Chapter 16

CONSTRUCTION AND PROPERTIES OF DISCRETE WALSH TRANSFORM MATRICES

Mikhail Sergeevich Bespalov
Dept. FAIP (mathematics), Vladimir State University
Gorkii, st. 87, 600000 Vladimir, Russia
bespalov@vpti.vladimir.ru

Abstract This paper discusses properties properties the discrete Walsh transform for different orderings of Walsh functions. Presented are some methods for construction of the related transform matrices.

1. Introduction

In technical applications [1] *Discrete Walsh Transform* (DWT) is used in three enumerations: Paley, Walsh and Hadamard. In technical literature the Discrete Walsh Transforms are called the Walsh Transform. Correctly, the term "Walsh Transform" refers to another notion in mathematics literature. The *Walsh Transform* has been introduced in [2] in 1950 by Fine and initially named the "Walsh-Fourier Transform" [3].

In technical applications the *Discrete Walsh Transform in Paley (or Walsh, or Hadamard) enumeration* is called the *Paley Transform* (the *Walsh Transform*, or the *Hadamard Transform*) and is denoted by PAL (or WAL, or HAD correspondingly).

By $W = (w_{kj})$ ($U = (u_{kj})$, or $H = (h_{kj})$, correspondingly) we denote the matrix of the DWT in Paley enumeration (Walsh enumeration, or Hadamard enumeration, respectively).

In mathematical books, as for instance [4], matrices W_n are introduced in the form

$$w_{kj} = w_{jk} = w_k(j/2^n), \quad 0 \le j, k < 2^n, \tag{16.1}$$

where $\{w_k(x)\}_{k=0}^{\infty}$ – is the *Walsh-Paley system*.

The matrices U_n are introduced in the form (16.1), where $\{w_k(x)\}_{k=0}^{\infty}$ – is the *original Walsh system* [5] (Walsh system in Walsh enumeration).

The Hadamard matrices H_n were introduced in another way [6]. Let

$$H = H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Then a matrix H_2 is a *Kronecker product* of H with H, thus, it is defined by

$$H_2 = H(H) = \begin{pmatrix} H & H \\ H & -H \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Then, a matrix H_n is a Kronecker power

$$H_n = H^{(n)} := H(H_{n-1}) = H_{n-1}(H).$$

Matrices W_n, U_n, H_n consists of the same rows and differ only in enumeration rows.

For example,

$$W_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}, \qquad U_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix}.$$

Let

$$\tilde{i} = (i_1\ i_2\ \ldots\ i_n)^T, \qquad i_k \in \{0, 1\} \tag{16.2}$$

be a *simply dyadic code* for a non-negative integer i which is less 2^n, when

$$i = \sum_{k=1}^{n} i_k \cdot 2^{k-1}. \tag{16.3}$$

Consider (see [8]) an *inverse* τ of a simply dyadic code (16.2)

$$\tau(\tilde{i}) = (i_n\ i_{n-1}\ \ldots\ i_2\ i_1)^T, \qquad \tau(i) = \sum_{j=0}^{n-1} i_{n-j} \cdot 2^j;$$

then elements of Hadamard matrix are defined as $h_{kj} = w_{\tau(k)}(j/2^n)$.

Using the *Gray code* [1], we can do analogous transition from W_n to U_n.

2. Construction of Walsh Matrices

We construct matrices W_n, U_n, H_n in another way, without using Walsh functions. We introduce *three forms of scalar product* for i, j $(0 \le i < 2^n)$ in the form (16.3):

$$(i,j) = (i,j)_n := \sum_{k=1}^{n} i_k j_k, \ < i,j > = < i,j >_n := \sum_{k=1}^{n} i_k j_{n-k+1}, \quad (16.4)$$

$$u(i,j) = u_n(i,j) := i_1 j_n + \sum_{k=1}^{n-1} i_{k+1}(j_{n-k+1} + j_{n-k}). \quad (16.5)$$

One may consider any operations (16.4) over the field $\mathbf{Z}_2$. Then the rule (16.4) is the definition of a *quadratic form* A for construction of the Discrete Walsh Transform matrices.

