Kronecker Products and Shuffle Algebra

MARC DAVIO

Abstract—**The paper relates three classical concepts, viz. mixed radix number system, Kronecker product of matrices, and perfect shuffle. It presents an algebra which describes the hardware organization of the computation of a product $M\underline{v}$, where M is a matrix in Kronecker product form and $\underline{v}$ is a vector. The algebraic formalism describes both the blockwise structure of the computation and the various possible connection patterns.**

Index Terms—**Kronecker product of matrices, mixed radix number systems, perfect shuffle.**

I. Introduction

CELLULAR logic has, for a long time, attracted the attention of designers. In the recent past, arrays of logical operators showing up a regular connection pattern, such as arithmetic arrays, have raised up a renewed interest in the perspective of their implementation in LSI form.

The present paper addresses a class of circuits whose aim is to compute the transform $\underline{w} = M\underline{v}$ of a vector $\underline{v}$ by a matrix M when the latter has a Kronecker product (or direct product) structure. The interest of this structure is that it corresponds to a decomposition of the circuit computing $\underline{w}$: in many practical instances, the resulting circuit will consist of a regular interconnection of identical operators.

Such a situation is encountered in quite a number of application fields viz. Hadamard transform [1], discrete Fourier transform [2]-[6], connection and substitution networks [7]-[9], [20], canonical expansion of discrete functions [10], [11], $\cdots$. It is only possible to give here a small sample of the subject literature and we tried to select, among the relevant references, those whose formalism was the closest to the one we use here. For additional references, refer, for example, to [12] and [13].

It is interesting to recall here some of the milestones in the development of the underlying theory:

1) discovery of the constant geometry networks computing the Hadamard transform (1958, [2]),

2) quantitative estimation of the advantages obtained from the Kronecker product structure, both in hardware investment and in storage requirement (1963, [10]),

3) description of the fast Fourier transform (FFT) as a product of transformation and of permutation matrices (1968, [4]), and

4) arithmetic description of the perfect shuffle establishing its relation with the binary number system (1971, [8]).

Most often these results have been obtained in a specific context (say the discrete transform theory) and are little or not known in other possible application contexts (say permutation networks). The main result of the present paper is to establish a common background for all these problems; it is achieved thanks to three basic concepts: the mixed radix number representation systems, the Kronecker product of matrices, and the (generalized) perfect shuffle. While these concepts are classical, their tight relationships probably never have been clearly stated. This is the subject matter of Section II, which furthermore lays the basis of a shuffle algebra and establishes a set of relations describing commonly encountered connection patterns. Section III is devoted to the factorization of Kronecker products. It first presents a decomposition theorem, which extends to Kronecker products of arbitrary matrices a factorization of Kronecker powers of square matrices first described by Lechner [10]. It next uses the shuffle algebra to derive from the basic decomposition theorem a number of equivalent circuits. The interconnection patterns of the Cooley-Tukey [3] and of the Yates [14], Good [2] types appear as particular cases of the obtained circuits.

Manuscript received April 2, 1979; revised March 10, 1980 and September 10, 1980.

The author is with Philips Research Laboratory, Brussels, Belgium.

II. Basic Concepts

A. Mixed Radix Number Representation Systems

1) *Introductory example:* If we wish to convert into seconds a duration such as 3 days 7 h 22 min 4 s (written [3, 7, 22, 4]), we use the formula

$$3.86400 + 7.3600 + 22.60 + 4 = 285724.$$

The obtained number of seconds appear as a weighted sum of the duration [3, 7, 22, 4]. The weights are given by the vector [86400, 3600, 60, 1].

2) *Definition and representation theorem:* This familiar situation is imbedded in the concept of *mixed radix number representation system* that we now define formally.

Consider an integer valued vector

$$\underline{b} = [b_{n-1}, \cdots, b_1, b_0]; \qquad b_i \geq 2. \tag{1}$$

This vector is called *basis vector.* Build, from this vector a second vector

$$\underline{w} = [w_n, w_{n-1}, \cdots, w_1, w_0] \tag{2}$$

called *weight vector* and defined by

$$w_0 = 1; w_i = w_{i-1}b_{i-1} = \prod_{j=0}^{i-1} b_j; \qquad i \in \{1, 2, \cdots, n\}. \tag{3}$$

Theorem 1: Any integer A such that

$$0 \leq A < w_n \tag{4}$$

0018-9340/81/0200-0116$00.75

has a unique representation $[a_{n-1}, \cdots, a_1, a_0]$ *satisfying the two following conditions:*

$$1)\ A = \sum_{i=0}^{n-1} a_i w_i \tag{5}$$

$$2)\ 0 \leqslant a_i < b_i; \qquad \forall i \in \{0, 1, \cdots, n-1\}. \tag{6}$$

Theorem 1 is merely restated here for the sake of completeness and its proof will not be reproduced. It may be found in [15] or [16]. The vector $[a_{n-1}, \cdots, a_1, a_0]$ is the *mixed radix representation of A* with respect to the basis $[b_{n-1}, \cdots, b_1, b_0]$. If $b_0 = b_1 = \cdots = b_{n-1} = b$, the corresponding representation is called *radix b representation.* Outside of the present context, mixed radix representations are also used in residue arithmetic. See, for example, [17].

B. Kronecker Product of Matrices

1) *Introductory remarks:* The Hadamard transform $\underline{h}(\underline{v})$ of the vector $\underline{v} = [v_0, v_1, v_2, v_3]$ is the vector $[h_0, h_1, h_2, h_3]$ computed according to the familiar matrix product

$$\begin{bmatrix} h_0 \\ h_1 \\ h_2 \\ h_3 \end{bmatrix} = \left[\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ \hline 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{array}\right] \begin{bmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \end{bmatrix} \tag{7}$$

or, in short,

$$\underline{h} = H\underline{v}. \tag{8}$$

The computation of $\underline{h}$ from $\underline{v}$ according to (7) apparently requires four scalar products, each involving three additions. For vectors $\underline{v}$ having 2^n components, the computation of the Hadamard transform would require 2^n scalar products, each involving $2^n - 1$ additions.

The particular block structure of the transformation matrix, suggested by the dotted lines in (7), allows one to perform the computation according to a better suited algorithm, using no more than $n.2^{n-1}$ additions or subtractions. When programmed on a digital computer, the algorithm only requires 2^n cells of working storage [10].

The matrix structure taken to advantage in order to achieve the above improvements is that of Kronecker product of matrices. Basically, the *Kronecker product* $M \otimes N$ of the two matrices

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}; \qquad N = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

is given by

$$M \otimes N = \left[\begin{array}{cc|cc} aA & aB & bA & bB \\ aC & aD & bC & bD \\ \hline cA & cB & dA & dB \\ cC & cD & dC & dD \end{array}\right] \tag{9}$$

and the key point to the understanding of the new algorithm to compute $\underline{h}$ will rest upon the relationship between the Kronecker product and the usual product of matrices. That property will appear as Theorem 3 in the next section.

Observe that if M and N are two square $p \times p$ matrices, their storage will require $2p^2$ memory locations, while the storage of their Kronecker product would require p^4 double precision memory locations. Similarly, when computing the matrix product $\underline{h} = H\underline{v}$, we shall only perform smaller matrix products involving the Kronecker factors of H; these factors have the form

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

The addition and multiplication involved in the two considered types of matrix products (Kronecker and usual) are, in the case of the Hadamard transform, the addition and multiplication of real numbers. A similar situation is observed however in other contexts involving other additive and multiplicative laws. For example, if one expresses the canonical disjunctive expansion of a Boolean function in Kronecker product form, the underlying operations will be the Boolean sum and product. Similarly, the canonical ring sum expansions of Boolean functions, sometimes known as the Reed-Muller expansions [11], will be expressed by means of the modulo two sum and product. Finally, the computation of the discrete Fourier transform is expressed with the addition and multiplication of complex numbers. To cover these various situations, we shall present the definition and properties of the Kronecker product in terms of an abstract algebraic structure.

