GENERALIZED FIXED POLARITY HELIX TRANSFORMS OVER GF(4)

Cheng Fu

Intelligent Systems Centre
Nanyang Technological University
50 Nanyang Drive, RTP, Singapore 637553
fucheng@ntu.edu.sg

Bogdan J. Falkowski

School of Electrical and Electronic Engineering
Nanyang Technological University
50 Nanyang Avenue, Block S1, Singapore 639798
efalkowski@ntu.edu.sg

ABSTRACT

New linearly independent quaternary transforms over Galois Field (4) called Generalized Fixed Polarity Helix transforms are introduced here. Their definitions based on recursive equations are described. Various properties of quaternary helix transform matrices, their mutual relations as well as their butterfly diagrams and computational costs versus quaternary Reed-Muller transform are also discussed.

1. INTRODUCTION

The algebra of linearly independent transforms constructed on the basis of different binary and ternary functions in Galois Field (GF)(2) and GF(3) have been developed in [1, 2]. Linearly independent logic has proved to be not only of great theoretical value, but also of practical value, to the design of fine-grain and cellular automata types of Field Programmable Gate Arrays (FPGAs) and different Programmable Logic Devices (PLDs) with XOR gates.

In this article, Fixed Polarity Quaternary Helix (FPQH) transforms are proposed that are based on four new transforms, which have very regular structure that results in their fast computation and some interesting properties. These transforms are named quaternary helix transforms due to their symmetrical structure along the diagonal in the transform matrices similar to our previous GF(3) article [3]. Relations and properties between different helix matrices are also shown. Butterfly diagrams and properties of these quaternary helix transforms are also discussed. As analyzed in computational costs, the introduced helix transforms are much faster in calculation of their spectra than Quaternary Reed-Muller transform (QRM) [4]. The concept of FPQH transforms is also extended into general case where each transform possesses 4^n different polarity expansions. They are named Generalized Fixed Polarity Quaternary Helix (GFPQH) transforms.

2. BASIC DEFINITIONS

Definition 1. Let M_n be a $4^n \times 4^n$ matrix with columns corresponding to some quaternary functions of *n*-variable over GF(4). If the set of columns is linearly independent with respect to bit-by-bit GF(4) operations, then M_n has one unique inverse M_n^{-1}, and is said to be linearly independent, i.e.

$$M_n \cdot M_n^{-1} = I_n \tag{1}$$

where I_n is a $4^n \times 4^n$ identity matrix and all the operations are performed over GF(4) as described in Tables 1 and 2.

The linearly independent transform based on Definition 1 can be described by the following general formulae performed over operations in GF(4):

$$M_n \cdot \vec{A} = \vec{F} \tag{2}$$

and

$$M_n^{-1} \cdot \vec{F} = \vec{A} \tag{3}$$

where $\vec{F} = [f_0, \quad f_1, \quad ..., \quad f_{4^n-1}]^T$ is a column vector defining the truth vector of a quaternary function $f(x_n)$ in natural quaternary ordering, M_n is a matrix of order $N = 4^n$ defined by any linearly independent set of *n*-variable quaternary functions and $\vec{A} = [a_0, \quad a_1, \quad ..., \quad a_{4^n-1}]^T$ is the spectral coefficient column vector for the particular transform matrix M_n with the inverse M_n^{-1} while *T* is the matrix transpose operator.

Formula (2) can be written as

$$f(x_n) = \sum_{i=0}^{4^n-1} a_i g_i \tag{4}$$

where g_i represents the truth vector of an *n*-variable quaternary function over GF(4), such that the matrix $M_n = [g_0, \quad g_1, \quad ..., \quad g_{4^n-1}]^T$, $0 \le i \le 4^n - 1$, and the symbol $\sum$ is the addition performed over GF(4).

