advantage of this approach is that the lift $\bar{f}$ contains much information that is not visible in the form of f.

The identities for the coefficients of bent functions also lead us to the discovery of a family of affine invariants of Boolean functions on $\mathbf{Z}_2^m$. These invariants are relatively easy to compute from the polynomial form of Boolean functions and are useful tools to determine affine non-equivalence among Boolean functions.

Received by the editors January 12, 1998 and, in revised form, June 12, 1998.
1991 *Mathematics Subject Classification.* Primary 05B10, 94B27; Secondary 94A60.
Key words and phrases. Bent function, Boolean function, affine invariant.
This work was supported by a grant from the Research Council of Wright State University.

2. The main theorem

The algebra of all functions from $\mathbf{Z}_2^m$ to $\mathbf{Z}_2$ is

$$\mathcal{P}_m = \mathbf{Z}_2[X_1, \cdots, X_m]/(X_1^2 - X_1, \ldots, X_m^2 - X_m). \tag{2.1}$$

For each $S \subset \{1, \ldots, m\}$, denote $\prod_{i\in S} X_i \in \mathcal{P}_m$ by X_S. Let $f = \sum_{S\subset\{1,\ldots,m\}} a_S X_S \in \mathcal{P}_m$, where $a_S \in \mathbf{Z}_2$. For each integer $k \geq 1$ and each $S \subset \{1, \ldots, m\}$, let

$$\begin{aligned} N_{k,S}(f) = \Big|\big\{\{S_1, \ldots, S_k\} : S_1, \ldots, S_k \subset S \text{ are distinct such that} \\ S_1 \cup \cdots \cup S_k = S \text{ and } a_{S_1} \cdots a_{S_k} = 1\big\}\Big|. \end{aligned} \tag{2.2}$$

Throughout this paper, the 2-adic order function is denoted by ν.

Theorem 2.1. *Let $f \in \mathcal{P}_{2t}$ $(t \geq 2)$ be a bent function and $S \subset \{1, \ldots, 2t\}$. Then*

$$\begin{aligned} &\nu\Big(N_{|S|-t,S}(f) - \frac{1}{2}N_{|S|-t-1,S}(f) + \cdots + \big(-\frac{1}{2}\big)^{|S|-t-1} N_{1,S}(f)\Big) \\ &\begin{cases} \geq 1, & \text{if } S \neq \{1, \ldots, 2t\}, \\ = 0, & \text{if } S = \{1, \ldots, 2t\}. \end{cases} \end{aligned} \tag{2.3}$$

The proof of Theorem 2.1 will be completed in Section 4. Let $k \geq 1$ be an integer such that $|S| > (k-1)\deg f$. Then $N_{1,S}(f) = \cdots = N_{k-1,S}(f) = 0$. If, in addition,

$$k \leq \begin{cases} |S| - t, & \text{when } S \neq \{1, \ldots, 2t\}, \\ t - 1, & \text{when } S = \{1, \ldots, 2t\}, \end{cases} \tag{2.4}$$

then (2.3) implies that $N_{k,S}(f) \equiv 0 \pmod 2$. Therefore, we have the following corollary.

Corollary 2.2. *Let $f = \sum_{S\subset\{1,\ldots,2t\}} a_S X_S \in \mathcal{P}_{2t}$ $(t \geq 2)$ be a bent function. Let $k \geq 1$ and $S \subset \{1, \ldots, 2t\}$. Then*

$$\begin{aligned} &\sum_{\substack{\{S_1,\ldots,S_k\} \\ S_1,\ldots,S_k \subset S \text{ distinct} \\ S_1\cup\cdots\cup S_k = S}} a_{S_1} \cdots a_{S_k} = 0, \\ &\text{if } 2t > |S| \geq \max\{k + t,\ (k-1)\deg f + 1\} \\ &\text{or } 2t = |S| \geq \max\{k + t + 1,\ (k-1)\deg f + 1\}. \end{aligned} \tag{2.5}$$

Equation (2.5) with $k = 2$ has been obtained in [14]. We remark that several previous computer searches for bent functions can be made much easier using Corollary 2.2 ([12], [19]). In [12], all cubic bent functions in 8 variables were determined up to affine equivalence using the following method. First, the representatives of the GL-orbits in $R(3,8)/R(2,8)$ are known [10], where $R(r,m) = \{f \in \mathcal{P}_m : \deg f \leq r\}$ is the rth order Reed-Muller code. There are 32 such representatives denoted by F_i $(1 \leq i \leq 32)$ in [10], [12]; they are the canonical cubic forms in 8 variables. Basically, for each $1 \leq i \leq 32$, [12] searched through all $Q \in R(2,8)$ for $F_i + Q$ to be bent. Bent functions were found for 6 of the canonical forms F_i; in the notation

of [10], [12], the 6 "surviving" canonical forms are

$$\begin{cases} F_1 = 0, \\ F_2 = X_{\{1,2,3\}}, \\ F_3 = X_{\{1,2,3\}} + X_{\{2,4,5\}}, \\ F_5 = X_{\{1,2,3\}} + X_{\{2,4,5\}} + X_{\{3,4,6\}}, \\ F_7 = X_{\{1,2,7\}} + X_{\{3,4,7\}} + X_{\{5,6,7\}}, \\ F_9 = X_{\{1,2,3\}} + X_{\{2,4,5\}} + X_{\{3,4,6\}} + X_{\{1,4,7\}}. \end{cases} \tag{2.6}$$

