Vítězslav Veselý

Algebraic theory of fast mixed-radix transforms. I. Generalized Kronecker product of matrices

Archivum Mathematicum, Vol. 25 (1989), No. 3, 149--161

Persistent URL: http://dml.cz/dmlcz/107352

ARCHIVUM MATHEMATICUM (BRNO)
Vol. 25, No. 3 (1989), 149–162

ALGEBRAIC THEORY OF FAST MIXED-RADIX TRANSFORMS: I. GENERALIZED KRONECKER PRODUCT OF MATRICES

VÍTĚZSLAV VESELÝ

(Received June 26, 1986)

Abstract. A new operation over matrices is introduced which is a generalization of the Kronecker (direct) product and its basic properties are derived. It is shown that matrices formed in this way define a class of the so called fast mixed-radix transforms as a natural generalization of the mixed-radix fast Fourier transforms. The new operation allows a straightforward and simple derivation of the appropriate factorization associated with the fast algorithm. The paper will be continued.

Key words. Generalized Kronecker product of matrices, fast mixed-radix transform, fast Fourier transform, factorization of matrices.

MS Classification: 15 A 23, 15 A 04, 68 Q 25, 65 F 30, 65 T 05.

INTRODUCTION

Linear transforms $\mathbf{x} \to \mathbf{y} = \mathbf{A}\mathbf{x}$, where $\mathbf{A}$ denotes a fixed matrix and $\mathbf{x}$ and $\mathbf{y}$ are data vectors of appropriate sizes, are widely used in various applications. Multiplication of a vector $\mathbf{x}$ by the matrix $\mathbf{A}$ may become a crucial operation on a computer if many such transforms are to be accomplished and/or $\mathbf{A}$ is a large matrix with many non-zero elements. In such a case it is desirable to find for the given matrix $\mathbf{A}$ a "fast" algorithm that reduces the amount of scalar multiplications and additions accomplishing $\mathbf{A}\mathbf{x}$. One is usually profiting from the knowledge of the concrete structure of $\mathbf{A}$ to find such a factorization $\mathbf{A} = \mathbf{A}^{(m)}\mathbf{A}^{(m-1)} \dots \mathbf{A}^{(1)}$ into sparse matrices $\mathbf{A}^{(i)}$ that $\mathbf{A}^{(i)}\mathbf{x}^{(i-1)}$ may be viewed with $\mathbf{x} = \mathbf{x}^{(0)}$ and $\mathbf{y} = \mathbf{x}^{(m)}$ as the i-th step ($i = 1, 2, \dots, m$) of a fast algorithm. Product of such matrices is said to be a fast (linear) transform.

The above approach is typical in the field of digital signal processing [1–5, 7, 8], where the mostly used transforms are orthogonal [3]. Chief among them is the *discrete Fourier transform* (DFT). A fast algorithm computing DFT is called *fast Fourier transform* (FFT). Discussion of various commonly used FFTs may be found e.g. in [1–4, 7].

I. J. Good [5] shows that the structure of the multidimensional FFT is characteristic for a class of linear transforms, the matrices of which may be expressed as Kronecker (direct) product [6], i.e. $\mathbf{A} = \mathbf{A}_1 \otimes \mathbf{A}_2 \otimes \ldots \otimes \mathbf{A}_m$. Then it is easy to see that $\mathbf{A}^{(i)} = \mathbf{I}_1 \otimes \ldots \otimes \mathbf{I}_{i-1} \otimes \mathbf{A}_i \otimes \mathbf{I}_{i+1} \otimes \ldots \otimes \mathbf{I}_m$ defines the i-th step of the corresponding fast algorithm ($\mathbf{I}_j$ denotes identity matrices of appropriate sizes) and thus Kronecker product is a typical operation forming matrices of this class of (fast) transforms. Similarly another class of linear transforms may be based on the structure of another FFT, the so called mixed-radix FFT. I. J. Good develops in [5] the appropriate factors $\mathbf{A}^{(i)}$ and illustrates a close relationship between both classes of fast transforms. Hereafter we shall call transforms of the latter class *mixed-radix transforms* (MRTs) and the corresponding fast algorithms *fast mixed-radix transforms* (FMRTs).

There arises a natural question whether one can find a simple algebraic operation over matrices typical for MRTs and having properties admitting the derivation of factors $\mathbf{A}^{(i)}$ of FMRT by simple and easy algebraic manipulations so as this is in the case of the Kronecker product.

This paper gives a positive answer to this question. In Sect. 2 we define in two ways a new operation over matrices which may be viewed as a generalization of the Kronecker product. Several basic algebraic properties of this generalized Kronecker product are proved which allow the desired easy derivation of the FMRTs.

1. NOTATION AND INTRODUCTORY REMARKS

1.1 Notation

- $\mathbf{N}$ ... the set of natural numbers.
- $\mathbf{Z}$ ... the set of integers.
- $\mathbf{Z}_N = \{0, 1, \ldots, N - 1\}$, $N \in \mathbf{N}$.
- $\mathbf{C}$ ... the field of complex numbers.
- $\mathbf{R}$ ... an arbitrary associative and commutative ring with unity, all matrices and vectors mentioned later on are over $\mathbf{R}$ if not stated otherwise.
- If $\mathbf{A}$ is a matrix of size $N \times K$ ($N, K \in \mathbf{N}$), then we shall denote $A(n, k)$ its entry in $(n + 1)$-th row and $(k + 1)$-th column, $n \in \mathbf{Z}_N$, $k \in \mathbf{Z}_K$. The set of all matrices of size $N \times K$ will be denoted as $\mathcal{M}(N \times K)$. We write $\mathbf{A} = (\mathbf{A}^{n_1,k_1})$, $\mathbf{A}^{n_1,k_1} \in \mathcal{M}(N_2 \times K_2)$, $n_1 \in \mathbf{Z}_{N_1}$, $k_1 \in \mathbf{Z}_{K_1}$ for a matrix $\mathbf{A}$ which is structured into $N_1 \times K_1$ blocks $\mathbf{A}^{n_1,k_1}$ of size $N_2 \times K_2$ ($N = N_1 N_2$, $K = K_1 K_2$), $n_1 + 1$ is the row position and $k_1 + 1$ the column position of the block $\mathbf{A}^{n_1,k_1}$.
- $\mathbf{x} = (x_0, x_1, \ldots, x_{N-1})^T$, $N \in \mathbf{N}$ denotes a column vector of length N, (^{T} is transposition).

- $|\mathbf{A}|$ ... determinant of a square matrix $\mathbf{A}$.
- $\mathbf{I}_N$ ... identity matrix of order N.
- $[i:j] = \{k \mid i \leq k \leq j,\ k \in \mathbf{Z}\}$, $i, j \in \mathbf{Z}$, $i \leq j$.
- Let $N_k \in \mathbf{N}$ for $k \in [i:j]$, then $N_{i,j} = N_i N_{i+1} \dots N_j$ if $i \leq j$ and $N_{i,j} = 1$ otherwise.
- $\delta_{i,j}$, $\delta(i,j)$ ... Kronecker's symbol.
- $n \mid m$ ... integer n is a divisor of integer m.
- $\mathscr{P}(M)$ ... permutation group of the set M.

We shall not distinguish between a permutation $P \in \mathscr{P}(\mathbf{Z}_N)$ and the corresponding matrix $\mathbf{P} \in \mathscr{M}(N \times N)$, $P(n,k) = \delta_{n,P(k)}$.

1.2 Definition. A mapping $\mathscr{N}: [i:j] \to \mathbf{N}$ is said to be a (finite) *number system* (NS). We shall write also $\mathscr{N} = (N_i, N_{i+1}, \dots, N_j)$ to visualize the function values $\mathscr{N}(k) = N_k$ for $k \in [i:j]$. Alternatively the notation $\mathscr{N}_{i,j}$ will be used instead of $\mathscr{N}$ to emphasize the index domain $[i:j]$.

1.3 Remark. Combining a NS $\mathscr{N}_{i,j}$ with a permutation $p \in \mathscr{P}([i:j])$, we arrive at a permuted NS $\mathscr{N}_{i,j}p = (N_{p(i)}, N_{p(i+1)}, \dots, N_{p(j)})$.

1.4 Lemma. *Let* $\mathscr{N} = (N_1, N_2, \dots, N_m)$ *be a number system associated with* $N = N_{1,m}$. *Then the mapping* $[.]_{\mathscr{N}}: \mathbf{Z}_{N_1} \times \mathbf{Z}_{N_2} \times \dots \times \mathbf{Z}_{N_m} \to \mathbf{Z}_N$ *defined as* $[n_1, n_2, \dots, n_m]_{\mathscr{N}} = n_1 N_{2,m} + n_2 N_{3,m} + \dots + n_{m-1} N_m + n_m = n$ *is a bijection.*

Proof. We proceed by induction on m. For $m = 1$ $[.]_{\mathscr{N}}$ is an identical mapping. Let $m > 1$. Clearly $n = kN_m + n_m$ with $k = [n_1, \dots, n_{m-1}]_{\mathscr{N}'}$, and $\mathscr{N}' = (N_1, N_2, \dots, N_{m-1})$. By induction hypothesis $0 \leq k \leq N_{1,m-1} - 1 \Rightarrow 0 \leq kN_m + n_m \leq N - N_m + n_m \leq N - 1 \Rightarrow n \in \mathbf{Z}_N$. $[.]_{\mathscr{N}}$ is injective: $n = n' = [n_1', n_2', \dots, n_{m-1}']_{\mathscr{N}'} N_m + n_m' \Rightarrow N_m \mid (n_m - n_m') \Rightarrow n_m = n_m'$ in view of $0 \leq |n_m - n_m'| \leq N_m - 1$. Hence $[n_1, n_2, \dots, n_{m-1}]_{\mathscr{N}'} = [n_1', n_2', \dots, n_{m-1}']_{\mathscr{N}'}$ and by induction hypothesis $n_i = n_i'$ for each $i \in [1 : m-1]$. ∎

1.5 Definition. The ordered m-tuple $(n_1, n_2, \dots, n_m)$ is called a *mixed-radix integer representation* of $n = [n_1, n_2, \dots, n_m]_{\mathscr{N}}$ with respect to the number system $\mathscr{N}$.