Definition 2. Let M_n be a matrix of order *N* following Definition 1. Additionally, M_n can be partitioned into 16 $4^{n-1} \times 4^{n-1}$ submatrices M_{n-1} as shown in the following equation,

$$M_n = \begin{bmatrix} M_{n-1}^{(1,1)} & ... & M_{n-1}^{(1,4)} \\ ... & ... & ... \\ M_{n-1}^{(4,1)} & ... & M_{n-1}^{(4,4)} \end{bmatrix} \tag{5}$$

Table 1 –Additions over GF(4)

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Table 2 –Multiplications over GF(4)

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

3. FIXED POLARITY QUATERNARY HELIX TRANSFORMS

In this section, four basic FPQH transforms will be presented. They are denoted as Right-Positive-Helix (***RPH***), Left-Positive-Helix (***LPH***), Right-Negative-Helix (***RNH***) and Left-Negative-Helix (***LNH***) transforms based on their different function expansions. All presented helix transforms follow strictly Definitions 1-2.

The kernel matrix of ***RPH*** transform is

$$RPH_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ x & 1 & x & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & x & 1 \end{bmatrix}. \qquad (6)$$

In all the matrices and equations, the parameter $x \in \{1,2,3\}$.

RPH is the transform matrix relating the truth vector $\vec{F}$ and spectral coefficients' vector $\vec{A}$. It can be verified using (2) that

$$f_{0\langle RPH\rangle} = a_0$$
$$f_{1\langle RPH\rangle} = x \cdot a_0 + a_1 + x \cdot a_2$$
$$f_{2\langle RPH\rangle} = a_2$$
$$f_{3\langle RPH\rangle} = x \cdot a_2 + a_3.$$

By (3) it can be obtained that

$$a_{0\langle RPH\rangle} = f_0$$
$$a_{1\langle RPH\rangle} = x \cdot f_0 + f_1 + x \cdot f_2$$
$$a_{2\langle RPH\rangle} = f_2$$
$$a_{3\langle RPH\rangle} = x \cdot f_2 + f_3.$$

It is clear, that the basic ***RPH*** transform matrix is a self-inverse matrix. For order *N*, ***RPH*** transform is extended by using Kronecker product [5, 6], which is performed over GF(4) as shown in the following formula,

$$RPH_n = \overset{n-1}{\otimes} \begin{bmatrix} 1 & 0 & 0 & 0 \\ x & 1 & x & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & x & 1 \end{bmatrix} = \overset{n-1}{\otimes} RPH_1. \qquad (7)$$

Property 1. Let ***RPH*$^{-1}$** be the inverse of ***RPH*** transform of order *N*, then

$$RPH_n^{-1} = RPH_n. \qquad (8)$$

The function expansion of the basic ***LPH*** transform can be derived from the expansion of the basic ***RPH*** transform by interchanging subscripts of the coefficients' vector elements a_i $(0 \le i \le 3)$ between 0 and 3 $(a_0 \Leftrightarrow a_3)$, and between 1 and 2 $(a_1 \Leftrightarrow a_2)$, as shown below:

$$f_{0\langle LPH\rangle} = a_3$$
$$f_{1\langle LPH\rangle} = x \cdot a_1 + a_2 + x \cdot a_3$$
$$f_{2\langle LPH\rangle} = a_1$$
$$f_{3\langle LPH\rangle} = a_0 + x \cdot a_1.$$

The ***LPH*** matrix can be obtained by horizontally flipping the ***RPH*** matrix of the same order *N*. The basic ***LPH*** transform matrix is given by

$$LPH_1 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & x & 1 & x \\ 0 & 1 & 0 & 0 \\ 1 & x & 0 & 0 \end{bmatrix}. \qquad (9)$$

The basic ***LPH*** transform matrix is also a self-inverse matrix so Property 1 applies to it too.

By interchanging subscripts of the truth vector's minterms f_j $(0 \le j \le 3)$ between 0 and 3 $(f_0 \Leftrightarrow f_3)$, and between 1 and 2 $(f_1 \Leftrightarrow f_2)$ in the function expansions of ***RPH*** and ***LPH*** transforms, the results are the expansions of ***RNH*** and ***LNH*** transforms, respectively. The basic transform matrices of ***RNH*** and ***LNH*** can be derived from the basic matrices of ***RPH*** and ***LPH*** by flipping the matrices along their diagonals. The transform matrices of ***RNH*** and ***LNH*** are also the inverse matrices of each other as shown in the following property.

