Bull. Korean Math. Soc. **60** (2023), No. 3, pp. 561–574
https://doi.org/10.4134/BKMS.b210374
pISSN: 1015-8634 / eISSN: 2234-3016

MACWILLIAMS-TYPE IDENTITIES ON VECTORIAL BOOLEAN FUNCTIONS WITH BENT COMPONENTS AND APPLICATIONS

Jong Yoon Hyun

Abstract. In this paper, we focus on establishing the MacWilliams-type identities on vectorial Boolean functions with bent component functions. As their applications, we provide a bound for the non-existence of vectorial dual-bent functions with prescribed minimum degree, and several Gleason-type theorems are presented as well.

1. Introduction

Bent functions, discovered by Rothaus [15], are Boolean functions with maximum possible non-linearity, equivalently the Walsh transform of a bent function in n variables has exactly two values $\pm 2^{n/2}$. Over the last four decades, they have been actively studied due to their considerably important role in coding theory as well as in cryptography. A survey on bent functions can be found in [1, 5, 12].

A vectorial Boolean function is a vector-valued Boolean function. The bentness of Boolean functions has been generalized to vectorial Boolean functions, called vectorial bent, which states that all the nonzero linear combinations of its coordinate functions are bent. Based on Maiorana-McFarland and partial spread bent functions, vectorial bent functions were initially constructed by Nyberg [13]. For further constructions of vectorial bent functions, we refer to [4], and a survey on bent vectorial bent functions can be found in [2, 12].

Recently, the authors of [6] introduced a new notion for a vectorial dual of a vectorial bent function and suggested some notions of self-duality for vectorial bent functions. This concept of a vectorial dual which is not unique in general is a generalization of the dual of a bent function. They also investigated the duality for a class of vectorial Maiorana-McFarland bent functions.

Received May 10, 2021; Revised July 16, 2022; Accepted March 2, 2023.
2010 *Mathematics Subject Classification.* 94B05, 94B25, 94C10, 06E30.
Key words and phrases. Extended Walsh transform, vectorial Boolean function, vectorial dual-bent function, MacWilliams-type identity, Gleason-type theorem.
This paper was supported by Konkuk University in 2020.

There is a connection between a linear code and its dual with respect to their the weight enumerators, called the MacWilliams identity [10]. The Gleason theorem [10] on self-dual linear codes is obtained by using the MacWilliams identity and invariant theory to prove that the weight enumerators of self-dual linear codes lie in the ring generated by X^2+Y^2 and $XY-Y^2$ over the complex numbers. On the other hand, in [8], they presented the MacWilliams-type identity between a self-dual bent function and its dual, and then Gleason-type theorem on self-dual bent functions was obtained. Furthermore, to derive a bound for the non-existence of a bent function with given minimum degree (see Definition 2.1 below), they used the MacWilliams-type identity in [9] between a self-dual bent function and its dual. Those bound has some analogy with the result in [11, 17], which states that for any non-negative integer k, there exists a positive integer N such that for $n \geq N$ there exist no homogeneous bent $(2n, 1)$-functions having algebraic degree $n-k$ or more, where N is the least integer satisfying

$$\binom{N}{1} + \cdots + \binom{N}{k+1} < 2^{N-1} - 1.$$

In this paper, we employ the vectorial Boolean functions with bent component functions to extend all results as mentioned previously.

The organization of this paper is as follows. In Section 2, we introduce basic concepts on vectorial Boolean functions; extended Walsh transform, the minimum degree of it (Definition 2.1), a dual of a vectorial bent function (Definition 2.3), and so on. In Section 3, we provide useful lemmas in deriving the MacWilliams-type identities on vectorial Boolean functions with bent component functions. In Section 4, we focus on the establishments (Theorems 4.1 and 4.4) to the MacWilliams-type identities on vectorial Boolean functions with bent component functions. As their applications, Section 5 includes two subsections. In the first subsection, we prove (Theorem 5.2) the non-existence of vectorial dual-bent functions with given minimum degree. In the second subsection, various Gleason-type theorems (Theorems 5.7 and 5.8) are presented.

2. Preliminaries

Throughout all sections, m and n are positive integers, and by 0 we denote the zero vector with appropriate length.

Let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements and let $\mathbb{F}_2^n$ be an n-dimensional vector space over $\mathbb{F}_2$. By $\mathbb{F}_2^{n*}$ we mean the set of non-zero elements of $\mathbb{F}_2^n$. The (Hamming) weight $|u|$ of $u \in \mathbb{F}_2^n$ is the number of non-zero coordinate positions. The weight enumerator $W_C(X, Y)$ of a subset C of $\mathbb{F}_2^n$ is defined as $W_C(X, Y) = \sum_{i=0}^{n} A_i(C)X^{n-i}Y^i$, where $A_i(C)$ is the number of vectors in C of weight i.

We say that a function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ is a (vectorial) (n, m)-function (or, vectorial Boolean function), and in particular, an $(n, 1)$-function is called a Boolean function. The algebraic normal form (ANF) of a Boolean function f on $\mathbb{F}_2^n$ is

$$f(x_1,\dots,x_n)=\sum_{a\in\mathbb{F}_2^n} t_a x_1^{a_1}\cdots x_n^{a_n},\ a=(a_1,\dots,a_n) \text{ and } t_a\in\mathbb{F}_2.$$

The algebraic degree of a Boolean function f is the number of variables in the highest order term with nonzero coefficient.

