THE RESEARCH ON THE PROPERTIES OF FOURIER MATRIX AND BENT FUNCTION

LI ZHANG∗
School of Mathematics and Statistics
Changshu Institute of Technology
Suzhou, 215500, China

XIAOFENG ZHOU
Shanghai Seed Power Enterprise Management Consulting Co., LTD
Minhang District, Shanghai, 201200, China

MIN CHEN
Asset Management Department
Jiangsu Zijin Rural Commercial Bank Co., LTD
Nanjing, 210023, China

Abstract. This paper first gives out basic background and some definitions and propositions for Fourier matrix and bent function. Secondly we construct an standard orthogonal basis by the eigenvectors of the corresponding Fourier matrix. At last the diagonalization work of Fourier matrix is completed and some theorems about them are proved.

1. Introduction. With development of science and technology, especially the rapid development of modern information technology, cryptography has become increasingly more and more important. From military information transmission to image compression in the field of electronic storage devices, they used all kinds of cryptography. After the definition of bent function given by Rothaus in 1976, many scholars have made much research on this hot spot, many papers on it can been seen in the book [1]. In a word, bent function is the kind of Boole function with the maximum nonlinearity degree. Bent functions with odd dimensions are not existing, but bent functions with even dimensions are existing definitely. For ordinary situations with \( n = 2k \), only several classes of bent functions are given out. So it is important to find out all bent functions with even dimensions. When the dimension \( n \leq 6 \), all kinds of bent functions are found out with concrete expressions. When the dimension \( n = 8 \), the problems are solved by P. Langevin in 2006[10]. When the dimension \( n \geq 10 \), it is not very clear. The main result of this paper is to find out the standard orthogonal basis composed by the eigenvectors of the corresponding Fourier matrix. Then it is clear to diagonalize the corresponding Fourier matrix. The structure of this paper is as follows. In Section 1, the background of this paper knowledge is given out. In Section 2, some basic knowledge and some properties
about Boole function, bent function and Fourier matrix are put forward. In Section 3, some lemmas and fundamental theorems are given out and find the concise method to diagonalize the corresponding Fourier matrix. In Section 4, conclusions and some remarks are given out at last.

2. Preliminary Knowledge. Set $F_2$ is the finite field with two elements 0 and 1. Set $V = F_2^n$ is one $N$-dimensional linear space on the field of $F_2$.

Definition 2.1. The function from $V$ to $F_2$ is called the Boole function.

Definition 2.2. Set $BF(n)$ is the set of all Boole functions on the set $V$. For any $x \in V$, the Hamming distance, called $WH(x)$, is the number of the non-zero indexes. The concrete expression is given out as follows:

$$WH(x) = |\{i | i \in N, x_i \neq 0\},$$

where $N = \{1, 2, \cdots, n\}$.

Definition 2.3. Set $BF(n)$ is the set of all Boole functions on the set $V$. For any $f \in BF(n)$, the Hamming distance, called $W_H(f)$, is the number of the non-zero indexes. The concrete expression is given out as follows.

$$W_H(f) = |\{x \in V | f(x) \neq 0\}|.$$

where $\{x \in V | f(x) \neq 0\}$ is called the support set of the function $f$, and it is written by $supp f$. For the any pair of functions $f$ and $g$, the distance of them is calculated by the following formula:

$$d(f, g) = W_H(f - g).$$

2.1. Boole Vector. Set $S, T$ are two sets and $F$ is the number field. Then one $S \times T$ matrix is given out as following:

$$(a_{x,y}),$$

where the index $x$ is changing in the set $S$, and the other index $y$ is changing in the set $T$. It is clear that any $S \times T$ matrix $A = (a_{x,y})_{x \in S, y \in T}$ is the same as one function $f : S \times T \rightarrow F$, which make the expression true:

$$f(x, y) = (a_{x,y}).$$

Then in this method, any function $f : S \rightarrow F$ can been treated as the $S \times \{1\}$ matrix. Set the function $f \in BF(n)$, that is to say,

$$f : V \rightarrow F_2.$$ 

Then we can treat the function $f$ as one $V$-dimensional column vector. At that moment, the function $f$ is one Boole vector.

