Fast Hadamard Transforms of Williamson Type

Hakob G. Sarukhanyan, Armen J. Anoyan

Institute for Informatics and Automation Problems of NAS RA and YSU

E-mail: hakop@ipia.sci.am, spl@ipia.sci.am

Abstract

The Hadamard transform of Sylvester's type, which is also known as the Walsh-Hadamard transform, is used in signal processing and communication. Note that the Walsh-Hadamard transform operates only with vectors whose length N is a power of 2. If N is not a power of two, then in order to compute the Walsh-Hadamard spectrum of the vector one has to either discard components or pad zeros up to the next power of two. In the first case we have an information loss and in the second case extra computations are needed. Thus, construction of fast Hadamard transforms of different orders is important problem. In this paper we develop fast Hadamard transforms based on special classes of Hadamard matrices, namely, the Williamson type Hadamard matrices.

Introduction

The Hadamard transform, which is known for its simplicity and efficiency in its execution, is one of important transform techniques for signal processing and compression. In the past years, the Hadamard transforms and its variations have been intensively used for audio and video applications [1]-[6]. In order to reduce computation several well-known fast algorithms have been proposed [7] - [11]. The fast algorithms for Hadamard transforms can be found in [8].

More than one hundred years ago in 1893 Jack Hadamard [12] proved that if $A = (a_{i,j})_{i,j=0}^{n-1}$ is an arbitrary real matrix of order n with entries $a_{i,j}$ satisfying the conditions $-1 \le a_{i,j} \le$

+1, then

$$|det A|^2 \leq \prod_{i=1}^n \sum_{j=1}^n a_{i,j}^2,$$

and the equality is achieved when A is an orthogonal matrix, and for $a_{i,j} = \pm 1$ the determinant will get maximal absolute value.

A (-1,+1)-matrix H of order n satisfying conditions

$$H^T H = H H^T = n I_n,$$

where T stands for transposition and I_n is the identity matrix of order n, is called a Hadamard matrix.

Note that first Hadamard matrices were constructed by Sylvester in 1867 [13]. Sylvesters' construction has the following form:

$$H_{2^k} = \begin{pmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{pmatrix}, \quad k = 1, 2, \dots, \tag{1}$$

where $H_1 = (1)$.

Originally matrix of the form (1) was called the Sylvester's type Hadamard matrix [18,

19, 7], but nowadays is better known as the Walsh-Hadamard transform matrix.

Hadamard matrix is called normalized if the first row and the first column consists only +1. It's evidently that to any Hadamard's matrix to correspond a normalized Hadamard matrix. Note that in 1933 Paley proved if H_n is an Hadamard matrix of order n, n > 2, then $n \equiv 0 \pmod{14}$, [14, 15]. The inverse problem i.e. the problem of the constructions or proof of the existence of Hadamard matrices of all orders multiple to four is unsolved up today, though hundreds of papers and some books have been published on Hadamard matrices construction and applications. (See, for example, [7],[16]-[19] and their references).

2 Fast Walsh-Hadamard Transform

Let $X = (x_0, x_1, \dots, x_{N-1})^T$ is a column-vector with real components and $N = 2^n$. Then the direct and inverse one dimensional Walsh-Hadamard transform of the vector X defined from formulae [8]

$$Y = H_N X, \quad X = \frac{1}{N} H_N Y. \tag{2}$$

Sometimes instead of the formulae (2) is considered the following formulae:

$$Y = \frac{1}{\sqrt{N}} H_N X, \quad X = \frac{1}{\sqrt{N}} H_N Y.$$

By using recurrent representation Sylvester matrices of order N, namely $H_N = H_{N/2} \otimes H_2$, it is clear that N-point Hadamard transform can be computed by first performing $\frac{N}{2}$ two-point Hadamard transforms and then performing two $\frac{N}{2}$ -point Hadamard transforms. Recursively using this idea to compute the smaller transforms, an algorithm results to compute the N-point Hadamard transform with $\frac{N}{2}\log_2 N$ two point Hadamard transform. Hence the complexity of one dimensional direct and also inverse Walsh-Hadamard transforms (2) defined from the formulae of the form

$$C_H(N) = N \log_2 N. \tag{3}$$

Note that this transform requires only addition/subtruction operations.