In the case of DWT in Hadamard enumeration it is the unit matrix: $A = A_H := E$.

For DWT in Paley enumeration it is a matrix with unity at the secondary diagonal only (all other elements are zero).

In the case of DWT in Walsh enumeration it is a matrix with unity at the secondary diagonal and at the sub-secondary diagonal,

$$A_W := \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 & 0 \\ 0 & 0 & 0 & \dots & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 & 0 \end{pmatrix}, A_U := \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 & 1 \\ 0 & 0 & 0 & \dots & 1 & 1 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 1 & 1 & \dots & 0 & 0 & 0 \\ 1 & 1 & 0 & \dots & 0 & 0 & 0 \end{pmatrix}.$$

Define elements of the Discrete Walsh Transform matrices by

$$w_{ij} = (-1)^{<i,j>}, \quad h_{ij} = (-1)^{(i,j)}, \quad u_{ij} = (-1)^{u(i,j)}. \quad (16.6)$$

LEMMA 16.1 *The rule (16.4) is a correct definition of the scalar product; it is a symmetric bilinear form.*

The proof is trivial.

COROLLARY 16.1 *Matrices W_n, U_n, H_n constructed by the rule (16.6) are symmetric.*

Usually [3], [4], Walsh functions are introduced as products of the Rademacher functions $r_n(x)$. By definition, $r_0(x) = (-1)^j$ for $x \in \left[\frac{j}{2}, \frac{j+1}{2}\right) = \Delta_1^j$, $j \in \{0,1\}$, and $r_0(x+1) = r_0(x)$ for $x \in [0,\infty)$.

Let $r_n(x) = r_{n-1}(2x)$ for $x \in [0,\infty)$.

REMARK 16.1 *If we consider a modified segment $[0,1]^*$, then we have $\Delta_1^0 = [0^+, \frac{1}{2}^-]$, $\Delta_1^1 = [\frac{1}{2}^+, 1^-]$ and so on.*

Then, the Walsh-Paley functions (for i in the form (16.3)) is (see [3], [4])

$$w_i(x) := \prod_{k=1}^{n} r_{k-1}^{i_k}(x).$$

By another equivalent definition, put

$$w_0(x) \equiv 1,\ w_{2^n}(x) = r_n(x)\ , w_{2^n+k}(x) = w_{2^n}(x) \cdot w_k(x) \quad \textit{for } k < 2^n.$$

A Walsh-Walsh functions (i.e., a Walsh function in ordering introduced initially by J.L. Walsh) is (see [7], [8]) $v_0 = w_0, v_1 = w_1$,

$$v_{2^n} = r_{n-1} \cdot r_n \quad \textit{for } n \in \mathbf{N}\ , \quad v_{2^n+k} = v_{2^n} \cdot v_k \quad \textit{for } k < 2^n. \quad (16.7)$$

The number of changes of the sign on the interval $[0,1)$ for each function of the Walsh-Walsh system coincides with the index of the function (see [9]).

LEMMA 16.2 *For a fixed n, for any i,j elements w_{ij} in the formula (16.1) and in the formula (16.6) are equal.*

Proof. For $x \in \left[\frac{j}{2^n}, \frac{j+1}{2^n}\right)$, $j = \sum_{k=1}^{n} j_k \cdot 2^{k-1}$, we get $x = \sum_{k=1}^{n} \frac{j_k}{2^{n-k+1}} + x_1$ with $x_1 \in [0, 2^{-n})$. Then, $r_{n-k}(x) = (-1)^{j_k}$, or $r_{k-1}(x) = (-1)^{j_{n-k+1}}$. By using (16.1), we get $w_i(x) = \prod_{k=1}^{n}(-1)^{j_{n-k+1}i_k} = (-1)^{<i,j>}$.

