Ivan Chajda

Matrix representation of homomorphic mappings of finite Boolean algebras

Archivum Mathematicum, Vol. 8 (1972), No. 3, 143--148

Persistent URL: `http://dml.cz/dmlcz/104770`

ARCH. MATH. 3, SCRIPTA FAC. SCI. NAT. UJEP BRUNENSIS,
VIII: 143-148, 1972

MATRIX REPRESENTATION OF HOMOMORPHIC MAPPINGS OF FINITE BOOLEON ALGEBRAS

IVAN CHAJDA

(Received February 18, 1972)

Sometimes it is advantageous to investigate some of the properties of Boolean algebras on models. A suitable model for the investigation of homomorphic mappings is just the B-modul defined in [1]. For this reason in this paper I do not deal with an abstract Boolean algebra but with its isomorphic representation—the B-modul.

1.

Definition 1. Let there be given a set $M = \{0, 1\}$. Let us call each element of the Cartesian power M^m the *m-dimensional B-vector* (or briefly *vector*) *over M* and denote it by symbol $a = (a_1, a_2, \dots, a_m)$ where $a_i \in M$ for $i = 1, 2, \dots, m$. Elements a_i are called coordinates of the B-vector. We shall call the set $\mathfrak{M}_m$ of all m-dimensional B-vectores the *m-dimensional B-modul over M*. The B-vector $a = (a_1, \dots, a_m)$ is equal to B-vector $b = (b_1, \dots, b_m)$ just when $a_i = b_i$ for all i. By *the sum of vectors a, b* we call vector $c = (c_1, \dots, c_m)$ where $c_i = a_i + b_i$, for the coordinates holding: $0 + 0 = 0$, $1 + 1 = 1$, $0 + 1 = 1 + 0 = 1$. By *the product of vectors a, b* we shal call vector $d = (d_1, \dots, d_m)$, where $d_i = a_i b_i$, for the coordinates holding $0 . 0 = 0$, $0 . 1 = 1 . 0 = 0$, $1 . 1 = 1$. The vector $j = (1, 1, \dots, 1)$ is called *a unit vector, vector* $o = (0, 0, \dots, 0)$ *a zero vector.* Vector $\bar{a}$ is called *complement of vector a,* if it holds $a + \bar{a} = j$, $a . \bar{a} = 0$.

It is easy to show (see [1]) that each Boolean algebra having 2^m elements is isomorphic with m-dimensional B-modul $\mathfrak{M}_m$. In the modul $\mathfrak{M}_m$ we define a further operation:

Definition 2. The operation of multiplying of a vector $a \in \mathfrak{M}_m$ by element $\varepsilon \in M$ is given by the rule:

$$\varepsilon . a = a . \varepsilon = \begin{cases} o \text{ when } \varepsilon = 0 \\ a \text{ when } \varepsilon = 1. \end{cases}$$

Properties of this multiplication are derived in [1]. Now it is possible to introduce in $\mathfrak{M}_m$ a concept of a linear combination:

A vector $c \in \mathfrak{M}_m$ is a *linear combination* of the vectors $a_j \in \mathfrak{M}_m$, $j = 1, \dots, s$ iff there exist $\varepsilon_j \in M$ such that

$$c = \varepsilon_1 a_1 + \varepsilon_2 a_2 + \dots + \varepsilon_s a_s = \sum_{j=1}^{s} \varepsilon_j a_j .$$

Vectors $e^{(1)} = (1, 0, \dots, 0)$, $e^{(2)} = (0, 1, 0, \dots, 0)$, $\dots$, $e^{(m)} = (0, \dots, 0, 1)$ are called *base vectors* of the B-modul $\mathfrak{M}_m$. Obviously it holds:

$$a = (a_1, a_2, \dots, a_m) \qquad a = \sum_{i=1}^{m} a_i e^{(i)}, \text{ where } a_i \in M.$$

In [1] it is furthermore proved that base $e^{(1)}, e^{(2)}, \ldots, e^{(m)}$ in $\mathfrak{M}_m$ is unique.

Definition 3. A matrix

$$A = \begin{bmatrix} a_{11}\, a_{12} \;\ldots\; a_{1n} \\ a_{21}\, a_{22} \;\ldots\; a_{2n} \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ a_{m1} a_{m2} \ldots a_{mn} \end{bmatrix} \quad \text{where } a_{ij} \in M$$

will be called *Boolean matrix* (or simply *B-matrix*) of type m/n.

The B-matrix 0, whose all elements are 0 will be called the *zero-B-matrix*, the B-matrix, whose all elements are *1* vill be called the *unit-B-matrix*, denoted by J. A matrix A is equal to a matrix B, if and only if they are of the same type and for all i, j it holds $a_{ij} = b_{ij}$, where $b_{ij} \in M$ are elements of matrix B. The sum of matrices A, B of the same type m/n is a matrix C of type m/n, whose elements satisfy $c_{ij} = a_{ij} + b_{ij}$, the product of matrices A, B is a matrix D of type m/n whose elements satisfy $d_{ij} = a_{ij}b_{ij}$, for the addition and multiplication of elements a_{ij}, b_{ij} holding the same rules as for coordinates of the B-vectores in definition 1.