3 Cyclic and Symmetric Williamson Type Matrices

In 1944 Williamson [20], [21] noted that if A, B, C, D are cyclic and symmetric (-1, +1)-matrices of order n satisfying the condition

$$A^2 + B^2 + C^2 + D^2 = 4nI_n,$$

then the matrix

$$H_{4n} = \begin{pmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{pmatrix}, \tag{4}$$

is an Hadamard matrix oorder 4n (further called as Williamson's type Hadamard matrix and A, B, C, D were called Williamson's type matrices).

As well as A, B, C, D are cyclic and symmetric matrices of order n, then they can be represented as follows

$$A = \sum_{i=0}^{n-1} a_i U^i$$
, $B = \sum_{i=0}^{n-1} b_i U^i$, $C = \sum_{i=0}^{n-1} c_i U^i$, $D = \sum_{i=0}^{n-1} d_i U^i$, (5)

where U is a cyclic matrix of order n with first row $(0,1,\ldots,0), U^0=U^n=I_n$ is an identity matrix of order n, and

$$U^{n+i} = U^i, a_i = a_{n-i}, b_i = b_{n-i}, c_i = c_{n-i}, d_i = d_{n-i}, i = 1, 2, \dots, n-1.$$

It is known that matrices

$$A = \begin{pmatrix} + & + & + \\ + & + & + \\ + & + & + \end{pmatrix}, \quad B = C = D = \begin{pmatrix} + & - & - \\ - & + & - \\ - & - & + \end{pmatrix}$$

are Williamson type matrices of order 3. Then after substitute these matrices in (4) we obtain Williamson type Hadamard matrix of order 12 which has the following form

Below there are given first rows of cyclic and symmetric matrices A, B, C, D of Williamson type of orders n, n = 3, 5, ..., 25 [18], [19].

Table of Williamson Type Cyclic and Symmetric Matrices of order n

++--+-+--+++++---+-+

4 Block-Cyclic Block-Symmetric Hadamard Matrices of Williamson Type and Its Fast Transform Algorithms

In [22] it was shown that if there exist Williamson type cyclic and symmetric matrices of order n then there exist block-cyclic block-symmetric Hadamard matrix of order 4n, where blocks of order 4 are themselves Hadamard matrices.

Let H_{4n} be a Williamson type Hadamard matrix of order 4n of the form (4), where A, B, C, D are cyclic and symmetric Williamson type matrices of order n, and consequently can be represented as (5), and for all $i = 1, 2, \ldots, n-1$ we have $a_i = a_{n-i}$, $b_i = b_{n-i}$, $c_i = c_{n-i}$, $d_i = d_{n-i}$.

One can show that the matrix H_{4n} can be represented in the following form of block-cyclic Hadamard matrices [18]

$$H_{4n} = \sum_{i=0}^{n-1} Q_i \otimes U^i, \tag{7}$$

where

$$Q_i = \begin{pmatrix} a_i & b_i & c_i & d_i \\ -b_i & a_i & -d_i & c_i \\ -c_i & d_i & a_i & -b_i \\ -d_i & -c_i & b_i & a_i \end{pmatrix},$$

are Hadamard matrices of Williamson type when $a_i, b_i, c_i, d_i = \pm 1$, for all i = 0, 1, ..., n-1.

Introduce the Williamson type Hadamard matrices of orders 4 which will be used to construct block-cyclic and block-symmetric Hadamard matrices of Williamson type of order 4n.

$$Q_{0} = \begin{pmatrix} + & + & + & + \\ - & + & - & + \\ - & + & + & - \\ - & - & + & + \end{pmatrix}, \quad Q_{1} = \begin{pmatrix} + & + & + & - \\ - & + & + & + \\ - & - & + & - \\ + & - & + & + \end{pmatrix}, Q_{2} = \begin{pmatrix} + & + & - & + \\ - & + & - & - \\ + & + & + & - \\ - & + & + & + \end{pmatrix},$$

$$Q_{3} = \begin{pmatrix} + & - & + & + \\ + & + & - & + \\ - & + & + & + \\ - & - & - & + \end{pmatrix}, \quad Q_{4} = \begin{pmatrix} + & - & - & - \\ + & + & + & - \\ + & - & + & - \\ + & + & - & + \end{pmatrix}.$$

For example block-cyclic and block-symmetric Hadamard matrix of order 12 formed by Q_0 Q_1 and has the following form and equivalence to the matrix (6)

Below the first block-rows of block-cyclic and block-symmetric Hadamard matrices of Williamson type of orders 4n, $n = 3, 5, \dots, 25$ are given [18].

