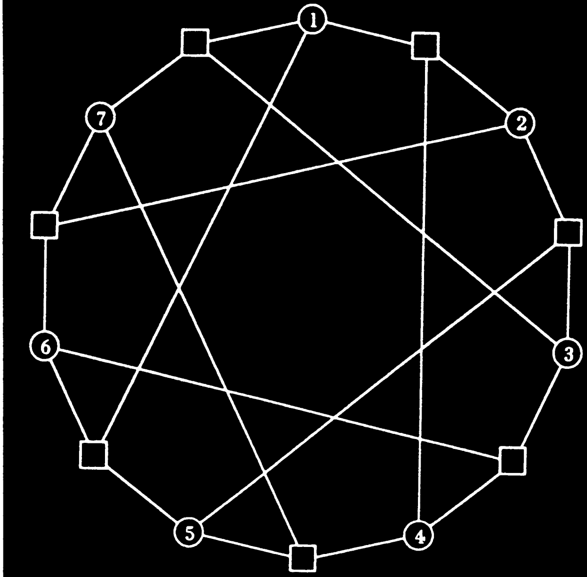
BULLETIN of the INSTITUTE of COMBINATORICS and its APPLICATIONS

Winnipeg
Canada



ISSN
1183-1278

A New Property of Maiorana-McFarland Functions

Yuliang Zheng
School of Network Computing
Monash University
McMahons Road, Frankston, VIC 3199, Australia
Email: yuliang.zheng@infotech.monash.edu.au

Xian-Mo Zhang
School of Information Technology & Computer Science
University of Wollongong
Wollongong, NSW 2522, Australia
Email: xianmo@cs.uow.edu.au

Abstract

Maiorana-McFarland functions were originally introduced in combinatorics. These functions are useful in constructing bent functions, although only in special cases. An interesting problem is therefore to investigate whether Maiorana-McFarland functions that are not bent can be used, indirectly, to obtain bent functions. This question is given an affirmative answer in this paper. More specifically, we show that the non-zero terms in the Fourier transform of a Maiorana-McFarland function that is associated with an one-to-one mapping, can be used to form the sequence of a bent function. This result presents new insights into the usefulness and properties of Maiorana-McFarland functions.

Key Words

Bent Functions, Fourier Transform, Maiorana-McFarland Functions.

1 Motivation

Let V_n be the vector space of n tuples of elements from $GF(2)$. For positive integers k and m, let Q be a mapping from V_k to V_m and r be a (Boolean) function on V_k. Define a function $f(y,x)$ on V_{m+k} as

$$f(y,x) = Q(y)x^T \oplus r(y)$$

where $x \in V_m$ and $y \in V_k$. Then we say that f is a *Maiorana-McFarland function.* Maiorana-McFarland functions play an important role in the design of cryptographic functions that satisfy cryptographically desirable properties such as high nonlinearity, propagation characteristics and correlation immunity[1, 2, 7, 8].

It is known that when $k = m$ and Q is a permutation on V_k, f is a bent function on V_{2k} [3, 4]. This provides us with a powerful method for constructing as many as $(2^k!)2^{2^k}$ different bent functions on V_{2k}. If we use nonsingular linear transformations on the variables, we will obtain even more bent functions from this kind of bent functions. Of course, there exist bent functions that are not equivalent to Maiorana-McFarland functions by any nonsingular linear transformation on the variables [5].

We know that when $k < m$, a Maiorana-McFarland function is not a bent function. This observation motivates us to ask a question, namely, given a Maiorana-McFarland function that is not bent in its own right, can it still be used to obtain a bent function after a simple transformation ? In this work, we provide an affirmative answer for the case of $k \leq m$. More specifically, we show that if $k \leq m$ and Q is an one-to-one mapping, then the non-zero terms in the Fourier transform of a Maiorana-McFarland function $f(y,x) = Q(y)x^T \oplus r(y)$, when concatenated together, form the sequence of a bent function on V_{2k}.