Hereafter we shall omit the subscript $\mathscr{N}$ and write simply $[n_1, n_2, \dots, n_m]$ whenever the NS is implicitely determined from the context. In particular the NS $\mathscr{N} = (N_1, N_2, \dots, N_m)$ associated with the factorization $N = N_{1,m}$ is assumed if not stated otherwise.

1.6 Lemma. *Let* $N = N_{1,m}$, $m \geqslant 2$. *Then for each* $i \in [1 : m-1]$ *it holds* $[[n_1, n_2, \dots, n_i], [n_{i+1}, n_{i+2}, \dots, n_m]] = [n_1, n_2, \dots, n_m]$.

Proof. $[n_1, \ldots, n_i] \in \mathbf{Z}_{N_{1,i}}, [n_{i+1}, \ldots, n_m] \in \mathbf{Z}_{N_{i+1,m}}, N = N_{1,i}N_{i+1,m} \Rightarrow$ $\Rightarrow [[n_1, \ldots, n_i], [n_{i+1}, \ldots, n_m]] = [n_1, \ldots, n_i] N_{i+1,m} + [n_{i+1}, \ldots, n_m] =$ $= (n_1 N_{2,i} + n_2 N_{3,i} + \ldots + n_i) N_{i+1,m} + n_{i+1} N_{i+2,m} + \ldots + n_m = [n_1, n_2, \ldots, \ldots, n_m]$. ∎

1.7 Definition. Let us have a NS $\mathcal{N} = (N_i, \ldots, N_j)$ and $N = N_{i,j}$. We define a mapping $\varphi_{\mathcal{N}} : \mathcal{P}([i:j]) \to \mathcal{P}(\mathbf{Z}_N)$ as follows:
$\varphi_{\mathcal{N}}(p) = P$, where $P([n_i, \ldots, n_j]_{\mathcal{N}}) = [n_{p(i)}, \ldots, n_{p(j)}]_{\mathcal{N}p}$.
It holds $\varphi_{\mathcal{N}}(1) = \mathbf{I}_N$ (here 1 is the identical permutation in $\mathcal{P}([i:j])$). But in general $\varphi_{\mathcal{N}}$ is not a homomorphism of permutation groups, e.g. $N_1 = 2$, $N_2 = 3$, $p(1) = 2$, $p(2) = 1$ is a counter-example.

1.8 Lemma. *Let* $\mathbf{A}_i \in \mathcal{M}(N_i \times K_i)$ *for* $i \in [1:m]$, $m \geq 2$, $N = N_{1,m}$, $K = K_{1,m}$, $\mathcal{N} = (N_1, \ldots, N_m)$ *and* $\mathcal{K} = (K_1, \ldots, K_m)$. *If we put* $\mathbf{A} = \mathbf{A}_1 \otimes \ldots \otimes \mathbf{A}_m$, $\mathbf{A}_p = \mathbf{A}_{p(1)} \otimes \ldots \otimes \mathbf{A}_{p(m)}$, $P_{\mathcal{N}} = \varphi_{\mathcal{N}}(p)$ *and* $P_{\mathcal{K}} = \varphi_{\mathcal{K}}(p)$ *for an arbitrary permutation* $p \in \mathcal{P}([1:m])$, *then it holds* $\mathbf{A}_p = \mathbf{P}_{\mathcal{N}} \mathbf{A} \mathbf{P}_{\mathcal{K}}^T$, *or equivalently* $A_p(P_{\mathcal{N}}(n), P_{\mathcal{K}}(k)) = A(n, k)$ *for each* $n \in \mathbf{Z}_N$ *and* $k \in \mathbf{Z}_K$.

Proof. $A_p(P_{\mathcal{N}}([n_1, \ldots, n_m]), P_{\mathcal{K}}([k_1, \ldots, k_m])) = A_p([n_{p(1)}, \ldots, n_{p(m)}]_{\mathcal{N}p}, [k_{p(1)}, \ldots, k_{p(m)}]_{\mathcal{K}p}) = A_{p(1)}(n_{p(1)}, k_{p(1)}) \ldots A_{p(m)}(n_{p(m)}, k_{p(m)}) = A_1(n_1, k_1) \ldots \ldots A_m(n_m, k_m) = A([n_1, \ldots, n_m], [k_1, \ldots, k_m])$ in view of commutativity of multiplication in the ring $\mathbf{R}$. ∎

1.9 Convention. Later on we shall agree on the following notation: $p_{i,j}$ and $1_{i,j}$ stand for an arbitrary and identical permutation, respectively belonging to $\mathcal{P}([i:j])$; $s_{i,j} \in \mathcal{P}([i:j])$ denotes a permutation defined by $s_{i,j}(i+k) = j - k$, $k \in [0:j-i]$. Similarly $P_{i,j} = \varphi_{\mathcal{N}_{i,j}}(p_{i,j})$, $\mathbf{I}_{N_{i,j}} = \varphi_{\mathcal{N}_{i,j}}(1_{i,j})$ and $S_{i,j} = \varphi_{\mathcal{N}_{i,j}}(s_{i,j})$ are the associated permutations belonging to $\mathcal{P}(\mathbf{Z}_{N_{i,j}})$. $S_{i,j}$ is called the *digit reversal* with respect to the NS $\mathcal{N}_{i,j}$. Subscripts i, j may be omitted whenever $i = 1$ and $j = m$. We shall write also $S_{\mathcal{N}}$ to emphasize that $S_{\mathcal{N}}$ is the digit reversal with respect to $\mathcal{N}$.

1.10 Theorem. *Let* $\mathcal{N} = (N_1, \ldots, N_m)$, $m \geq 2$ *and* $p = p_{1,i} \cup p_{i+1,m} \in \mathcal{P}([1:m])$ *for some* $i \in [1:m-1]$. *Then* $\varphi_{\mathcal{N}}(p) = \mathbf{P} = \mathbf{P}_{1,i} \otimes \mathbf{P}_{i+1,m}$.

Proof. We are going to verify $\mathbf{P} = \tilde{\mathbf{P}}$ where $\tilde{\mathbf{P}} = \mathbf{P}_{1,i} \otimes \mathbf{P}_{i+1,m}$. Let $n = [n_1, \ldots, n_m]$, $k = [k_1, \ldots, k_m] \in \mathbf{Z}_{N_{1,m}}$ be arbitrary. Using 1.6 we get $\tilde{P}(n, k) = \tilde{P}([[n_1, \ldots, n_i], [n_{i+1}, \ldots, n_m]], [[k_1, \ldots, k_i], [k_{i+1}, \ldots, k_m]]) = P_{1,i}([n_1, \ldots, \ldots, n_i], [k_1, \ldots, k_i]) P_{i+1,m}([n_{i+1}, \ldots, n_m], [k_{i+1}, \ldots, k_m]) = \delta([n_1, \ldots, n_i], [k_{p_{1,i}(1)}, \ldots, k_{p_{1,i}(i)}]) \delta([n_{i+1}, \ldots, n_m], [k_{p_{i+1,m}(i+1)}, \ldots, k_{p_{i+1,m}(m)}]) = \delta([n_1, \ldots, \ldots, n_m], [k_{p(1)}, \ldots, k_{p(m)}]) = \delta_{n, P(k)} = P(n, k)$. ∎

1.11 Corollary. *Let* $p_1 = p_{1,i} \cup 1_{i+1,m}$ *and* $p_2 = 1_{1,i} \cup p_{i+1,m}$ *then* $p = p_{1,i} \cup \cup p_{i+1,m} = p_1 p_2 = p_2 p_1$ *and* $P = \varphi_{\mathcal{N}}(p) = \varphi_{\mathcal{N}}(p_1)\, \varphi_{\mathcal{N}}(p_2) = \varphi_{\mathcal{N}}(p_2)\, \varphi_{\mathcal{N}}(p_1)$ *where* $\varphi_{\mathcal{N}}(p_1) = \mathbf{P}_{1,i} \otimes \mathbf{I}_{N_{i+1,m}}$, $\varphi_{\mathcal{N}}(p_2) = \mathbf{I}_{N_{1,i}} \otimes \mathbf{P}_{i+1,m}$.

Proof. $\mathbf{P} = (\mathbf{P}_{1,i} \otimes \mathbf{I}_{N_{i+1,m}})(\mathbf{I}_{N_{1,i}} \otimes \mathbf{P}_{i+1,m}) = (\mathbf{I}_{N_{1,i}} \otimes \mathbf{P}_{i+1,m})(\mathbf{P}_{1,i} \otimes \otimes \mathbf{I}_{N_{i+1,m}})$ is a well-known property of $\otimes$. The factors are equal to $\varphi_{\mathcal{N}}(p_1)$ and $\varphi_{\mathcal{N}}(p_2)$ due to 1.10 and by $\varphi_{\mathcal{N}_{1,i}}(1_{1,i}) = \mathbf{I}_{N_{1,i}}$ and $\varphi_{\mathcal{N}_{i+1,m}}(1_{i+1,m}) = \mathbf{I}_{N_{i+1,m}}$. ∎

1.12 Corollary. *Let* $i \in [1 : m-1]$, $m \geq 2$ *be arbitrary and* $\mathbf{S}_i = \varphi_{(N_{1,i}, N_{i+1,m})}(s)$. *Then it holds* $\varphi_{\mathcal{N}}(s_{1,m}) = \mathbf{S} = \mathbf{S}_i(\mathbf{S}_{1,i} \otimes \mathbf{S}_{i+1,m}) = (\mathbf{S}_{i+1,m} \otimes \mathbf{S}_{1,i})\, \mathbf{S}_i$.