LEMMA 16.3 *The number of sign changes in the i-th row is equal to the index i for the case of the DWT matrix in Walsh enumeration $U = (u_{ij})$ in the form (16.6).*

Proof. Denote by $l = i - i_n 2^{n-1} = \sum_{k=1}^{n-1} i_k 2^{k-1}$ and $m = [j/2] = \sum_{k=2}^{n} j_k 2^{k-1}$ the part of sums (16.3) of simply the dyadic codes for numbers i and j. We have

$$u_n(i,j) = i_1 j_n + i_2(j_n + j_{n-1}) + \ldots + i_{n-1}(j_3 + j_2) + i_n(j_2 + j_1) =$$

$$= u_{n-1}(l,m) + i_n(j_2 + j_1).$$

For the fixed index i of the row, let j runs from 0 to $2^n - 1$. Then m runs from 0 to $2^{n-1} - 1$.

The proof is by induction on n. For $n = 1$, there is nothing to prove.

We introduce a notation v_{ij} for elements of the matrix U_{n-1}, for which the inductive assumption is true. We obtain

$$u_{ij} = (-1)^{u_n(i,j)} = (-1)^{u_{n-1}(l,m)+i_n(j_2+j_1)} = v_{lm} \cdot (-1)^{i_n(j_2+j_1)}. \quad (16.8)$$

If $i_n = 0$, then we consider a upper half matrix U_n. For $i_n = 0$: this formula (16.8) make clear the independence of u_{ij} of j_1. First, by (16.8) we have $u_{ij} = v_{lm}$ and second $l = i$. It follows that the numbers of the sign changes in the i-th row of matrices U_{n-1} and U_n coincide.

If $i_n = 1$, then we consider a lower half matrix U_n. A row with an index $i = 2^{n-1} + l$ in matrix U_n corresponds to a l-th row of matrix U_{n-1} for (16.8). If $l = 0$, then the 2^{n-1}-th row has the form $1\ -1\ -1\ 1$ in period and there are 2^{n-1} changes of the sign. This is clear because by the factor $(-1)^{j_2+j_1}$ in (16.8).

The formula (16.8) corresponds to definition (16.7): the $(2^{n-1}+l)$-th row is an element-wise product of the 2^{n-1}-th row and the l-th row. Places of change of the sign for 2^{n-1}-th row and l-th row are different. Therefore, the number of changes of the sign in the row with the index $i = 2^{n-1} + l$ is equal to the index i.

COROLLARY 16.2 . *The matrix $U = (u_{ij})$ in (16.6) is the DWT matrix in Walsh enumeration in (16.1).*

In [7], Schipp have denoted $\mathbf{Z}_2$-linear rearrangements of the Walsh system. Each linear rearrangement is given by *the system of generating functions*.

For example, the Rademacher system $\{r_n(x)\}_{n=0}^{\infty}$ is a system of generating functions for the Walsh-Paley system. The system $\{R_n(x)\}_{n=0}^{\infty}$ (when $R_0 = r_0$, $R_n = r_{n-1} \cdot r_n$ as in (16.7)) is a system of generating functions for the Walsh-Walsh system. By definition in [3], $\mathbf{Z}_2$*-linear rearrangements of the Walsh system* $\{v_n(x)\}_{n=0}^{\infty}$ are

$$v_0(x) = w_0(x),\ v_{2^n}(x) = R_n(x), \quad v_{2^n+k}(x) = v_{2^n}(x) \cdot v_k(x) \quad \text{for } k < 2^n,$$

when R_n is any Walsh function such that $R_n \notin \{v_0, v_1, \ldots, v_{2^n-1}\}$.

This will be a definition of the rearrangements of Walsh system iff the map $\{w_n(x)\}_{n=0}^{\infty}$ to $\{v_n(x)\}_{n=0}^{\infty}$ is a bijection.

The rearrangement $\{v_n(x)\}$ of the Walsh system is called *regular* if $v_0(x) \equiv 1$, $v_1(x) = w_1(x)$, and the sets $\{v_k(x)\}_{k=2^n}^{2^{n+1}-1}$ and $\{w_k(x)\}_{k=2^n}^{2^{n+1}-1}$ coincide for any natural n.