2 Boolean Functions

The *truth table* of a function f on V_n is a $(0,1)$-sequence defined by

$$(f(\alpha_0),\ f(\alpha_1),\ldots,f(\alpha_{2^n-1})),$$

and the *sequence* of f is a $(1,-1)$-sequence defined by

$$((-1)^{f(\alpha_0)},(-1)^{f(\alpha_1)},\ldots,(-1)^{f(\alpha_{2^n-1})}),$$

where $\alpha_0 = (0,\ldots,0,0)$, $\alpha_1 = (0,\ldots,0,1)$, ..., $\alpha_{2^{n-1}-1} = (1,\ldots,1,1)$. The *matrix* of f is a $(1,-1)$-matrix of order 2^n defined by

$$M = ((-1)^{f(\alpha_i \oplus \alpha_j)})$$

where $\oplus$ denotes the addition in $GF(2)$.

Given two sequences $\tilde{a} = (a_1, \cdots, a_m)$ and $\tilde{b} = (b_1, \cdots, b_m)$, we define *the component-wise product* of the two sequences by $\tilde{a} * \tilde{b} = (a_1 b_1, \cdots, a_m b_m)$. In particular, if $m = 2^n$ and $\tilde{a}$, $\tilde{b}$ are the sequences of functions f and g on V_n respectively, then $\tilde{a} * \tilde{b}$ is the sequence of $f \oplus g$, where $\oplus$ denotes the addition in $GF(2)$.

Let $\tilde{a} = (a_1, \cdots, a_m)$ and $\tilde{b} = (b_1, \cdots, b_m)$ be two sequences or vectors, the *scalar product* of $\tilde{a}$ and $\tilde{b}$, denoted by $\langle \tilde{a}, \tilde{b} \rangle$, is defined as the sum of component-wise multiplications. In particular, when $\tilde{a}$ and $\tilde{b}$ are from V_m, $\langle \tilde{a}, \tilde{b} \rangle = a_1 b_1 \oplus \cdots \oplus a_m b_m$, where the addition and multiplication are over $GF(2)$, and when $\tilde{a}$ and $\tilde{b}$ are $(1, -1)$-sequences, $\langle \tilde{a}, \tilde{b} \rangle = \sum_{i=1}^{m} a_i b_i$, where the addition and multiplication are over the reals.

An *affine* function f on V_n is a function that takes the form of $f(x_1, \ldots, x_n) = a_1 x_1 \oplus \cdots \oplus a_n x_n \oplus c$, where $a_j, c \in GF(2)$, $j = 1, 2, \ldots, n$. Furthermore f is called a *linear* function if $c = 0$.

A $(1, -1)$-matrix A of order n is called a *Hadamard* matrix if $AA^T = nI_n$, where A^T is the transpose of A and I_n is the identity matrix of order n. A Sylvester-Hadamard matrix of order 2^n, denoted by H_n, is generated by the following recursive relation

$$H_0 = 1, \; H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}, \; n = 1, 2, \ldots.$$

Let ℓ_i, $0 \le i \le 2^n - 1$, be the i row of H_n. It is known that ℓ_i is the sequence of a linear function $\varphi_i(x)$ defined by the scalar product $\varphi_i(x) = \langle \alpha_i, x \rangle$, where α_i is the ith vector in V_n according to the ascending alphabetical order.

The *Hamming weight* of a $(0, 1)$-sequence ξ, denoted by $HW(\xi)$, is the number of ones in the sequence. Given two functions f and g on V_n, the *Hamming distance* $d(f, g)$ between them is defined as the Hamming weight of the truth table of $f(x) \oplus g(x)$, where $x = (x_1, \ldots, x_n)$.

Let f be a function on V_n and ξ denote the sequence of f. Then we call a sequence defined by

$$2^{-\frac{1}{2}n} \xi H_n$$

the *Fourier transform* of the function f. Note that generally each coordinate of $2^{-\frac{1}{2}n} \xi H_n$ can take a value ranging from $-2^{\frac{1}{2}n}$ to $2^{\frac{1}{2}n}$. An interesting fact is that if $2^{-\frac{1}{2}n} \xi H_n$ is a $(1, -1)$-sequence, then f must be a *bent function* [6].