On the other hand, let $t = 4$, $|S| = 6$, $k = 2$, and $\deg f = 3$ in Corollary 2.2. Then (2.5) becomes

$$\sum_{\substack{\{S_1,S_2\} \\ |S_1|=|S_2|=3 \\ S_1 \cup S_2 = S}} a_{S_1} a_{S_2} = 0, \tag{2.7}$$

which is an equation in the coefficients of the cubic terms of f. It can be easily checked that for each of the cubic forms F_i, $i \in \{1, \cdots, 32\} \backslash \{1, 2, 3, 5, 7, 9\}$, equation (2.7) is not satisfied for some S. (For example, for $F_8 = X_{\{1,2,3\}} + X_{\{4,5,6\}} + X_{\{1,4,7\}}$, (2.7) is not satisfied when $S = \{1, \cdots, 6\}$.) Then $F_i + Q$ ($Q \in R(2, 8)$) is bent only if $i = 1, 2, 3, 5, 7, 9$ and the computer search in [12] is greatly reduced. The computer search for bent functions in 6 variables in [19] can be reduced by Corollary 2.2 similarly.

3. Lifting of bent functions

In this section, we describe a characterization of lifts of bent functions obtained by Carlet and Guillot [5]. (Also see [14].) This characterization will be the starting point of the proof of Theorem 2.1.

For each $x = (x_1, \ldots, x_m)$, $y = (y_1, \ldots, y_m) \in \mathbf{Z}_2^m$, define $xy = (x_1 y_1, \ldots, x_m y_m)$ and say $x \le y$ if $\operatorname{supp} x \subset \operatorname{supp} y$. Let

$$F_x = \{y \in \mathbf{Z}_2^m : y \le x\} \quad \text{for each } x \in \mathbf{Z}_2^m. \tag{3.1}$$

For each $S \subset \mathbf{Z}_2^m$, 1_S is the characteristic function of S in $\mathbf{Z}_2^m$. Every function $f : \mathbf{Z}_2^m \to \mathbf{Z}_2$ uniquely determines a function $\bar{f} : \mathbf{Z}_2^m \to \{0, 1\} \subset \mathbf{Z}$ such that $f = \pi \circ \bar{f}$, where $\pi : \mathbf{Z} \to \mathbf{Z}_2$ is the canonical homomorphism. $\bar{f}$ is called the lift of f. If $f : \mathbf{Z}_2^{2t} \to \mathbf{Z}_2$ is bent, there is a unique function $\tilde{f} : \mathbf{Z}_2^{2t} \to \mathbf{Z}_2$ such that $\widehat{[(-1)^f]} = (-1)^{\tilde{f}}$. The function $\tilde{f}$ is also bent and is called the dual of f [19].

Theorem 3.1 ([5]). *A function $f : \mathbf{Z}_2^{2t} \to \mathbf{Z}_2$ is bent if and only if*

$$\bar{f} = -2^{t-1} 1_{\{0\}} + \sum_{x \in \mathbf{Z}_2^{2t}} m_x 1_{F_x}, \tag{3.2}$$

where $m_x \in \mathbf{Z}$ and $m_x \equiv 0 \pmod{2^{\max\{0,\, t-|x|\}}}$ for all $x \in \mathbf{Z}_2^{2t}$. When f is bent,

$$\bar{\tilde{f}} = -2^{t-1} 1_{\{0\}} + \sum_{x \in \mathbf{Z}_2^{2t}} 2^{t-|x|} m_{\bar{x}} 1_{F_x}, \tag{3.3}$$

where $\bar{x} = x + (1, \ldots, 1)$.

Theorem 3.1 was proved in [5] but was not stated as a theorem there. The explicit statement of Theorem 3.1 is in [14]. The reader is cautioned that Theorem

3.1 does not solve the problem of bent functions since the function in (3.2) is not automatically $\{0,1\}$-valued.

4. Proof of Theorem 2.1

For each integer $b \geq 0$ with 2-adic expansion $b = b_0 2^0 + b_1 2^1 + \cdots$, where $b_i = 0, 1$, let $|b|_2 = b_0 + b_1 + \cdots$. It is easy to see that

$$\nu(b!) = b - |b|_2. \tag{4.1}$$

Another useful fact is that if $b_0 2^0 + b_1 2^1 + \cdots = 2^l$, where $b_i \geq 0$ are integers with $b_0 > 0$, then

$$b_0 + b_1 + \cdots \geq l + 1. \tag{4.2}$$

Consider a bent function $f : \mathbf{Z}_2^{2t} \to \mathbf{Z}_2$ with

$$\bar{f} = -2^{t-1} 1_{\{0\}} + \sum_{x \in \mathbf{Z}_2^{2t}} m_x 1_{F_x}, \tag{4.3}$$

where $\nu(m_x) \geq \max\{0, t - |x|\}$ for all $x \in \mathbf{Z}_2^{2t}$. For each integer $k \geq 1$ and $x \in \mathbf{Z}_2^{2t}$, let

$$\begin{aligned} n_{k,x}(f) = \Big| \big\{ \{x_1, \ldots, x_k\} : x_1, \ldots, x_k \in \mathbf{Z}_2^{2t} \text{ are distinct such that} \\ x_1 \cdots x_k = x \text{ and } m_{x_1} \cdots m_{x_k} \text{ is odd} \big\} \Big|. \end{aligned} \tag{4.4}$$

What we prove here is a result slightly stronger than Theorem 2.1.