2) *Definition and properties of the Kronecker product:* Consider an algebraic system $\langle B, +, \cdot \rangle$ involving the set B and two operations, the addition $(+)$ and the multiplication ($\cdot$ or no symbol) satisfying the following axioms ($\forall x, y, z, \in B$).

1) (*associativity*) $x + (y + z) = (x + y) + z$; $x(yz) = (xy)z$.
2) (*commutativity*) $x + y = y + x$; $xy = yx$.
3) (*distributivity*) $x(y + z) = xy + xz$.
4) (*neutral elements*) $\exists 0, 1 \in B: 0 + x = x$; $1.x = x$.

Observe that our algebraic system could be a complete distributive lattice or a commutative ring with unit. A (r, c) *matrix* M over B is a set of rc elements of B disposed in r rows and c columns. The rows and columns of M are numbered from 0 to $(r - 1)$ and from 0 to $(c - 1)$, respectively. The matrix element belonging to row number i and to column number j is represented by $m(i, j)$. A (b, b)-matrix is a *square matrix* of order b. The axioms governing the algebraic system B allow one to define in the usual way the *addition of matrices* $(+)$ and the (*usual*) *product* $M_1 \cdot M_0$ or $M_1 M_0$ of an (r_1, c_1)-matrix M_1 by a (r_0, c_0)-matrix M_0. The addition of matrices is both associative and commutative. The product of matrices is associative and distributive over the addition. Furthermore, one may define the *unit matrix* of order b, 1_b by

$$1_b(i, j) = 1 \quad \text{iff } i = j \qquad = 0 \quad \text{iff } i \neq j \tag{10}$$

and check that for any (r, c)-matrix M

$$1_r \cdot M = M \cdot 1_c = M. \tag{11}$$

All these facts are elementary consequences of our axioms.

The *Kronecker product* $M_1 \otimes M_0$ of an (r_1, c_1)-matrix M_1 by an (r_0, c_0)-matrix M_0 is an $(r_1 r_0, c_1 c_0)$-matrix M defined by

$$m(i,j) = m_1(i_1, j_1)m_0(i_0, j_0);$$
$$i = i_1 r_0 + i_0; j = j_1 c_0 + j_0. \quad (12)$$

The row and column indexes of the Kronecker product M thus have the representations $[i_1, i_0]$ and $[j_1, j_0]$ in the mixed radix systems with basis vectors $[r_1, r_0]$ and $[c_1, c_0]$, respectively. The block structure of M is fairly apparent: i_1 and j_1 are the block coordinates, while i_0 and j_0 are the element coordinates within the (i_1, j_1)-block.

Consider as an example the Kronecker product $C = A \otimes B$ of a (2, 3)-matrix A by a (4, 2)-matrix B

$$A = \begin{bmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \end{bmatrix}; \quad B = \begin{bmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \\ b_{20} & b_{21} \\ b_{30} & b_{31} \end{bmatrix}. \quad (13)$$

C is thus the (8, 6)-matrix

$$C = \begin{bmatrix} c_{00} & c_{01} & c_{02} & c_{03} & c_{04} & c_{05} \\ c_{10} & c_{11} & c_{12} & c_{13} & c_{14} & c_{15} \\ c_{20} & c_{21} & c_{22} & c_{23} & c_{24} & c_{25} \\ c_{30} & c_{31} & c_{32} & c_{33} & c_{34} & c_{35} \\ c_{40} & c_{41} & c_{42} & c_{43} & c_{44} & c_{45} \\ c_{50} & c_{51} & c_{52} & c_{53} & c_{54} & c_{55} \\ c_{60} & c_{61} & c_{62} & c_{63} & c_{64} & c_{65} \\ c_{70} & c_{71} & c_{72} & c_{73} & c_{74} & c_{75} \end{bmatrix} = \left[\begin{array}{cc|cc|cc} a_{00}b_{00} & a_{00}b_{01} & a_{01}b_{00} & a_{01}b_{01} & a_{02}b_{00} & a_{02}b_{01} \\ a_{00}b_{10} & a_{00}b_{11} & a_{01}b_{10} & a_{01}b_{11} & a_{02}b_{10} & a_{02}b_{11} \\ a_{00}b_{20} & a_{00}b_{21} & a_{01}b_{20} & a_{01}b_{21} & a_{02}b_{20} & a_{02}b_{21} \\ a_{00}b_{30} & a_{00}b_{31} & a_{01}b_{30} & a_{01}b_{31} & a_{02}b_{30} & a_{02}b_{31} \\ \hline a_{10}b_{00} & a_{10}b_{01} & a_{11}b_{00} & a_{11}b_{01} & a_{12}b_{00} & a_{12}b_{01} \\ a_{10}b_{10} & a_{10}b_{11} & a_{11}b_{10} & a_{11}b_{11} & a_{12}b_{10} & a_{12}b_{11} \\ a_{10}b_{20} & a_{10}b_{21} & a_{11}b_{20} & a_{11}b_{21} & a_{12}b_{20} & a_{12}b_{21} \\ a_{10}b_{30} & a_{10}b_{31} & a_{11}b_{30} & a_{11}b_{31} & a_{12}b_{30} & a_{12}b_{31} \end{array}\right]$$

If, for example, we wish to express c_{74} as a product $a_{ij}b_{kl}$, we have to obtain the mixed radix representations of 7 and 4 with respect to the bases [2, 4] and [3, 2], respectively. Clearly,

$$7 = i.4 + k = 1.4 + 3; \qquad 4 = j2 + l = 2.2 + 0.$$

Hence, $i = 1, k = 3, j = 2, l = 0$, and $c_{74} = a_{12}b_{30}$.

The main properties of the Kronecker product of matrices are gathered in the following theorem.

Theorem 2: Consider the matrices M_2, M_1, M_0, N_1, N_0 over B. The following properties hold true whenever the corresponding operations are defined.

1) (Associativity of the Kronecker product):

$$M_2 \otimes (M_1 \otimes M_0) = (M_2 \otimes M_1) \otimes M_0. \quad (14)$$

2) (Distributivity of the Kronecker product with respect to the addition of matrices):

$$M_0 \otimes (N_1 + N_0) = (M_0 \otimes N_1) + (M_0 \otimes N_0) \quad (15)$$

$$(M_1 + M_0) \otimes N_0 = (M_1 \otimes N_0) + (M_0 \otimes N_0). \quad (16)$$

3) (Relationship between the ordinary and Kronecker products of matrices):

$$(M_1 \otimes M_0) \quad (N_1 \otimes N_0) = (M_1 N_1) \otimes (M_0 N_0). \quad (17)$$

4) If T *denotes transposition:*

$$(M_1 \otimes M_0)^T = M_1^T \otimes M_0^T. \quad (18)$$

5) *If M_1 and M_0 are invertible square matrices having the inverses M_1^{-1} and M_0^{-1}:*

$$(M_1 \otimes M_0)^{-1} = M_1^{-1} \otimes M_0^{-1}. \quad (19)$$

These properties are now classical and their proofs may be found in [11], [18]; they have been restated here for reference. The most important of these properties is probably contained in (17), which relates the ordinary and the Kronecker matrix products. That property contains the essence of the simplifying mechanism mentioned in Section II-B1. Basically, this mechanism may be described as follows: if, in the computation of the matrix product $\underline{\underline{w}} = M.\underline{\underline{v}}$, the transformation matrix M may be expressed as the Kronecker product $M_1 \otimes M_0$, then, it is possible to compute $\underline{\underline{w}}$ from independent transformations described by the matrices M_1 and M_0; (17), in fact, contains a decomposition process: the latter will be illustrated in Section III. Equation (17) may be extended in various ways that will be described in Theorem 3 below. Before stating this theorem, we need some additional notations.