Proof. It is sufficient to show $\mathbf{S} = \mathbf{S}_i\mathbf{P}$ with $\mathbf{P} = \varphi_{\mathcal{N}}(p)$, $p = s_{1,i} \cup s_{i+1,m}$. For each $n = [n_1, \ldots, n_m] \in \mathbf{Z}_{N_{1,m}}$ we can write in view of 1.6 $S_iP(n) = = S_iP([n_1, \ldots, n_m]) = S_i([n_{p(1)}, \ldots, n_{p(m)}]) = S_i([n_i, n_{i-1}, \ldots, n_1, n_m, n_{m-1}, \ldots, \ldots, n_{i+1}]) = S_i([[n_i, \ldots, n_1], [n_m, \ldots, n_{i+1}]]) = [[n_m, \ldots, n_{i+1}], [n_i, \ldots, n_1]] = = [n_m, \ldots, n_1] = S(n)$. Then $\mathbf{P} = \mathbf{S}_{1,i} \otimes \mathbf{S}_{i+1,m}$ by 1.10 and also $\mathbf{S} = \mathbf{S}_i\mathbf{P}\mathbf{S}_i^T\mathbf{S}_i$ where $\mathbf{S}_i\mathbf{P}\mathbf{S}_i^T = \mathbf{S}_{i+1,m} \otimes \mathbf{S}_{1,i}$ by 1.8. ∎

2. GENERALIZED KRONECKER PRODUCT OF MATRICES

By definition, the Kronecker product $\mathbf{A} = \mathbf{A}_1 \otimes \mathbf{A}_2$, $\mathbf{A}_1 \in \mathcal{M}(N_1 \times K_1)$, $\mathbf{A}_2 \in \in \mathcal{M}(N_2 \times K_2)$ is a matrix having block form $\mathbf{A} = (\mathbf{A}^{n_1,k_1}) \in \mathcal{M}(N \times K)$, $N = N_1N_2$, $K = K_1K_2$ where for each $n_1 \in \mathbf{Z}_{N_1}$ and $k_1 \in \mathbf{Z}_{K_1}$

$$\mathbf{A}^{n_1,k_1} = A_1(n_1, k_1)\, \mathbf{A}_2 . \tag{2.1}$$

Clearly, either of the following two equations is equivalent to (2.1):

$$\mathbf{A}^{n_1,k_1} = \mathbf{A}_2 \overrightarrow{\mathbf{A}}_1^{n_1,k_1}, \quad \overrightarrow{\mathbf{A}}_1^{n_1,k_1} = = \operatorname{diag}(A_1(n_1, k_1), \ldots, A_1(n_1, k_1)) \in \mathcal{M}(K_2 \times K_2), \tag{2.2}$$

$$\mathbf{A}^{n_1,k_1} = \overleftarrow{\mathbf{A}}_1^{n_1,k_1} \mathbf{A}_2, \quad \overleftarrow{\mathbf{A}}_1^{n_1,k_1} = = \operatorname{diag}(A_1(n_1, k_1), \ldots, A_1(n_1, k_1)) \in \mathcal{M}(N_2 \times N_2). \tag{2.3}$$

Allowing different elements to enter into the diagonal of $\overrightarrow{\mathbf{A}}_1^{n_1,k_1}$ or $\overleftarrow{\mathbf{A}}_1^{n_1,k_1}$, a Kronecker product generalized in two ways may be obtained according to the following definition.

2.1 Definition. *Generalized Kronecker product of matrices.*

Let $N = N_1N_2$, $K = K_1K_2$, $\mathbf{A}_1 \in \mathcal{M}(N_1 \times K_1K_2)$, $\mathbf{A}_2 \in \mathcal{M}(N_2 \times K_2)$, $\mathbf{B}_1 \in \in \mathcal{M}(N_1N_2 \times K_1)$ and $\mathbf{B}_2 \in \mathcal{M}(N_2 \times K_2)$. Then the matrix $\mathbf{A} = \mathbf{A}_1 \otimes_R \mathbf{A}_2 \in \in \mathcal{M}(N \times K)$ ($\mathbf{B} = \mathbf{B}_1 \otimes_L \mathbf{B}_2 \in \mathcal{M}(N \times K)$) is said to be a right (left) generalized Kronecker product of matrices $\mathbf{A}_1$ and $\mathbf{A}_2$ ($\mathbf{B}_1$ and $\mathbf{B}_2$) if $A([n_1, n_2], [k_1, k_2]) = A_1(n_1, [k_1, k_2])\, A_2(n_2, k_2)$ and $B([n_1, n_2], [k_1, k_2]) = = B_1([n_1, n_2], k_1)\, B_2(n_2, k_2)$ holds for each $n_i \in \mathbf{Z}_{N_i}$ and $k_i \in Z_{K_i}$ with $i = 1, 2$.

Clearly, $\mathbf{A} = (\mathbf{A}^{n_1,k_1})$ where

$$\mathbf{A}^{n_1,k_1} = \mathbf{A}_2 \overrightarrow{\mathbf{A}}_1^{n_1,k_1},$$

$$(2.4) \qquad \overrightarrow{\mathbf{A}}_1^{n_1,k_1} = \operatorname{diag}(A_1(n_1, [k_1, 0]), A_1(n_1, [k_1, 1]), \ldots, \ldots, A_1(n_1, [k_1, K_2 - 1]))$$

and $\mathbf{B}_2 = (\mathbf{B}^{n_1,k_1})$ where

$$\mathbf{B}^{n_1,k_1} = \overleftarrow{\mathbf{B}}_1^{n_1,k_1}\mathbf{B}_2,$$

$$(2.5) \qquad \overleftarrow{\mathbf{B}}^{n_1,k_1} = \operatorname{diag}(B_1([n_1, 0], k_1), B_1([n_1, 1], k_1), \ldots, \ldots, B_1([n_1, N_2 - 1], k_1)).$$

2.2 Remark. Kronecker product $\otimes$ may be considered as a special case of both $\otimes_R$ and $\otimes_L$ writing instead of $\mathbf{A} = \mathbf{A}_1 \otimes \mathbf{A}_2$ either $\mathbf{A} = \mathbf{A}_{1,R} \otimes_R \mathbf{A}_2$ or $\mathbf{A} = \mathbf{A}_{1,L} \otimes_L \mathbf{A}_2$ where $A_{1,R}(n_1, [k_1, k_2]) = A_{1,L}([n_1, n_2], k_1) = A_1(n_1, k_1)$.

2.3 Lemma. *For* $\mathbf{A}_1 \in \mathcal{M}(N_1 \times K_1K_2)$ *and* $\mathbf{B}_1 \in \mathcal{M}(N_1N_2 \times K_1)$ *it holds* $\mathbf{A}_1 \otimes_R \mathbf{I}_{K_2} = \overrightarrow{\mathbf{A}}_1 = (\overrightarrow{\mathbf{A}}_1^{n_1,k_1})$ *and* $\mathbf{B}_1 \otimes_L \mathbf{I}_{N_2} = \overleftarrow{\mathbf{B}}_1 = (\overleftarrow{\mathbf{B}}_1^{n_1,k_1})$ *where* $\overrightarrow{\mathbf{A}}_1^{n_1,k_1}$ *and* $\overleftarrow{\mathbf{B}}_1^{n_1,k_1}$ *are diagonal matrices* of (2.4) *and* (2.5), *respectively. Moreover* $\mathbf{S}_{(N_1,K_2)}\overrightarrow{\mathbf{A}}_1\mathbf{S}^T_{(K_1,K_2)} = \operatorname{diag}(\mathbf{A}_{1,0}, \mathbf{A}_{1,1}, \ldots, \mathbf{A}_{1,K_2-1})$ *and* $\mathbf{S}_{(N_1,N_2)}\overleftarrow{\mathbf{B}}_1\mathbf{S}^T_{(K_1,N_2)} = \operatorname{diag}(\mathbf{B}_{1,0}, \mathbf{B}_{1,1}, \ldots, \mathbf{B}_{1,N_2-1})$ *where* $\mathbf{A}_{1,k_2}, \mathbf{B}_{1,n_2} \in \mathcal{M}(N_1 \times K_1)$, $A_{1,k_2}(n_1, k_1) = A_1(n_1, [k_1, k_2])$ *and* $B_{1,n_2}(n_1, k_1) = B_1([n_1, n_2], k_1)$ *for each* $n_i \in \mathbf{Z}_{N_i}$ *and* $k_i \in \mathbf{Z}_{K_i}$, $i = 1, 2$.

Proof. By definition 2.1, $\overrightarrow{A}_1([n_1, k_2'], [k_1, k_2]) = A_1(n_1, [k_1, k_2])\ \delta_{k_2',k_2}$ is the element positioned in $(k_2' + 1)$-th row and $(k_2 + 1)$-th column of the block $\overrightarrow{\mathbf{A}}_1^{n_1,k_1}$, which says that $\overrightarrow{\mathbf{A}}_1^{n_1,k_1}$ is exactly the diagonal matrix of (2.4). At the same time it is the element in $([k_2', n_1] + 1)$-th row and $([k_2, k_1] + 1)$-th column of $\mathbf{S}_{(N_1,K_2)}\overrightarrow{\mathbf{A}}_1\mathbf{S}^T_{(K_1,K_2)}$, which means that the only non-zero blocks of size $N_1 \times K_1$ are those with $k_2 = k_2'$, i.e. $A_1(n_1, [k_1, k_2])$ is the element in $(n_1 + 1)$-th row and $(k_1 + 1)$-th column of $(k_2 + 1)$-th diagonal block $\mathbf{A}_{1,k_2}$. For $\mathbf{B}_1$ is the argumentation analogical. ∎

2.4 Theorem. *Duality principle.*

Under assumptions of definition 2.1 *it holds* $(\mathbf{A}_1 \otimes_R \mathbf{A}_2)^T = \mathbf{A}_1^T \otimes_L \mathbf{A}_2^T$ and $(\mathbf{B}_1 \otimes_L \mathbf{B}_2)^T = \mathbf{B}_1^T \otimes_R \mathbf{B}_2^T$.