Set $A = (a_{x,y})$ is the $S \times T$ matrix and $B = (b_{y,z})$ is the $T \times Z$ matrix. If one $S \times R$ matrix $C = (c_{x,z})$ is called the product of $A$ and $B$ which is satisfied with the following condition:

$$c_{x,z} = \sum_{y \in T} a_{x,y} b_{y,z}, \forall x \in S, z \in R$$

and at that moment it is written by $C = AB$. 
2.2. Fourier Change and Fourier Matrix.

**Definition 2.4.** The function from the set $V = F_2^n$ to $R$ is called Pseudo Boole function. The set $PBF(n)$ is the set of all Pseudo Boole functions on $V$. The natural base of $V = F_2^n$ is listed as follows.

$$e_1 = (1, 0, 0, \cdots, 0), e_2 = (0, 1, 0, \cdots, 0), \cdots, e_n = (0, 0, \cdots, 1)$$

Now the inner product $(−, −)$ on the set $V$ is given out:

$$(x, y) = \sum_{i=1}^{n} x_i y_i,$$

where $x = \sum_{i=1}^{n} x_i$ and $y = \sum_{i=1}^{n} y_i$.

**Definition 2.5.** For any $\phi \in PBF(n)$, the function $\hat{\phi}$ is given out as follows:

$$\hat{\phi} = \sum_{i=1}^{n} \phi(x)(−1)^{(x, \phi)}.$$ 

Then the function $\hat{\phi}$ is called the Fourier transform.

The function from the set $V = F_2^n$ to $R$ is called the Pseudo Boole function. The set $PBF(n)$ is the set of all Pseudo Boole functions on $V$.

**Definition 2.6.** The kind of $V \times V$ matrix $M_n = ((−1)^{(x, y)})_{x \in V, y \in V}$ is called the Fourier matrix.

From the definition, the Fourier matrix $M_n$ is an symmetric matrix. For the Pseudo Boolean function is regarded as an $V$-dimensional column vector, the Fourier matrix $M_n$ is representing the corresponding Fourier transformation. In another word, for any $\phi \in PBF(n)$,

$$\hat{\phi} = M_n \phi.$$ 

From the above expression, we can deduce as follows:

$$\hat{\hat{\phi}} = 2^n \phi, \quad \hat{\phi} = M_n^2 \phi.$$ 

So it is clear that

$$M_n^2 = 2^n E,$$

where $E$ is the unit matrix. Now set $V_n = F_2^n$. By the following injective mapping,

$$V_{n-1} \rightarrow V_n : (x_1, x_2, \cdots, x_{n-1}) \rightarrow (x_1, x_2, \cdots, x_{n-1}, 0).$$

The set $V_{n-1}$ is regarded as one subset of the $V_n$. Then we have

$$V_n = V_{n-1} + V_{n-1}',$$

where $V_{n-1}' = \{(x, 1)|x \in V_{n-1}\}$.

At the same time, $V_{n-1}$ is equivalent to $V_{n-1}'$ by the following bijective mapping:

$$V_{n-1} \rightarrow V_{n-1}' : x \rightarrow (x, 1).$$

So it is obvious that the following formula is true:

$$M_n = \left( \begin{array}{cc} M_{n-1} & M_{n-1} \\ M_{n-1} & -M_{n-1} \end{array} \right).$$
2.3. **Bent function.** For any $a \in V_n$, the function $l_n(x) = a \cdot x$ is called linear function, where $a \cdot x \in \{0, 1\}$ and $a \cdot x = (a, x) \mod 2$.

**Definition 2.7.** For any $f \in BF(n)$, the nonlinearity of the function $f$ is defined as following expression:

$$nl(f) = \min_{a, b \in V_n} d(f, l_a + b).$$

It is not difficult to prove that $nl(f) \leq 2^n - 2^{\frac{n}{2}-1}$ for any $f \in BF(n)$. The detail is seen in [1].