Theorem 4.1. *Let $f : \mathbf{Z}_2^{2t} \to \mathbf{Z}_2$ ($t \geq 2$) be a bent function whose lift is given by (4.3). For any $x \in \mathbf{Z}_2^{2t}$, let*

$$\mu(x) = \begin{cases} \nu(m_x), & \text{if } x \neq 0, \\ t - 1, & \text{if } x = 0. \end{cases} \tag{4.5}$$

Then

$$\nu\Big(n_{\mu(x)+1,x}(f) - \frac{1}{2} n_{\mu(x),x}(f) + \cdots + \big(-\frac{1}{2}\big)^{\mu(x)} n_{1,x}(f) \Big) = 0 \text{ for all } x \in \mathbf{Z}_2^{2t}. \tag{4.6}$$

Proof. Choose $l \geq 2\mu(x) + 1$. We have

$$\begin{aligned} \bar{f}^{2^l} = & \sum_{x \in \mathbf{Z}_2^{2t}} \Big(\sum_{\substack{x_1, \ldots, x_{2^l} \in \mathbf{Z}_2^{2t} \\ x_1 \cdots x_{2^l} = x}} m_{x_1} \cdots m_{x_{2^l}} \Big) 1_{F_x} \\ & + \Big[\Big(\sum_{y \in \mathbf{Z}_2^{2t}} m_y - 2^{t-1} \Big)^{2^l} - \Big(\sum_{y \in \mathbf{Z}_2^{2t}} m_y \Big)^{2^l} \Big] 1_{\{0\}}. \end{aligned} \tag{4.7}$$

Then the identity $\bar{f}^{2^l} = \bar{f}$ implies that

$$\begin{cases} \displaystyle\sum_{\substack{x_1, \ldots, x_{2^l} \in \mathbf{Z}_2^{2t} \\ x_1 \cdots x_{2^l} = x}} m_{x_1} \cdots m_{x_{2^l}} = m_x, \quad \text{if } x \neq 0, \\ \displaystyle\sum_{\substack{x_1, \ldots, x_{2^l} \in \mathbf{Z}_2^{2t} \\ x_1 \cdots x_{2^l} = 0}} m_{x_1} \cdots m_{x_{2^l}} + \Big(\sum_{y \in \mathbf{Z}_2^{2t}} m_y - 2^{t-1} \Big)^{2^l} - \Big(\sum_{y \in \mathbf{Z}_2^{2t}} m_y \Big)^{2^l} = -2^{t-1} + m_0. \end{cases} \tag{4.8}$$

From (4.8), one easily sees that

$$\nu\Big(\sum_{\substack{x_1,\dots,x_{2^l}\in\mathbf{Z}_2^{2t}\\ x_1\cdots x_{2^l}=x}} m_{x_1}\cdots m_{x_{2^l}}\Big)=\mu(x)\quad\text{for all } x\in\mathbf{Z}_2^{2t}. \tag{4.9}$$

The sum in (4.9) is

$$\begin{aligned}&\sum_{\substack{x_1,\dots,x_{2^l}\in\mathbf{Z}_2^{2t}\\ x_1\cdots x_{2^l}=x}} m_{x_1}\cdots m_{x_{2^l}}\\ &=\sum_{k\ge1}\sum_{(\lambda_1,\dots,\lambda_k)\vdash 2^l}\frac{2^l!}{\lambda_1!\cdots\lambda_k!}\sum_{(\eta_1,\dots,\eta_k)\sim(\lambda_1,\dots,\lambda_k)}\sum_{\substack{\{x_1,\dots,x_k\}\\ x_1,\dots,x_k\text{ distinct}\\ x_1\cdots x_k=x}} m_{x_1}^{\eta_1}\cdots m_{x_k}^{\eta_k},\end{aligned} \tag{4.10}$$

where $(\lambda_1,\dots,\lambda_k)\vdash 2^l$ means that $(\lambda_1,\dots,\lambda_k)$ is a partition of 2^l, i.e., $1\le\lambda_1\le\cdots\le\lambda_k$ and $\lambda_1+\cdots+\lambda_k=2^l$; $(\eta_1,\dots,\eta_k)\sim(\lambda_1,\dots,\lambda_k)$ means that $(\eta_1,\dots,\eta_k)$ is a permutation of the sequence $(\lambda_1,\dots,\lambda_k)$. We claim that

$$\frac{2^l!}{\eta_1!\cdots\eta_k!}\sum_{\substack{\{x_1,\dots,x_k\}\\ x_1,\dots,x_k\text{ distinct}\\ x_1\cdots x_k=x}} m_{x_1}^{\eta_1}\cdots m_{x_k}^{\eta_k}\equiv\frac{2^l!}{\eta_1!\cdots\eta_k!}n_{k,x}(f)\pmod{2^{\mu(x)+1}}. \tag{4.11}$$