A bent function on V_n exists only for n even. The algebraic degree of bent functions on V_n is at most $\frac{1}{2}n$ [6]. From the same paper, it is known that f is a bent function on V_n if and only if the matrix of f is an Hadamard matrix. Although the concept of bent functions was initially introduced in combinatorics, they have since found numerous applications in logic synthesis, digital communications and cryptography.

3 Maiorana-McFarland Functions

Consider a *Maiorana-McFarland function* defined by

$$f(z) = f(y,x) = Q(y)x^T \oplus r(y) \tag{1}$$

where Q is a mapping from V_k to V_m, r is a function on V_k, $x \in V_m$, $y \in V_k$ and $z = (y,x)$.

Let $c_0, c_1, \ldots, c_{2^k-1}$ be an arbitrary $(1,-1)$-sequence of length 2^k and $\{j_0, j_1, \ldots, j_{2^k-1}\}$ be an arbitrary subset of $\{0,1,\ldots,2^m-1\}$, where j_0, j_1, $\ldots$, j_{2^k-1} are not necessarily mutually distinct. Let ℓ_i denote the ith row of H_m, $0 \le i \le 2^m - 1$. Set

$$\xi = c_0\ell_{j_0}, c_1\ell_{j_1}, \ldots, c_{2^k-1}\ell_{j_{2^k-1}} \tag{2}$$

where $\{j_0, j_1, \ldots, j_{2^k-1}\} = \{0,1,\ldots,2^k-1\}$.

Given a Maiorana-McFarland function f defined in (1), let $c_0, c_1, \ldots,$ c_{2^k-1} be the sequence of r which is involved in the construction of f. Furthermore let j_0 be the integer representation of $Q(\alpha_0)$, j_1 the integer representation of $Q(\alpha_1)$, $\ldots$, and j_{2^k-1} the integer representation of $Q(\alpha_{2^k-1})$. Then (2) is the sequence of the function f in (1).

Conversely, assume that we are given $\{j_0, j_1, \ldots, j_{2^k-1}\} \subseteq \{0,1,\ldots,2^m-1\}$, where $j_0, j_1, \ldots, j_{2^k-1}$ are not necessarily mutually distinct, and a $(1,-1)$-sequence, $c_0, c_1, \ldots, c_{2^k-1}$. Let r be the function whose sequence is $c_0, c_1, \ldots, c_{2^k-1}$, and similarly let Q be the mapping from V_k to V_m such that $Q(\alpha_0)$ is the binary representation of j_0, $Q(\alpha_1)$ is the binary representation of j_1, $\ldots$, and $Q(\alpha_{2^k-1})$ is the binary representation of j_{2^k-1}. Then (1) must be a function whose sequence is (2).

The above observations indicate that the sequence of each function on V_{m+k}, defined in (1), can be expressed in (2), and conversely, each sequence in (2) can be expressed in (1).

4 Bent Functions via Maiorana-McFarland Functions

Maiorana-McFarland functions play an important role in the construction of bent functions, as well as in the design of cryptographic functions that satisfy cryptographically desirable properties. We are particularly interested in the case when $m = k$ and Q is a permutation on V_k. For the sake of convenience, we use P to denote the permutation on V_k. Then the Maiorana-McFarland function introduced in (1) can be specialized as

$$f(z) = f(y,x) = P(y)x^T \oplus r(y) \tag{3}$$

where $y, x \in V_k$ and $z = (y, x)$.

In [3, 4], Dillon proves that the function f in (3) is a bent function on V_{2k}.

Interchanging x and y in (3) also gives a bent function. Namely,

$$g(z) = g(y, x) = P(x)y^T \oplus r(x) \tag{4}$$

is also a bent function on V_{2k}, where $x, y \in V_k$ and $z = (y, x)$.

In a sense, (3) and (4) complement each other. A question that arises naturally is how functions defined in (3) relate to those defined (4).