**Definition 2.8.** For any $f \in BF(n)$, if

$$nl(f) = 2^n - 2^{\frac{n}{2}-1},$$

the function $f$ is called the bent function.

**Lemma 2.9.** The function $f$ is a bent function if and only if

$$f(x) = \pm 2^{\frac{n}{2}}, \forall x \in V.$$

where $f(x) = (-1)^{f(x)}$.

**Proof.** The detail is seen in [1].

Now suppose that $f$ is one bent function. Set $\phi = f_R$. From Lemma 2.9, it is clear that

$$\hat{\phi} = \pm 2^{\frac{n}{2}}.$$

Now set $\phi^\circ(x) = 2^{-\frac{n}{2}} \phi, \forall x \in V$. Then the function is one Pseudo Boole function with the value field $\{1, -1\}$. So the function $f^\circ = \frac{1}{2}(1 - \phi^\circ)$ is one Boole function. The function $f^\circ$ is called the dual function of the function $f$. By some computation, it is clear that $(f^\circ)_R = \phi^\circ$. Now we notice that

$$\phi^\circ = 2^{-\frac{n}{2}} M_n \phi,$$

and with $M_n^2 = 2^n E$, we have

$$M_n \phi^\circ = 2^{\frac{n}{2}} \phi.$$

So the function $f$ is one bent function at the same time. Thus the following lemma is also true.

**Lemma 2.10.** If the function $f$ is a bent function, then we have that

$$(f^\circ)^\circ = f.$$

3. **Diagonalization of the Fourier matrix.** From Section 2, we can see that the Fourier matrix is closely related with the bent function. In actually, $\phi + \phi^\circ$ and $\phi - \phi^\circ$ are all the eigenvectors of the matrix $M_n$. So it is vital to find out the standard orthogonal basis by the eigenvectors of the matrix $M_n$. Now the whole process of this work is given out as follows.

3.1. **The definition of $L_+$ and $L_-**. Now set

$$L_+ = \{x | M_n x = 2^{\frac{n}{2}} x\},$$

$$L_- = \{x | M_n x = -2^{\frac{n}{2}} x\}.$$

It is clear that $L_+$ and $L_-$ are all the linear space of the the eigenvectors of the matrix $M_n$.
3.2. To find out $\dim L_+$ and $\dim L_-$. Because 

$$M_n^2 = 2^n E,$$

we have that 

$$(M_n - 2^\frac{n}{2} E)(M_n + 2^\frac{n}{2} E) = 0,$$

so the all column vectors of the matrix $M_n + 2^\frac{n}{2} E$ is the eigenvectors belonging to the characteristic value $2^\frac{n}{2}$, and the all column vectors of the matrix $M_n - 2^\frac{n}{2} E$ is the eigenvectors belonging to the characteristic value $-2^\frac{n}{2}$.

In another way, 

$$M_n + 2^\frac{n}{2} E = \begin{pmatrix} M_{n-1} + 2^\frac{n}{2} E & M_{n-1} \\ M_{n-1} & -M_{n-1} + 2^\frac{n}{2} E \end{pmatrix}.$$

Then we have 

$$M_n + 2^\frac{n}{2} E \rightarrow \begin{pmatrix} 2^\frac{n}{2} E & 2M_{n-1} - 2^\frac{n}{2} E \\ M_{n-1} & -M_{n-1} + 2^\frac{n}{2} E \end{pmatrix} \rightarrow \begin{pmatrix} 2^\frac{n}{2} E & 2M_{n-1} - 2^\frac{n}{2} E \\ 0 & 0 \end{pmatrix}.$$