$$n=3: Q_0, -Q_1; -Q_1;$$

$$n=5: Q_0, -Q_2, -Q_1; -Q_1, -Q_2;$$

$$n=7: Q_0, Q_2, -Q_2, Q_1, Q_1, -Q_2, Q_2;$$

$$n = 9: Q_0, Q_1, -Q_2, Q_1, -Q_1, -Q_1, Q_1, -Q_2, Q_1;$$

$$n = 11: Q_0, -Q_4, Q_4, Q_1, -Q_3, -Q_2, -Q_2, -Q_3, Q_1, Q_4, -Q_4$$

$$n = 13: Q_0, Q_2, -Q_1, -Q_1, Q_1, Q_2, -Q_2; -Q_2, Q_2, Q_1, -Q_1, -Q_1, Q_2;$$

$$n = 15: Q_0, -Q_2, Q_1, -Q_1, -Q_1, -Q_2, -Q_1, Q_2, Q_2, -Q_1, -Q_2, -Q_1, -Q_1, Q_1, -Q_2;$$

$$n=17:\ Q_0,-Q_2,-Q_1,-Q_2,-Q_3,-Q_3,Q_3,Q_2,-Q_1,-Q_1,Q_2,Q_3,-Q_3,-Q_3,-Q_2,\\ -Q_1,-Q_2;$$

$$n=19: Q_0,Q_2,Q_1,-Q_2,-Q_1,-Q_1,Q_1,-Q_1,Q_2,-Q_1,-Q_1,Q_2,-Q_1,Q_1,-Q_1,-Q_1,\\ -Q_2,Q_1,Q_2;$$

$$\begin{split} n = 21: & Q_0, Q_1, Q_1, -Q_1, Q_1, -Q_2, -Q_2, Q_2, Q_1, Q_2, -Q_1, -Q_1, Q_2, Q_1, Q_2, -Q_2, \\ & -Q_2, Q_1, -Q_1, Q_1, Q_1; \end{split}$$

$$\begin{split} n &= 23: & Q_0, Q_2, Q_1, -Q_2, Q_4, Q_3, Q_1, -Q_3, Q_4, -Q_4, -Q_2, -Q_4, -Q_4, -Q_2, -Q_4, Q_4, \\ & -Q_3, Q_1, Q_3, Q_4, -Q_2, Q_1, Q_2; \end{split}$$

$$\begin{split} n &= 25: \quad Q_0, -Q_1, -Q_2, -Q_1, -Q_2, Q_2, -Q_2, Q_1, Q_1, -Q_1, -Q_1, Q_2, Q_2, -Q_1, \\ &-Q_1, Q_1, -Q_2, Q_2, -Q_2, -Q_1, -Q_2, -Q_2, -Q_1. \end{split}$$

In practice, the problem is to compute efficiently the coefficients of transforms $Y_i = Q_i X$, where Q_i , i = 0, 1, 2, 3, 4 given above and $X = (x_0, x_1, x_2, x_3)^T$ and $Y_i = (y_i^0, y_i^1, y_i^2, y_i^3)^T$, are

input and output vectors respectively. Let us denote $r_1 = x_1 + x_2 + x_3$, $r_2 = r_1 - x_0$. Then, directly from Q_i we see that the following relations hold

$$\begin{aligned} y_0^0 &= (x_0 + x_1) + (x_2 + x_3), & y_0^1 &= -(x_0 - x_1) - (x_2 - x_3), \\ y_0^2 &= -(x_0 - x_1) + (x_2 - x_3), & y_0^3 &= -(x_0 + x_1) + (x_2 + x_3), \\ y_1^0 &= (x_0 + x_1) + (x_2 - x_3), & y_1^1 &= -(x_0 - x_1) + (x_2 + x_3), \\ y_1^2 &= -(x_0 + x_1) + (x_2 - x_3), & y_1^3 &= (x_0 - x_1) + (x_2 + x_3), \\ y_2^0 &= (x_0 + x_1) - (x_2 - x_3), & y_2^1 &= -(x_0 - x_1) - (x_2 + x_3), \\ y_2^2 &= (x_0 + x_1) + (x_2 - x_3), & y_2^3 &= -(x_0 - x_1) + (x_2 + x_3), \\ y_3^0 &= (x_0 - x_1) + (x_2 + x_3), & y_3^1 &= (x_0 + x_1) - (x_2 - x_3), \\ y_3^2 &= -(x_0 - x_1) + (x_2 + x_3), & y_3^1 &= -(x_0 + x_1) - (x_2 - x_3), \\ y_4^0 &= (x_0 - x_1) - (x_2 + x_3), & y_4^1 &= (x_0 + x_1) + (x_2 - x_3), \\ y_4^0 &= (x_0 - x_1) + (x_2 - x_3), & y_4^1 &= (x_0 + x_1) - (x_2 - x_3), \\ y_4^2 &= (x_0 - x_1) + (x_2 - x_3), & y_4^3 &= (x_0 + x_1) - (x_2 - x_3), \end{aligned}$$