The Kronecker product

$$M = M_{n-1} \otimes \cdots \otimes M_1 \otimes M_0 \quad (20)$$

is unambiguously written without parentheses by the associative law (14). From now on, we shall represent (20) by

$$M = \bigotimes_{k=n-1}^{0} M_k. \quad (21)$$

Let us represent by $m(i,j)$ and by $m(i_k, j_k)$ the (i,j) entry of M and the (i_k, j_k) entry of M_k. Let us furthermore assume that M_k is an (r_k, c_k)-matrix. It is then easy to show that

$$m(i,j) = \prod_{k=0}^{n-1} m_k(i_k, j_k) \quad (22)$$

where i and j have the unique representations $[i_{n-1}, \cdots, i_1, i_0]$ and $[j_{n-1}, \cdots, j_1, j_0]$ in the mixed radix systems with basis vectors $[r_{n-1}, \cdots, r_1, r_0]$ and $[c_{n-1}, \cdots, c_1, c_0]$, respectively.

Finally, the Kronecker product $M \otimes M \otimes \cdots \otimes M$ of n identical factors is called nth Kronecker power of M and is denoted by $M^{[n]}$. Observe that

$$1_{r^n} = 1_r^{[n]}. \quad (23)$$

We now turn to the extensions of Theorem 2 (3). These general relationships between the ordinary and Kronecker matrix products will play an important role in what follows.

Theorem 3: Whenever all the involved matrix products are defined, the following properties hold true:

$$1) \left(\bigotimes_{k=n-1}^{0} M_k\right) \cdot \left(\bigotimes_{k=n-1}^{0} N_k\right) = \bigotimes_{k=n-1}^{0} (M_k N_k) \quad (24)$$

$$2)\quad \left(\overset{0}{\underset{k=n-1}{\prod}} M_k\right) \otimes \left(\overset{0}{\underset{k=n-1}{\prod}} N_k\right) = \overset{0}{\underset{k=n-1}{\prod}} (M_k \otimes N_k) \qquad (25)$$

$$3)\quad \overset{0}{\underset{k=p-1}{\otimes}} \left(\overset{0}{\underset{l=n-1}{\prod}} M_{kl}\right) = \overset{0}{\underset{l=n-1}{\prod}} \left(\overset{0}{\underset{k=p-1}{\otimes}} M_{kl}\right). \qquad (26)$$

For the proof by recurrence of these properties, use (17) as the starting point. The property (24) is apparently the only published extension of (17). The other two properties will be used in Section III.

3) *Circuit diagram interpretation—Normal factors:* The transformation $\underline{\underline{w}} = M\underline{\underline{v}}$ is easily interpreted in circuit terms: an operator M seen as a black box acts upon an input vector $\underline{\underline{v}}$ to produce an output vector $\underline{\underline{w}}$. We shall prove in Section III that if the transformation matrix M may be expressed as a Kronecker product $\otimes M_k$, the unique operator M splits up in sets of smaller operators (black boxes) of the types M_k. Our purpose is to describe accurately this decomposition process and, in particular, the connection patterns relating the sets of operators M_k. In the present section, we shall discover a hint pointing to that decomposition. For this purpose, we consider two particular cases

$$\underline{\underline{w}} = (1_b \otimes M_0)\underline{\underline{v}} \quad \text{and} \quad \underline{\underline{w}} = (M_0 \otimes 1_b)\underline{\underline{v}}$$

of the general transformation $\underline{\underline{w}} = M\underline{\underline{v}}$. The circuit diagrams corresponding to these two transformations are exemplified in Fig. 1(a) and (b), respectively. We assumed $b = 3$ and M_0 a 2×2 matrix. In both cases, the components of the input and output vector are listed in lexicographic order.

It is now immediate to conclude that the transformation $(1_b \otimes M_0)$ is represented, in a circuit diagram, by a set of b copies of the operator M_0 simply laid side by side. On the other hand, the circuit diagram corresponding to $(M_0 \otimes 1_b)$ contains a similar arrangement of b copies of M_0, but the components of the input and output vector have now to undergo an appropriate permutation. In Section II-C, we shall describe these permutations as *perfect shuffles*. We shall only observe now that the Kronecker products of the type $(1_b \otimes M_0)$ have a particularly simple interpretation in terms of circuit diagrams. This is the reason why these Kronecker products are *normal factors*.

Consider now the transformation $\underline{\underline{w}} = M\underline{\underline{v}}$ and assume that the transformation matrix M is the ordinary product M_1M_0 of two matrices. In the corresponding circuit diagram, the overall transformation will be represented by the cascade connection of the operators M_0 and M_1. This is illustrated in Fig. 2. Observe, to avoid any confusion, that M_0 acts first on the input vector, while M_1, which appears as the leftmost factor in M_1M_0, only acts in a second transformation stage. Now we immediately deduce that a Kronecker product of the type $(M_0 \otimes 1_b)$ will admit an ordinary product representation: perfect shuffle · normal factor · perfect shuffle.

We conclude this section by relating the concepts of normal factor $(1_b \otimes M_0)$ and of mixed radix system. Assume that M_0 is an (r_0, c_0)-matrix. Then the inputs to the circuit (or equivalently the components of the transformed vector $\underline{\underline{v}}$) may be numbered in the mixed radix system with basis $[b, r_0]$. Similarly, the circuit outputs are numbered in the mixed radix system with basis $[b, c_0]$. The most significant digit of these

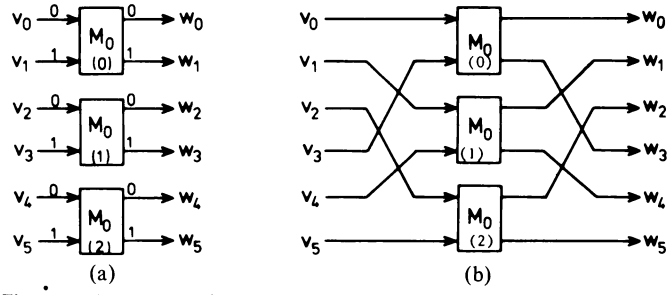


Fig. 1. The concept of normal factor. (a) $M = (1_3 \otimes M_0)$. (b) $M = M_0 \otimes 1_3)$.

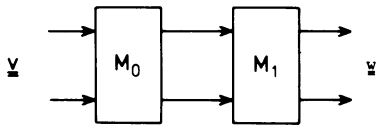


Fig. 2. The transformation $\underline{\underline{w}} = M_1M_0\underline{\underline{v}}$.

numberings identifies one of the copies of the operator M_0. Clearly then, for i fixed the outputs labeled $(i, 0), (i, 1), \cdots, (i, c_0 - 1)$ only depend on the inputs $(i, 0)(i, 1), \cdots, (i, r_0 - 1)$. Therefore, the decomposition described by the normal factor $(1_b \otimes M_0)$ has a simple interpretation in mixed radix terms.

C. Perfect Shuffles

1) *Introductory example:* Consider the problem of adding two 4-bit numbers $A = (a_3, a_2, a_1, a_0)$ and $B = (b_3, b_2, b_1, b_0)$ initially stored in two 4-bit registers R_0 and R_1 by means of a cascade of 4 full-adders. The corresponding circuit diagram is shown in Fig. 3. The register outputs, the full-adders, and the full-adders inputs have been systematically numbered as indicated in the figure. The retained numbering has an interesting property which allows one to describe accurately the connection pattern relating the registers and the full-adders: the ith output of register R_j is connected to the jth input of full-adder FA_i. This type of description is the essential feature that we wish to retain in our definition of the perfect shuffle.