Any (n,m)-function F can be expressed by

$$F(x)=(f_1(x),\dots,f_m(x)),\ x=(x_1,\dots,x_n)\in\mathbb{F}_2^n,$$

where f_j's are $(n,1)$-functions, called the coordinate functions of F. For $b\in\mathbb{F}_2^{m*}$, we call $b_1f_1(x)+\cdots+b_mf_m(x)$ the component function of F. We define a subset $D_{F,b}$ for $b\in\mathbb{F}_2^m$ of $\mathbb{F}_2^n$ as

$$D_{F,b}=\{x\in\mathbb{F}_2^n : F(x)\in\langle b\rangle^{\perp}\}.$$

Notice that $D_{f,1}$ for an $(n,1)$-function f equals $f^{-1}(0)$ being the pre-image of 0 under f.

The character sum $\chi_a(C)$ for $a\in\mathbb{F}_2^n$ and $C\subseteq\mathbb{F}_2^n$ is defined as

$$\chi_a(C)=\sum_{x\in C}(-1)^{a\cdot x},$$

where the dot is the standard inner product defined by $a\cdot x=a_1x_1+\cdots+a_nx_n \pmod 2$.

The Walsh transform S_f of a Boolean function f on $\mathbb{F}_2^n$ is an integer-valued function such that

$$S_f(a)=\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+a\cdot x}.$$

An $(n,1)$-function f is bent if $S_f(a)^2=2^n$ for any $a\in\mathbb{F}_2^n$. In this case, n is even, and $S_f(a)$ can be written as $S_f(a)=(-1)^{f^*(a)}2^{\frac{n}{2}}$ for some $(n,1)$-function f^*, called the dual of f. It is known that f^* is also bent and $f^{**}=f$. A bent function f is self-dual if $f=f^*$.

The extended Walsh transform S_F of an (n,m)-function $F=(f_1,\dots,f_m)$ is an integer-valued function of $\mathbb{F}_2^n\times\mathbb{F}_2^m$ such that

$$S_F(a,b)=\sum_{x\in\mathbb{F}_2^n}(-1)^{b\cdot F(x)+a\cdot x},$$

and thus we have that $S_{b\cdot F}(a)=S_F(a,b)$ for any $a\in\mathbb{F}_2^n$ and $b\in\mathbb{F}_2^m$.

The inversion formula of an (n,m)-function F is then

$$(-1)^{b\cdot F(a)}=\frac{1}{2^n}\sum_{x\in\mathbb{F}_2^n}S_F(x,b)(-1)^{a\cdot x}.$$

This shows that every (n,m)-function is uniquely determined by its extended Walsh transform.

We say that an (n, m)-function F is vectorial bent if $S_{b\cdot F}(a)^2 = 2^n$ for any $a \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2^{m*}$. Equivalently, every component function $b \cdot F$ of F for $b \in \mathbb{F}_2^{m*}$ is bent. In this case, it is known [14] that $m \leq n/2$. We can write $S_{b\cdot F}(a)$ as $S_{b\cdot F}(a) = (-1)^{(b\cdot F)^*(a)} 2^{\frac{n}{2}}$ for any $a \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2^{m*}$. In the framework of finite fields, $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is a vectorial bent (n, m)-function if the component function $F_\alpha : \mathbb{F}_{2^n} \to \mathbb{F}_2$ defined by $F_\alpha(x) = \mathrm{Tr}_m(\alpha F(x))$ is bent for all non-zero $\alpha \in \mathbb{F}_{2^m}$. Here, Tr_m is the absolute trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ defined by $\mathrm{Tr}_m(x) = \sum_{i=0}^{m-1} x^{2^i}$.

By $\mathcal{BC}_F$ (resp., $\mathcal{BC}_F^*$) we denote the set of bent (resp., dual-bent) component functions of an (n, m)-function F. Let $b \in \mathbb{F}_2^{m*}$ and let F be an (n, m)-function with bent component functions. For $b \cdot F \in \mathcal{BC}_F$, we define a subset $\mathcal{D}(b \cdot F)$ of the (n, m)-functions by $\mathcal{D}(b \cdot F) = \{G : \mathbb{F}_2^n \to \mathbb{F}_2^m : b \cdot G = (b \cdot F)^*\}$. If $G \in \mathcal{D}(b \cdot F)$, then $S_{b\cdot G}(a) = (-1)^{(b\cdot G)^*(a)} 2^{\frac{n}{2}} = (-1)^{b\cdot F(a)} 2^{\frac{n}{2}}$ for any $a \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2^{m*}$.

We define a subset M_f of $\mathbb{F}_2^n$ for a Boolean function f in n variables by

$$M_f = \{(a_1, \ldots, a_n) \in \mathbb{F}_2^n : x_1^{a_1} \cdots x_n^{a_n} \text{ is a monomial term in the ANF of } f\}.$$

Definition 2.1. (i) Let f be an $(n, 1)$-function. The minimum degree $\mathrm{mdeg}(f)$ of f is the minimum weight of M_f.

(ii) Let F be an (n, m)-function. The minimum degree $\mathrm{mdeg}(F)$ of F is the minimum value among the minimum degrees of coordinate functions of F.

Homogeneous Boolean functions (see [17]) and rotational symmetric Boolean functions (see [16]) of algebraic degree k are of minimum degree k.

Let F be a vectorial bent (n, m)-function. Then $\mathcal{BC}_F$ together with zero function forms an m-dimensional vector space and $\mathcal{BC}_F$ consists of bent functions. Motivated by this, the dual concept of a vectorial bent function is first introduced by [6]. Before stating the notion of vectorial dual-bent, we provide the following lemma whose proof can be readily verified.