Property 2. Let ***RNH*$^{-1}$** and ***LNH*$^{-1}$** be the inverses of ***RNH*** and ***LNH*** transforms of order *N*, then

$$RNH_n^{-1} = LNH_n. \qquad (10)$$

and

$$LNH_n^{-1} = RNH_n. \qquad (11)$$

In our previous article [2], a fast algorithm was introduced based on decomposition of partial transform matrices. This method is also applied to the four introduced FPQH transforms and used to derive their forward and inverse butterfly diagrams. In Table 3, all FPQH transforms together with their forward butterfly diagrams for *n*=2 are presented. From Properties 1 and 2, the inverse butterfly diagrams of the four FPQH transforms can be also easily derived. The dashed lines correspond to the values of the parameter *x*.

For general case, all quaternary helix expansions can be extended into 4^n different polarity expansions, which are called Generalized Fixed Polarity Quaternary Helix (GFPQH) transforms. Let $RPH_n^{\langle k \rangle}$ represent the *k*-th polarity of the ***RPH*** transform. For order *N*, the generalized ***RPH*** transform $RPH_n^{\langle k \rangle}$ can be derived by

$$RPH_n^{\langle k_0 k_1 \ldots k_{n-1} \rangle} = RPH_1^{\langle k_0 \rangle} \otimes RPH_1^{\langle k_1 \rangle} \otimes \ldots RPH_1^{\langle k_{n-2} \rangle} \otimes RPH_1^{\langle k_{n-1} \rangle} \quad (12)$$

For $n = 1$ and $k = 1$, the new expansions are

$$f_{0\langle RPH^1 \rangle} = f_{1\langle RPH^0 \rangle} = x \cdot a_0 + a_1 + x \cdot a_2$$

$$f_{1\langle RPH^1 \rangle} = f_{0\langle RPH^0 \rangle} = a_0$$

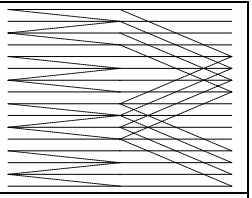
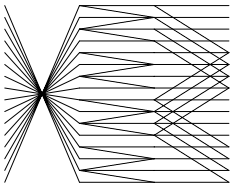
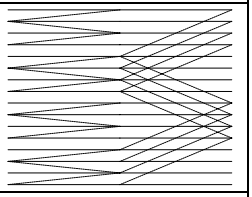
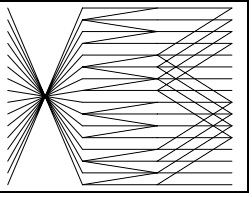
$$f_{2\langle RPH^1 \rangle} = f_{3\langle RPH^0 \rangle} = x \cdot a_2 + a_3$$

$$f_{3\langle RPH^1 \rangle} = f_{2\langle RPH^0 \rangle} = a_2 .$$

In the matrix form,

$$RPH_1^{\langle 1 \rangle} = \begin{bmatrix} x & 1 & x & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & x & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \quad (13)$$

Table 3 –FPQH transforms and their corresponding butterfly diagrams for *n* = 2

RPH	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ x & 1 & x & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & x & 1 \end{bmatrix}$	
LPH	$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & x & 1 & x \\ 0 & 1 & 0 & 0 \\ 1 & x & 0 & 0 \end{bmatrix}$	
RNH	$\begin{bmatrix} 1 & x & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & x & 1 & x \\ 0 & 0 & 0 & 1 \end{bmatrix}$	
LNH	$\begin{bmatrix} 0 & 0 & x & 1 \\ 0 & 0 & 1 & 0 \\ x & 1 & x & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$	

The inverse matrix is

$$\left(RPH_1^{\langle 1 \rangle}\right)^{-1} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & x & 0 & x \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & x \end{bmatrix}. \quad (14)$$

Similarly, for polarities $k = 2$ and $k = 3$, the basic ***RPH*$^{<k>}$** transform matrices are obtained by re-ordering the rows of the forward matrix ***RPH*$^{<0>}$** while the inverse matrices ***RPH*$^{-1}$** are derived by re-ordering their columns.

$$\left(RPH_1^{\langle 2 \rangle}\right)^{-1} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & x & 1 & x \\ 0 & 1 & 0 & 0 \\ 1 & x & 0 & 0 \end{bmatrix}, \quad (15)$$

and

$$\left(RPH_1^{\langle 3 \rangle}\right)^{-1} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ x & 0 & x & 1 \\ 1 & 0 & 0 & 0 \\ x & 1 & 0 & 0 \end{bmatrix}. \quad (16)$$