If $\nu(\eta_i)\ge\mu(x)+1$ for all i, we have

$$m_{x_1}^{\eta_1}\cdots m_{x_k}^{\eta_k}\equiv\begin{cases}1 \pmod{2^{\mu(x)+1}}, & \text{if } m_{x_1}\cdots m_{x_k}\text{ is odd},\\ 0 \pmod{2^{\mu(x)+1}}, & \text{if } m_{x_1}\cdots m_{x_k}\text{ is even},\end{cases} \tag{4.12}$$

and (4.11) holds. If $\min_i\nu(\eta_i)\le\mu(x)$, by applying (4.2) to $\eta_1+\cdots+\eta_k=2^l$, we have

$$|\eta_1|_2+\cdots+|\eta_k|_2\ge l-\min_i\nu(\eta_i)+1\ge l-\mu(x)+1. \tag{4.13}$$

Thus by (4.1) and (4.13),

$$\nu\Big(\frac{2^l!}{\eta_1!\cdots\eta_k!}\Big)=-1+|\eta_1|_2+\cdots+|\eta_k|_2\ge l-\mu(x)\ge\mu(x)+1, \tag{4.14}$$

which also implies (4.11).

Now from (4.9), (4.10) and (4.11), we have

$$\mu(x)=\nu\Big(\sum_{k\ge1}n_{k,x}(f)\sum_{(\lambda_1,\dots,\lambda_k)\vdash 2^l}\frac{2^l!}{\lambda_1!\cdots\lambda_k!}\sum_{(\eta_1,\dots,\eta_k)\sim(\lambda_1,\dots,\lambda_k)}1\Big), \tag{4.15}$$

where

$$\begin{aligned}
&\sum_{(\lambda_1,\dots,\lambda_k)\vdash 2^l} \frac{2^l!}{\lambda_1!\cdots\lambda_k!} \sum_{(\eta_1,\dots,\eta_k)\sim(\lambda_1,\dots,\lambda_k)} 1\\
&= \sum_{\substack{\alpha_1,\alpha_2,\cdots\ge 0\\ \alpha_1+2\alpha_2+\cdots=2^l\\ \alpha_1+\alpha_2+\cdots=k}} \frac{2^l!}{(1!)^{\alpha_1}(2!)^{\alpha_2}\cdots}\cdot\frac{k!}{\alpha_1!\alpha_2!\cdots}\\
&= 2^l\cdot\left(\text{the coefficient of } x^{2^l} \text{ in } \Big[\big(\frac{x}{1!}+\frac{x^2}{2!}+\cdots\big)^k=(e^x-1)^k\Big]\right) \qquad (4.16)\\
&= \sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i}i^{2^l}\\
&\equiv \sum_{i \text{ odd}}(-1)^{k-i}\binom{k}{i} \pmod{2^{\mu(x)+1}}\\
&= (-2)^{k-1}.
\end{aligned}$$

Therefore

$$\mu(x)=\nu\Big(\sum_{k\ge 1}(-2)^{k-1}n_{k,x}(f)\Big), \qquad (4.17)$$

and (4.6) follows. □

Proof of Theorem 2.1. Let $f=\sum_{S\subset\{1,\dots,2t\}}a_SX_S$ be the given bent function. Then $g(X_1,\dots,X_{2t})=f(X_1+1,\dots,X_{2t}+1)$ is also bent. Write

$$\bar{g}=-2^{t-1}1_{\{0\}}+\sum_{x\in\mathbf{Z}_2^{2t}}m_x1_{F_x}. \qquad (4.18)$$

Then $\pi(m_x)=a_{\mathrm{supp}(\bar{x})}$ for all $x\in\mathbf{Z}_2^{2t}$, where $\pi:\mathbf{Z}\to\mathbf{Z}_2$ is the canonical map and $\bar{x}=x+(1,\dots,1)$. Thus

$$n_{k,x}(g)=N_{k,\mathrm{supp}(\bar{x})}(f) \quad \text{for all } k\ge 1 \text{ and } x\in\mathbf{Z}_2^{2t}. \qquad (4.19)$$

By Theorem 4.1,

$$\nu\Big(n_{\mu(x)+1,x}(g)-\frac{1}{2}n_{\mu(x),x}(g)+\cdots+\big(-\frac{1}{2}\big)^{\mu(x)}n_{1,x}(g)\Big)=0 \quad \text{for all } x\in\mathbf{Z}_2^{2t}, \qquad (4.20)$$

where

$$\mu(x)=\begin{cases}\nu(m_x)\ge t-|x|, & \text{if } x\ne 0,\\ t-1, & \text{if } x=0.\end{cases} \qquad (4.21)$$

Thus (2.3) follows from (4.19), (4.20) and (4.21). □

5. Affine invariants of Boolean functions on $\mathbf{Z}_2^m$

Let $f=\sum_{S\subset\{1,\dots,m\}}a_SX_S\in\mathcal{P}_m$. For each $k\ge 1$ and $S\subset\{1,\dots,m\}$, define

$$\alpha_{k,S}(f)=\sum_{\substack{\{S_1,\dots,S_k\}\\ S_1,\dots,S_k \text{ distinct}\\ S_1\cup\cdots\cup S_k=S}} a_{S_1}\cdots a_{S_k}=\pi\big(N_{k,S}(f)\big). \qquad (5.1)$$

When $f \in \mathcal{P}_{2t}$ is bent, Corollary 2.2 can be stated as

$$\alpha_{k,S}(f) = 0 \quad \begin{array}{l} \text{if } 2t > |S| \geq \max\{k+t,\ (k-1)\deg f + 1\} \\ \text{or } 2t = |S| \geq \max\{k+t+1,\ (k-1)\deg f + 1\}. \end{array} \tag{5.2}$$

For any invertible affine transformation ϕ of $\mathbf{Z}_2^{2t}$, $f \circ \phi$ is also bent and its coefficients are linear combinations of the coefficients of f. Thus $\alpha_{k,S}(f \circ \phi) = 0$ for k and S satisfying the conditions in (5.2); these are also polynomial equations in the coefficients of f. Are these new equations for the coefficients of f? Unfortunately, the answer is no by the following lemma. However, in answering this question, we have discovered a family of affine invariants of Boolean functions on $\mathbf{Z}_2^m$.