Lemma 2.2. *Let F be a vectorial (n, m)-function. Then the linear span of $\mathcal{BC}_F$ is an m-dimensional vector space if and only if the linear span of $F(\mathbb{F}_2^n)$ is the ambient space $\mathbb{F}_2^m$.*

Definition 2.3 ([6])**.** Let F be a vectorial bent (n, m)-function. We say that F is a vectorial dual-bent function if $\mathcal{BC}_F^* = \{(b \cdot F)^* : b \in \mathbb{F}_2^{m*}\}$ together with zero function forms an m-dimensional vector space and $\mathcal{BC}_F^*$ consists of bent functions. We can write the linear span of $\mathcal{BC}_F^*$ as $\langle g_1^*, \ldots, g_m^* \rangle$. The dual F^* of F is then defined by $F^* = (g_1^*, \ldots, g_m^*)$. For a vectorial dual-bent F, we say that F is self-dual if $\mathcal{BC}_F = \mathcal{BC}_F^*$.

We point out the following remarks in importance and refer to [6] for more information:

(i) the dual F^* of F relies on the choice of basis for $\langle \mathcal{BC}_F^* \rangle$ being the linear span of $\mathcal{BC}_F^*$;

(ii) it is not necessarily true that if f and g are bent, then $f^* + g*$ is bent as well, and so every vectorial bent function is not necessarily vectorial dual-bent;

(iii) there is an invertible matrix A with entries from $\mathbb{F}_2$ satisfying $F = F^{**}A$;

(iv) the dual of coordinate functions of F is not necessarily basis for the space of F^*.

We list two families of vectorial dual-bent functions which can be applied to our main results.

Remark 2.4 ([3,6]). Consider a vectorial Maiorana-McFarland bent function F from $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ defined by $F(x,y) = xy$. Then $F_\alpha(x,y) = \mathrm{Tr}_m(\alpha xy)$ for $\alpha \in \mathbb{F}_{2^m}^*$ are bent component functions of F with dual-bents $(F_\alpha)^*(x,y) = \mathrm{Tr}_m(xy/\alpha)$ for $\alpha \in \mathbb{F}_{2^m}^*$, so that F is vectorial dual-bent. Furthermore, we have that $\{F_\alpha : \alpha \in \mathbb{F}_{2^n}^*\} = \{(F_\alpha)^* : \alpha \in \mathbb{F}_{2^n}^*\}$, and so F is a vectorial self-dual bent function.

A Boolean function is balanced if its Walsh transform at the zero vector is the zero. A vectorial Boolean function is balanced if all of its component functions are balanced.

Let $s \le n$ and let $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^s}$ be a balanced function with $G(0) = 0$. Let $y/x = 0$ if $x = 0$ by convention. Then $F : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_{2^s}$ defined as $F(x,y) = G(y/x)$ is vectorial dual-bent with $(F_\alpha)^*(x,y) = \mathrm{Tr}_\mathrm{s}(\alpha G(x/y))$ for all non-zero $\alpha \in \mathbb{F}_{2^s}$. Under the additional condition on G that $G(\alpha) = G(1/\alpha)$ for all non-zero $\alpha \in \mathbb{F}_{2^s}$, we obtain that $F_\alpha = (F_\alpha)^*$. This shows that F is vectorial self-dual and has an interesting property that $(F^*)_\alpha = (F_\alpha)^*$ for all non-zero $\alpha \in \mathbb{F}_{2^s}$, namely, F is component-wise self-dual bent.

3. Auxiliary results

This section includes the helpful results to derive two types of MacWilliams identities on vectorial Boolean functions with bent component functions.

Lemma 3.1. *Let F be an (n,m)-function. Then for all $c \in \mathbb{F}_2^m$, we have that*

$$\sum_{b\in\mathbb{F}_2^m} S_{b\cdot(c+F)}(a) = 2^m \chi_a(F^{-1}(c)),$$

where $(c+F)(x) = c + F(x)$.

Proof. The result follows from that

$$\begin{aligned}\sum_{b\in\mathbb{F}_2^m} S_{b\cdot(c+F)}(a) &= \sum_{b\in\mathbb{F}_2^m}\sum_{x\in\mathbb{F}_2^n} (-1)^{b\cdot(c+F(x))+a\cdot x}\\ &= \sum_{x\in\mathbb{F}_2^n}(-1)^{a\cdot x}\sum_{b\in\mathbb{F}_2^m}(-1)^{b\cdot(c+F(x))} = 2^m\sum_{x\in\mathbb{F}_2^n}(-1)^{a\cdot x}\delta_{c,F(x)},\end{aligned}$$

where δ is the Kronecker delta function. □

The MacWilliams transform of a subset C of $\mathbb{F}_2^n$ is presented in a polynomial version. See [7, Lemma 2.1] or [10].

Lemma 3.2 ([7], [10])**.** *Let C be a subset of $\mathbb{F}_2^n$. Then*

$$\sum_{a\in\mathbb{F}_2^n} \chi_a(C)X^{n-|a|}Y^{|a|} = W_C(X+Y, X-Y).$$

Lemma 3.3. *Let F be an (n,m)-function. Then for all $b \in \mathbb{F}_2^{m*}$,*

$$\sum_{a\in\mathbb{F}_2^n} S_{b\cdot F}(a)X^{n-|a|}Y^{|a|} = -2^nX^n + 2W_{D_{F,b}}(X+Y, X-Y).$$

Proof. We have that

$$\begin{aligned} S_{b\cdot F}(a) &= \sum_{x\in\mathbb{F}_2^n} (-1)^{b\cdot F(x)+a\cdot x} \\ &= \sum_{x\in\mathbb{F}_2^n} (1-2b\cdot F(x))(-1)^{a\cdot x} \\ &= 2^n\delta_{0,a} - 2\sum_{x\in\mathbb{F}_2^n} b\cdot F(x)(-1)^{a\cdot x} \\ &= 2^n\delta_{0,a} - 2\sum_{x\in\mathbb{F}_2^n, b\cdot F(x)=1} (-1)^{a\cdot x} \\ &= 2^n\delta_{0,a} - 2\left(2^n\delta_{0,a} - \sum_{x\in\mathbb{F}_2^n, b\cdot F(x)=0} (-1)^{a\cdot x}\right). \end{aligned}$$