Note that above equations can be rewritten more compact form as follows

$$\begin{array}{llll} y_0^0 = r_1 + x_0, & y_0^1 = r_2 - 2x_2, & y_0^2 = r_2 - 2x_3, & y_0^3 = r_2 - 2x_1; \\ y_1^0 = y_0^0 - 2x_3, & y_1^1 = r_2, & y_1^2 = y_0^3 - 2x_3, & y_1^3 = y_0^0 - 2x_1; \\ y_2^0 = y_0^0 - 2x_2, & y_2^1 = y_0^2 - 2x_2, & y_2^2 = y_0^0 - 2x_3, & y_3^2 = r_2; \\ y_3^0 = y_0^0 - 2x_1, & y_3^1 = y_0^0 - 2x_2, & y_3^2 = r_2, & y_3^3 = y_0^3 - 2x_2; \\ y_4^0 = -r_2, & y_4^1 = y_0^0 - 2x_3, & y_3^2 = y_0^0 - 2x_1, & y_3^3 = y_0^0 - 2x_2; \end{array}$$

Analysis of given above 4-point transforms shows that if we use them separately we need to implement 7 additions/substructions and 3 shift operations. However, using them together requires less operations. For example, the combined transformation Q_0 and Q_1 of vector X requires only 10 addition/subtraction operations and 3 shift operations.

Now we will evaluate the complexity of the block-cyclic block-symmetric Hadamard transform. Let k be the number of various blocks in the first block-row of the matrix H_{4n} and k_i is the number of repetition of the i-th pair of blocks, $i=1,2\ldots,k_t$. Then the Williamson type block-cyclic block-symmetric Hadamard transform requires only 3n one-bit shift operations and

 $C(H_{4n}) = n(4+3k) + 2(n-1)(2n+t-\sum_{i=1}^{t} k_i)$ (9)

additions and subtractions. For example, a 20-point transform requires only 145 additions and subtractions and 15 one-bit shift operations.

Give an example. From the table of block-cyclic and block-symmetric Hadamard matrices of Williamson type it follows that block-cyclic block-symmetric Hadamard matrix of

Williamson type of order 12 has the following form

$$H_{12}\begin{pmatrix} Q_0 & -Q_1 & -Q_1 \\ -Q_1 & Q_0 & -Q_1 \\ -Q_1 & -Q_1 & Q_0 \end{pmatrix}.$$

Input vector F_{12} represent as $F_{13}^T = (X_0^T, X_1^T, X_2^T)$, where $X_0^T = (f_0, f_1, f_2, f_3)$, $X_1^T = (f_4, f_8, f_6, f_7)$, $X_3^T = (f_8, f_9, f_{10}, f_{11})$.

The 12-point block-cyclic block-symmetric Hadamard transform can be represented by

$$H_{12}F_{12}=Y_0+Y_1+Y_2,$$

where

$$Y_0 = \begin{pmatrix} Q_0 X_0 \\ -Q_1 X_0 \\ -Q_1 X_0 \end{pmatrix}, \quad Y_1 = \begin{pmatrix} -Q_1 X_1 \\ Q_0 X_1 \\ -Q_1 X_1 \end{pmatrix}, \quad Y_2 = \begin{pmatrix} -Q_1 X_2 \\ -Q_1 X_2 \\ Q_0 X_0 \end{pmatrix}.$$

It is not difficult to see 10 additions/substructions and 3 shift operations are needed to compute each of the vectors Y_i , i = 0, 1, 2. Hence 12-point block-cyclic block-symmetric Hadamard transform requires only 54 additions/substructions and 9 one bit shift operations.

In the table below we show the necessary number of operations for given Hadamard transforms.