Walsh-Kaczmarz system (see [3], [4]) is a regular and non-linear rearrangement of the Walsh system. In [7], Schipp called a such system as *piecewise-linear rearrangement*.

The rearrangement of 2^n initial Walsh functions in Hadamard enumeration is the linear rearrangement with the Rademacher functions r_{n-1}, r_{n-2},..., r_2, r_1, r_0 as the system of generating functions. This rearrangement is not regular.

Before we introduced the matrices A such that each row correspond to a generating function (for the rearrangement of 2^n initial Walsh functions): the indexes of the Rademacher functions are taken in the inverse order; each unity in a row has the index of the Rademacher function included into the product; this product is an ordinary generating function. Similar matrices (denoted by B) were introduced in [7], [10]; but numbers of the Rademacher functions were taken in the usual order. If we write columns of the matrix A in inverse order, we obtain the matrix B.

THEOREM 16.1 *Any non-singular matrix A of a quadratic form of order n over the field $\mathbf{Z}_2$ allows to construct a Discrete Walsh Transform matrix of order 2^n in a new ordering by means of an algorithm consisting of two steps (see (16.2), (16.3)):*

$$\begin{aligned} v(i,j) &= (\tilde{i}, A\tilde{j}) = \tilde{i}^T A\tilde{j} \quad \textit{(bilinear form)}, \\ v_{ij} &= (-1)^{v(i,j)} \quad \textit{(elements of the new matrix DWT)}. \end{aligned}$$

Conversely, any matrix DWT of order 2^n with the 0-th row consisting of 1 has a similar non-singular matrix A (matrix of a quadratic form).

A DWT matrix of order 2^n with the 0-th row consisting of 1 is symmetric iff a matrix A of a quadratic form is symmetric.

This theorem can be proven by direct calculations.

In [11], p. 26, the author introduced the definition of *infinite non-singular matrix with finite columns over a finite field.*

THEOREM 16.2 *Any infinite non-singular matrix of a quadratic form A with finite rows over the field $\mathbf{Z}_2$ allows to introduce a linear rearrangement of the Walsh system. Each row of the matrix A is a code of the ordinary generating function.*

Conversely, any linear rearrangement of the Walsh system has the similar infinite non-singular matrix A of a quadratic form.

The proof is omitted.

Denote by $M_{n,m}$ the class of $(n \times m)$ matrices.

LEMMA 16.4 *The matrix H_n in form (16.6) and Hadamard matrix in a form of the Kronecker power $H_n = H^{(n)}$ coincide for any n.*

Proof. Let $H_n = (h_{ij}^{(n)})_{i,j=0}^{2^n-1} \in M_{2^n,2^n}$. By using (16.6), we obtain

$$h_{ij} = (-1)^{(i,j)_n} = (-1)^{(m2^k, r2^k)_n} \cdot (-1)^{(l,t)_n} = (-1)^{(m,r)_{n-k}} \cdot (-1)^{(l,t)_k},$$

for $i = m2^k + l$, $j = r2^k + t$, $0 \le l, t < 2^k$, $0 \le m, r < 2^{n-k}$. This formula is

$$h_{ij}^{(n)} = h_{mr}^{(n-k)} \cdot h_{lt}^{(k)}.$$

For fixed m, r if l and t runs from 0 to $2^k - 1$, we get a block $h_{mr}^{(n-k)} \cdot H_k$ of matrix H_n represented by block form. A place of this block in Hadamards matrix corresponds to the definition of the matrix $H_{n-k}(H_k)$.

Finally, we obtain $H_n = H_{n-k}(H_k)$ for any $1 \le k < n$.

We shall introduced *a new form of the matrix product*. This product has block structure and a dimension of a block is analogous to the form and dimension of blocks in the Kronecker product.