Proof. $\mathbf{A} = \mathbf{A}_1 \otimes_R \mathbf{A}_2 \Rightarrow A^T([k_1, k_2], [n_1, n_2]) = A([n_1, n_2], [k_1, k_2]) = A_1(n_1, [k_1, k_2])\ A_2(n_2, k_2) = A_1^T([k_1, k_2], n_1)\ A_2^T(k_2, n_2) \Rightarrow \mathbf{A}^T = \mathbf{A}_1^T \otimes_L \mathbf{A}_2^T$. $(\mathbf{B}^T)^T = \mathbf{B} = \mathbf{B}_1 \otimes_L \mathbf{B}_2 = (\mathbf{B}_1^T)^T \otimes_L (\mathbf{B}_2^T)^T = (\mathbf{B}_1^T \otimes_R \mathbf{B}_2^T)^T \Rightarrow \mathbf{B}^T = \mathbf{B}_1^T \otimes_R \mathbf{B}_2^T$. ∎

We shall prove some basic properties of $\otimes_R$ and $\otimes_L$ analogical to those of the ordinary Kronecker product $\otimes$ (cf. [6]). Moreover, these properties of $\otimes$ are obtained by 2.2 as a special case of the corresponding properties of $\otimes_R$ or $\otimes_L$ (see 2.5, 2.6, 2.11 and 2.12).

2.5 Theorem. *Either of the operations $\otimes_R$ and $\otimes_L$ is associative and distributive*:

1° *If* $\mathbf{A}_i \in \mathcal{M}(N_i \times K_{i,3})$ *and* $\mathbf{B}_i \in \mathcal{M}(N_{i,3} \times K_i)$ for $i = 1, 2, 3$ *then*

$$(\mathbf{A}_1 \otimes_R \mathbf{A}_2) \otimes_R \mathbf{A}_3 = \mathbf{A}_1 \otimes_R (\mathbf{A}_2 \otimes_R \mathbf{A}_3),$$
$$(\mathbf{B}_1 \otimes_L \mathbf{B}_2) \otimes_L \mathbf{B}_3 = \mathbf{B}_1 \otimes_L (\mathbf{B}_2 \otimes_L \mathbf{B}_3).$$

2° *If* $\mathbf{A}_i, \mathbf{A}_i' \in \mathcal{M}(N_i \times K_{i,2})$ *and* $\mathbf{B}_i, \mathbf{B}_i' \in \mathcal{M}(N_{i,2} \times K_i)$ *for* $i = 1, 2$ *then*

$$(\mathbf{A}_1 + \mathbf{A}_1') \otimes_R \mathbf{A}_2 = \mathbf{A}_1 \otimes_R \mathbf{A}_2 + \mathbf{A}_1' \otimes_R \mathbf{A}_2,$$
$$\mathbf{A}_1 \otimes_R (\mathbf{A}_2 + \mathbf{A}_2') = \mathbf{A}_1 \otimes_R \mathbf{A}_2 + \mathbf{A}_1 \otimes_R \mathbf{A}_2',$$
$$(\mathbf{B}_1 + \mathbf{B}_1') \otimes_L \mathbf{B}_2 = \mathbf{B}_1 \otimes_L \mathbf{B}_2 + \mathbf{B}_1' \otimes_L \mathbf{B}_2,$$
$$\mathbf{B}_1 \otimes_L (\mathbf{B}_2 + \mathbf{B}_2') = \mathbf{B}_1 \otimes_L \mathbf{B}_2 + \mathbf{B}_1 \otimes_L \mathbf{B}_2'.$$

Proof. We shall prove the assertion only for $\otimes_R$ because for $\otimes_L$ it follows by the duality principle.

1° $\mathbf{A}_1 \in \mathcal{M}(N_1 \times K_1 K_{2,3})$, $\mathbf{A}_2 \in \mathcal{M}(N_2 \times K_{2,3}) \Rightarrow \mathbf{B} = \mathbf{A}_1 \otimes_R \mathbf{A}_2 \in \mathcal{M}(N_{1,2} \times K_1 K_{2,3})$. $\mathbf{A}_2 \in \mathcal{M}(N_2 \times K_2 K_3)$, $\mathbf{A}_3 \in \mathcal{M}(N_3 \times K_3) \Rightarrow \tilde{\mathbf{B}} = \mathbf{A}_2 \otimes_R \mathbf{A}_3 \in \mathcal{M}(N_{2,3} \times K_{2,3})$. Hence $\mathbf{A} = \mathbf{B} \otimes_R \mathbf{A}_3 \in \mathcal{M}(N_{1,2} N_3 \times K_{1,2} K_3)$ and $\tilde{\mathbf{A}} = \mathbf{A}_1 \otimes_R \tilde{\mathbf{B}} \in \mathcal{M}(N_1 N_{2,3} \times K_1 K_{2,3})$ are correctly defined matrices of the same size $N_{1,3} \times K_{1,3}$. We are going to prove $\mathbf{A} = \tilde{\mathbf{A}}$. In view of 1.6, $B([n_1, n_2], [[k_1, k_2], k_3]) = B([n_1, n_2], [k_1, [k_2, k_3]]) = A_1(n_1, [k_1, [k_2, k_3]])\, A_2(n_2, [k_2, k_3])$. Thus $A([[n_1, n_2], n_3], [[k_1, k_2], k_3]) = B([n_1, n_2], [[k_1, k_2], k_3])\, A_3(n_3, k_3) = (A_1(n_1, [k_1, [k_2, k_3]])\, A_2(n_2, [k_2, k_3]))\, A_3(n_3, k_3) = A_1(n_1, [k_1, [k_2, k_3]]) \,.\, \tilde{B}([n_2, n_3], [k_2, k_3]) = \tilde{A}([n_1, [n_2, n_3]], [k_1, [k_2, k_3]])$ holds by the associativity of multiplication in the ring **R**. Using 1.6 once more, we get $A([n_1, n_2, n_3], [k_1, k_2, k_3]) = \tilde{A}([n_1, n_2, n_3], [k_1, k_2, k_3])$.

2° follows immediately by definition 2.1 and by the distributivity of multiplication in the ring **R**. ∎

2.6 Theorem. *Let* $\mathbf{A}_i' \in \mathcal{M}(M_i \times N_i)$, $\mathbf{A}_i \in \mathcal{M}(N_i \times K_{i,2})$, $\mathbf{B}_i \in \mathcal{M}(N_{i,2} \times K_i)$ *and* $\mathbf{B}_i' \in \mathcal{M}(K_i \times L_i)$ *for* $i = 1, 2$. *Then it holds*

$$(\mathbf{A}_1' \otimes \mathbf{A}_2')(\mathbf{A}_1 \otimes_R \mathbf{A}_2) = \mathbf{A}_1'\mathbf{A}_1 \otimes_R \mathbf{A}_2'\mathbf{A}_2,$$
$$(\mathbf{B}_1 \otimes_L \mathbf{B}_2)(\mathbf{B}_1' \otimes \mathbf{B}_2') = \mathbf{B}_1\mathbf{B}_1' \otimes_L \mathbf{B}_2\mathbf{B}_2'.$$

Proof. Let us denote $\mathbf{A}' = \mathbf{A}_1' \otimes \mathbf{A}_2' \in \mathcal{M}(M_1 M_2 \times N_1 N_2)$, $\mathbf{A} = \mathbf{A}_1 \otimes_R \mathbf{A}_2 \in \mathcal{M}(N_1 N_2 \times K_1 K_2)$, $\tilde{\mathbf{A}}_1 = \mathbf{A}_1'\mathbf{A}_1 \in \mathcal{M}(M_1 \times K_1 K_2)$ and $\tilde{\mathbf{A}}_2 = \mathbf{A}_2'\mathbf{A}_2 \in \mathcal{M}(M_2 \times K_2)$. We see that $\mathbf{C} = \mathbf{A}'\mathbf{A}$ and $\tilde{\mathbf{C}} = \tilde{\mathbf{A}}_1 \otimes_R \tilde{\mathbf{A}}_2$ are correctly defined matrices of the same size $M_1 M_2 \times K_1 K_2$. We are going to show $\mathbf{C} = \tilde{\mathbf{C}}$. As $A'([m_1, m_2], [n_1, n_2]) = A_1'(m_1, n_1)\, A_2'(m_2, n_2)$ by 2.2 and $A([n_1, n_2], [k_1, k_2]) = A_1(n_1, [k_1, k_2]) \,.\, A_2(n_2, k_2)$ by 2.1, we have $C([m_1, m_2], [k_1, k_2]) = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} (A_1'(m_1, n_1) \,.$

$. \mathbf{A}_2'(m_2, n_2)) (A_1(n_1, [k_1, k_2]) A_2(n_2, k_2)) = (\sum_{n_1=0}^{N_1-1} A_1'(m_1, n_1) A_1(n_1, [k_1, k_2])) \cdot$
$\cdot (\sum_{n_2=0}^{N_2-1} A_2'(m_2, n_2) A_2(n_2, k_2)) = \tilde{A}_1(m_1, [k_1, k_2]) \tilde{A}_2(m_2, k_2) = \tilde{C}([m_1, m_2],$
$[k_1, k_2])$ by 2.1 and in view of commutativity, associativity and distributivity of multiplication in the ring $\mathbf{R}$.