2) *Definition and elementary properties:* Consider the set $L_m = \{0, 1, \cdots, m - 1\}$ and assume that

$$m = b_1b_0. \qquad (27)$$

The current element i may be represented in the mixed radix systems having the basis vectors $[b_1, b_0]$ and $[b_0, b_1]$. Let

$$i = i_1b_0 + i_0 = i_1^*b_1 + i_0^*;\ i_0, i_1^* \in \{0, 1, \cdots, b_0 - 1\};$$
$$i_1, i_0^* \in \{0, 1, \cdots, b_1 - 1\}. \qquad (28)$$

A (b_1, b_0)-*shuffle* on L_m is a permutation $\sigma(b_1, b_0)$ of L_m defined by

$$\sigma(b_1, b_0): i = i_1b_0 + i_0 \rightarrow j = i_0b_1 + i_1 \qquad (29)$$

where $j = i\sigma$ is the image of i. Thus, if i has the representation $[i_1, i_0]$, its image $j = i\sigma$ has the representation $[j_1^*, j_0^*] = [i_0, i_1]$. The elements of L_m may obviously be partitioned in two ways as follows.

π_1) : b_1 blocks of b_0 elements each. The element $i = [i_1, i_0]$ will appear as element number i_0 in block number i_1;

π_2) : b_0 blocks of b_1 elements each. The element $j = [j_1^*, j_0^*]$ will appear as element number j_0^* in block number j_1^*.

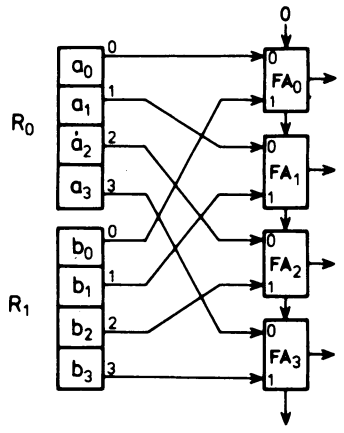


Fig. 3. Addition of two 4-bit numbers.

The definition of the perfect shuffle now simply states that the image of element i_0 of block i_1 in π_1 is the element i_1 of block i_0 in π_2. Fig. 4 illustrates a (3, 5)-shuffle. Similarly, the shuffle appearing in Fig. 3 is a (2, 4)-shuffle while the shuffles appearing in Fig. 1(b) are from left to right a (2, 3)-shuffle and a (3, 2)-shuffle. It is immediate to observe that

$$\sigma(b_1, b_0) = \sigma^{-1}(b_0, b_1). \tag{30}$$

The above definition may now be applied in the broader context of an arbitrary mixed radix system. Let

$$m = b_{n-1} \cdot \cdots \cdot b_1 \cdot b_0. \tag{31}$$

As in Section II-A, we shall represent by w_{n-1} the product $b_{n-2} \cdot \cdots \cdot b_1 \cdot b_0$. Consider now the mixed radix representation $[i_{n-1}, \cdots, i_1, i_0]$ of an integer i $(0 \leqslant i \leqslant m-1)$ with respect to the basis vector $[b_{n-1}, \cdots, b_1, b_0]$. Then,

Theorem 4: The mixed radix representation of $i\sigma(b_{n-1}, w_{n-1})$ *with respect to the basis vector* $[b_{n-2}, \cdots, b_1, b_0, b_{n-1}]$ *is* $[i_{n-2}, \cdots, i_1, i_0, i_{n-1}]$.

Proof: It suffices to observe that the mixed radix representation of i with respect to the basis vector $[b_{n-1}, w_{n-1}]$ is

$$\left[i_{n-1}, \sum_{k=0}^{n-2} i_k w_k\right].$$

Hence, the representation of $i\sigma(b_{n-1}, w_{n-1})$ with respect to the basis vector $[w_{n-1}, b_{n-1}]$ is

$$\left[\sum_{k=0}^{n-2} i_k w_k, i_{n-1}\right],$$

i.e.,

$$i\sigma(b_{n-1}, w_{n-1}) = \left(\sum_{k=0}^{n-2} i_k w_k\right) b_{n-1} + i_{n-1}.$$

Q.E.D.

Observe that the action of $\sigma(b_{n-1}, w_{n-1})$ operates a cyclic shift of one position to the left both on the mixed radix representation of i on the basis vector b. The property is clearly of particular interest when $m = b^n$ and when i is given by its radix b representation. In that situation [20], the radix b representation of $i\sigma(b, b^{n-1})$ and of $i\sigma(b^{n-1}, b)$ are deduced from the radix b representation of i by one position left and right cyclic shifts, respectively.

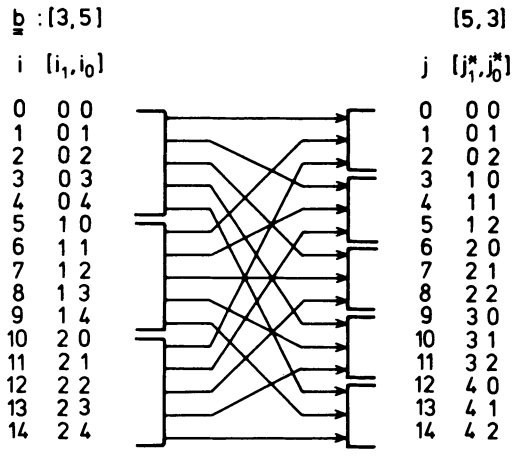


Fig. 4. A $\sigma(3, 5)$-shuffle.

3) *Matrix formulation:* Up to now, the shuffle has been defined as a permutation, i.e., as a mapping on sets. To keep consistent with our general discussion formalism, we now introduce a matrix representation of the shuffles. As any permutation, a (b_1, b_0)-shuffle may be represented by its adjacency matrix S_{b_1,b_0}. This matrix is a square matrix of order $b_1 b_0$ whose rows and columns are numbered from 0 to $b_1 b_0 - 1$. We denote by $S_{b_1,b_0}(j, i)$ the element of the matrix belonging to row j and column i. The adjacency matrix is then defined by

$$S_{b_1,b_0}(j, i) = 1 \quad \text{iff } j = i\sigma$$
$$S_{b_1,b_0}(j, i) = 0 \quad \text{otherwise.} \tag{32}$$

For example, the adjacency matrix $S_{3,5}$ associated to the (3, 5)-shuffle of Fig. 4 is given by

$$S_{3,5} = \begin{bmatrix} 1 & & & & & & & & & & & & & & \\ & & & 1 & & & & & & & & & & & \\ & & & & & & & & 1 & & & & & & \\ & 1 & & & & 1 & & & & & & & & & \\ & & & & & & & & & 1 & & & & & \\ & & 1 & & & & & & & & & & & & \\ & & & & 1 & & & & & & & & & & \\ & & & & & & & & & & 1 & & & & \\ & & & & & & & 1 & & & & & & & \\ & & & & & & & & & & & & 1 & & \\ & & & 1 & & & & & & & & & & & \\ & & & & & & 1 & & & & & & & & \\ & & & & & & & & & & & & & & 1 \end{bmatrix};$$

blank entries represent zeroes. Thus, in a transformation $\underline{\underline{w}} = S_{3,5}\underline{\underline{v}}$, one has, for instance, $w_6 = v_2$. As we already observed, to the mapping $\tau = \sigma_1\sigma_2 : i \to j = i\sigma_1\sigma_2$ is associated the matrix representation $\underline{\underline{w}} = S_2 \cdot S_1 \cdot \underline{\underline{v}}$: the factors S_2 and S_1 of the matrix product appear in reverse order as the permutation σ_1 is the first one to act on the element i. This should not cause any confusion.

Before discussing additional properties of the shuffles and of their adjacency matrices, we shall first interpret in terms of mixed radix systems some important permutation matrices which are built up from shuffle-matrices and Kronecker products. These matrices will play an important role in the sequel.

1) Consider first the permutation matrix

$$1_{b_2} \otimes S_{b_1,b_0} \tag{33}$$

acting on a set of $m = b_2 b_1 b_0$ points. It represents a set of b_2 independent (b_1, b_0)-shuffles acting separately inside blocks of $b_1 b_0$ points: this is a particular case of normal factor, as described in Section II-B3. Computing the (j, i)-entry of the matrix (33), one easily checks that if an input point i is given by its representation $[i_2, i_1, i_0]$ with respect to the basis $[b_2, b_1, b_0]$, it will be mapped onto the output point j represented as $[i_2, i_0, i_1]$ in the $[b_2, b_0, b_1]$ system. In particular, the matrix

$$1_b^{[n-k]} \otimes S_{b^{k-1},b} \tag{34}$$

operates a cyclic shift of one position to the right on the k less significant digits of the radix b representation of any domain point.