In the above expression, the first transform is $r_1 - r_2 \rightarrow r_1$. The first transform is $2^\frac{n}{2} M_{n-1} r_1 + r_2 \rightarrow r_2$. By the above expression, we have that 

$$R(M_{n-1} + 2^\frac{n}{2} E) = 2^{n-1}.$$

At the same time, 

$$M_n - 2^\frac{n}{2} E = \begin{pmatrix} M_{n-1} - 2^\frac{n}{2} E & M_{n-1} \\ M_{n-1} & -M_{n-1} - 2^\frac{n}{2} E \end{pmatrix}.$$

We also have 

$$M_n - 2^\frac{n}{2} E \rightarrow \begin{pmatrix} 2^\frac{n}{2} E & 2M_{n-1} + 2^\frac{n}{2} E \\ M_{n-1} & -M_{n-1} - 2^\frac{n}{2} E \end{pmatrix} \rightarrow \begin{pmatrix} 2^\frac{n}{2} E & 2M_{n-1} + 2^\frac{n}{2} E \\ 0 & 0 \end{pmatrix}.$$

In the above expression, the first transform is $r_1 - r_2 \rightarrow r_1$. The first transform is $2^\frac{n}{2} M_{n-1} r_1 + r_2 \rightarrow r_2$. By the above expression, we have that 

$$R(M_{n-1} - 2^\frac{n}{2} E) = 2^{n-1}.$$

By the computation and the two expressions, we give the following theorems.

**Theorem 3.1.** Suppose the sets $L_+, L_-$ are defined as the above part, then we have that 

$$\dim L_+ = \dim L_- = 2^{n-1}.$$

**Proof.** Because we have the result that $R(M_{n-1} + 2^\frac{n}{2} E) = 2^{n-1}$ and all column vectors are in the set $L_+$, so it is clear that 

$$\dim L_+ \geq 2^{n-1}.$$

At the same time, we also can have that 

$$\dim L_- \geq 2^{n-1}.$$

But we have the condition $\dim L_+ + \dim L_- \leq 2^n$. So we get the conclusion as follows:

$$\dim L_+ = \dim L_- = 2^{n-1}.$$
3.3. The construction of standard orthogonal basis. Let $\alpha$ be one root of the equation $x^2 - 2x - 1 = 0$. Set the group of vectors $\beta_1, \beta_2, \cdots, \beta_{2^n-1}$ is the set of all column vectors of the following matrix $A$,

$$A = \begin{pmatrix} (1 + \alpha)M_{n-1} + 2\frac{\alpha}{2}E \\ (1 - \alpha)M_{n-1} + \alpha 2\frac{\alpha}{2}E \end{pmatrix}.$$ 

Notice that

$$\begin{pmatrix} (1 + \alpha)M_{n-1} + 2\frac{\alpha}{2}E \\ (1 - \alpha)M_{n-1} + \alpha 2\frac{\alpha}{2}E \end{pmatrix} = \begin{pmatrix} M_{n-1} + 2\frac{\alpha}{2}E \\ M_{n-1} \end{pmatrix} + \alpha \begin{pmatrix} M_{n-1} \\ -M_{n-1} + 2\frac{\alpha}{2}E \end{pmatrix}.$$ 

So it is clear that

$$\beta_1, \beta_2, \cdots, \beta_{2^n-1} \in L_+.$$ 

At the same time, we have that

$$A^T A = \begin{pmatrix} (1 + \alpha)M_{n-1} + 2\frac{\alpha}{2}E \\ (1 - \alpha)M_{n-1} + \alpha 2\frac{\alpha}{2}E \end{pmatrix}^T \begin{pmatrix} (1 + \alpha)M_{n-1} + 2\frac{\alpha}{2}E \\ (1 - \alpha)M_{n-1} + \alpha 2\frac{\alpha}{2}E \end{pmatrix}$$

$$= (1 + \alpha)^2M_{n-1}^2 + 2nE + 2(1 + \alpha)2\frac{\alpha}{2}M_{n-1} + 2(1 - \alpha)2\frac{\alpha}{2}M_{n-1} + (1 - \alpha)^22\frac{\alpha}{2}M_{n-1} + (1 + \alpha)^22\frac{\alpha}{2}M_{n-1} + 2(1 - \alpha)^22\frac{\alpha}{2}M_{n-1} + (1 - \alpha)^22\frac{\alpha}{2}M_{n-1}$$