The assertion for $\otimes_L$ is easy to prove by the duality principle:

$$(\mathbf{B}_1 \otimes_L \mathbf{B}_2)(\mathbf{B}_1' \otimes \mathbf{B}_2') = ((\mathbf{B}_1' \otimes \mathbf{B}_2')^T (\mathbf{B}_1 \otimes_L \mathbf{B}_2)^T)^T =$$
$$= ((\mathbf{B}_1'^T \otimes \mathbf{B}_2'^T)(\mathbf{B}_1^T \otimes_R \mathbf{B}_2^T))^T = (\mathbf{B}_1'^T \mathbf{B}_1^T \otimes_R \mathbf{B}_2'^T \mathbf{B}_2^T)^T =$$
$$= ((\mathbf{B}_1 \mathbf{B}_1')^T \otimes_R (\mathbf{B}_2 \mathbf{B}_2')^T)^T = \mathbf{B}_1 \mathbf{B}_1' \otimes_L \mathbf{B}_2 \mathbf{B}_2'. \blacksquare$$

The associativity of $\otimes_R$ and $\otimes_L$ allows one to extend the notion of the generalized right and left Kronecker product to m factors ($m \geqq 2$):

2.7 Definition. *Mixed-radix transform.*

Let $N = N_{1,m}$, $K = K_{1,m} (m \geqq 2)$, $\mathbf{A}_i \in \mathcal{M}(N_i \times K_{i,m})$ and $\mathbf{B}_i \in \mathcal{M}(N_{i,m} \times K_i)$ for $i \in [1:m]$. Then the linear transform defined by the matrix $\mathbf{A} = \mathbf{A}_1 \otimes_R \mathbf{A}_2 \otimes_R \ldots \otimes_R \mathbf{A}_m \in \mathcal{M}(N \times K)$ or $\mathbf{B} = \mathbf{B}_1 \otimes_L \mathbf{B}_2 \otimes_L \ldots \otimes_L \mathbf{B}_m \in \mathcal{M}(N \times K)$ is said to be a mixed-radix transform (MRT).

2.8 Remark. It is easy to see by induction on m and in view of 1.6 that $\mathbf{A} = \mathbf{A}_1 \otimes_R \mathbf{A}_2 \otimes_R \ldots \otimes_R \mathbf{A}_m$ iff $A([n_1, \ldots, n_m], [k_1, \ldots, k_m]) = A_1(n_1, [k_1, \ldots, k_m]) A_2(n_2, [k_2, \ldots, k_m]) \ldots A_m(n_m, k_m)$ for each $n_i \in \mathbf{Z}_{N_i}$ and $k_i \in \mathbf{Z}_{K_i}$, $i \in [1:m]$. Similarly $\mathbf{B} = \mathbf{B}_1 \otimes_L \mathbf{B}_2 \otimes_L \ldots \otimes_L \mathbf{B}_m$ iff $B([n_1, \ldots, n_m], [k_1, \ldots, k_m]) = B_1([n_1, \ldots, n_m], k_1) B_2([n_2, \ldots, n_m], k_2) \ldots B_m(n_m, k_m)$ for each $n_i \in \mathbf{Z}_{N_i}$ and $k_i \in \mathbf{Z}_{K_i}$, $i \in [1:m]$.

2.9 Theorem. *Fast mixed-radix transform.*

If $\mathbf{A}$ *and* $\mathbf{B}$ *are* MRT *matrices defined in 2.7 then the following factorizations, called* fast mixed-radix transforms (FMRTs), *take place*:
$\mathbf{A} = \mathbf{A}^{(m)} \mathbf{A}^{(m-1)} \ldots \mathbf{A}^{(1)}$ *and* $\mathbf{B} = \mathbf{B}^{(1)} \mathbf{B}^{(2)} \ldots \mathbf{B}^{(m)}$ *where for* $i \in [1:m]$
$\mathbf{A}^{(i)} = \mathbf{I}_{N_{1,i-1}} \otimes (\mathbf{A}_i \otimes_R \mathbf{I}_{K_{i+1,m}}) \in \mathcal{M}(N_{1,i} K_{i+1,m} \times N_{1,i-1} K_{i,m})$ *and*
$\mathbf{B}^{(i)} = \mathbf{I}_{K_{1,i-1}} \otimes (\mathbf{B}_i \otimes_L \mathbf{I}_{N_{i+1,m}}) \in \mathcal{M}(K_{1,i-1} N_{i,m} \times K_{1,i} N_{i+1,m})$.

Proof. First we shall prove the factorization of $\mathbf{A}$ by induction on m.

1. $m = 2$: $\mathbf{A}^{(2)} \mathbf{A}^{(1)} = (\mathbf{I}_{N_1} \otimes \mathbf{A}_2)(\mathbf{A}_1 \otimes_R \mathbf{I}_{K_2}) = \mathbf{I}_{N_1} \mathbf{A}_1 \otimes_R \mathbf{A}_2 \mathbf{I}_{K_2} = \mathbf{A}_1 \otimes_R \mathbf{A}_2 = \mathbf{A}$ is an immediate consequence of theorem 2.6.

2. $m > 2$: $\mathbf{A} = \mathbf{A}_1 \otimes_R \mathbf{A}'$ where $\mathbf{A}' = \mathbf{A}_2 \otimes_R \ldots \otimes_R \mathbf{A}_m$. By induction hypothesis $\mathbf{A}' = \mathbf{A}'^{(m)} \mathbf{A}'^{(m-1)} \ldots \mathbf{A}'^{(2)}$ with $\mathbf{A}'^{(i)} = \mathbf{I}_{N_{2,i-1}} \otimes (\mathbf{A}_i \otimes_R \mathbf{I}_{K_{i+1,m}})$, $\mathbf{A} = (\mathbf{I}_{N_1} \otimes \mathbf{A}')(\mathbf{A}_1 \otimes_R \mathbf{I}_{K_{2,m}}) = (\mathbf{I}_{N_1} \otimes \mathbf{A}') \mathbf{A}^{(1)}$ and $\mathbf{I}_{N_1} \otimes \mathbf{A}' = \mathbf{I}_{N_1} \otimes (\mathbf{A}'^{(m)} \mathbf{A}'^{(m-1)} \ldots \mathbf{A}'^{(2)}) = (\mathbf{I}_{N_1} \otimes \mathbf{A}'^{(m)})(\mathbf{I}_{N_1} \otimes \mathbf{A}'^{(m-1)}) \ldots (\mathbf{I}_{N_1} \otimes \mathbf{A}'^{(2)})$ where $\mathbf{I}_{N_1} \otimes \mathbf{A}'^{(i)} = \mathbf{I}_{N_1} \otimes \mathbf{I}_{N_{2,i-1}} \otimes (\mathbf{A}_i \otimes_R I_{K_{i+1,m}}) = \mathbf{I}_{N_{1,i-1}} \otimes (\mathbf{A}_i \otimes_R \mathbf{I}_{K_{i+1,m}}) = \mathbf{A}^{(i)}$ for $i \in [2:m]$.

The factorization of **B** is an immediate consequence of the factorization of **A** when putting $\mathbf{A} = \mathbf{B}^T$, $\mathbf{A}_i = \mathbf{B}_i^T$ and using the duality principle (N_i and K_i interchange their roles): $\mathbf{B} = ((\mathbf{B}_1 \otimes_L \mathbf{B}_2 \otimes_L \dots \otimes_L \mathbf{B}_m)^T)^T = (\mathbf{B}_1^T \otimes_R \mathbf{B}_2^T \otimes_R \dots \otimes_R \otimes_R \mathbf{B}_m^T)^T = (\mathbf{A}_1 \otimes_R \mathbf{A}_2 \otimes_R \dots \otimes_R \mathbf{A}_m)^T = \mathbf{A}^T = (\mathbf{A}^{(m)}\mathbf{A}^{(m-1)} \dots \mathbf{A}^{(1)})^T = \mathbf{A}^{(1)T}\mathbf{A}^{(2)T} \dots \mathbf{A}^{(m)T}$ where $\mathbf{B}^{(i)} = \mathbf{A}^{(i)T} = (\mathbf{I}_{K_{1,i-1}} \otimes (\mathbf{A}_i \otimes_R \mathbf{I}_{N_{i+1,m}}))^T = \mathbf{I}_{K_{1,i-1}} \otimes (\mathbf{A}_i^T \otimes_L \mathbf{I}_{N_{i+1,m}}) = \mathbf{I}_{K_{1,i-1}} \otimes (\mathbf{B}_i \otimes_L \mathbf{I}_{N_{i+1,m}})$. ∎

Similarly as for FFTs (see [4, p. 88]), still more FMRTs may be obtained by inserting a factored identity matrix between two factors of the appropriate matrix product of **A** or **B**. E.g., if $\mathbf{P}_i \in \mathscr{P}(\mathbf{Z}_{N_{1,i-1}K_{i,m}})$ is not an identity permutation for all $i \in [2 : m]$ then $\tilde{\mathbf{A}}^{(m)} = \mathbf{A}^{(m)}\mathbf{P}_m^T$, $\tilde{\mathbf{A}}^{(i)} = \mathbf{P}_{i+1}\mathbf{A}^{(i)}\mathbf{P}_i^T$, $i \in [2 : m-1]$ and $\tilde{\mathbf{A}}^{(1)} = \mathbf{P}_2\mathbf{A}^{(1)}$ define another FMRT. We have $\mathbf{A} = \tilde{\mathbf{A}}^{(m)}\tilde{\mathbf{A}}^{(m-1)} \dots \tilde{\mathbf{A}}^{(1)}$ because $\mathbf{P}_i^T\mathbf{P}_i$ is an identity matrix which, being inserted between factors $\mathbf{A}^{(i)}$ and $\mathbf{A}^{(i-1)}$, leaves the matrix product unchanged.

As in fact the factorization of **B** in theorem 2.9 is obtained by matrix transpose of $\mathbf{A} = \mathbf{B}^T$, all FMRTs may be derived from the factorization $\mathbf{A} = \mathbf{A}^{(m)}\mathbf{A}^{(m-1)} \dots \dots \mathbf{A}^{(1)}$ by inserting factored identity matrix and/or by matrix transpose.

Due to 2.3 the structure of the generating factors $\mathbf{A}^{(i)}$ may be presented in a very simple form as a block diagonal matrix with $N_{1,i-1}$ identical blocks $\vec{\mathbf{A}}_i$ along the diagonal, i.e. $\mathbf{A}^{(i)} = \operatorname{diag}(\vec{\mathbf{A}}_i, \vec{\mathbf{A}}_i, \dots, \vec{\mathbf{A}}_i)$ where $\vec{\mathbf{A}}_m = \mathbf{A}_m$ and for $i \in [1 : m-1]$ each $\vec{\mathbf{A}}_i = (\vec{\mathbf{A}}_i^{n_i,k_i}) \in \mathscr{M}(N_iK_{i+1,m} \times K_{i,m})$ is a matrix with $N_i \times K_i$ diagonal blocks $\vec{\mathbf{A}}_i^{n_i,k_i} = \operatorname{diag}(A_i(n_i, [k_i, 0]), A_i(n_i, [k_i, 1]), \dots, A_i(n_i, [k_i, K_{i+1,m}-1])) \in \mathscr{M}(K_{i+1,m} \times K_{i+1,m})$.