Lemma 5.1. *Let $f \in \mathcal{P}_m$, $\deg f \geq 1$, $k \geq 1$, and $S \subset \{1, \ldots, m\}$ with $|S| > (k-1)\deg f$. Let ϕ be an invertible affine transformation of $\mathbf{Z}_2^m$. Then*

$$\alpha_{k,S}(f \circ \phi) = \sum_{\substack{l,T \\ l \leq k \\ |T| \geq |S| - (k-l)}} c_{l,T}^{k,S} \alpha_{l,T}(f), \tag{5.3}$$

where $c_{l,T}^{k,S} \in \mathbf{Z}_2$ depends only on k, S, l, T and ϕ.

Proof. Let

$$f = \sum_{S \subset \{1,\ldots,m\}} a_S X_S, \tag{5.4}$$

$$f \circ \phi = \sum_{S \subset \{1,\ldots,m\}} b_S X_S. \tag{5.5}$$

It suffices to prove (5.3) in two cases: 1. $f \circ \phi = f(X_1 + X_2, X_2, \ldots, X_m)$ and 2. $f \circ \phi = f(X_1 + 1, X_2, \ldots, X_m)$.

Case 1. $f \circ \phi = f(X_1 + X_2, X_2, \ldots, X_m)$. Clearly,

$$b_S = \begin{cases} a_S + a_{(S \cup \{1\}) \setminus \{2\}} + a_{S \cup \{1\}}, & \text{if } 1 \notin S,\ 2 \in S, \\ a_S, & \text{otherwise.} \end{cases} \tag{5.6}$$

Let $\mathcal{P}$ be the power set of $\{1, \ldots, m\}$. For each $\mathcal{S} \subset \mathcal{P}$, let $a_{\mathcal{S}} = \prod_{S \in \mathcal{S}} a_S$ and $b_{\mathcal{S}} = \prod_{S \in \mathcal{S}} b_S$. Also let $\mathcal{Q}$ be the power set of $\{3, \ldots, m\}$. For each $U \in \mathcal{Q}$ and $\mathcal{U} \subset \mathcal{Q}$, let $U^1 = U \cup \{1\}$ and $\mathcal{U}^1 = \{U^1 : U \in \mathcal{U}\}$. The definitions of U^2, U^{12}, $\mathcal{U}^2$, $\mathcal{U}^{12}$ are similar.

Now fix $k \geq 1$, $S \subset \mathcal{P}$ such that $|S| > (k-1)\deg f$.

Case 1.1. $2 \notin S$. Then $\alpha_{k,S}(f \circ \phi) = \alpha_{k,S}(f)$.

Case 1.2. $1 \notin S$ but $2 \in S$; say $S = T^2$ where $T \in \mathcal{Q}$. We have

$$\alpha_{k,S}(f \circ \phi) = \sum_{\substack{\mathcal{S} \subset \mathcal{P} \\ |\mathcal{S}| = k \\ \bigcup \mathcal{S} = S}} b_{\mathcal{S}} = \sum_{\substack{\mathcal{U}, \mathcal{V} \subset \mathcal{Q} \\ |\mathcal{U}| + |\mathcal{V}| = k,\ \bigcup(\mathcal{U} \cup \mathcal{V}) = T \\ |\mathcal{V}| > 0}} a_{\mathcal{U}} b_{\mathcal{V}^2}, \tag{5.7}$$

where, by (5.6),

$$b_{\mathcal{V}^2} = \sum_{\substack{\mathcal{X}, \mathcal{Y}, \mathcal{Z} \text{ disjoint} \\ \mathcal{X} \cup \mathcal{Y} \cup \mathcal{Z} = \mathcal{V}}} a_{\mathcal{X}^1} a_{\mathcal{Y}^2} a_{\mathcal{Z}^{12}}. \tag{5.8}$$

Thus

$$\alpha_{k,S}(f\circ\phi)=\sum_{\substack{\mathcal{U},\mathcal{X},\mathcal{Y},\mathcal{Z}\subset\mathcal{Q}\\ |\mathcal{U}|+|\mathcal{X}|+|\mathcal{Y}|+|\mathcal{Z}|=k,\bigcup(\mathcal{U}\cup\mathcal{X}\cup\mathcal{Y}\cup\mathcal{Z})=T\\ \mathcal{X},\mathcal{Y},\mathcal{Z}\text{ disjoint},|\mathcal{X}|+|\mathcal{Y}|+|\mathcal{Z}|>0}} a_{\mathcal{U}}a_{\mathcal{X}^1}a_{\mathcal{Y}^2}a_{\mathcal{Z}^{12}}. \tag{5.9}$$