Since $\sum_{x\in\mathbb{F}_2^n, b\cdot F(x)=0}(-1)^{a\cdot x} = \chi_a(D_{F,b})$, we get that

$$S_{b\cdot F}(a) = -2^n\delta_{0,a} + 2\chi_a(D_{F,b}).$$

Using this and Lemma 3.2, we have that

$$\begin{aligned} \sum_{a\in\mathbb{F}_2^n} S_{b\cdot F}(a)X^{n-|a|}Y^{|a|} &= \sum_{a\in\mathbb{F}_2^n} (-2^n\delta_{0,a} + 2\chi_a(D_{F,b}))X^{n-|a|}Y^{|a|} \\ &= -2^nX^n + 2W_{D_{F,b}}(X+Y, X-Y), \end{aligned}$$

and the proof is completed. □

It is demonstrated [8, Proposition 2.5] that MacWilliams-type duality holds between a bent function and its dual.

Observe that $D_{f,1} = f^{-1}(0)$ and $W_{D_{f,1}}(X,Y) + W_{D_{f,0}}(X,Y) = (X+Y)^n$ for all Boolean function f in n variables. The following result thus follows from [8, Proposition 2.5].

Lemma 3.4 ([8])**.** *Let f be a bent $(n,1)$-function, and let f^* be its dual bent. Then*

$$W_{D_{f^*,1}}(X,Y) = -2^{\frac{n}{2}-1}X^n + 2^{-1}(X+Y)^n + 2^{-\frac{n}{2}}W_{D_{f,1}}(X+Y, X-Y).$$

Lemma 3.5. *Let $b \in \mathbb{F}_2^{m*}$, and let F be an (n, m)-function with bent component function $b \cdot F$. Then for all $G \in \mathcal{D}(b \cdot F)$, we have*

$$W_{D_{b\cdot F,1}}(X,Y) = 2^{\frac{n}{2}-1}X^n + 2^{-1}(X+Y)^n - 2^{-\frac{n}{2}}W_{D_{G,b}}(X+Y, X-Y),$$
$$W_{D_{b\cdot G,1}}(X,Y) = 2^{\frac{n}{2}-1}X^n + 2^{-1}(X+Y)^n - 2^{-\frac{n}{2}}W_{D_{F,b}}(X+Y, X-Y).$$

Proof. Let $G \in \mathcal{D}(b \cdot F)$ for $b \in \mathbb{F}_2^{m*}$. Then $b \cdot G = (b \cdot F)^*$. Since $b \cdot F$ is bent, we can write $S_{b\cdot G}$ as $S_{b\cdot G}(a) = (-1)^{(b\cdot G)^*(a)}2^{\frac{n}{2}} = (-1)^{b\cdot F(a)}2^{\frac{n}{2}}$ and $S_{b\cdot F}$ as $S_{b\cdot F}(a) = (-1)^{(b\cdot F)^*(a)}2^{\frac{n}{2}} = (-1)^{b\cdot G(a)}2^{\frac{n}{2}}$.

We see that

$$\begin{aligned}
&2^{-\frac{n}{2}} \sum_{a\in\mathbb{F}_2^n} S_{b\cdot G}(a)X^{n-|a|}Y^{|a|}\\
=& \sum_{a\in\mathbb{F}_2^n} (-1)^{b\cdot F(a)}X^{n-|a|}Y^{|a|}\\
=& \sum_{a\in\mathbb{F}_2^n, b\cdot F(a)=0} X^{n-|a|}Y^{|a|} - \sum_{a\in\mathbb{F}_2^n, b\cdot F(a)=1} X^{n-|a|}Y^{|a|}\\
=& -(X+Y)^n + 2W_{D_{F,b}}(X,Y).
\end{aligned}$$

On the other hand, by Lemma 3.3, we have that

$$\sum_{a\in\mathbb{F}_2^n} S_{b\cdot G}(a)X^{n-|a|}Y^{|a|} = -2^nX^n + 2W_{D_{G,b}}(X+Y, X-Y).$$

The first identity of this lemma follows by solving those two equations. We have shown that if $S_{b\cdot G}(a) = (-1)^{b\cdot F(a)}2^{\frac{n}{2}}$, then the weight enumerator of $D_{b\cdot F}$ is expressed in terms of the weight enumerator of $D_{G,b}$. From this observation, the second identity of this lemma is proved because $S_{b\cdot F}(a) = (-1)^{b\cdot G(a)}2^{\frac{n}{2}}$. □

4. MacWilliams-type identities

MacWilliams-type identities on vectorial Boolean functions with bent component functions are presented in two forms as follows. Both of them are generalizations of the result in [8, Proposition 2.5] as stated in Lemma 3.4.