We shall now derive an important FMRT by inserting identity matrices factored by the permutation of the digit reversal (see 1.9). The resulting factorization attains a more compact form if it is applied rather to the modified matrices $\mathbf{A}^- = \mathbf{S}_{\mathscr{N}}\mathbf{A}\mathbf{S}_{\mathscr{K}}^T$ and $\mathbf{B}^- = \mathbf{S}_{\mathscr{N}}\mathbf{B}\mathbf{S}_{\mathscr{K}}^T$ obtained by writing rows and columns of **A** and **B** in digit-reversed order than for the **A** and **B** themselves. That is why the linear transform defined by $\mathbf{A}^-$ or $\mathbf{B}^-$ will be termed *digit-reversed* MRT (DRMRT) and the corresponding fast algorithm *fast digit-reversed* MRT (FDRMRT).

2.10 Theorem. *Fast digit-reversed* MRT.

Let $\mathbf{A}^- = \mathbf{S}_{\mathscr{N}}\mathbf{A}\mathbf{S}_{\mathscr{K}}^T$ *and* $\mathbf{B}^- = \mathbf{S}_{\mathscr{N}}\mathbf{B}\mathbf{S}_{\mathscr{K}}^T$ *where* $\mathscr{N} = (N_1, \dots, N_m)$, $\mathscr{K} = (K_1, \dots, K_m)$ *and* **A** *and* **B** *are* MRT *matrices defined in 2.7. Then the following factorizations,* called fast digit-reversed MRTs, *are true*: $\mathbf{A}^- = \mathbf{A}^{-(m)}\mathbf{A}^{-(m-1)} \dots \mathbf{A}^{-(1)}$ *and* $\mathbf{B}^- = \mathbf{B}^{-(1)}\mathbf{B}^{-(2)} \dots \mathbf{B}^{-(m)}$, *where* $\mathbf{A}^{-(i)} = \operatorname{diag}(\mathbf{A}_{i,\alpha_i(0)}, \mathbf{A}_{i,\alpha_i(1)}, \dots, \dots, \mathbf{A}_{i,\alpha_i(K_{i+1,m}-1)}) \otimes \mathbf{I}_{N_{1,i-1}}$, $\mathbf{B}^{-(i)} = \operatorname{diag}(\mathbf{B}_{i,\beta_i(0)}, \mathbf{B}_{i,\beta_i(1)}, \dots, \mathbf{B}_{i,\beta_i(N_{i+1,m}-1)}) \otimes \otimes \mathbf{I}_{K_{1,i-1}}$ for $i \in [1 : m-1]$, $\mathbf{A}^{-(m)} = \mathbf{A}_m \otimes I_{N_{1,m-1}}$ *and* $\mathbf{B}^{-(m)} = \mathbf{B}_m \otimes \mathbf{I}_{K_{1,m-1}}$. $\mathbf{A}_{i,k}$ $(\mathbf{B}_{i,n})$ *are matrices of size* $N_i \times K_i$ *associated with* $\mathbf{A}_i$ $(\mathbf{B}_i)$ *according to lemma* 2.3, *but arranged along the diagonal in digit-reversed order by* $\alpha_i^T = \varphi_{\mathscr{K}_{i+1,m}}(s_{i+1,m})$ $(\beta_i^T = \varphi_{\mathscr{N}_{i+1,m}}(s_{i+1,m}))$. *For* $i = m - 1$ *this ordering is natural because* α_{m-1} and β_{m-1} *are identical permutations.*

Proof. As the factorization of $\mathbf{B}^-$ is easy to be derived by that of $\mathbf{A}^-$ in view of the duality principle, we shall be concerned with $\mathbf{A}^-$ only. We can write by theorem 2.9 $\mathbf{A}^- = \mathbf{S}_{\mathscr{N}}\mathbf{A}\mathbf{S}_{\mathscr{K}}^T = \mathbf{A}^{-(m)}\mathbf{A}^{-(m-1)} \dots \mathbf{A}^{-(1)}$ where $\mathbf{A}^{-(i)} = \mathbf{S}^{(i+1)}\mathbf{A}^{(i)}\mathbf{S}^{(i)T}$ and $\mathbf{S}^{(i)} = \varphi_{\mathscr{N}^{(i)}}(s)$ is the digit reversal with respect to $\mathscr{N}^{(i)} = (N_1, \dots, N_{i-1}, K_i, \dots, K_m)$ for each $i \in [1 : m + 1]$. $\mathbf{A}^{-(m)} = \mathbf{S}^{(m+1)}(\mathbf{I}_{N_{1,m-1}} \otimes \mathbf{A}_m)\, \mathbf{S}^{(m)T} = \mathbf{A}_m \otimes \mathbf{I}_{N_{1,m-1}}$ by 1.8. Let $i \in [1 : m - 1]$ be arbitrary and let us denote $\mathscr{N}_i = \mathscr{N}_{i,m}^{(i)} = (K_i, \dots, K_m)$, $\mathscr{N}_i' = \mathscr{N}_{i,m}^{(i+1)} = (N_i, K_{i+1}, \dots, K_m)$ and $\mathbf{S}_i = \varphi_{\mathscr{N}_i}(s_{i,m})$, $\mathbf{S}_i' = \varphi_{\mathscr{N}_i'}(s_{i,m})$ the associated permutations. First we shall prove that $\mathbf{A}^{-(i)} = \mathbf{S}_i'(\mathbf{A}_i \otimes_R \mathbf{I}_{K_{i+1,m}})\, \mathbf{S}_i^T \otimes \mathbf{I}_{N_{1,i-1}}$. For $i = 1$ this is evident because $\mathbf{A}^{-(1)} = \mathbf{S}^{(2)}(\mathbf{A}_1 \otimes_R \mathbf{I}_{K_{2,m}})\, \mathbf{S}^{(1)T}$ and $\mathbf{S}^{(2)} = \mathbf{S}_1'$ and $\mathbf{S}^{(1)} = \mathbf{S}_1$. For $i > 1$ one can split $\mathbf{S}^{(i+1)}$ and $\mathbf{S}^{(i)T}$ into two parts using 1.12, namely $\mathbf{S}^{(i+1)} = \mathbf{S}_{i-1}^{(i+1)}(\mathbf{S}_{1,i-1} \otimes \mathbf{S}_i')$ and $\mathbf{S}^{(i)T} = (\mathbf{S}_{1,i-1}^T \otimes \mathbf{S}_i^T)\, \mathbf{S}_{i-1}^{(i)T}$ where $\mathbf{S}_{i-1}^{(i)} = \varphi_{(N_{1,i-1}, K_{i,m})}(s)$, $\mathbf{S}_{i-1}^{(i+1)} = \varphi_{(N_{1,i-1}, N_i K_{i+1,m})}(s)$ and $\mathbf{S}_{1,i-1} = \varphi_{\mathscr{N}_{1,i-1}}(s_{1,i-1})$. Hence $\mathbf{A}^{-(i)} = \mathbf{S}_{i-1}^{(i+1)}(\mathbf{S}_{1,i-1} \otimes \mathbf{S}_i')\,(\mathbf{I}_{N_{1,i-1}} \otimes (\mathbf{A}_i \otimes_R \mathbf{I}_{K_{i+1,m}}))\,(\mathbf{S}_{1,i-1}^T \otimes \mathbf{S}_i^T)\, \mathbf{S}_{i-1}^{(i)T} = \mathbf{S}_{i-1}^{(i+1)} \cdot (\mathbf{S}_{1,i-1}\mathbf{S}_{1,i-1}^T \otimes \mathbf{S}_i'(\mathbf{A}_i \otimes_R \mathbf{I}_{K_{i+1,m}})\, \mathbf{S}_i^T)\, \mathbf{S}_{i-1}^{(i)T} = \mathbf{S}_i'(\mathbf{A}_i \otimes_R \mathbf{I}_{K_{i+1,m}})\, \mathbf{S}_i^T \otimes \mathbf{I}_{N_{1,i-1}}$ by 1.8. It remains to verify $\mathbf{S}_i'(\mathbf{A}_i \otimes_R \mathbf{I}_{K_{i+1,m}})\, \mathbf{S}_i^T = \operatorname{diag}(\mathbf{A}_{i,\alpha_i(0)}, \dots, \mathbf{A}_{i,\alpha_i(K_{i+1,m}-1)})$. $\mathbf{S}_i'$ and $\mathbf{S}_i^T$ may be split using 1.12 once more: $\mathbf{S}_i' = (\boldsymbol{\alpha}_i^T \otimes \mathbf{I}_{N_i})\, \tilde{\mathbf{S}}_i'$ and $\mathbf{S}_i^T = \tilde{\mathbf{S}}_i^T(\boldsymbol{\alpha}_i \otimes \mathbf{I}_{K_i})$ where $\tilde{\mathbf{S}}_i' = \varphi_{(N_i, K_{i+1,m})}(s)$ and $\tilde{\mathbf{S}}_i = \varphi_{(K_i, K_{i+1,m})}(s)$. Hence by 2.3 $(\boldsymbol{\alpha}_i^T \otimes \mathbf{I}_{N_i})\, \tilde{\mathbf{S}}_i'(\mathbf{A}_i \otimes_R \mathbf{I}_{K_{i+1,m}})\, \tilde{\mathbf{S}}_i^T(\boldsymbol{\alpha}_i \otimes \mathbf{I}_{K_i}) = (\boldsymbol{\alpha}_i^T \otimes \mathbf{I}_{N_i})\, \operatorname{diag}(\mathbf{A}_{i,0}, \mathbf{A}_{i,1}, \dots, \mathbf{A}_{i,K_{i+1,m}-1})\,(\boldsymbol{\alpha}_i \otimes \mathbf{I}_{K_i}) = \operatorname{diag}(\mathbf{A}_{i,\alpha_i(0)}, \dots, \mathbf{A}_{i,\alpha_i(K_{i+1,m}-1)})$. ∎

2.11 Corollary. *If* $\mathscr{N} = \mathscr{K}$ *then*

$$|\mathbf{A}| = |\mathbf{A}^-| = \prod_{i=1}^{m} (|\mathbf{A}_{i,0}|\, |\mathbf{A}_{i,1}| \dots |\mathbf{A}_{i,N_{i+1,m}-1}|)^{N_{1,i-1}}, \qquad \mathbf{A}_{m,0} = \mathbf{A}_m$$

and

$$|\mathbf{B}| = |\mathbf{B}^-| = \prod_{i=1}^{m} (|\mathbf{B}_{i,0}|\, |\mathbf{B}_{i,1}| \dots |\mathbf{B}_{i,N_{i+1,m}-1}|)^{N_{1,i-1}}, \qquad \mathbf{B}_{m,0} = \mathbf{B}_m .$$

In particular $\mathbf{A}$ $(\mathbf{B})$ *is invertible iff* $\mathbf{A}_{i,n}$ $(\mathbf{B}_{i,n})$ *are invertible for each* $i \in [1 : m]$ *and* $n \in \mathbf{Z}_{N_{i+1,m}}$.