However, if $\mathcal{X},\mathcal{Y},\mathcal{Z}$ are not pairwise disjoint and $\mathcal{U},\mathcal{X},\mathcal{Y},\mathcal{Z}$ satisfy all other conditions in the sum in (5.9), one can see that $a_{\mathcal{U}}a_{\mathcal{X}^1}a_{\mathcal{Y}^2}a_{\mathcal{Z}^{12}}=0$ using the fact $|S|>(k-1)\deg f$. Therefore,

$$\begin{aligned}\alpha_{k,S}(f\circ\phi)&=\sum_{\substack{\mathcal{U},\mathcal{X},\mathcal{Y},\mathcal{Z}\subset\mathcal{Q}\\ |\mathcal{U}|+|\mathcal{X}|+|\mathcal{Y}|+|\mathcal{Z}|=k\\ \bigcup(\mathcal{U}\cup\mathcal{X}\cup\mathcal{Y}\cup\mathcal{Z})=T\\ |\mathcal{X}|+|\mathcal{Y}|+|\mathcal{Z}|>0}} a_{\mathcal{U}}a_{\mathcal{X}^1}a_{\mathcal{Y}^2}a_{\mathcal{Z}^{12}}\\ &=\alpha_{k,T^{12}}(f)+\alpha_{k,T^1}(f)+\alpha_{k,T^2}(f).\end{aligned} \tag{5.10}$$

Case 1.3. $1,2\in S$; say $S=T^{12}$ where $T\in\mathcal{Q}$. We have

$$\begin{aligned}\alpha_{k,S}(f\circ\phi)&=\sum_{\substack{\mathcal{S}\subset\mathcal{P}\\ |\mathcal{S}|=k\\ \bigcup\mathcal{S}=S}} b_{\mathcal{S}}\\ &=\sum_{\substack{\mathcal{U},\mathcal{V},\mathcal{W},\mathcal{T}\subset\mathcal{Q}\\ |\mathcal{U}|+|\mathcal{V}|+|\mathcal{W}|+|\mathcal{T}|=k\\ \bigcup(\mathcal{U}\cup\mathcal{V}\cup\mathcal{W}\cup\mathcal{T})=T\\ |\mathcal{V}|+|\mathcal{W}|>0,|\mathcal{T}|+|\mathcal{W}|>0}} a_{\mathcal{U}}a_{\mathcal{V}^1}a_{\mathcal{W}^{12}}b_{\mathcal{T}^2}\\ &=\sum_{\substack{\mathcal{U},\mathcal{V},\mathcal{W},\mathcal{X},\mathcal{Y},\mathcal{Z}\subset\mathcal{Q}\\ |\mathcal{U}|+\cdots+|\mathcal{Z}|=k,\bigcup(\mathcal{U}\cup\cdots\cup\mathcal{Z})=T\\ \mathcal{X},\mathcal{Y},\mathcal{Z}\text{ disjoint}\\ |\mathcal{V}|+|\mathcal{W}|>0,|\mathcal{X}|+|\mathcal{Y}|+|\mathcal{Z}|+|\mathcal{W}|>0}} a_{\mathcal{U}}a_{\mathcal{V}^1}a_{\mathcal{W}^{12}}a_{\mathcal{X}^1}a_{\mathcal{Y}^2}a_{\mathcal{Z}^{12}}.\end{aligned} \tag{5.11}$$

In the last sum of (5.11), $a_{\mathcal{U}}a_{\mathcal{V}^1}a_{\mathcal{W}^{12}}a_{\mathcal{X}^1}a_{\mathcal{Y}^2}a_{\mathcal{Z}^{12}}=0$ when $\mathcal{X},\mathcal{Y},\mathcal{Z}$ are not pairwise disjoint, since $|S|>(k-1)\deg f$. Thus

$$\begin{aligned}&\alpha_{k,S}(f\circ\phi)\\ &=\sum_{\substack{\mathcal{U},\mathcal{V},\mathcal{W},\mathcal{X},\mathcal{Y},\mathcal{Z}\subset\mathcal{Q}\\ |\mathcal{U}|+\cdots+|\mathcal{Z}|=k,\bigcup(\mathcal{U}\cup\cdots\cup\mathcal{Z})=T\\ |\mathcal{V}|+|\mathcal{W}|>0,|\mathcal{X}|+|\mathcal{Y}|+|\mathcal{Z}|+|\mathcal{W}|>0}} a_{\mathcal{U}}a_{\mathcal{V}^1}a_{\mathcal{W}^{12}}a_{\mathcal{X}^1}a_{\mathcal{Y}^2}a_{\mathcal{Z}^{12}}\\ &=\sum_{\substack{\mathcal{U},\mathcal{V},\mathcal{W},\mathcal{X},\mathcal{Y},\mathcal{Z}\\ |\mathcal{U}|+\cdots+|\mathcal{Z}|=k\\ \bigcup(\mathcal{U}\cup\cdots\cup\mathcal{Z})=T}} a_{\mathcal{U}}a_{\mathcal{V}^1}a_{\mathcal{W}^{12}}a_{\mathcal{X}^1}a_{\mathcal{Y}^2}a_{\mathcal{Z}^{12}}+\sum_{\substack{\mathcal{U},\mathcal{X},\mathcal{Y},\mathcal{Z}\\ |\mathcal{U}|+|\mathcal{X}|+|\mathcal{Y}|+|\mathcal{Z}|=k\\ \bigcup(\mathcal{U}\cup\mathcal{X}\cup\mathcal{Y}\cup\mathcal{Z})=T}} a_{\mathcal{U}}a_{\mathcal{X}^1}a_{\mathcal{Y}^2}a_{\mathcal{Z}^{12}}\\ &\quad+\sum_{\substack{\mathcal{U},\mathcal{V}\\ |\mathcal{U}|+|\mathcal{V}|=k\\ \bigcup(\mathcal{U}\cup\mathcal{V})=T}} a_{\mathcal{U}}a_{\mathcal{V}^1}+\sum_{\substack{\mathcal{U}\\ |\mathcal{U}|=k,\bigcup\mathcal{U}=T}} a_{\mathcal{U}}\\ &=\sum_{\substack{\mathcal{U},\mathcal{X},\mathcal{Y},\mathcal{Z}\\ |\mathcal{U}|+2|\mathcal{X}|+|\mathcal{Y}|+2|\mathcal{Z}|=k\\ \bigcup(\mathcal{U}\cup\mathcal{X}\cup\mathcal{Y}\cup\mathcal{Z})=T}} a_{\mathcal{U}}a_{\mathcal{X}^1}a_{\mathcal{Y}^2}a_{\mathcal{Z}^{12}}+\alpha_{k,T^{12}}(f)+\alpha_{k,T^2}(f)+\alpha_{k,T}(f).\end{aligned} \tag{5.12}$$