Notation 1 *Let Ω_{2k} denote the set of bent functions on V_{2k} expressed in (3), and similarly let Γ_{2k} denote the set of bent functions on V_{2k} expressed in (4).*

Then one can verify that $f \in \Omega_{2k} \cap \Gamma_{2k}$ if and only if $f(y, x) = xy^T$, where $x, y \in V_{2k}$. Hence we have $\#(\Omega_{2k} \cap \Gamma_{2k}) = 1$. In addition, we have $\#\Omega_{2k} = \#\Gamma_{2k} = (2^k!)2^{2^k}$. Thus (3) and (4) allow us to construct exponentially many bent functions all of which, except $f(y, x) = xy^T$, are distinct.

We note that by the use of nonsingular linear transformations on the variables, a further greater number of bent functions can be obtained from those in Ω_{2k} and Γ_{2k}. Nevertheless, it is important to point out that there exist bent functions that are neither in Ω_{2k} or Γ_{2k}, nor can they be obtained by applying a nonsingular linear transformation on the variables of bent functions in Ω_{2k} or Γ_{2k} (see [5]).

To prove the main result in this paper, we examine in more detail the sequence of f in (4).

Definition 1 *$B = (b_{ij})$ is called a* $2^k \times 2^k$ permutation matrix *if there exists a permutation σ on $\{0, 1, \ldots, 2^k - 1\}$ such that* $b_{ij} = \begin{cases} 1 & \textit{if } i = \sigma(j) \\ 0 & \textit{otherwise.} \end{cases}$

Let $C = diag(c_0, c_1 \cdots c_{2^k-1})$ be a $2^k \times 2^k$ diagonal matrix where each $c_j = \pm 1$. Denote the entry on the cross of the ith row and the jth column of H_k by h_{ij}, $i, j = 0, 1, \ldots, 2^k - 1$. Let h_i denote the ith row of H_k, i.e., $h_i = (h_{i0}, h_{i1}, \ldots, h_{i2^k-1})$. Set $N = H_kBC$. Denote the entry on the cross of the ith row and the jth column of N by n_{ij}, $i, j = 0, 1, \ldots, 2^k - 1$. Let η_i denote the ith row of N, i.e., $\eta_i = (n_{i0}, n_{i1}, \ldots, n_{i2^k-1})$, $i = 0, 1, \ldots, 2^k - 1$. Hence we have

$$\eta_i = (c_0 h_{i\sigma(0)}, c_1 h_{i\sigma(1)}, \ldots, c_{2^k-1} h_{i\sigma(2^k-1)}) \tag{5}$$

Set

$$\eta = (\eta_0, \eta_1, \cdots, \eta_{2^k-1}), \tag{6}$$

Note that η is a (1, -1)-sequence of length 2^{2k}.

Let Γ'_{2k} denote the set of all the functions on V_{2k}, whose sequences take the form expressed in (6). We now prove that $\Gamma'_{2k} = \Gamma_{2k}$.

Consider η which is defined in (6). Recall that H_k is symmetric and the ith row (the ith column) is the sequence of a linear function on V_k, denoted by $\varphi(x) = \langle\alpha_i, x\rangle$, where α_i is the binary representation of an integer i, $0 \le i \le 2^k - 1$. Hence we have $h_{ij} = (-1)^{\langle\alpha_j,\alpha_i\rangle}$. From σ, a permutation on $\{0, 1, \ldots, 2^k - 1\}$, we define P, a new permutation on V_k, as follows: $P(\alpha_j) = \alpha_{\sigma(j)}$, where α_j is the binary representation of an integer j, $j = 0, 1, \ldots, 2^k - 1$. Furthermore, from $c_0, c_1, \ldots, c_{2^k-1}$, we define a function r on V_k such that $c_0, c_1, \ldots, c_{2^k-1}$ is the sequence of r. Hence for any $j, i \in \{0, 1, \ldots, 2^k - 1\}$, we have $f(\alpha_j, \alpha_i) = P(\alpha_j)\alpha_i^T \oplus r(\alpha_j) = \alpha_{\sigma(j)}\alpha_i^T \oplus r(\alpha_j) = \langle\alpha_{\sigma(j)}, \alpha_i\rangle \oplus r(\alpha_j)$. This proves that

$$(-1)^{f(\alpha_j,\alpha_i)} = (-1)^{\langle\alpha_{\sigma(j)},\alpha_i\rangle\oplus r(\alpha_j)} = c_j h_{i\sigma(j)} \qquad (7)$$

Hence we have $\Gamma'_{2k} \subseteq \Gamma_{2k}$.