2) Similarly, in

$$S_{b_2,b_1} \otimes 1_{b_0} \tag{35}$$

$b_2 b_1$ blocks of b_0 points each are submitted to a shuffle of blocks, the position of the points within the blocks remaining unchanged by the transformation. In particular, the matrix

$$S_{b^{k-1},b} \otimes 1_b^{[n-k]}$$

operates a cyclic shift of one position to the right on the k most significant digits of the radix b representation of any domain point i. The matrices (33) and (35) are illustrated in the right-hand part of Fig. 5(b).

3) Consider finally the permutation matrix

$$1_b^{[n-k-1]} \otimes ((1_b \otimes S_{b,b^{k-1}}) \cdot S_{b^k,b}) \tag{37}$$

acting on the n digits of the radix b representation $[i_{n-1}, \cdots i_{k+1}, i_k, \cdots, i_1, i_0]$. The $(k+1)$ less significant digits first undergo a cyclic right shift due to $S_{b^k,b}$. The k less significant digits next undergo a cyclic left shift due to $S_{b,b^{k-1}}$. Clearly, the permutation described by (37) acts as the transposition of digits (i_k, i_0) in the radix b representation of i.

The interpretation in mixed radix terms of permutation matrices of the types (33), (35), and (37) illustrates an interesting proof methodology. A first application of this methodology will be found in the following Theorem 5 which presents two factorizations of shuffles.

Theorem 5:

$$1)\ S_{b_2,b_1b_0} = S_{b_2b_0,b_1} \cdot S_{b_2b_1,b_0} = S_{b_2b_1,b_0} \cdot S_{b_2b_0,b_1}. \tag{38}$$

$$2)\ S_{b_2b_1,b_0} = (S_{b_2,b_0} \otimes 1_{b_1})(1_{b_2} \otimes S_{b_1,b_0}). \tag{39}$$

Proof: Let $[i_2, i_1, i_0]$ be the representation of i with respect to the basis vector $[b_2, b_1, b_0]$. We study the transformations undergone by $[i_2, i_1, i_0]$ in the various operations. The bookkeeping of the basis vector is unnecessary since its evolution parallels that of $[i_2, i_1, i_0]$.

1) We only prove the first equality: the second equality is obtained by interchanging b_1 and b_0.

$$[i_2, i_1, i_0] \xrightarrow{S_{b_2,b_1b_0}} [i_1, i_0, i_2]$$

$$[i_2, i_1, i_0] \xrightarrow{S_{b_2b_1,b_0}} [i_0, i_2, i_1] \xrightarrow{S_{b_2b_0,b_1}} [i_1, i_0, i_2]$$

2) Similarly,

$$[i_2, i_1, i_0] d \xrightarrow{S_{b_2b_1,b_0}} [i_0, i_2, i_1]$$

$$[i_2, i_1, i_0] \xrightarrow{1_{b_2} \otimes S_{b_1,b_0}} [i_2, i_0, i_1] \xrightarrow{S_{b_2,b_0} \otimes 1_{b_1}} [i_0, i_2, i_1]$$

Q.E.D.

The interpretation of the above two properties is of interest. Property (38) states that it is possible to decompose a perfect shuffle acting on a small number of large size input blocks as a cascade of two shuffles acting on a large number of small size input blocks. Property (39) is even more striking since it decomposes the shuffle $S_{b_2b_1,b_0}$ into smaller shuffles S_{b_1,b_0} and S_{b_2,b_0}, the former acting inside small blocks and the latter acting as a shuffle of blocks. Those properties are illustrated in Fig. 5 for $b_2 = 2$, $b_1 = 2$, $b_0 = 3$.

4) *Kronecker products and perfect shuffles:* So far, we have studied the relationship existing between perfect shuffles and number representation systems and we used that relation to enrich our repertory of shuffle properties. We shall now ascertain the relation existing between Kronecker products and perfect shuffles. Such a relationship had been demonstrated informally in Section II-B3 in the study of $(M_0 \otimes 1_b)$ and motivated our study of shuffles. As the Kronecker product is not commutative, we first study the relationship existing between $M_1 \otimes M_0$ and $M_0 \otimes M_1$.

Theorem 6: If M_1 and M_0 are (r_1, c_1)- and (r_0, c_0)-matrices, respectively, then,

$$M_1 \otimes M_0 = S_{r_0,r_1} \cdot (M_0 \otimes M_1) \cdot S_{c_1,c_0}. \tag{40}$$

Proof: We compute the (i, j)-entry of the matrices in both members of (40). If $i = i_1 r_0 + i_0$ and $j = j_1 c_0 + j_0$, the (i, j)-entry of the left-hand member is $m_1(i_1, j_1) m_0(i_0, j_0)$. To perform the same computation in the right-hand member, we denote by P the matrix $M_0 \otimes M_1$. Then the (i, j)-entry of the right-hand member, represented by the sum

$$\sum_{k=0}^{r_0 r_1 - 1} \sum_{l=0}^{c_0 c_1 - 1} S_{r_0,r_1}(i, k) P(k, l) S_{c_1,c_0}(l, j) \tag{41}$$

reduces to a single term. Indeed, there is a single value of k, call it $\tilde{k}$, such that

$$S_{r_0 r_1}(i, \tilde{k}) = 1.$$

By (32), this particular k is given by $i = \tilde{k}\sigma(r_0, r_1)$, i.e., $\tilde{k} = i\sigma(r_1, r_0) = i_0 r_1 + i_1$. Similarly, there is a single value of l, call it $\tilde{l}$, such that

$$S_{c_1,c_0}(\tilde{l}, j) = 1.$$

Again, by (32) $\tilde{l} = j\sigma(c_1, c_0) = j_0 c_1 + j_1$. Finally, by (12) the only nonzero term $P(\tilde{k}, \tilde{l})$ in (41) is equal to $m_0(i_0, j_0) m_1(i_1, j_1)$.

Q.E.D.

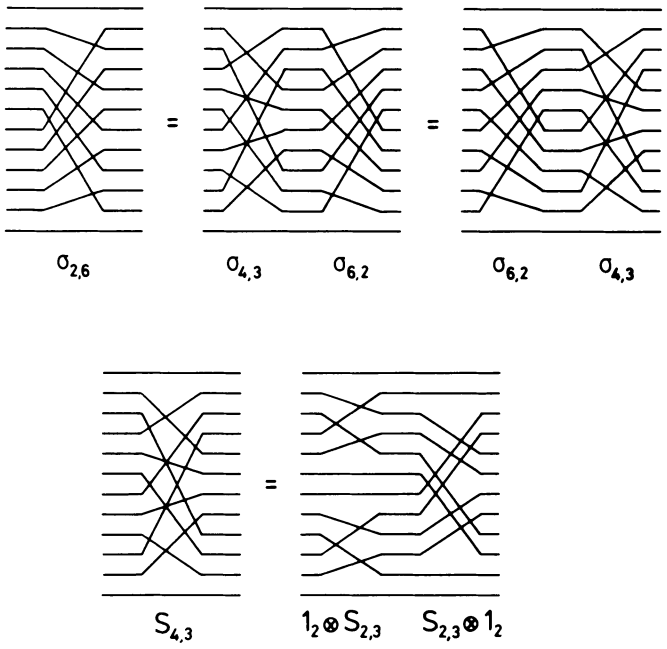


Fig. 5. Factorization of perfect shuffles (Theorem 5).

As an immediate consequence, we obtain the following.