In the last $\sum$ of (5.12), $a_{\mathcal{U}}a_{\mathcal{X}^1}a_{\mathcal{Y}^2}a_{\mathcal{Z}^{12}}=0$ unless $|\mathcal{X}|=|\mathcal{Z}|=0$ or $|\mathcal{X}|=1$ but $|\mathcal{Y}|=|\mathcal{Z}|=0$. (This again follows from $|S|>(k-1)\deg f$.) Therefore,

$$\begin{aligned}\alpha_{k,S}(f\circ\phi)&=\sum_{\substack{\mathcal{U},\mathcal{X}\\ |\mathcal{U}|+|\mathcal{X}|=k-1,\ \bigcup(\mathcal{U}\cup\mathcal{X})=T\\ |\mathcal{X}|=1}} a_{\mathcal{U}}a_{\mathcal{X}^1}+\sum_{\substack{\mathcal{U},\mathcal{Y}\\ |\mathcal{U}|+|\mathcal{Y}|=k\\ \bigcup(\mathcal{U}\cup\mathcal{Y})=T}} a_{\mathcal{U}}a_{\mathcal{Y}^2}\\ &\quad+\alpha_{k,T^{12}}(f)+\alpha_{k,T^2}(f)+\alpha_{k,T}(f)\\ &=\sum_{\substack{\mathcal{U},\mathcal{X}\\ |\mathcal{U}|+|\mathcal{X}|=k-1,\ \bigcup(\mathcal{U}\cup\mathcal{X})=T\\ |\mathcal{X}|=1}} a_{\mathcal{U}}a_{\mathcal{X}^1}+\alpha_{k,T^{12}}(f)\\ &=\sum_{\substack{\mathcal{U},\mathcal{X}\\ |\mathcal{U}|+|\mathcal{X}|=k-1,\ \bigcup(\mathcal{U}\cup\mathcal{X})=T\\ |\mathcal{X}|>0}} a_{\mathcal{U}}a_{\mathcal{X}^1}+\alpha_{k,T^{12}}(f)\\ &\quad(\text{in the }\textstyle\sum,\ a_{\mathcal{U}}a_{\mathcal{X}^1}=0\text{ when }|\mathcal{X}|>1)\\ &=\alpha_{k-1,T^1}(f)+\alpha_{k,T^{12}}(f).\end{aligned}\tag{5.13}$$

Case 2. $f\circ\phi=f(X_1+1,X_2,\dots,X_m)$. In a similar way, one can show that

$$\alpha_{k,S}(f\circ\phi)=\begin{cases}\alpha_{k,S}(f), & \text{if } 1\in S,\\ \alpha_{k,S}(f)+\alpha_{k,S\cup\{1\}}(f), & \text{if } 1\notin S.\end{cases}\tag{5.14}$$

□

Definition 5.2. Let $f\in\mathcal{P}_m$ with $\deg f\ge 1$. Define $d_1(f)=\deg f$; for each $k>1$, define

$$\begin{aligned}d_k(f)=\min\big\{&d: d\ge(k-1)\deg f,\ d>d_{k-1}(f),\\ &\text{and } \alpha_{k,S}(f)=0 \text{ for all } S\subset\{1,\dots,m\} \text{ with } |S|>d\big\}.\end{aligned}\tag{5.15}$$

Of course, when $\max\{(k-1)\deg f,\ d_{k-1}(f)+1\}\ge m$, $d_k(f)$ stops carrying any new information.

Corollary 5.3. *Let $f\in\mathcal{P}_m$ with $\deg f\ge 1$ and let ϕ be an invertible affine transformation of $\mathbf{Z}_2^m$. Then $d_k(f\circ\phi)=d_k(f)$ for all $k\ge 1$. Namely, $d_k(f)$ is an affine invariant of f.*

Proof. The conclusion is immediate using Lemma 5.1 and induction. □

Example 5.4. Let $f=X_1X_2X_3+X_2X_4X_5+X_1X_8+X_2X_7+X_3X_6+X_4X_8+X_5X_6\in\mathcal{P}_8$. Then $d_1(f)=3$, $d_2(f)=5$, $d_3(f)=6$.