The columns of the Table give: Orders of cyclic and symmetric Williamson matrices; Corresponding orders of Hadamard matrices of Williamsin type; Number of addition and substruction for block-cyclic block-symmetric Hadamard transform; Number of operation of the above transform with shifts; and Number of shifts.

n	4n	Block-symmetric block-cyclic Hadamard trans.	Block-symmetric block-cyclic Hadamard trans. with shifts	Number of shifts
3	12	60	54	9
5	20	160	145	15
7	28	268	247	21
9	36	400	373	27
11	44	704	629	33
13	52	760	721	39
15	60	912	867	45
17	68	1236	1168	51
19	76	1158	1219	57
21	84	1576	1393	63
23	92	2442	2329	69
25	100	2080	2005	75

References

 Ryszard Stasinski, Janusz Konrad. A New Class of Fast Shape-Adaptive Orthogonal Transforms and Their Application to Region-Based Image Compression. IEEE Trans. on Circuits and Systems for Video Technology, vol. 9, No. 1, 1999, p.16-34.

- [2] Barazande-Pour M., Jon W. Mark. Adaptive MHDCT. IEEE, 1994, p. 90-94.
- [3] Reddy G.R., Satyanarayana P., Interpolation Algorithm Using Walsh-Hadamard and Discrete Fourier/Hartley Transforms. IEEE, 1991, p. 545-547.
- 4 Cheung-Fat Chan. Efficient Implementation of a Class of Isotropic Quadratic Filters by Using Whalsh-Hadamard Transform. IEEE Int. Symposium on Circuits and Systems, June 9-12, Hong Kong, 1997, p. 2601-2604.
- [5] Brian K. Harms, Jin Bae Park, Stephan A. Dyer. OptimalMeasurement Techniques Utilizing Hadamard Transforms. IEEE Trans. on Instrumentation and Measurement, vol. 43, No. 3, June 1994, p. 397-402.
- [6] Chen Anshi, Li Di, Zhou Renzhong. A Reshearch on Fast Hadamard Transform (FHT) Digital Systems. IEEE TENCON+93/Beijing, 1993, p. 541-546.
- [7] Sarukhanyan H.G. Hadamard Matrices: Construction Methods and Applications. Proc. First Int. Workshop on Transforms and Filter Banks. Tampere, Finland, 1998, p. 95-130.
- [8] Orthogonal Transforms for Digital Signal Processing. Springer- Verlag, New York, 1975.
- Agaian S.S., Sarukhanyan H.G. Hadamard Matrices Representation by (-1,+1)-vectors.
 Proc. of Int. Conf. Dedicated to Hadamard Problem's Centenary, Australia, 1993, 1p.
- 10] Sarukhanyan H.G. Decomposition of the Hadamard Matrices and Fast Hadamard Transform. Computer Analysis of Images and Patterns, Lecture Notes in Computer Sciences, vol. 1298, 1997, p. 575-581.
- [11] Yarlagadda Rao R.K., Hershey E.J. Hadamard Matrix Analysis and Synthesis with Applications and Signal/Image Processing, 1997.
- [12] Hadamard J., "Resolution d'une Question Relative aux Determinants", Bull. des Sci. Math., vol. 17, pp. 240-246, 1893.
- [13] Sylvester J.J. Thoughts on Inverse Orthogonal Matrices, Simultaneous Sign Successions and Tesselated Pavements in Newton's Rule, Ornamental Til-Work, and the Theory of Numbers. Phil. Mag., vol. 34, 1867, p. 461-475.
- [14] Palay R.E.A.G., On Orthogonal Matrices. J. Math. and Phis., vol. 12, No. 3, 1933, p. 311-320.
- [15] Hall M, Jr. Combinatorial Theory, London, 1967.
- [16] Wallis W.D., Street A.P., Wallis J.S. Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices. Lecture Notes in Mathematics, vol. 292, 1972.
- [17] Hedayat A., Wallis W.D. Hadamard Matrices and Their Applications. The Annals of Statistics, vol. 6, No. 5, 1978, p. 1184-1293.
- [18] Agaian S.S., Hadamard Matrices and Their Applications. Lecture Notes in Math., vol. 1168, 1985.

- [19] Seberry J., Yamada M. Hadamard Matrices, Sequences and Block Designs. Surveys in Contemporary Design Theory, New York, 1992.
- [20] Williamson J. Hadamard Determinant Theorem and Sum of Four Squares. Duke Math. J., No. 11, 1944, p. 65-81.
- [21] Williamson J. Note on Hadamard's Determinant Theorem. Bull. Amer. Math. Soc., No. 53, 1947, p. 608-613.
- [22] Agaian S.S., "Design of planar and spatial block Hadamard matrices", Matematicheskie voprosi kibernetiki i vichislitelnoi techniki (in russian), vol. 12, pp.5-50, 1984.

the latter will be the latter or other