Finally, it is easy to verify that $\#\Gamma'_{2k} = \#\Gamma_{2k} = 2^k! \cdot 2^{2^k}$. This property, together with the fact that $\Gamma'_{2k} \subseteq \Gamma_{2k}$, shows that $\Gamma'_{2k} = \Gamma_{2k}$ is indeed true.

Thus we have proved the following result:

Lemma 1 *For any positive integer k, any $2^k \times 2^k$ permutation matrix B and any $2^k \times 2^k$ diagonal matrix C with diagonal entries ± 1, set $N = H_k BC$. Denote the ith row of N by η_i, $i = 0, 1, \ldots, 2^k - 1$. Then ($\eta_0$, η_1, $\ldots$, η_{2^k-1}) is the sequence of a bent function on V_{2k}.*

This lemma will be used in the next section in proving Theorem 1, our main result in this paper.

5 Bent Functions in the Fourier Transform of Maiorana-McFarland Functions

Let k be a positive integer with $k \le m$. Let F be a mapping from V_k to V_m that satisfies the condition of $F(\alpha) \ne F(\alpha')$ for $\alpha \ne \alpha'$ (i.e., F is an *one-to-one mapping*). Also let r be a function on V_k. Set

$$f(z) = f(y, x) = F(y)x^T \oplus r(y)$$

where $x \in V_m$, $y \in V_k$ and $z = (y, x)$.

Discussions in Section 3 indicate that the sequence of f can be expressed as

$$\xi = (c_0\ell_{j_0}, c_1\ell_{j_1}, \ldots, c_{2^k-1}\ell_{j_{2^k-1}})$$

where each $c_j = \pm 1$, $\{j_0, j_1, \ldots, j_{2^k-1}\}$ is an arbitrary subset of $\{0, 1, \ldots, 2^m - 1\}$ and each ℓ_i denotes the ith row of H_m, $0 \leq i \leq 2^m - 1$. Since F is an one-to-one mapping, $j_0, j_1, \ldots, j_{2^k-1}$ are mutually distinct.

Let L_j denote the jth row of H_{m+k}, $0 \leq j \leq 2^{m+k} - 1$, and e_s the sth row of H_k, $0 \leq s \leq 2^k - 1$. Since $H_{m+k} = H_k \times H_m$, where $\times$ denotes the Kronecker product [9], we have

$$H_k \times \ell_i = \begin{bmatrix} L_i \\ L_{i+2^m} \\ \vdots \\ L_{i+2^m(2^k-1)} \end{bmatrix}$$

for each fixed i, $0 \leq i \leq 2^m - 1$.

As in Section 3, we denote by h_{ij} the entry on the cross of the ith row and the jth column of H_k, where $i, j = 0, 1, \ldots, 2^k - 1$, and denote by h_i the ith row of H_k, i.e., $h_i = (h_{i0}, h_{i1}, \ldots, h_{i2^k-1})$. Then we have

$$(h_s H_k) \times \ell_i = \sum_{u=0}^{2^k-1} h_{su} L_{i+u2^m} \tag{8}$$

Note that $2^{-k} h_s H_k = (0, \ldots, 0, 1, 0, \ldots, 0)$ where all the entries, except the sth, are zero. We further have

$$2^{-k}(h_s H_k) \times \ell_i = (0, \ldots, 0, \ell_i, 0, \ldots, 0) \tag{9}$$

where each 0 denotes the all-zero sequence of length 2^m and the sth sequence of length 2^m is ℓ_i. Comparing (9) and (8), we conclude

$$(0, \ldots, 0, \ell_i, 0, \ldots, 0) = 2^{-k} \sum_{u=0}^{2^k-1} h_{su} L_{i+u2^m}$$

and hence

$$\begin{aligned} \xi &= (c_0 \ell_{j_0}, c_1 \ell_{j_1}, \ldots, c_{2^k-1} \ell_{j_{2^k-1}}) \\ &= 2^{-k}(c_0 \sum_{u=0}^{2^k-1} h_{0u} L_{j_0+u2^m},\ c_1 \sum_{u=0}^{2^k-1} h_{1u} L_{j_1+u2^m}, \ldots \\ &\quad \ldots, c_{2^k-1} \sum_{u=0}^{2^k-1} h_{2^k-1u} L_{j_{2^k-1}+u2^m}) \end{aligned} \tag{10}$$