Proof. $\mathscr{N} = \mathscr{K}$ and $|\mathbf{S}|\, |\mathbf{S}^T| = 1 \Rightarrow |\mathbf{A}| = |\mathbf{S}|\, |\mathbf{A}|\, |\mathbf{S}^T| = |\mathbf{A}^-| = \prod_{i=1}^{m} |\mathbf{A}^{-(i)}|$ where $|\mathbf{A}^{-(i)}| = (|\mathbf{A}_{i,\alpha_i(0)}|\, |\mathbf{A}_{i,\alpha_i(1)}| \dots |\mathbf{A}_{i,\alpha_i(N_{i+1,m}-1)}|)^{N_{1,i-1}} = (|\mathbf{A}_{i,0}|\, |\mathbf{A}_{i,1}| \dots |\mathbf{A}_{i,N_{i+1,m}-1}|)^{N_{1,i-1}}$. The same holds for $|\mathbf{B}|$. Finally, a square matrix over a commutative ring $\mathbf{R}$ with unity is invertible iff its determinant is an invertible element in $\mathbf{R}$. ∎

2.12 Corollary. *Let* $\mathcal{N} = \mathcal{K}$ *and* **A** (**B**) *be an invertible* MRT *matrix. Then* $\mathbf{A}^{-1}$ ($\mathbf{B}^{-1}$) *is an* MRT *matrix uniquely determined by* $\mathbf{A}^{-1} = \mathbf{A}_1^* \otimes_L \mathbf{A}_2^* \otimes_L \ldots \otimes_L \otimes_L \mathbf{A}_m^*$ ($\mathbf{B}^{-1} = \mathbf{B}_1^* \otimes_R \mathbf{B}_2^* \otimes_R \ldots \otimes_R \mathbf{B}_m^*$) *where* $A_i^*([n_i, \ldots, n_m], n_i') = A^{-1}_{i,[n_{i+1},\ldots,n_m]}(n_i, n_i')$ ($\mathbf{B}_i^*(n_i', [n_i, \ldots, n_m]) = \mathbf{B}^{-1}_{i,[n_{i+1},\ldots,n_m]}(n_i', n_i)$) for $i \in [1 : m-1]$ *and* $\mathbf{A}_m^* = \mathbf{A}_m^{-1}$ ($\mathbf{B}_m^* = \mathbf{B}_m^{-1}$).

Proof. Let $\mathbf{A}^* = \mathbf{A}_1^* \otimes_L \mathbf{A}_2^* \otimes_L \ldots \otimes_L \mathbf{A}_m^*$. As $\mathbf{A}_{i,n}^* = \mathbf{A}_{i,n}^{-1}$ for each $i \in [1 : m]$ and $n \in \mathbf{Z}_{N_{i+1,m}}$ ($\mathbf{A}_{m,0}^* = \mathbf{A}_m^*$ and $\mathbf{A}_{m,0} = \mathbf{A}_m$), we have $\mathbf{A}^{-(i)}\mathbf{A}^{*-(i)} = \mathbf{I}_N$ for each $i \in [1:m]$, which means that $\mathbf{A}^-\mathbf{A}^{*-} = \mathbf{I}_N$. Consequently $\mathbf{AA}^* = \mathbf{S}^T\mathbf{A}^-\mathbf{SS}^T\mathbf{A}^{*-}\mathbf{S} = \mathbf{S}^T\mathbf{A}^-\mathbf{A}^{*-}\mathbf{S} = \mathbf{S}^T\mathbf{S} = \mathbf{I}_N$. $\mathbf{A}^*\mathbf{A} = \mathbf{I}_N$ follows analogically. The same argumentation may be applied to **B**. ∎

2.13 Remark. As $\otimes$ is a special case of both $\otimes_R$ and $\otimes_L$ in the sense of 2.2, lemma 1.8 suggests with $\mathbf{P}_{\mathcal{N}} = \mathbf{S}_{\mathcal{N}}$ and $\mathbf{P}_{\mathcal{K}} = \mathbf{S}_{\mathcal{K}}$ another definition of the so called *digit-reversed generalized Kronecker product* $\otimes_{R^-}$ or $\otimes_{L^-}$, namely by $\mathbf{S}_{\mathcal{N}}\mathbf{AS}_{\mathcal{K}}^T = \mathbf{A}^-$ where $\mathbf{A} = \mathbf{A}_1 \otimes_R \ldots \otimes_R \mathbf{A}_m$ and $\mathbf{A}^- = \mathbf{A}_m^- \otimes_{R^-} \ldots \otimes_{R^-} \mathbf{A}_1^-$ or by $\mathbf{S}_{\mathcal{N}}\mathbf{BS}_{\mathcal{K}}^T = \mathbf{B}^-$ where $\mathbf{B} = \mathbf{B}_1 \otimes_L \ldots \otimes_L \mathbf{B}_m$ and $\mathbf{B}^- = \mathbf{B}_m^- \otimes_{L^-} \ldots \otimes_{L^-} \mathbf{B}_1^-$. Accepting the symmetrically reversed number systems $\mathcal{N}$s and $\mathcal{K}$s as the basic ones, we can adopt $A^-([n_m, \ldots, n_1], [k_m, \ldots, k_1]) = A_m^-(n_m, k_m)\, A_{m-1}^-(n_{m-1}, [k_m, k_{m-1}]) \ldots A_1^-(n_1, [k_m, \ldots, k_1])$ and $B^-([n_m, \ldots, n_1], [k_m, \ldots, k_1]) = B_m^-(n_m, k_m)\, B_{m-1}^-([n_m, n_{m-1}], k_{m-1}) \ldots B_1^-([n_m, \ldots, n_1], k_1)$ as the defining relations for $\otimes_{R^-}$ and $\otimes_{L^-}$, respectively (cf. 2.8).

The following relations between $\otimes_R$ and $\otimes_{R^-}$ ($\otimes_L$ and $\otimes_{L^-}$), or more precisely between **A** and $\mathbf{A}^-$ (**B** and $\mathbf{B}^-$), are easy to establish:

(1) $\mathbf{A}_i^-$($\mathbf{B}_i^-$) is obtained by writing columns (rows) of $\mathbf{A}_i$ ($\mathbf{B}_i$) in digit-reversed order, i.e. $\mathbf{A}_i^- = \mathbf{A}_i\mathbf{S}_{\mathcal{K}_{i,m}}^T$ ($\mathbf{B}_i^- = \mathbf{S}_{\mathcal{N}_{i,m}}\mathbf{B}_i$); specifically for $i = m$ we get $\mathbf{A}_m^- = \mathbf{A}_m$ ($\mathbf{B}_m^- = \mathbf{B}_m$).

(2) Let $i \in [1:m-1]$. Then $\mathbf{A}_{i,k}^- = \mathbf{A}_{i,\alpha_i(k)}$, $k \in \mathbf{Z}_{K_{i+1,m}}$ and $\mathbf{B}_{i,n}^- = \mathbf{B}_{i,\beta_i(n)}$, $n \in \mathbf{Z}_{N_{i+1,m}}$ where α_i and β_i have been defined in 2.10, and $A_{i,[k_m,\ldots,k_{i+1}]}^-(n_i, k_i) = A_i^-(n_i, [k_m, \ldots, k_i])$ and $B_{i,[n_m,\ldots,n_{i+1}]}^-(n_i, k_i) = B_i^-([n_m, \ldots, n_i], k_i)$.

(3) Let $i \in [1 : m-1]$. Then the matrices $\mathbf{A}_i$ ($\mathbf{B}_i$) arise from the family of matrices $\{\mathbf{A}_{i,k}\}_{k\in\mathbf{Z}_{K_{i+1,m}}}$ ($\{\mathbf{B}_{i,n}\}_{n\in\mathbf{Z}_{N_{i+1,m}}}$) by grouping all columns (rows) with the same position in each $\mathbf{A}_{i,k}$ ($\mathbf{B}_{i,n}$) into blocks, more precisely $\mathbf{A}_i = (\mathbf{A}_{i,0}, \mathbf{A}_{i,1}, \ldots \mathbf{A}_{i,K_{i+1,m}-1})\, \mathbf{S}_{(K_i, K_{i+1,m})}$ ($\mathbf{B}_i = \mathbf{S}^T_{(N_i, N_{i+1,m})}(\mathbf{B}_{i,0}, \mathbf{B}_{i,1}, \ldots, \mathbf{B}_{i,N_{i+1,m}-1})^{BT}$ where ^{BT} stands for transposition of whole blocks).