4.1. MacWilliams-type identity I

Theorem 4.1. *Let $b \in \mathbb{F}_2^{m*}$, and let F be an (n, m)-function with bent component function $b \cdot F$. Then for all $G \in \mathcal{D}(b \cdot F)$, we have*

$$W_{D_{G,b}}(X,Y) = -2^{\frac{n}{2}-1}X^n + 2^{-1}(X+Y)^n + 2^{-\frac{n}{2}}W_{D_{F,b}}(X+Y, X-Y).$$

Proof. Let $G \in \mathcal{D}(b \cdot F)$. Then $b \cdot G = (b \cdot F)^*$, and so by Lemma 3.4, we get that

$$W_{D_{b\cdot G,1}}(X,Y) = -2^{\frac{n}{2}-1}X^n + 2^{-1}(X+Y)^n + 2^{-\frac{n}{2}}W_{D_{b\cdot F,1}}(X+Y, X-Y). \tag{1}$$

By changing of variables in the first identity of Lemma 3.5 as $X \mapsto X+Y$ and $Y \mapsto X-Y$, we have that

$$W_{D_{b\cdot F,1}}(X+Y, X-Y) = 2^{\frac{n}{2}-1}(X+Y)^n + 2^{n-1}X^n - 2^{\frac{n}{2}} W_{D_{G,b}}(X,Y). \tag{2}$$

Comparing the identity obtained from plugging (2) into (1) with the second identity of Lemma 3.5, we get that

$$\begin{aligned} & 2^{\frac{n}{2}-1}X^n + 2^{-1}(X+Y)^n - 2^{-\frac{n}{2}} W_{D_{F,b}}(X+Y, X-Y) \\ = & -2^{\frac{n}{2}-1}X^n + 2^{-1}(X+Y)^n \\ & + 2^{-\frac{n}{2}}\left(2^{\frac{n}{2}-1}(X+Y)^n + 2^{n-1}X^n - 2^{\frac{n}{2}} W_{D_{G,b}}(X,Y)\right), \end{aligned}$$

which yields

$$2^{\frac{n}{2}-1}X^n - 2^{-\frac{n}{2}} W_{D_{b\cdot F,1}}(X+Y, X-Y) = 2^{-1}(X+Y)^n - W_{D_{G,b}}(X,Y),$$

and thus the result follows. □

In the case that F being an (n,m)-function has a self-dual bent component function, we have the following corollary.

Corollary 4.2. *Let $b \in \mathbb{F}_2^{m*}$, and let F be an (n,m)-function with bent component function $b \cdot F$. If $F \in \mathcal{D}(b \cdot F)$, we have*

$$W_{D_{F,b}}(X,Y) = -2^{\frac{n}{2}-1}X^n + 2^{-1}(X+Y)^n + 2^{-\frac{n}{2}} W_{D_{F,b}}(X+Y, X-Y).$$

Let $F = (f_1, \ldots, f_m)$ be a vectorial dual-bent (n,m)-function. It can be readily checked that $G \in \cap_{b \in \mathbb{F}_2^{m*}} \mathcal{D}(b \cdot F)$ if and only if $G = (f_1^*, \ldots, f_m^*)$ and $b \cdot G = (b \cdot F)^*$ for all $b \in \mathbb{F}_2^{m*}$. When this is the case, $\cap_{b \in \mathbb{F}_2^{m*}} \mathcal{D}(b \cdot F) = \{F^*\}$ and F is vectorial self-dual bent with component-wise self-dual bent functions.

Corollary 4.3. *Let F be a vectorial dual-bent (n,m)-function with component-wise self-dual bent functions. Then for all $b \in \mathbb{F}_2^{m*}$, we have*

$$W_{D_{F,b}}(X,Y) = -2^{\frac{n}{2}-1}X^n + 2^{-1}(X+Y)^n + 2^{-\frac{n}{2}} W_{D_{F,b}}(X+Y, X-Y).$$

Proof. By the previous discussion and Theorem 4.1, the result follows. □

4.2. MacWilliams-type identity II

Theorem 4.4. *Let F be a vectorial dual-bent (n,m)-function. Then for all $c \in \mathbb{F}_2^m$ and all dual bent functions F^* of F, we have*

$$W_{(F^*)^{-1}(c)}(X,Y) = -2^{\frac{n}{2}-m}X^n + 2^{-m}(X+Y)^n + 2^{-\frac{n}{2}} W_{F^{-1}(c)}(X+Y, X-Y).$$

Proof. By Lemma 3.1 and $S_{0\cdot F}(a) = 2^n \delta_{0,a}$, we have that

$$\sum_{b \in \mathbb{F}_2^{m*}} S_{b\cdot F}(a) = 2^m \chi_a(F^{-1}(0)) - 2^n \delta_{0,a}. \tag{3}$$

Let $S_{b\cdot F}(a) = 2^{\frac{n}{2}}(-1)^{(b\cdot F)^*(a)}$ and let $\{g_1^*, \ldots, g_m^*\}$ be a basis for the space of the dual F^* of F. It then follows that

$$\sum_{b \in \mathbb{F}_2^{m*}} (-1)^{(b\cdot F)^*(a)} = \sum_{b \in \mathbb{F}_2^{m*}} (-1)^{b\cdot F^*(a)}.$$

With this observation, the left hand side of (3) equals

$$2^{\frac{n}{2}} \sum_{b\in\mathbb{F}_2^{m*}} (-1)^{(b\cdot F)^*(a)} = 2^{\frac{n}{2}} \sum_{b\in\mathbb{F}_2^{m*}} (-1)^{b\cdot F^*(a)} = 2^{\frac{n}{2}}(2^m\delta_{0,F^*(a)} - 1),$$

and so we have

$$2^{\frac{n}{2}}(2^m\delta_{0,F^*(a)} - 1) = 2^m\chi_a(F^{-1}(0)) - 2^n\delta_{0,a}.$$

By taking the summation that runs over $\mathbb{F}_2^n$, we get

$$2^{\frac{n}{2}} \sum_{a\in\mathbb{F}_2^n}(2^m\delta_{0,F^*(a)} - 1)X^{n-|a|}Y^{|a|} = \sum_{a\in\mathbb{F}_2^n}(2^m\chi_a(F^{-1}(0)) - 2^n\delta_{0,a})X^{n-|a|}Y^{|a|}.$$