Theorem 7: If M is an (r_1, c_1)-matrix

1) $$M \otimes 1_{b_0} = S_{b_0,r_1} \cdot (1_{b_0} \otimes M) \cdot S_{c_1,b_0} \quad (42)$$

2) $$1_{b_2} \otimes M \otimes 1_{b_0} = S_{b_0,b_2r_1} \cdot (1_{b_2b_0} \otimes M) \cdot S_{b_2c_1,b_0} \quad (43)$$

3) $$1_{b_2} \otimes M \otimes 1_{b_0} = (1_{b_2} \otimes S_{b_0,r_1})(1_{b_2b_0} \otimes M)(1_{b_2} \otimes S_{c_1,b_0}). \quad (44)$$

Proof: 1) is obtained from (40) by replacing in (40) M_0 by 1_{b_0}. 2) is obtained from (42) by replacing in (42) M by the (b_2r_1, b_2c_1)-matrix $(1_{b_2} \otimes M)$ and by using the obvious property $1_{b_2} \otimes 1_{b_0} = 1_{b_2b_0}$. 3) by (42), we also obtain

$$1_{b_2} \otimes (M \otimes 1_{b_0}) = 1_{b_2}^3 \otimes (S_{b_0,r_1} \cdot (1_{b_0} \otimes M) \cdot S_{c_1,b_0}).$$

The proof is then completed by using Theorem 3-2). Q.E.D.

The property (42) was in fact our starting hint already illustrated in Fig. 1. Observe also that the right-hand members of (43) and (44) only contain shuffles and normal factors as product factors. The consequence of this observation is that we now have accurate circuit descriptions of $1_{b_2} \otimes M \otimes 1_{b_0}$, including the input and output connection patterns. Essentially, we should remember that the transformation $1_{b_2} \otimes M \otimes 1_{b_0}$ may be viewed in circuit terms as a set of b_2b_0 operators performing the transformation M preceded and followed by perfect shuffles.

III. Factorization of Kronecker Products

A. Fundamental Factorization Theorem

In the present section, we consider the Kronecker product

$$M_{n-1} \otimes \cdots \otimes M_1 \otimes M_0 \quad (45)$$

of $n(r_i, c_i)$-matrices M_i. Our purpose is to represent the Kronecker product (45) as the ordinary matrix product of n factors of compatible sizes. In fact, the factorization Theorem 8 exhibits $n!$ such representations. Let χ represent a permutation of $\{0, 1, \cdots, n-1\}$. Then,

Theorem 8:

$$\bigotimes_{i=n-1}^{0} M_i = \prod_{\substack{j=n-1 \\ j=i\chi}}^{0} (1_{\alpha_{n-1}^i} \cdots \alpha_{i+1}^i \otimes M_i \otimes 1_{\alpha_{i-1}^i} \cdots \alpha_0^i) \quad (46)$$

where

$$\alpha_k^i = r_k \quad \text{if } i\chi > k\chi;\ \alpha_k^i = c_k \text{ if } i\chi < k\chi.$$

Comment: Let us first interpret (46). Observe that it replaces the Kronecker product (45) by an ordinary product of n factors having the form $1_b \otimes M_i \otimes 1_{b'}$; by Theorem 7 we shall be able to exhibit the corresponding normal factors and shuffles. Remember now the concluding comment of the preceding section: it shows that the transformation described by (45) and performed as indicated by the right-hand member of (46) may be viewed in circuit terms as the cascade connection of n stages; the jth stage only contains copies of the operator performing the transformation M_j. Appropriate permutations will relate the outputs of stage j to the inputs of stage $(j+1)$. The use of the permutation χ allows one to vary at will the order of the stages. That flexibility results of the relative independence of the factors in a Kronecker product. Indeed, the operators corresponding to the factor M_i in (45) act on sets of r_i elements having all their coordinates identical but the ith. The need for interposed shuffles is then justified by the fact that normal factors only act on the least significant coordinate: the shifting property of shuffles is used to bring in turn each of the n coordinates in the least significant position.

Proof: Start from the left-hand member of (46). Replace each Kronecker factor M_i by the equivalent ordinary matrix product of n factors

$$1_{r_i}^{n-1-i\chi} \cdot M_i \cdot 1_{c_i}^{i\chi} \quad (47)$$

in such a way that M_i appears in position $i\chi$ of that product (positions are numbered from right to left). The proof is then immediately completed by Theorem 3-3) and by the following observation: assume $k > i$; then, in (40), M_i will be multiplied on the left (in the Kronecker sense) by a factor $1_{\alpha_k^i}$. Clearly, this factor is 1_{r_k} if $k\chi < i\chi$ and 1_{c_k} in the opposite situation. A similar observation holds true if $k < i$. Q.E.D.

Examples: a) For $n = 2$, Theorem 8 yields the two factorizations

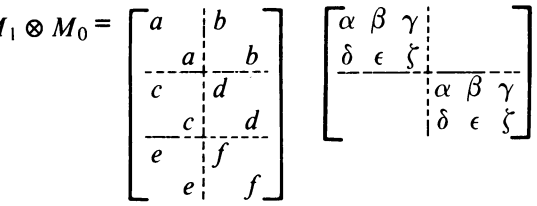
$$M_1 \otimes M_0 = (M_1 \otimes 1_{r_0})(1_{c_1} \otimes M_0) = (1_{r_1} \otimes M_0)(M_1 \otimes 1_{c_0}). \quad (48)$$

For example, if

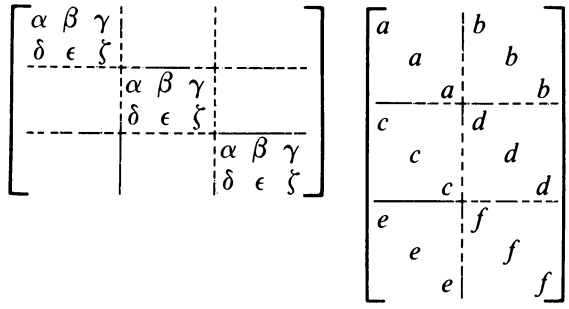
$$M_1 = \begin{bmatrix} a & b \\ c & d \\ e & f \end{bmatrix} \text{ and } M_0 = \begin{bmatrix} \alpha & \beta & \gamma \\ \delta & \epsilon & \zeta \end{bmatrix}$$

then

$$M_1 \otimes M_0 =$$



$$=$$



b) The six factorizations corresponding to $n = 3$ are given in Table I.

Remarks: 1) The $n!$ factorizations described by Theorem 8 are actually distinct, since they may in particular involve matrices of different sizes. They may, however, be derived from each other by applying step by step a simple rule, illustrated here for $i < k$.

$$\cdots \cdot (\cdots \otimes 1_{r_k} \otimes \cdots \otimes M_i \otimes \cdots) \cdot (\cdots \otimes M_k \otimes \cdots \otimes 1_{c_i} \otimes \cdots) \cdot \cdots$$
$$= \cdots \cdot (\cdots \otimes M_k \otimes \cdots \otimes 1_{r_i} \otimes \cdots) \cdot (\cdots \otimes 1_{c_k} \otimes \cdots \otimes M_i \otimes \cdots) \cdot \cdots .$$

This rule may be called a *quasi-commutative rule:* it indeed reduces to the usual commutativity if all the matrices M_i are square matrices (of any order).

2) Theorem 9 generalizes to an arbitrary Kronecker product a factorization of the nth Kronecker power of a square matrix used by Lechner [6], [10].

B. Circuit Application

It now only remains to make a joint use of the results obtained in Sections II-C and III-A to complete the description of a variety of circuits performing a product $M\underline{v}$ when M has a Kronecker product structure. It is immediate to observe that all the factors appearing in the right-hand side of (46) are of the type studied in Theorem 7-2) and 3). Accordingly, in the most general situation, we shall be able to exhibit roughly $2^n \cdot n!$ distinct circuits performing the product $M\underline{v}$ when M is of the form (45): indeed, in each of the $n!$ factorizations (46) we may replace each of the n factors by either one of its expressions (43) or (44).