Two functions $f,g\in\mathcal{P}_m$ are called affinely equivalent if $g=f\circ\phi$ for some invertible affine transformation ϕ of $\mathbf{Z}_2^m$. Affine classifications of elements in various subsets and quotient sets of $\mathcal{P}_m$ are important problems in coding theory. However, these are very difficult problems with only a few results ([1], [9], [10], [17]). One of the difficulties here is the lack of good affine invariants for Boolean functions. The affine invariants introduced in this paper could be valuable new tools in the study of the classification problems. In the following example, we observe that in some cases, the new invariants can separate affine equivalence classes of Boolean functions easily while other invariants fail.

Example 5.5. For $f\in\mathcal{P}_m$, $a\in\mathbf{Z}_2^m$, define

$$D_af=f\big((X_1,\cdots,X_m)+a\big)-f(X_1,\cdots,X_m).$$

A bent function of the form

$$X_1P_1(Y) + \cdots + X_tP_t(Y) + Q(Y) \in \mathcal{P}_{2t} \tag{5.16}$$

is called a Maiorana-McFarland (MM) bent function, where $Y = (X_{t+1}, \cdots, X_{2t})$. There are bent functions that are not affinely equivalent to any MM bent function, but previous proofs of such nonequivalence are either ad hoc or complicated ([7], [13]). If a function $f \in \mathcal{P}_{2t}$ is affinely equivalent to a function of the form (5.16), then so is D_af for all $a \in \mathbf{Z}_2^{2t}$. Then clearly, $d_2(D_af) \leq t + 2$. There are bent functions of the form $f = X_{2t}A(X_1, \cdots, X_{2t-1}) + B(X_1, \cdots, X_{2t-1}) \in \mathcal{P}_{2t}$, where $A(X_1, \cdots, X_{2t-1}) = X_1 \cdots X_{t-1} + X_t \cdots X_{2t-2} +$ terms of lower degrees. (Cf. the examples of [13].) For such a bent function, $D_af = A(X_1, \cdots, X_{2t-1})$ with $a = (0, \cdots, 0, 1)$, and $d_2(D_af) = 2t - 2$. Thus when $t > 4$, such a bent function is not affinely equivalent to any MM bent function.

References

1. E. Berlekamp and L. R. Welch, *Weight distribution of the cosets of the (32,6) Reed-Muller code*, IEEE Trans. Inform. Theory **18** (1972), 203–207. MR **52:**16844
2. C. Carlet, *Two new classes of bent functions*, Lecture Notes in Computer Science **765**, Springer-Verlag, Berlin, 1994, 77–101. MR **95f:**94016
3. C. Carlet, *Generalized partial spreads*, IEEE Trans. Inform. Theory **41** (1995), 1482–1487. MR **97b:**94043
4. C. Carlet, *A construction of bent functions*, London Math. Soc. Lecture Series **233**, Cambridge Univ. Press, 1996, 47–58. MR **97k:**94081
5. C. Carlet and P. Guillot, *A characterization of binary bent functions*, J. Combin. Theory Ser A **76** (1996), 328–335. MR **99b:**94054
6. H. Chung and P. V. Kummar, *A new general construction for generalized bent functions*, IEEE Trans. Inform. Theory **35** (1989), 206–209. CMP 21:12
7. J. F. Dillon, *Elementary Hadamard Difference Sets*, Ph.D. Thsis, Univ. of Maryland, 1974.
8. H. Dobbertin, *Constructions of bent functions and balanced Boolean functions with high nonlinearity*, Lecture Notes in Computer Science **1008**, Springer-Verlag, Berlin, 1995, 61–74.
9. X. Hou, $AGL(m, 2)$ *acting on* $R(r, m)/R(s, m)$, J. Algebra **171** (1995), 921–938. MR **96j:**94023
10. X. Hou, $GL(m, 2)$ *acting on* $R(r, m)/R(r - 1, m)$, Discrete Math. **149** (1996), 99–122. MR **97g:**94030
11. X. Hou, *q-ary bent functions constructed from chain rings*, Finite Fields Appl. **4** (1998), 55–61. CMP 98:09
12. X. Hou, *Cubic bent functions*, Discrete Math. **189** (1998), 149–161.
13. X. Hou, *New constructions of bent functions*, J. Statistical Planning and Inference, to appear.
14. X. Hou and P. Langevin, *Results on bent functions*, J. Combin. Theory Ser A **80** (1997), 232–246. MR **99b:**05025
15. P. V. Kumar, R. A. Scholtz and L. R. Welch, *Generalized bent functions and their properties*, J. Combin. Theory Ser A **40** (1985), 90–107. MR **87i:**05075
16. P. Langevin, *On generalized bent functions*, CISM Courses and Lectures **339**, Springer-Verlag, Wien, 1992, 147–157. MR **95d:**11166
17. J. Maiorana, *A classification of the cosets of the Reed-Muller code* $R(1, 6)$, Math. Comp. **57** (1991), 403–414. MR **91j:**94023
18. R. L. McFarland, *A family of difference sets in noncyclic groups*, J. Combin. Theory Ser A **15** (1973), 1–10. MR **47:**3198
19. O. S. Rothaus, *On "bent" functions*, J. Combin. Theory Ser A **20** (1976), 300–305. MR **53:**7797

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

E-mail address: xhou@euler.math.wright.edu