Equivalently, by Lemma 3.2,

$$(4)\quad 2^{\frac{n}{2}}\left(2^m W_{(F^*)^{-1}(0)}(X,Y) - (X+Y)^n\right) = 2^m W_{F^{-1}(0)}(X+Y,X-Y) - 2^n X^n,$$

which yields the result for the case that c is the zero vector in $\mathbb{F}_2^m$. For $c = (c_1,\ldots,c_m) \in \mathbb{F}_2^{m*}$, put $F_c = c + F$. Then F_c is also vectorial dual-bent with dual $(F_c)^* = (g_1^* + c_1,\ldots,g_m^* + c_m) = F^* + c$ of F_c. The result thus follows by plugging F_c and $(F_c)^*$ into (4). □

Corollary 4.5. *Let F be a vectorial dual-bent (n,m)-function. Then for all $c \in \mathbb{F}_2^m$, we have*

$$W_{(F^{**})^{-1}(c)}(X,Y) = W_{F^{-1}(c)}(X,Y),$$

$$W_{F^{-1}(c)}(X,Y) = -2^{\frac{n}{2}-m}X^n + 2^{-m}(X+Y)^n + 2^{-\frac{n}{2}}W_{(F^*)^{-1}(c)}(X+Y,X-Y).$$

Proof. Since the linear spans of $\mathcal{BC}_F$ and $\mathcal{BC}_F^{**}$ are the same, there is an invertible matrix A with entries from $\mathbb{F}_2$ such that $F = F^{**}A$. By replacing F by F^* in Theorem 4.4, we get by $(F^{**})^{-1}(c) = F^{-1}(cA)$ for all $c \in \mathbb{F}_2^n$ that

$$(5)\qquad W_{F^{-1}(cA)}(X,Y) = -2^{\frac{n}{2}-m}X^n + 2^{-m}(X+Y)^n + 2^{-\frac{n}{2}}W_{(F^*)^{-1}(c)}(X+Y,X-Y).$$

After replacing X and Y by $X+Y$ and $X-Y$ in Theorem 4.4, respectively, plugging it into (5) we obtain the first part. Because F^* is also vectorial dual-bent, by plugging F into F^* in Theorem 4.4, the second part is derived by the first part of this corollary. □

5. Applications

This section includes two subsections. In the first subsection, we derive a bound for the non-existence of vectorial bent functions in $2n$ variables with given minimum degree $n-k$ for $k = 0,1,\ldots,n-1$. In the second subsection, using the MacWilliams-type identities of Theorems 4.1 and 4.4, Gleason-type theorems are presented in two forms.

5.1. A bound

Lemma 5.1. *Let F be an $(2n,m)$-function with minimum degree $n-k$ for $k=0,1,\ldots,n-1$. If $F(0)=0$, then $A_l(F^{-1}(c))=0$ for all $c\in\mathbb{F}_2^{m*}$ and $l=0,1,\ldots,n-k-1$.*

Proof. It is straightforward. □

Theorem 5.2. *Let $k=0,1,\ldots,n-1$ and let m be a positive integer. Let $N_{k,m}$ be the smallest positive integer satisfying*

$$\binom{N_{k,m}+k+1}{k+1} < (2^m-1)2^{N_{k,m}-m}-1.$$

Then there is no vectorial dual-bent $(2n,m)$-function with minimum degree $n-k$ for all $n\geq N_{k,m}$.

Proof. Assume that there is a vectorial dual-bent $(2n,m)$-function F with minimum degree $n-k$. We may assume that $F(0)=0$ because $G(x)=F(x)+F(0)$ and G is also vectorial dual-bent. Replacing X and Y by $(X/2)+1$ and $X/2$, respectively, in Theorem 4.4 yields that for all $c\in\mathbb{F}_2^m$,

$$W_{F^{-1}(c)}(X+1,1)-2^{-n}W_{(F^*)^{-1}(c)}(X+2,1)=2^{-m}(X+2)^{2n}-2^{n-m}(X+1)^{2n}.$$

Equivalently, for $i=0,1,\ldots,2n$ and all $c\in\mathbb{F}_2^m$,

$$\sum_{j=0}^{2n-i}A_j(F^{-1}(c))\binom{2n-j}{i}-2^{n-i}\sum_{j=0}^{i}A_j((F^*)^{-1}(c))\binom{2n-j}{n-i}$$
$$=(2^{2n-i-m}-2^{n-m})\binom{2n}{i}.$$

Setting $i=n-1$, we get that

$$\sum_{j=0}^{n+1}A_j(F^{-1}(c))\binom{2n-j}{n-1}\geq 2^{n-m}\binom{2n}{n-1}. \tag{6}$$

Let us put $p_j=\sum_{c\in\mathbb{F}_2^{m*}}A_j(F^{-1}(c))$ for $j=0,1,\ldots,2n$. By Lemma 5.1 and (6), we get that

$$\sum_{j=n-k}^{n+1}\binom{2n-j}{n-1}p_j=\sum_{j=0}^{n+1}\binom{2n-j}{n-1}p_j=\sum_{c\in\mathbb{F}_2^{m*}}\sum_{j=0}^{n+1}A_j(F^{-1}(c))\binom{2n-j}{n-1}$$
$$\geq(2^m-1)2^{n-m}\binom{2n}{n-1}.$$

We observe that $p_n\leq\binom{2n}{n}$, $p_j\leq\binom{2n}{n-1}$ for $j=0,1,\ldots,n-1$ and $\binom{2n}{n}=\frac{n+1}{n}\binom{2n}{n-1}$.