DEFINITION 16.1 *For any matrices* $A \in M_{n,m}$, $B \in M_{k,l}$ *we denote by* $C = A\{B\} \in M_{nk,ml}$ *a block matrix of the form*

$$C = \begin{pmatrix} A^1B_1 & A^2B_1 & \dots & A^mB_1 \\ A^1B_2 & A^2B_2 & \dots & A^mB_2 \\ \vdots & \vdots & \ddots & \vdots \\ A^1B_k & A^2B_k & \dots & A^mB_k \end{pmatrix} \tag{16.9}$$

with blocks $A^j \cdot B_i \in M_{n,l}$ *such that* A^j *is a* j*-th column of the matrix* A*, and* B_i *is* i*-th row of the matrix* B.

Therefore, a new form of the matrix product is constructed by two rules for block matrices:

1 Rule 1 for enumeration of blocks - *a row of the second factor on a column of the first factor*

2 Rule 2 for the form of blocks - *a column of the first factor times a row of the second factor*.

Notice that any block A^iB_j of the matrix (16.8) is the Kronecker product

$$A^i \cdot B_j = A^i(B_j) = B_j(A^i). \tag{16.10}$$

Rows and columns of the matrix (16.9) are represented by Kronecker products of rows and columns of matrices A and B:

$$C_I = A_i(B_r) \text{ for } \quad I = (r-1)n + i, \tag{16.11}$$

$$C^J = B^j(A^p) \text{ for } \quad J = (p-1)l + j. \tag{16.12}$$

If we have enumeration of elements of a matrix from zero (but not from 1), then $I = rn + i$, $J = pl + j$.

LEMMA 16.5 *The definition of a power*

$$A^{\{d\}} = A\{A^{\{d-1\}}\} = A^{\{d-1\}}\{A\}$$

for new form of the matrix product is correct.

Proof. Let enumeration of elements of matrix begin from zero. The $(i + jn + kn^2)$-th row of a matrix $A^{\{3\}}$ have the form $A_i(A_j(A_k))$ for any i, j, k by (16.12). The $(i + jn + kn^2 + mn^3)$-th row of a matrix $A^{\{4\}}$ have the form $A_i(A_j(A_k(A_m)))$ and so on. Columns can be presented analogous.

Obviously, the Kronecker product $A(B)$ is symmetric if A and B are symmetric matrices. But, a new form of the matrix product $A\{B\}$ is not symmetric for example

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

LEMMA 16.6 *If matrices A and B are symmetric, then $(A\{B\})^T = B\{A\}$.*

Proof. Let to transpose a block matrix (16.9)

$$(A\{B\})^T = \begin{pmatrix} (A^1B_1)^T & (A^1B_2)^T & \dots & (A^1B_1)^T \\ \vdots & \vdots & \ddots & \vdots \\ (A^nB_1)^T & (A^nB_2)^T & \dots & (A^nB_1)^T \end{pmatrix}.$$

We get a statement by using a formula $(A^iB_j)^T = B_j^T \cdot (A^i)^T = B^jA_i$.

COROLLARY 16.3 *If the matrix A is symmetric, then the new power of matrix $A^{\{d\}}$ is symmetric also.*

THEOREM 16.3 *The matrix of DWT in Paley enumeration (16.1) can be defined as a new power (16.9) of the matrix $W_1 = H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$:*

$$W_n = W_k\{W_{n-k}\}.$$

Proof. Let $0 \le i, j < 2^n$ are presented in the form $i = m2^k + l$, $j = r2^{n-k} + t$, for $0 \le l, r < 2^k$, $0 \le m, t < 2^{n-k}$. Then,

$$< i, j >_n = \sum_{s=1}^{k} i_s j_{n-s+1} + \sum_{s=k+1}^{n} i_s j_{n-s+1} = < l, r2^{n-k} >_n + < m2^k, t >_n,$$

or they may by presented in the form

$$< i, j >_n = < l, r >_k + < m, t >_{n-k} .$$

By (16.6) we get

$$w_{ij}^{(n)} = (-1)^{<l,r>_k} \cdot (-1)^{<m,t>_{n-k}} = w_{lr}^{(k)} \cdot w_{mt}^{(n-k)}. \tag{16.13}$$