For order *N*, the generalized inverse ***RPH*** transform $\left(RPH_n^{\langle k \rangle}\right)^{-1}$ can be derived by

$$\left(RPH_n^{\langle k_0 k_1 \ldots k_{n-1} \rangle}\right)^{-1} = \left(RPH_1^{\langle k_0 \rangle}\right)^{-1} \otimes \left(RPH_1^{\langle k_1 \rangle}\right)^{-1} \otimes \ldots \left(RPH_1^{\langle k_{n-2} \rangle}\right)^{-1} \otimes \left(RPH_1^{\langle k_{n-1} \rangle}\right)^{-1} . \quad (17)$$

The concept of GFPQH can be easily extended to other three FPQH transforms. For any *n*-variable quaternary function $f(x_n)$, the *k*-th polarity spectrum $f^{\langle k \rangle}$ can be obtained from the original quaternary function $f(x_n)$ by the following equation performed over GF(4)

$$f^{\langle k \rangle} = \left(RPH_n^{-1}\right)^{\langle k \rangle} \cdot f . \quad (18)$$

4. COMPUTATIONAL COST

The number of non-zero elements in the matrix of FPQH transforms determines the additions required to calculate the spectrum. The four FPQH transforms have the same computational cost due to their close relations.

The total number of 2-place additions to compute FPQH transforms of any *n*-variable quaternary function by direct matrix computational method is

$$S_n = 7^n - 4^n . \quad (19)$$

Based on the fast transform method presented in [2], the additions are reduced to

$$S'_n = n \cdot (7 \cdot 4^{n-1} - 4^n) = 3n \cdot 4^{n-1} . \quad (20)$$

Table 4 gives the comparison of the computational costs between the FPQH transforms and QRM transform both in the direct matrix computation method and through the fast transform algorithms as described in [4].

5. CONCLUSION

The concept of GFPQH transforms over GF(4) is considered for the first time in this paper. Various properties for the helix transforms have been described. In order to make the calculation of these quaternary expansions efficient, the matrix decomposition and corresponding butterfly diagrams are also shown. In addition, the computational costs for FPQH transforms are compared with QRM transform. The GFPQH transforms can also be the bases of new quaternary word decision diagrams in a manner similar to the ones developed in [7].

REFERENCES

[1] B.J. Falkowski and S. Rahardja, "Classification and properties of fast linearly independent logic transformations," *IEEE Trans. on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 44, no. 8, pp. 646–655, Aug. 1997.

[2] B.J. Falkowski and C. Fu, "Classification of new linearly independent transforms over GF(3)," *Journal of Circuits, Systems, and Computers*, World Science Publisher, vol. 14, no. 2, pp. 395-421, April 2005.

[3] C. Fu and B.J. Falkowski, "Multi-polarity helix transform over GF(3)," in *Proc. 37th IEEE Int. Symp. on Circuits and Systems*, Vancouver, Canada, May 2004, pp. 289–292.

[4] D.H. Green, "Reed-Muller expansions with fixed and mixed polarities over GF(4)," *IEE Proc. Computers and Digital Techniques*, vol. 137, no. 5, pp. 380–388, Sept. 1990.

[5] S. Agaian, J. Astola, K. Egiazarian, *Binary Polynomial Transforms and Nonlinear Digital Filters*. New York: Marcel Dekker, 1995.

[6] A. Graham, *Kronecker Products and Matrix Calculus with Applications*. New York: John Wiley, 1981.

[7] R.S. Stankovic and J.T. Astola, *Spectral Interpretation of Decision Diagram*. New York: Springer-Verlag, 2003.

Table 4 –Computational costs

	QRM		QRM^{-1}		FPQH	
n	direct	fast	direct	fast	direct	fast
	$13^n - 4^n$	$9n \cdot 4^{n-1}$	$11^n - 4^n$	$7n \cdot 4^{n-1}$	$7^n - 4^n$	$3n \cdot 4^{n-1}$
1	9	9	7	7	3	3
2	153	72	105	56	33	24
3	2133	432	1267	336	279	144
4	28305	2304	14385	1792	2145	768
5	370269	11520	160027	8960	15783	3840
6	4822713	55296	1767465	43008	113553	18432
7	62732133	258048	19470787	200704	807159	86016