Using these observations, we have that

$$\begin{aligned}\sum_{j=n-k}^{n+1}\binom{2n-j}{n-1}p_j &= p_{n+1}+\binom{n}{n-1}p_n+\sum_{j=n-k}^{n-1}\binom{2n-j}{n-1}p_j\\ &\le \binom{2n}{n+1}+\binom{n}{n-1}\binom{2n}{n}+\sum_{j=n-k}^{n-1}\binom{2n-j}{n-1}\binom{2n}{n-1}.\end{aligned}$$

The last two terms in the inequality are less than or equal to

$$\begin{aligned}&(n+1)\binom{2n}{n-1}+\binom{2n}{n-1}\sum_{j=n-k}^{n+1}\binom{2n-j}{n-1}\\ &=(n+1)\binom{2n}{n-1}+\binom{2n}{n-1}\sum_{j=n-1}^{n+k}\binom{j}{n-1}.\end{aligned}$$

It follows from $\sum_{j=n-1}^{n+k}\binom{j}{n-1}=\binom{n+k+1}{n}$ that

$$1+\binom{n+k+1}{n}\ge(2^m-1)2^{n-m},$$

and the proof is completed. □

Corollary 5.3. *If $m\ge 2$, then there is no vectorial dual-bent $(2n,m)$-function with minimum degree n for $n\ge 3$.*

As a direct consequence of Theorem 5.2 we obtain a known result in [9, Theorem 4.6].

Corollary 5.4 ([9])**.** *Let $k=0,1,\dots,n-1$ and let $N_{k,1}$ be the smallest positive integer satisfying*

$$\binom{N_{k,1}+k+1}{k+1}<2^{N_{k,1}-1}-1.$$

Then there is no bent $(2n,1)$-function with minimum degree $n-k$ for $n\ge N_{k,1}$.

Remark 5.5. Recall from Introduction, it was proved in [11] that for any non-negative integer k, there exists a positive integer N such that for $n\ge N$ there exist no homogeneous bent $(2n,1)$-functions having algebraic degree $n-k$ or more, where N is the least integer satisfying

$$\binom{N}{1}+\cdots+\binom{N}{k+1}<2^{N-1}-1;$$

our bound in Corollary 5.4 is applied to more wider classes of Boolean functions. In [9, 11, 17], they proved that there is no homogeneous bent $(2n,1)$-function with algebraic degree n for $n\ge 4$. This is a direct consequence of Corollary 5.4. By Theorem 5.2 and $N_{k,m}\ge N_{k,1}$, we can obtain a lower bound better than Corollary 5.4. For example, there is no vectorial dual-bent $(2n,2)$-function with minimum degree $n-1$ for $n\ge 8$.

5.2. Gleason-type theorems

In this subsection, we derive the Gleason-type theorems on vectorial Boolean functions with bent component functions.

Lemma 5.6 ([10, p. 605, Theorem 5])**.** *Let $H(X,Y)$ be a homogeneous polynomial in two variables over $\mathbb{C}$ satisfying $H(x,y) = H(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}})$. Then $H(x,y) \in \mathbb{C}[x^2+y^2, xy-y^2]$.*

We begin with the case when a vectorial Boolean function has self-dual bent as a component function.

Theorem 5.7. *Let $b \in \mathbb{F}_2^{m*}$ and let F be an (n,m)-function with bent component function $b \cdot F$. If $F \in \mathcal{D}(b \cdot F)$, then*

$$W_{D_{F,b}}(X,Y) = -2^{\frac{n}{2}-1}X^n + \sum_{j=0}^{\frac{n}{2}} a_j (X^2+Y^2)^{\frac{n}{2}-j}(XY-Y^2)^j,$$

where a_j's are integers. In particular, if F is a vectorial dual-bent (n,m)-function with component-wise self-dual, then for all $b \in \mathbb{F}_2^{m*}$, we have

$$W_{D_{F,b}}(X,Y) = -2^{\frac{n}{2}-1}X^n + \sum_{j=0}^{\frac{n}{2}} a_j (X^2+Y^2)^{\frac{n}{2}-j}(XY-Y^2)^j,$$

where a_j's are integers.

Proof. The results follow from Corollaries 4.2, 4.3 and Lemma 5.6. □

Theorem 5.8. *Let $n \geq 4$ and let F be a vectorial self-dual bent (n,m)-function. Then for all $c \in \mathbb{F}_2^m$, we have*

$$W_{F^{-1}(c)}(X,Y) = -2^{\frac{n}{2}-m}X^n + \sum_{j=0}^{\frac{n}{2}} a_j (X^2+Y^2)^{\frac{n}{2}-j}(XY-Y^2)^j,$$

where a_j's are integers.

Proof. Since the linear spans of $\mathcal{BC}_F$ and $\mathcal{BC}_F^*$ are the same, there is an invertible matrix A with entries from $\mathbb{F}_2$ such that $F = F^*A$. By Theorem 4.4 and $(F^*)^{-1}(c) = F^{-1}(cA)$ for all $c \in \mathbb{F}_2^n$, we get that

$$\begin{aligned} W_{F^{-1}(cA)}(X,Y) = & -2^{\frac{n}{2}-m}X^n + 2^{-m}(X+Y)^n \\ & + 2^{-\frac{n}{2}} W_{F^{-1}(c)}(X+Y, X-Y). \end{aligned} \tag{7}$$

By Corollary 4.5, we have that

$$\begin{aligned} W_{F^{-1}(c)}(X,Y) = & -2^{\frac{n}{2}-m}X^n + 2^{-m}(X+Y)^n \\ & + 2^{-\frac{n}{2}} W_{F^{-1}(cA)}(X+Y, X-Y). \end{aligned} \tag{8}$$

Let us put $W^+(X,Y) = W_{F^{-1}(c)}(X,Y) + W_{F^{-1}(cA)}(X,Y)$. Adding (7) and (8) yields that

$$\begin{aligned}(9) \qquad W^+(X,Y) = & -2^{\frac{n}{2}-m+1}X^n + 2^{-m+1}(X+Y)^n \\ & + 2^{-\frac{n}{2}}W^+(X+Y, X-Y).\end{aligned}$$