The first block of the matrix W_n (for $m = r = 0$) consists of elements $w_{lt}^{(n)} = w_{l0}^{(k)} \cdot w_{0t}^{(n-k)} \equiv 1$, and its block can represented as the 0-th column of the matrix W_k multiplied by the 0-th row of the matrix W_{n-k}. Any block of dimension $2^k \times 2^{n-k}$ (for fixed m, r) of the matrix W_n has the form (16.13); its block can be represented as the r-th column of the matrix W_k multiplied by m-th row of the matrix W_{n-k}, and its block is disposed as mr-th block. This is the definition of $W_k\{W_{n-k}\}$.

We recall [12] that $\|A\|_E = \sqrt{\sum_{k,l=1}^{n,m} a_{kl}^2}$ is the *Euclidean norm*. We introduced the *Euclidean orthogonality of matrices* $A, B \in M_{n,m}$: we write $A \perp B$, if $\sum_{k,l=1}^{n,m} a_{kl} \cdot b_{kl} = 0$. This definition coincides with the notion of *orthogonal vectors*, whose coordinates are all elements of the matrix in any fixed order.

We say that the collection of matrices $\{A(k)\}_{k=1}^{n \cdot m}$ constitute the *orthonormal E-basis* (basis for the Euclidean norm) in the class $M_{n,m}$, if $A(k) \perp A(l)$ for $k \neq l$ and $\|A(k)\|_E = 1$ for any k. For example, the standard orthonormal E-basis is a complete collection of different matrices such that all elements are equal to zero except one equal to 1.

A matrix is called *orthogonal* if $A \cdot A^T = E$ [13].

Collection of vectors $\{A_i\}$ is called *orthonormal* if $(A_i, A_j) = \delta_{ij}$ (Kronecker symbol).

Let ψ_k be rows of the DWT matrix in Paley enumeration W_n. In [10], for the case $n = 2N$, Bochkarev have solved the extremal problem:

$$\min_{\varepsilon_k = \pm 1} \| \sum_{k=0}^{2^n - 1} \varepsilon_k \psi_k \|_\infty = 2^N,$$

vectors $e_{N,j}$ are the solution of this problem.

Write the following vectors

$$e_{1,0} = (-1\ 1\ 1\ 1),\ e_{1,1} = (1\ -1\ 1\ 1),\ e_{1,2} = (1\ 1\ -1\ 1),\ e_{1,3} = (1\ 1\ 1\ -1).$$

in the form of a matrix. Then, vectors $e_{m,4i+j} = e_{1,j}(e_{m-1,i})$ are defined as Kronecker products of matrices.

Note that the solution of this extremal problem for odd n is different:

$$\min_{\varepsilon} \|W_{2N-1}\varepsilon\|_\infty = 2^N,$$

for $N = 1, 2, 3$.

By [10], the system $\{e_{N,j}\}_{j=0}^{2^n-1}$ is the total orthogonal eigenvector system for some linear rearrangement of the matrix DWT; this matrix is the Kronecker power $(W_2)^{(n-1)}$. But, this rearrangement is not the DWT matrix in Paley, Walsh or Hadamard enumeration.

By this way we get a general method of constructing the basis.

LEMMA 16.7 *A collection of vectors (in the form of the Kronecker product) $\{A_i(B_j)\}_{i,j=1}^{n,k}$ is orthonormal if both vector collections $\{A_i\}_{i=1}^{n}$, $\{B_j\}_{j=1}^{k}$ are orthonormal.*

Proof. We get for the scalar product $(A_i(B_j), A_k(B_l)) =$

$$= \sum_{r=1}^{m}(a_{ir}B_j, a_{kr}B_l) = \sum_{r=1}^{m} a_{ir}a_{kr} \cdot (B_j, B_l) = (A_i, A_k) \cdot (B_j, B_l) = \delta_{ik} \cdot \delta_{jl}.$$