On the other hand, the matrices $\mathbf{A}_i^-$ ($\mathbf{B}_i^-$) are obtained from $\{\mathbf{A}_{i,k}^-\}_{k\in\mathbf{Z}_{K_{i+1,m}}}$ ($\{\mathbf{B}_{i,n}^-\}_{n\in\mathbf{Z}_{N_{i+1,m}}}$) by placing all $\mathbf{A}_{i,k}^-$ ($\mathbf{B}_{i,n}^-$) side by side into one row (column), more precisely $\mathbf{A}_i^- = (\mathbf{A}_{i,0}^-, \ldots, \mathbf{A}_{i,K_{i+1,m}-1}^-)$ ($\mathbf{B}_i^- = (\mathbf{B}_{i,0}^-, \ldots, \mathbf{B}_{i,N_{i+1,m}-1}^-)^{BT}$).

(4) Following the analogy of (2.4) and (2.5), we have for $m = 2$: $\mathbf{A}^- = (\mathbf{A}^{-n_2,k_2})$.

and $\mathbf{B}^- = (\mathbf{B}^{-n_2,k_2})$ where $\mathbf{A}^{-n_2,k_2} = A_2(n_2, k_2)\,\mathbf{A}^-_{1,k_2}$ and $\mathbf{B}^{-n_2,k_2} = B_2(n_2, k_2)\,.$ $.\,\mathbf{B}^-_{1,n_2}$, which may serve as the starting-point motivation for the definition of $\otimes_{R^-}$ and $\otimes_{L^-}$, similarly as (2.4) and (2.5) did for $\otimes_R$ and $\otimes_L$.

From (4) we get immediately $\mathbf{I}_{K_2} \otimes_{R^-} \mathbf{A}^-_1 = \operatorname{diag}(\mathbf{A}^-_{1,0}, \ldots, \mathbf{A}^-_{1,K_2-1})$ and $\mathbf{I}_{N_2} \otimes$ $\otimes_{L^-} \mathbf{B}^-_1 = \operatorname{diag}(\mathbf{B}^-_{1,0}, \ldots, \mathbf{B}^-_{1,N_2-1})$ as an analogy of 2.3. Thus $\otimes_{R^-}$ and $\otimes_{L^-}$ provide an algebraic method of forming block diagonal matrices with generally different blocks of equal sizes along the diagonal, which is a natural extension of $\mathbf{I}_{K_2} \otimes \mathbf{A}_1(\mathbf{I}_{N_2} \otimes \mathbf{B}_1)$ where all blocks $\mathbf{A}^-_{1,k_2}(\mathbf{B}^-_{1,n_2})$ are equal to $\mathbf{A}_1(\mathbf{B}_1)$. Using this and (2) it is easy to rewrite $\mathbf{A}^{-(i)}$ and $\mathbf{B}^{-(i)}$ of the FDRMRT from 2.10 in terms of $\otimes_{R^-}$ and $\otimes_{L^-}$ as follows: $\mathbf{A}^{-(i)} = (\mathbf{I}_{K_{i+1,m}} \otimes_{R^-} \mathbf{A}^-_i) \otimes \mathbf{I}_{N_{1,i-1}}$, $\mathbf{B}^{-(i)} =$ $= (\mathbf{I}_{N_{i+1,m}} \otimes_{L^-} \mathbf{B}^-_i) \otimes \mathbf{I}_{K_{1,i-1}}$ for $i \in [1 : m - 1]$ and $\mathbf{A}^{-(m)} = \mathbf{A}^-_m \otimes \mathbf{I}_{N_{1,m-1}}$, $\mathbf{B}^{-(m)} = \mathbf{B}^-_m \otimes \mathbf{I}_{K_{1,m-1}}$ in view of (1).

It is easy to establish properties of $\otimes_{R^-}$ and $\otimes_{L^-}$ analogical to those stated by 2.4–2.6, 2.11, 2.12 for $\otimes_R$ and $\otimes_L$, either applying the relations (1)–(2) directly or paraphrasing the appropriate proofs.

In the sense of lemma 1.8 $\otimes_R$, $\otimes_L$ and $\otimes_{R^-}$, $\otimes_{L^-}$ may be viewed as operations associated with $1 \in \mathscr{P}([1 : m])$ and $s \in \mathscr{P}([1 : m])$, respectively. In general of course one can associate an operation $\otimes_{R_p}$ or $\otimes_{L_p}$ with any permutation $p \in \mathscr{P}([1 : m])$ by the formula $\mathbf{P}_{\mathscr{N}}\mathbf{A}\mathbf{P}^T_{\mathscr{K}} = \mathbf{A}^p = \mathbf{A}^p_{p(1)} \otimes_{R_p} \cdots \otimes_{R_p} \mathbf{A}^p_{p(m)}$ or $\mathbf{P}_{\mathscr{N}}\mathbf{B}\mathbf{P}^T_{\mathscr{K}} = \mathbf{B}^p =$ $= \mathbf{B}^p_{p(1)} \otimes_{L_p} \cdots \otimes_{L_p} \mathbf{B}^p_{p(m)}$ and derive a fast algorithm by inserting identity matrices factored by means of $\mathbf{P}^{(i)} = \varphi_{\mathscr{N}^{(i)}}(p)$ so as this was done in the proof of 2.10 with $\mathbf{P}^{(i)} = \mathbf{S}^{(i)}$. But for most permutations p a complex structure of the resulting factors $\mathbf{A}^{p(m)}$ or $\mathbf{B}^{p(m)}$ is to be expected, which makes the appropriate $\otimes_{R_p}$ and $\otimes_{L_p}$ less attractive for practical applications. Let us observe that it was exactly the property 1.12 of the digit reversal that has brought about the neat form of the factors.

2.14 Remark. *Multidimensional* MRT.

$\mathbf{A}' = \mathbf{A}'_1 \otimes \mathbf{A}'_2 \otimes \ldots \otimes \mathbf{A}'_r$ is said to be a matrix of an *r-dimensional* MRT ($r \geqq 2$) if each $\mathbf{A}'_j \in \mathscr{M}(N'_j \times K'_j)$ is an MRT matrix. Clearly $\mathbf{A}' = \mathbf{A}'^{(r)}\mathbf{A}'^{(r-1)} \ldots$ $\ldots \mathbf{A}'^{(1)}$ where $\mathbf{A}'^{(j)} = \mathbf{I}_{N'_{1,j-1}} \otimes \mathbf{A}'_j \otimes \mathbf{I}_{K'_{j+1,r}}$, $j \in [1 : r]$. Each $\mathbf{A}'^{(j)}$ may be again decomposed according to 2.9: Assume $N'_j = N_1 \ldots N_m$, $K'_j = K_1 \ldots K_m$ and $\mathbf{A}'_j =$ $= \mathbf{A}_1 \otimes_R \cdots \otimes_R \mathbf{A}_m$, $\mathbf{A}_i \in \mathscr{M}(N_i \times K_{i,m})$ for a fixed j. Then $\mathbf{A}'^{(j)} = \mathbf{I}_{N'_{1,j-1}} \otimes$ $\otimes \mathbf{A}^{(m)} \ldots \mathbf{A}^{(1)} \otimes \mathbf{I}_{K'_{j+1,r}} = \mathbf{A}^{(m)}_j \ldots \mathbf{A}^{(1)}_j$ where $\mathbf{A}^{(i)}_j = \mathbf{I}_{N'_{1,j-1}N_{1,i-1}} \otimes (\mathbf{A}_i \otimes_R$ $\otimes_R \mathbf{I}_{K_{i+1,m}}) \otimes \mathbf{I}_{K'_{j+1,r}}$ is one step of the final fast r-dimensional MRT. In view of 2.3 we can write also $\mathbf{A}^{(i)}_j = \mathbf{I}_{N'_{1,j-1}N_{1,i-1}} \otimes (\tilde{\mathbf{A}}_i \otimes_R \mathbf{I}_{K_{i+1,m}K'_{j+1,r}})$ where $\tilde{\mathbf{A}}_i \in$ $\in \mathscr{M}(N_i \times K_{i,m}K'_{j+1,r})$ is obtained from $\mathbf{A}_i$ repeating $K'_{j+1,r}$-times the entry of each column in $\mathbf{A}_i$. In this way steps of fast multidimensional MRT have the same structure as those of fast one-dimensional MRT. We can proceed similarly if $\mathbf{A}'_j = \mathbf{B}_1 \otimes_L \cdots \otimes_L \mathbf{B}_m$.

REFERENCES

[1] E. O. Brigham, *The Fast Fourier Transform.* Prentice—Hall, Englewood Cliffs, New Jersey, 1974.

[2] V. Čížek, *Diskrétní Fourierova transformace a její použití.* SNTL, Praha, 1981 (Czech).

[3] Eh. E. Dagman; G. A. Kukharev, *Bystrye diskretnye ortogonal'nye preobrazovaniya* (Fast Discrete Orthogonal Transformations). Izdatel'stvo „Nauka", Sibirskoe otdelenie, Novosibirsk, 1983 (Russian).

[4] D. F. Elliott; K. R. Rao, *Fast Transforms, Algorithms, Analyses, Applications.* Academic Press, New York, London, 1982.

[5] I. J. Good, *The Relationship Between Two Fast Fourier Transforms.* IEEE Trans. C-20 (1971), 310—317.

[6] P. Lancaster, *Theory of Matrices.* Academic Press, New York, London, 1969.

[7] H. J. Nussbaumer, *Fast Fourier Transform and Convolution Algorithms.* 2-nd ed., Springer-Verlag Berlin, Heidelberg, New York, 1982.

[8] V. A. Ponomarev; O. V. Ponomareva, *A Modification of Discrete Fourier Transform for Solution of Interpolation and Functional Convolution Problems.* Radiotekhn. i Elektron. 29 (1984), No. 8, 1561—1570 (Russian); translated as Radio Engrg. Electron. Phys. 29 (1984), No. 9, 79—88.

Vítězslav Veselý
Institute of Physical Metallurgy
Czechoslovak Academy of Sciences
616 62 Brno, Žižkova 22
Czechoslovakia