Let us put $W^\circ(X,Y) = W^+(X,Y) + 2^{\frac{n}{2}-m+1}X^n$. By using (9), we can derive

$$W^\circ(X+Y, X-Y) = 2^{\frac{n}{2}}W^\circ(X,Y).$$

By Lemma 5.6, we get

$$(10) \qquad W^+(X,Y) = -2^{\frac{n}{2}-m+1}X^n + \sum_{j=0}^{\frac{n}{2}} a_j(X^2+Y^2)^{\frac{n}{2}-j}(XY-Y^2)^j,$$

where a_j's are integers. Let us put

$$W^-(X,Y) = W_{F^{-1}(c)}(X,Y) - W_{F^{-1}(cA)}(X,Y).$$

Subtracting (7) from (8) yields that $W^-(X,Y) = 2^{-\frac{n}{2}}W^-(X+Y, X-Y)$. By using Lemma 5.6 again, we get

$$(11) \qquad W^-(X,Y) = \sum_{j=0}^{\frac{n}{2}} b_j(X^2+Y^2)^{\frac{n}{2}-j}(XY-Y^2)^j,$$

where b_j's are integers by comparing their coefficients. The result follows by adding two equations (10), (11), and by comparing their coefficients in (10), (11) and the resulting identity. □

Acknowledgments. We express our gratitude to the reviewer for his/her very helpful comments, which lead to improvement of the exposition of this paper.

References

[1] C. Carlet, *Boolean functions for cryptography and error correcting codes*, in Boolean Models and Methods in Mathematics, Computer Science, and Engineering, P. L. Hammer and Y. Crama, Eds. Cambridge, U.K.: Cambridge Univ. Press, 2010.

[2] C. Carlet, *Vectorial Boolean functions for cryptography*, in Boolean Models and Methods in Mathematics, Computer Science, and Engineering, P. L. Hammer and Y. Crama, Eds. Cambridge, U.K.: Cambridge Univ. Press, 2010.

[3] C. Carlet, L. E. Danielsen, M. G. Parker, and P. Solé, *Self-dual bent functions*, Int. J. Inf. Coding Theory **1** (2010), no. 4, 384–399. https://doi.org/10.1504/IJICOT.2010.032864

[4] C. Carlet and S. Mesnager, *On the construction of bent vectorial functions*, Int. J. Inf. Coding Theory **1** (2010), no. 2, 133–148. https://doi.org/10.1504/IJICOT.2010.032131

[5] C. Carlet and S. Mesnager, *Four decades of research on bent functions*, Des. Codes Cryptogr. **78** (2016), no. 1, 5–50. https://doi.org/10.1007/s10623-015-0145-8

[6] A. Çeşmelioğlu, W. Meidl, and A. Pott, *Vectorial bent functions and their duals*, Linear Algebra Appl. **548** (2018), 305–320. https://doi.org/10.1016/j.laa.2018.03.016

[7] J. Y. Hyun, *Generalized MacWilliams identities and their applications to perfect binary codes*, Des. Codes Cryptogr. **50** (2009), no. 2, 173–185. https://doi.org/10.1007/s10623-008-9222-6

[8] J. Y. Hyun, H. Lee, and Y. Lee, *MacWilliams duality and a Gleason-type theorem on self-dual bent functions*, Des. Codes Cryptogr. **63** (2012), no. 3, 295–304. https://doi.org/10.1007/s10623-011-9554-5

[9] J. Y. Hyun, H. Lee, and Y. Lee, *Boolean functions with MacWilliams duality*, Des. Codes Cryptogr. **72** (2014), no. 2, 273–287. https://doi.org/10.1007/s10623-012-9762-7

[10] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes. II*, North-Holland Mathematical Library, Vol. 16, North-Holland, Amsterdam, 1977.

[11] Q. S. Meng, H. Zhang, M. Yang, and J. Cui, *On the degree of homogeneous bent functions*, Discrete Appl. Math. **155** (2007), no. 5, 665–669. https://doi.org/10.1016/j.dam.2006.10.008

[12] S. Mesnager, *Bent Functions*, Springer, 2016. https://doi.org/10.1007/978-3-319-32595-8

[13] K. Nyberg, *Perfect nonlinear S-boxes*, in Advances in cryptology—EUROCRYPT '91 (Brighton, 1991), 378–386, Lecture Notes in Comput. Sci., 547, Springer, Berlin, 1991. https://doi.org/10.1007/3-540-46416-6_32

[14] K. Nyberg and M. Hermelin, *Multidimensional Walsh Transform and a Characterization of Bent Functions*, In Tor Helleseth, P.V.K., Ytrehus, O., eds.: Proceedings of the 2007 IEEE Information Theory Workshop on Information Theory for Wireless Networks. IEEE 83–86, 2007.

[15] O. S. Rothaus, *On "bent" functions*, J. Combin. Theory Ser. A **20** (1976), no. 3, 300–305. https://doi.org/10.1016/0097-3165(76)90024-8

[16] P. Stănică and S. Maitra, *Rotation symmetric Boolean functions—count and cryptographic properties*, Discrete Appl. Math. **156** (2008), no. 10, 1567–1580. https://doi.org/10.1016/j.dam.2007.04.029

[17] T. B. Xia, J. Seberry, J. Pieprzyk, and C. Charnes, *Homogeneous bent functions of degree n in $2n$ variables do not exist for $n > 3$*, Discrete Appl. Math. **142** (2004), no. 1-3, 127–132. https://doi.org/10.1016/j.dam.2004.02.006

Jong Yoon Hyun
Konkuk University, Glocal Campus
Chungju-si 27478, Korea
Email address: hyun33@kku.ac.kr