By Lemma 16.7, we obtain

Proposition 1. *If matrices $A \in M_{n,n}$, $B \in M_{k,k}$ are orthogonal, then matrices $A(B)$ and $A\{B\}$ are also orthogonal. In this cases, the collection of blocks $\{A^iB_j\}_{i,j=1}^{n,k}$ in the matrix $A\{B\}$ is an orthonormal E-basis of the class $M_{n,k}$.*

Proof. Let enumeration begin from zero. A $j = (rk + s)$-th row of matrix $A(B)$ have the form $A_r(B_s)$. A $j = (rk + s)$-th column of matrix $A\{B\}$ have the form $B^s(A^r)$. By (16.10) for blocks we have proven the statement.

3. Fast Walsh Transform

In this section, previous considerations will be used to formulate the fast calculation algorithms for the discrete Walsh transform for different enumerations.

PROPOSITION 16.1 *For any $A, B \in M_{n,n}$ we have*

$$H_1(A \cdot B) = H_1(A) \cdot E_1(B) = E_1(A) \cdot H_1(B).$$

Proof. By direct calculations

$$H(A)\cdot E(B) = \begin{pmatrix} A & A \\ A & -A \end{pmatrix} \cdot \begin{pmatrix} B & 0 \\ 0 & B \end{pmatrix} = \begin{pmatrix} AB & AB \\ AB & -AB \end{pmatrix} = H(A\cdot B).$$

Second equality can be proved in an analogous way.

Good used [13] the Proposition 16.1 for a construction of *Fast algorithms for discrete Walsh transform in Hadamard enumeration*.

COROLLARY 16.4 *This algorithm is algorithm of the* **Fast Walsh Transform (FWT)**

$$H_n = H(E_{n-1})\cdot E(H(E_{n-2}))\cdot E_2(H(E_{n-3}))\cdot\ldots\cdot E_{n-2}(H(E))\cdot E_{n-1}(H),$$

$$H_n = E_{n-1}(H)\cdot E_{n-2}(H(E))\cdot E_{n-3}(H(E_2))\cdot\ldots\cdot E(H(E_{n-2}))\cdot H(E_{n-1}).$$

REMARK 16.2 *We denote a unit matrix of order 2^n by E_n, as it is the similar notation for W_n, U_n and H_n.*

Clearly for matrices any order

$$E(A\cdot B) = E(A)\cdot E(B). \tag{16.14}$$

THEOREM 16.4 *For any $A, B \in M_{n,n}$ we have*

$$H_1\{A\cdot B\} = H_1\{A\}\cdot E_1(B).$$

Proof. We repeat the proof of the Proposition 16.1, but we permute rows of matrices $H(A)$ and $H(AB)$ in the order 0, 2^{n-1}, 1, $2^{n-1}+1$, 2, $2^{n-1}+2$, $3,\ldots$. In this way matrices $H(A)$ and $H(AB)$ convert into matrices $H\{A\}$ and $H\{AB\}$.

The submatrix of the matrix $H_1\{A\}$ consisting of even rows coincides with the upper half of the matrix $H_1(A)$. The submatrix of the matrix $H_1\{A\}$ consisting of odd rows coincides with the bottom half of the matrix $H_1(A)$.

By using the Proposition 16.1 and multiplication of matrices for a submatrix of matrix $H\{A\}$ and the matrix $E(B)$, we obtain the analogous submatrix of the matrix $H\{AB\}$.

COROLLARY 16.5 *For matrices DWT in Paley enumeration we have the recurrence*

$$W_n = H_1\{E_{n-1}\}\cdot E_1(W_{n-1}).$$

By using this relation, we get the following algorithm of **the Fast discrete Walsh transform** *in Paley enumeration*

$$W_3 = H_1\{E_2\}\cdot E_1(H_1\{E_1\})\cdot E_2(H_1),$$

$$W_4 = H\{E_3\}\cdot E(H\{E_2\})\cdot E_2(H\{E\})\cdot E_3(H),$$

$$W_5 = H\{E_4\}\cdot E(H\{E_3\})\cdot E_2(H\{E_2\})\cdot E_3(H\{E\})\cdot E_4(H)$$

and so on.