Let us first illustrate our design philosophy by a simple example. Consider the product $M_1 \otimes M_0$, where M_1 is a (2, 3)-matrix and M_0 is a (3, 2)-matrix. By (48), we obtain

$$M_1 \otimes M_0 = (M_1 \otimes 1_2) \cdot (1_2 \otimes M_0) = (1_3 \otimes M_0)(M_1 \otimes 1_3).$$

Let us now apply (42) to $M_1 \otimes 1_2$ and to $M_1 \otimes 1_3$, respectively. We obtain

TABLE I
FACTORIZATIONS OF $M_2 \otimes M_1 \otimes M_0$

2	χ 1	0	$M_2 \otimes M_1 \otimes M_0$
2	1	0	$(M_2 \otimes 1_{r_1r_0})(1_{c_2} \otimes M_1 \otimes 1_{r_0})(1_{c_2c_1} \otimes M_0)$
2	0	1	$(M_2 \otimes 1_{r_1r_0})(1_{c_2r_1} \otimes M_0)(1_{c_2} \otimes M_1 \otimes 1_{c_0})$
1	2	0	$(1_{r_2} \otimes M_1 \otimes 1_{r_0})(M_2 \otimes 1_{c_1r_0})(1_{c_2c_1} \otimes M_0)$
1	0	2	$(1_{r_2r_1} \otimes M_0)(M_2 \otimes 1_{r_1c_0})(1_{c_2} \otimes M_1 \otimes 1_{c_0})$
0	2	1	$(1_{r_2} \otimes M_1 \otimes 1_{r_0})(1_{r_2c_1} \otimes M_0)(M_2 \otimes 1_{c_1c_0})$
0	1	2	$(1_{r_2r_1} \otimes M_0)(1_{r_2} \otimes M_1 \otimes 1_{c_0})(M_2 \otimes 1_{c_1c_0})$

$$M_1 \otimes M_0 = S_{2,3} \cdot (1_2 \otimes M_1) \cdot S_{2,2} \cdot (1_2 \otimes M_0)$$

$$M_1 \otimes M_0 = (1_3 \otimes M_0) \cdot S_{3,3} \cdot (1_3 \otimes M_1) \cdot S_{2,3}.$$

The corresponding circuit diagrams are shown in Fig. 6(a) and (b).

Our present purpose is however not to give explicit descriptions of all the possible circuits, but merely to concentrate on some particular cases and to relate these circuits to previously described ones. From now on, we restrict ourselves to the particular case where all the M_i's are square matrices of order b_i and where χ is the identity mapping on $\{0, 1, \cdots, n-1\}$. Under these assumptions, formula (46) may be restated as

$$\bigotimes_{i=n-1}^{0} M_i = \prod_{i=n-1}^{0} (1_{b_{n-1} \cdots b_{i+1}} \otimes M_i \otimes 1_{b_{i-1} \cdots b_0}). \quad (49)$$

To shorten the notations, we also define

$$B_i = \prod_{\substack{j=0 \\ j \neq i}}^{n-1} b_j. \quad (50)$$

We now have

Theorem 9:

$$\bigotimes_{i=n-1}^{0} M_i = \prod_{i=n-1}^{0} [S_{B_i,b_i} \cdot (1_{B_i} \otimes M_i)]. \quad (51)$$

Proof: By replacing in (49) each of the right-hand side factors by its expression (43), one first obtains

$$\bigotimes_{i=n-1}^{0} M_i = \prod_{i=n-1}^{0} [S_{b_{i-1} \cdots b_0, b_{n-1} \cdots b_i} \cdot (1_{B_i} \otimes M_i) S_{b_{n-1} \cdots b_{i}, b_{i-1} \cdots b_0}].$$

In the latter expression, the factors $(1_{B_i} \otimes M_i)$ and $(1_{B_{i-1}} \otimes M_{i-1})$ are separated by the product of shuffles

$$S_{b_{n-1} \cdots b_i, b_{i-1} \cdots b_0} \cdot S_{b_{i-2} \cdots b_0, b_{n-1} \cdots b_{i-1}}.$$

An immediate computation making use of (38) finally shows that the latter product of shuffles is actually equal to $S_{B_{i-1},b_{i-1}}$. Q.E.D.

The philosophy underlying Theorem 9 is quite simple. Given the initial representation $[i_{n-1}, \cdots, i_1, i_0]$ of an input point in the basis $[b_{n-1}, \cdots, b_1, b_0]$, one replaces the action of the Kronecker product appearing in the left-hand member of (51) by the consecutive actions of a series of normal factors $(1_{B_i} \otimes M_i)$, each of which acts on blocks of points differing only by

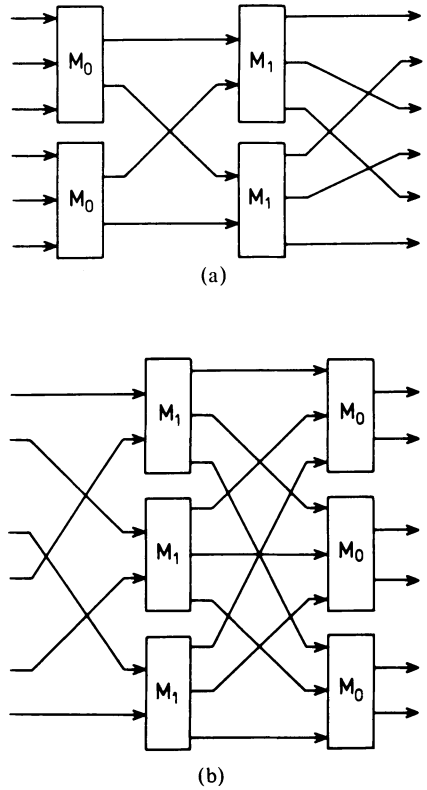


Fig. 6. Circuit diagram for $M_1 \otimes M_0$. (a) $(1_2 \otimes M_0)$; $S_{2,2}$; $(1_2 \otimes M_1)$; $S_{2,3}$. (b) $S_{2,3}$; $(1_3 \otimes M_1)$; $S_{3,3}$; $(1_3 \otimes M_0)$.

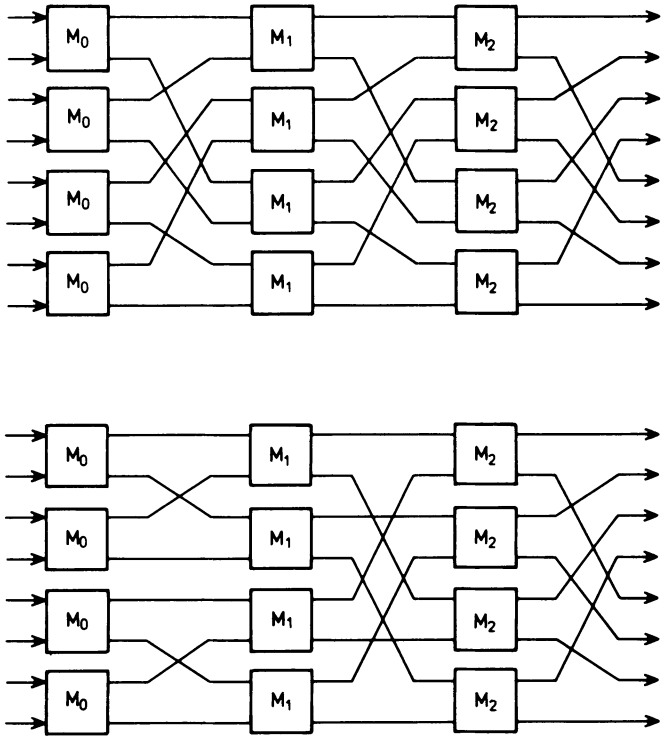


Fig. 7. Circuit diagrams for $M_2 \otimes M_1 \otimes M_0$.

the ith digit of their initial representations. These digits are in turn lead to the unit position by consecutive cyclic shifts caused by the shuffles S_{B_i,b_i}.