$$= (2 + 2\alpha^2)M_{n-1}^2 + (1 + \alpha^2)2nE + (2 + 4\alpha - 2\alpha^2)M_{n-1}2\frac{\alpha}{2}$$

$$= (2 + 2\alpha^2)M_{n-1}^2 + (1 + \alpha^2)2nE - 2(\alpha^2 - 2\alpha - 1)M_{n-1}2\frac{\alpha}{2}$$

$$= [(2 + 2\alpha^2)2^{n-1} + (1 + \alpha^2)2^n]E$$

$$= 2^{n-1}[4 + 4\alpha^2]E$$

$$= 2^{n+1}[1 + \alpha^2]E$$

$$= 2^{n+2}[1 + \alpha]E.$$ 

Now set

$$\beta'_i = \frac{1}{\sqrt{2^{n+2}(1 + \alpha)}} \beta_i, i = 1, 2, \cdots, 2^n-1$$

The group of vectors $\beta'_1, \beta'_2, \cdots, \beta'_{2^n-1}$ is the standard orthogonal basis of $L_+$. 

Let $\alpha$ be one root of the equation $x^2 - 2x - 1 = 0$. Set the group of vectors $\gamma_1, \gamma_2, \cdots, \gamma_{2^n-1}$ is the set of all column vectors of the following matrix $B$,

$$B = \begin{pmatrix} (1 + \alpha)M_{n-1} - 2\frac{\alpha}{2}E \\ (1 - \alpha)M_{n-1} - \alpha 2\frac{\alpha}{2}E \end{pmatrix}.$$ 

Notice that

$$\begin{pmatrix} (1 + \alpha)M_{n-1} - 2\frac{\alpha}{2}E \\ (1 - \alpha)M_{n-1} - \alpha 2\frac{\alpha}{2}E \end{pmatrix} = \begin{pmatrix} M_{n-1} - 2\frac{\alpha}{2}E \\ M_{n-1} \end{pmatrix} + \alpha \begin{pmatrix} M_{n-1} \\ -M_{n-1} - 2\frac{\alpha}{2}E \end{pmatrix}.$$ 

So it is clear that

$$\gamma_1, \gamma_2, \cdots, \gamma_{2^n-1} \in L_-.$$
At the same time, we have

\[ B^T B = \begin{pmatrix} (1 + \alpha)M_{n-1} - 2^\frac{n}{2}E \\ (1 - \alpha)M_{n-1} - \alpha 2^\frac{n}{2}E \end{pmatrix}^T \begin{pmatrix} (1 + \alpha)M_{n-1} - 2^\frac{n}{2}E \\ (1 - \alpha)M_{n-1} - \alpha 2^\frac{n}{2}E \end{pmatrix} \]

\[ = (1 + \alpha)^2M_n^2 + 2^nE - 2(1 + \alpha)2^\frac{n}{2}M_{n-1} - 2(1 - \alpha)2^\frac{n}{2}\alpha M_{n-1} \]

\[ + (1 - \alpha)^2M_n^2 + \alpha 2^nE \]

\[ = (2 + 2\alpha^2)M_{n-1}^2 + (1 + \alpha^2)2^nE + (-2 + 4\alpha^2)M_{n-1}2^\frac{n}{2} \]

\[ = (2 + 2\alpha^2)M_{n-1}^2 + (1 + \alpha^2)2^nE - 2(\alpha^2 - 2\alpha - 1)M_{n-1}2^\frac{n}{2} \]

\[ = [(2 + 2\alpha^2)2^{n-1} + (1 + \alpha^2)2^n]E \]

\[ = 2^{n-1}[4 + 4\alpha^2]E \]

\[ = 2^{n+1}[1 + \alpha^2]E \]

\[ = 2^{n+2}[1 + \alpha]E. \]

Now set

\[ \gamma'_i = \frac{1}{\sqrt{2^{n+2}(1 + \alpha)}}\beta_i, i = 1, 2, \ldots, 2^{n-1} \]

The group of vectors \( \gamma'_1, \gamma'_2, \ldots, \gamma'_{2^{n-1}} \) is the standard orthogonal basis of \( L_- \). Based on the computations and conclusions, we can get the following theorem clearly.