Proof. By using Theorems 16.3 and 16.4, we get

$$W_n = H\{W_{n-1}\cdot E_{n-1}\} = H\{E_{n-1}\}\cdot E_1(W_{n-1}).$$

In particular, $W_2 = H\{E\}\cdot E(H)$.

Combining this result and (16.14), we get $W_3 = H_1\{E_2\} \cdot E_1(W_2) =$

$= H_1\{E_2\} \cdot E_1(H\{E\} \cdot E(H)) = H_1\{E_2\} \cdot E_1(H_1\{E_1\}) \cdot E_2(H_1).$

Analogously we obtain

$$W_4 = H\{E_3\} \cdot E(W_3) = H\{E_3\} \cdot E(H\{E_2\} \cdot E(H\{E\}) \cdot E_2(H)),$$

$$W_4 = H\{E_3\} \cdot E(H\{E_2\}) \cdot E_2(H\{E\}) \cdot E_3(H)$$

.

EXAMPLE 16.1 *An example of this algorithm of the Fast discrete Walsh transform in Paley enumeration is the following:*

$$W_2 = H\{E\} \cdot E(W) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix},$$

$$H_1\{E_2\} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \end{pmatrix},$$

$$E_1(H_1\{E_1\}) = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \end{pmatrix},$$

$$E_2(H_1) = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}.$$

This algorithm is more simpler than algorithms of the Fast Walsh Transform in [1], [13] and is similar to the Fast Fourier Transform.

For this reason, this result has been included in textbook [14].

References

[1] Zalmanzon, L.A., *Transforms Fourier, Walsh, Haar and its Application for Control, Communication and Other Fields*, Nauka, Moscow, 1989 (in Russian).

[2] Fine, N.J., "The generalized Walsh functions", *Trans. Amer. Math. Soc.*, 69, (1950), 66-77.

[3] Schipp, F., Wade, W.R., Simon, P., with assitance of Pál, J., *Walsh Series - An Introduction to the Dyadic Harmonic Analysis*, Adam Hilger, London, 1990.

[4] Golubov, B. I., Efimov A.V., Skvortsov V.A., *Walsh Series and Transform: Theory and Applications*, Nauka, Moscow, 1987, (in Russian), English transl. Kluwer, Dordrecht, 1991.

[5] Walsh, J.L., "A closed set of normal orthogonal functions", *Amer. J. Math.*, 45, (1923), 5-24.

[6] Hadamard, J., "Resolution d'une question relative aux determinants", *Bull. Sci. Math. Ser. 2*, Part 1, 17, (1893), 240-246.

[7] Schipp, F., "Certain rearrangements of series in the Walsh series", *Mat. Notes.*, Vol. 18, No. 2, (1975), 193-201.

[8] Bespalov, M.S., "Permutations of the Walsh system that preserve Lebesque constants", *Mat. Notes.*, Vol. 68, No. 1, (2000), 32-42.

[9] Levizov, S.V., "Some properties of the Walsh system", *Mat. Notes.*, Vol. 27, No. 5, (1980), 715-720.

[10] Bochkarev, S.V., "Some properties of the Walsh matrices", *Dokl. Sem. Inst. Applied Math. I.N. Vekua*, Tbilisi, Vol. 3, No. 2, (1988), 15-18.

[11] Bespalov, M.S., "Mathematical methods for informatics and computer technology", Part 1., Elements of algebra and mathematical analysis, VlSU, Vladimir, 2006, (in Russian).

[12] Horn R., Johnson, C., *Matrix Analysis*, Cambridge University Press, 1986.

[13] Good, I.J., "The interaction algorithm and practical Fourier analysis", *J. Royal Stat. Soc. Ser. B.*, 20, (1958), 361-372.

[14] Bespalov, M.S., "Mathematical methods for informatics and computer technology", Part 2. Introduction to applied harmonic analysis, VlSU, Vladimir, 2007, (in Russian).