By using (10), we obtain

$$\langle \xi, L_i \rangle = \begin{cases} 0 & \text{if } i \neq j_0 + u2^m, j_1 + u2^m, \ldots, j_{2^k-1} + u2^m, \\ & \text{where } u = 0, 1, \ldots, 2^k - 1 \\ 2^m c_s h_{su} & \text{if } i = j_s + u2^m \text{ for some } s \text{ and } u, \\ & 0 \leq s, u \leq 2^k - 1 \end{cases} \tag{11}$$

Let $t_0, t_1, \ldots, t_{2^k-1}$ be a rearrangement of $j_0, j_1, \ldots, j_{2^k-1}$ such that $t_0 < t_1 < \cdots < t_{2^k-1}$ and τ be the permutation on $\{j_0, j_1, \ldots, j_{2^k-1}\}$ such that

$$\tau(j_0) = t_0, \tau(j_1) = t_1, \ldots, \tau(j_{2^k-1}) = t_{2^k-1}.$$

Note that $t_j + v2^m < t_i + u2^m$ if $v \leq u$ and $j < i$, where $0 \leq u, v, i, j \leq 2^k - 1$.

Next we rearrange $c_0, c_1, \ldots, c_{2^k-1}$ in such a way that c_s is placed before $c_{s'}$ if and only if $j_s < j_{s'}$. We write the rearranged sequence as

$$b_0, b_1, \ldots, b_{2^k-1}.$$

Now we can use (11) to list all the non-zero terms in $2^{-m}\xi H_{m+k}$, from the left to the right, as follows

$$\begin{array}{l} b_0 h_{t_0 0}, b_1 h_{t_1 0}, \ldots, b_{2^k-1} h_{t_{2^k-1} 0}, \\ b_0 h_{t_0 1}, b_1 h_{t_1 1}, \ldots, b_{2^k-1} h_{t_{2^k-1} 1}, \\ \ldots, \\ b_0 h_{t_0 2^k-1}, b_1 h_{t_1 2^k-1}, \ldots, b_{2k-1} h_{t_{2^k-1} 2^k-1} \end{array} \tag{12}$$

Another way to look at the non-zero terms in $2^{-m}\xi H_{m+k}$, from the left to the right, is as follows:

$$\begin{array}{l} b_0 h_{\tau(j_0)0}, b_1 h_{\tau(j_1)0}, \ldots, b_{2^k-1} h_{\tau(j_{2^k-1})0}, \\ b_0 h_{\tau(j_0)1}, b_1 h_{\tau(j_1)1}, \ldots, b_{2^k-1} h_{\tau(j_{2^k-1})1}, \\ \ldots, \\ b_0 h_{\tau(j_0)2^k-1}, b_1 h_{\tau(j_1)2^k-1}, \ldots, b_{2^k-1} h_{\tau(j_{2^k-1})2^k-1} \end{array} \tag{13}$$

Furthermore, we define a permutation σ on $\{0, 1, \ldots, 2^k - 1\}$ such that

$$\sigma(0) = j_0, \sigma(1) = j_1, \ldots, \sigma(2^k - 1) = j_{2^k-1}.$$

Since H_k is symmetric, (13) can be rewritten as

$$\begin{array}{l} b_0 h_{0\tau\sigma(0)}, b_1 h_{0\tau\sigma(1)}, \ldots, b_{2^k-1} h_{0\tau\sigma(2^k-1)}, \\ b_0 h_{1\tau\sigma(0)}, b_1 h_{1\tau\sigma(1)}, \ldots, b_{2^k-1} h_{1\tau\sigma(2^k-1)}, \\ \ldots, \\ b_0 h_{2^k-1\tau\sigma(0)}, b_1 h_{2^k-1\tau\sigma(1)}, \ldots, b_{2^k-1} h_{2^k-1\tau\sigma(2^k-1)} \end{array} \tag{14}$$

Noting (5) and (6), together with Lemma 1, we have proved that (14) is the sequence of a bent function on V_{2k}. Thus the following theorem holds.