**Theorem 3.2.** For any matrix \( M_n \), there are one orthogonal matrix \( P \), which make the equation true as follows:

\[ P^T M_n P = \begin{pmatrix} 2^\frac{n}{2}E & 0 \\ 0 & -2^\frac{n}{2}E \end{pmatrix}. \]

**Proof.** Set

\[ P = (\beta_1', \beta_2', \ldots, \beta_{2^{n-1}}', \gamma'_1, \gamma'_2, \ldots, \gamma'_{2^{n-1}}). \]

Through the above calculation, so we can get the following equation:

\[ P^T M_n P = \begin{pmatrix} 2^\frac{n}{2}E & 0 \\ 0 & -2^\frac{n}{2}E \end{pmatrix}, \]

so the conclusion is true.

\[ \square \]

4. **Results and discussions.** In this paper, we give out the background of Boole function, bent function and so on. Some basic relations among them and some properties are given out. By careful analysis and computations, the dimensions of \( L_+ \) and \( L_- \) are found out accurately. Then a group of column vectors of corresponding matrixes is put forward. The work of diagonalization for the Fourier matrix is completed and some good theorems are proved at last.

**REFERENCES**

[1] C. Carlet, *Boolean Function For Cryptography And Error Correcting Codes*, Cambridge University, 2007.

[2] C. Hughes, Partially-bent functions, *Proceedings of The 12th Annual International Cryptography Conference on Advances In Cryptography*, 74 (1992), 280–291.

[3] J. Ding, H. Zhen, Q. Wen and Y. Yang, Construction and enumeration of multiple-output orthogonal Boolean functions, *Journal of Beijing University of Posts and Telecommunications*, 4 (2005), 9–11.
[4] V. Kumear, A. Scholtz and R. Welch, Generalized bent functions and their properties, *Journal of Combinatorial Theory*, 4 (1985), 90–107.

[5] R.Lint and H. Niederreiter, *Finite Fields*, Addison-Wesley Publishing Company, New York, 1984.

[6] O. Rothaus, On bent functions, *Journal of Combinatorial Theory*, 20 (1976), 300–305.

[7] X. Hou and P. Langevin, Results on bent functions, *Journal of Combinatorial Theory*, 80 (1997), 232–246.

[8] P. Langevin, On generalized bent functions, *CISM Course and Lectures*, 339 (1992), 147–159.

[9] P. Langevin and X. Hou, Computing partial spread functions in eight variables, *IEEE Trans. Inf. Theory*, 57 (2011), 2263–2269.

[10] P. Langevin, P. Rabizzoni, P. Veron and J. Zanotti, On the number of bent functions with 8 variables, *Proceedings of the Conference BFCA 2006*, Publications des universites de Rousen et du Havre (2006), 125–136.

[11] Y. Yuan, D. Jin, Y. Zhao and S. Zhang, Relationship between generalized partially bent functions and generalized bent functions over finite fields, *Journal of Information Engineering University*, 9 (2009), 313–317.

[12] Y. Zhao and S. Li, Generalized partially-bent functions and characteristics of the autocorrelation functions and spectrum, *Journal of Engineering Mathematics*, 4 (1999), 91–96.

[13] W. Sun and Y. Yuan, *Optimization Theory and Methods: Nonlinear Programming*, Springer, New York, 2006.

[14] Y. Yuan and W. Sun, *Optimization Theory and Methods*, Science Press, Beijing, 1997.

Received April 2020; 1st revision August 2020; Final revision September 2020.

E-mail address: zhang2006@cslg.edu.cn
E-mail address: txzxf@163.com
E-mail address: 19722772@qq.com