Observe, furthermore, that if all the matrices M_i are of order b, the interstage connection pattern now described by $S_{b^{n-1},b}$ is constant throughout the circuit. In particular, if all the matrices M_i are identical, formula (51) written as

$$M^{[n]} = [S_{b^{n-1},b} \cdot (1_{b^{n-1}} \otimes M)]^n \tag{52}$$

will easily be recognized as Good's factorization [2].

An equivalent circuit is obtained if one uses (44) instead of (43) to obtain a circuit description of the Kronecker product operation. We shall only illustrate the highlights of the corresponding interpretation in the case where all the matrices M_i have the same order b. In this case, formula (49) may be restated as

$$\bigotimes_{i=n-1}^{0} M_i = \prod_{i=n-1}^{0} (1_b^{[n-i-1]} \otimes M_i \otimes 1_b^{[i]}). \tag{53}$$

If one replaces in (53) each factor of the right-hand side by its expression (44), one obtains

$$\bigotimes_{i=n-1}^{0} M_i = \prod_{i=n-1}^{0} [(1_b^{[n-i-1]} \otimes S_{b^i,b}) \times (1_{b^{n-1}} \otimes M_i)(1_b^{[n-i-1]} \otimes S_{b,b^i})].$$

Consider in the latter expression the factors inserted between $(1_{b^{n-1}} \otimes M_{i+1})$ and $(1_{b^{n-1}} \otimes M_i)$. These factors are

$$(1_b^{[n-i-2]} \otimes S_{b,b^{i+1}})(1_b^{[n-i-1]} \otimes S_{b^i,b}).$$

The latter product may be written as

$$1_b^{[n-i-2]} \otimes [S_{b,b^{i+1}} \cdot (1_b \otimes S_{b^i,b})].$$

The latter expression is interpreted as (37). In this approach, the consecutive digits $i_{n-1}, \cdots, i_1, i_0$ of the representation of a domain point i are lead in the unit position by a sequence of transpositions of the type (i_k, i_0). The interconnection pattern obviously changes from stage to stage and will easily be recognized to belong to the familiar Cooley-Tukey type [3].

Examples: 1) For $b_2 = 2$, $b_1 = 3$, $b_0 = 5$, formula (51) yields

$$M_2 \otimes M_1 \otimes M_0 = S_{15,2}(1_{15} \otimes M_2)S_{10,3} \times (1_{10} \otimes M_1)S_{6,5}(1_6 \otimes M_0).$$

2) For $n = 2^3$ $(b = 2)$, one obtains, similarly,

$$M_2 \otimes M_1 \otimes M_0 = S_{4,2}(1_4 \otimes M_2)S_{4,2} \times (1_4 \otimes M_1)S_{4,2}(1_4 \otimes M_0).$$

This circuit is illustrated by Fig. 7(a). The corresponding handling by (53) and (54) yields

$$M_2 \otimes M_1 \otimes M_0 = S_{4,2}(1_4 \otimes M_2)S_{2,4} \times (1_2 \otimes S_{22})(1_4 \otimes M_1)(1_2 \otimes S_{22})(1_4 \otimes M_0).$$

This circuit is illustrated by Fig. 7(b).

IV. Conclusions

The essential result obtained in this paper is probably the discovery of a simple algebra able to describe a wide class of switching circuits, ranging from discrete transform circuits to permutation networks. The most interesting property of the described algebra is probably the ease with which one may derive families of equivalent circuits. It is, for example, interesting to know that the constant geometry patterns, dis-

covered by Good in the context of Hadamard transform, are also applicable to permutation networks in the Waksman style.

From a theoretical point of view, we tried to use as few tools as possible and managed to describe the main families of practical circuits using only Kronecker products and perfect shuffles. The complexity of (37) and (54), which basically describe an elementary concept (transposition), suggests however, an enrichment of our set of tools. This would probably provide us with more concise and more sensible circuit descriptions.

ACKNOWLEDGMENT

The author is indebted to Miss C. Gossart for fruitful discussions. He also wishes to thank the referees of the paper for extremely detailed and fruitful comments and criticisms.

REFERENCES

[1] C. K. Rushford, "Fast Fourier Hadamard decoding of orthogonal codes," *Inform. Contr.*, vol. 15, pp. 33-47, 1969.
[2] I. J. Good, "The interaction algorithm and practical Fourier analysis," *J. Roy. Stat. Soc.*, ser. B, vol. 20, pp. 361-372, 1958.
[3] J. W. Cooley and J. W. Tukey, "An algorithm for the machine computation of complex Fourier," *Series. Math. Comput.*, vol. 19, pp. 297-301, 1965.
[4] M. C. Pease, "An adaptation of the fast Fourier transform for parallel processing," *J. Ass. Comput. Mach.*, vol. 15, pp. 252-264, 1968.
[5] I. J. Good, "The relationship between two fast Fourier transforms," *IEEE Trans. Comput.*, vol. C-20, pp. 310-317, 1971.
[6] R. J. Lechner, "Harmonic analysis of switching functions," in *Recent Developments in Switching Theory*, A. Mukhopadhyay, Ed. New York: Academic, 1971.
[7] A. Waksman, "A permutation network," *J. Ass. Comput. Mach.*, vol. 15, pp. 159-163, 1968.
[8] H. S. Stone, "Parallel processing with the perfect shuffle," *IEEE Trans. Comput.*, vol. C-20, pp. 153-161, 1971.
[9] J. Lenfant, "Parallel permutations of data: A Benes network control algorithm for frequently used permutations," *IEEE Trans. Comput.*, vol. C-27, pp. 637-647, 1978.
[10] R. J. Lechner, "Transformations among switching function canonical forms," *IEEE Trans. Electron. Comput.*, vol. EC-12, no. 2, pp. 129-130, 1963.
[11] M. Davio, J. P. Deschamps, and A. Thayse, *Discrete and Switching Functions*. New York: McGraw-Hill, 1978.
[12] B. J. Fino and R. Algazi, "A unified treatment of discrete fast unitary transforms," *SIAM J. Comput.*, vol. 6, pp. 700-717, 1977.
[13] E. O. Brigham, *The Fast Fourier Transform*. Englewood Cliffs, NJ: Prentice-Hall, 1974.
[14] F. Yates, *The Design and Analysis of Factorial Experiments*. Harpenden: Imperial Bureau of Soil Science, 1937.
[15] D. E. Knuth, *The Art of Computer Programming. Vol. 2: Seminumerical Algorithms*. Reading, MA: Addison-Wesley, 1969.
[16] M. Davio and J. P. Deschamps, "Addition in signed digit number systems," in *Proc. 8th Int. Conf. on Multiple Valued Logics*, Chicago, IL, 1978, pp. 104-113.
[17] N. S. Szabo and R. J. Tanaka, *Residue Arithmetic and its Applications to Computer Technology*. New York: McGraw-Hill, 1967.
[18] R. Bellman, *Introduction to Matrix Analysis*. New York: McGraw-Hill, 1960.
[19] S. W. Golomb, "Permutations by cutting and shuffling," *SIAM Rev.*, vol. 3, pp. 293-297, 1961.
[20] J. B. Kam and G. I. Davida, "Structured design of substitution-permutation encryption networks," *IEEE Trans. Comput.*, vol. C-28, pp. 747-753, Oct. 1979.
[21] S. B. Morris and R. E. Hartwig, "The generalized Faro shuffle," *Discrete Math.*, vol. 15, pp. 333-346, 1976.
[22] I. Cahit, "Realization of graceful permutations by a shuffle-exchange network," *Informat. Process. Lett.*, vol. 6, pp. 171-173, 1977.

Marc Davio was born in Monceau-sur-Sambre, Belgium, in June 1938. He received the M.Sc. and Ph.D. degrees in electrical engineering from the University of Louvain, Louvain, Belgium, in 1961 and 1968, respectively.

He is currently a Research Group Leader at the Philips Research Laboratory, Brussels, and Professor at the University of Louvain, Louvain-la-Neuve. He is engaged in research on digital circuit design and algorithm implementation.