Theorem 1 *Let $k \leq m$ and F be an one-to-one mapping from V_k to V_m and r be a function on V_k. Define a function on V_{k+m}:*

$$f(z) = f(y,x) = F(y)x^T \oplus r(y)$$

where $x \in V_m$, $y \in V_k$ and $z = (y,x)$. Let ξ denote the sequence of f. Then the sequence obtained by concatenating the non-zero terms in $2^{-m}\xi H_{m+k}$, from the left to the right, is the sequence of a bent function on V_{2k}.

As a consequence, we have

Corollary 1 *The sequence of a bent function on V_{2k}, obtained in Theorem 1, takes the form of (6), and also the form of (4).*

It should be noted that Theorem 1 does not contradict the well-known fact that a function is bent if and only if its Fourier transform is bent [6]. This is simply because the sequence $2^{-m}\xi H_{k+m}$ in Theorem 1 is a $(1,-1,0)$-sequence, but not a $(1,-1)$-sequence. In addition, we also note that the Fourier transform of f on V_{k+m}, defined in Theorem 1, is $2^{-\frac{1}{2}(k+m)}\xi H_{k+m}$, but not $2^{-m}\xi H_{k+m}$. However, as $2^{-\frac{1}{2}(k+m)}\xi H_{k+m}$ can be obtained by multiplying $2^{-m}\xi H_{k+m}$ by a factor of $2^{\frac{1}{2}(m-k)}$, we can think of the bent function defined in Theorem 1 as one that is "hidden" in (the non-zero terms of) the Fourier transform of f.

6 Conclusions

It is well-known that when $k = m$ and Q is a permutation in (1), the resultant Maiorana-McFarland function is bent; and in contrast, when $k < m$ the Maiorana-McFarland function is not bent. Results in this paper show that the Fourier transform of a Maiorana-McFarland function contains a "hidden" bent function, provided that when $k \leq m$ and Q is an one-to-one mapping. We hope that this new property will contribute to the further understanding of Maiorana-McFarland functions and its applications both in combinatorics and engineering fields.

7 Acknowledgement

The second author was supported by a Queen Elizabeth II Fellowship (227 23 1002).

References

[1] P. Camion, C. Carlet, P. Charpin, and N. Sendrier. On correlation-immune functions. In *Advances in Cryptology - CRYPTO'91*, volume 576 of *Lecture Notes in Computer Science*, pages 87–100. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

[2] C. Carlet and P. Codes. More correlation-immune and resilient functions over Galois fields and Galois ring. In *Advances in Cryptology - EUROCRYPT'98*, volume 1233 of *Lecture Notes in Computer Science*, pages 422–433. Springer-Verlag, Berlin, Heidelberg, New York, 1997.

[3] J. F. Dillon. A survey of bent functions. *The NSA Technical Journal*, pages 191–215, 1972. (unclassified).

[4] J. F. Dillon. *Elementary Hadamard Difference Sets.* Ph.D. dissertation, University of Maryland, 1974.

[5] J. F. Dillon. *Elementary Hadamard difference sets.* In *Proceeding of the Sixth Southeastern Conference on Combinatorics, Graph Theory, and Computing*, pages 237–249, 1975.

[6] O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory*, Ser. A, 20:300–305, 1976.

[7] J. Seberry, X. M. Zhang, and Y. Zheng. On constructions and nonlinearity of correlation immune functions. In *Advances in Cryptology - EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 181–199. Springer-Verlag, Berlin, Heidelberg, New York, 1994.

[8] J. Seberry, X. M. Zhang, and Y. Zheng. Nonlinearity and propagation characteristics of balanced boolean functions. *Information and Computation*, 119(1):1–13, 1995.

[9] R. Yarlagadda and J. E. Hershey. Analysis and synthesis of bent sequences. *IEE Proceedings (Part E)*, 136:112–123, 1989.