Definition 4. By a *B-matrix decomposition of the matrix A* of type m/n we shall call all B-matrices $A_1, A_2, \ldots, A_h$, for which it holds:

1. $A_1, A_2, \ldots, A_h$ are of the same type m/n; $A_r \neq A_s$ for $r \neq s$.
2. Each A_j $(j = 1, \ldots, h)$ has at most one unity in each its column.
3. If the r-th column of A is non-zero then the r-th column of each A_j is non-zero.
4. $A_1 + A_2 + \ldots + A_h = A$.

Example: B-matrix decomposition of $A = \begin{bmatrix} 1&0&1&0 \\ 0&0&1&1 \\ 0&0&1&1 \end{bmatrix}$ is just the following one:

$$A = \begin{bmatrix} 1&0&1&0 \\ 0&0&0&1 \\ 0&0&0&0 \end{bmatrix} + \begin{bmatrix} 1&0&0&0 \\ 0&0&1&1 \\ 0&0&0&0 \end{bmatrix} + \begin{bmatrix} 1&0&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{bmatrix} + \begin{bmatrix} 1&0&1&0 \\ 0&0&0&0 \\ 0&0&0&1 \end{bmatrix} + \begin{bmatrix} 1&0&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{bmatrix} + \begin{bmatrix} 1&0&0&0 \\ 0&0&0&0 \\ 0&0&1&1 \end{bmatrix}.$$

Let the B-modul $\mathfrak{M}_m$ be given, i.e. the Boolean algebra with 2^m elements and B-modul $\mathfrak{M}_n$, i.e. the Boolean algebra with 2^n elements. If $m < n$, the homomorphic mapping of $\mathfrak{M}_m$ into $\mathfrak{M}_n$ can be considered, if $m \geqq n$, also the homomorphic mapping $\mathfrak{M}_m$ onto $\mathfrak{M}_n$ can be considered. By the homomorphic mapping of $\mathfrak{M}_m$ onto $\mathfrak{M}_n$ the zero vector from $\mathfrak{M}_m$ is always mapped onto the zero vector of B-modul $\mathfrak{M}_n$, however, for the mapping *into* this fact need not hold. For this reason we shall here consider only those homomorphisms which image the zero vector onto zero vector.

Definition 5. Let the B-matrix A of the type m/n be given, whose rows are B-vectors $a_1, a_2, \ldots, a_m \in \mathfrak{M}_n$. Let $\varphi \in \mathfrak{M}_m$, $\varphi = (f_1, f_2, \ldots, f_m)$, $f_i \in M$. Then *the matrix A represents a mapping α of modul $\mathfrak{M}_m$ into $\mathfrak{M}_n$*, defined as follows:

$$\alpha(\varphi) = \psi \in \mathfrak{M}_n, \text{ where } \psi = \sum_{i=1}^{m} f_i a_i .$$

It is obvious that α is really the mapping of $\mathfrak{M}_m$ into $\mathfrak{M}_n$, because each vector $\varphi \in \mathfrak{M}_m$ has only one image in $\mathfrak{M}_n$, furthermore it is evident that $\alpha(o) = o$. The image of an arbitrary vector $\varphi \in \mathfrak{M}_m$ may be determined in the following way: behind matrix A we write vertically vector φ and add as vectors those rows matrix A, in which the verticaly written vecto rφ has unities. This sum is an image of vector φ in modul $\mathfrak{M}_n$.

Example 1.

$$A = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

B-matrix A represents mapping α of modul $\mathfrak{M}_3$ into $\mathfrak{M}_4$. Let $\varphi = (1\ 1\ 0)$, then

$$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \quad \text{thus } \psi = (1\ 0\ 1\ 0) + (0\ 1\ 0\ 0) = (1\ 1\ 1\ 0).$$

For homomorphic mappings the following theorem is holding:

Theorem 1. A mapping α, represented by B-matrix A of the type m/n is a homomorphic mapping of $\mathfrak{M}_m$ into $\mathfrak{M}_n$, fulfilling $\alpha(o) = o$, iff the matrix A has in each column at most one unity.

Proof: Let us denote by $a_1, \dots, a_m \in \mathfrak{M}_n$ rows of the matrix A. Then obviously base vector $e^{(1)} \in \mathfrak{M}_m$ is imaged onto a_1, vector $e^{(2)}$ onto $a_2, \dots, e^{(m)}$ is imaged onto a_m.

1. Let the matrix a have in each column at most one unity. Then it holds $a_i a_j = o$ for $i \neq j$. From the definition 5 it follows

$$\alpha(e^{(i)} + e^{(j)}) = a_i + a_j = \alpha(e^{(i)}) + \alpha(e^{(j)})$$

and furthermore, from the properties of base vectors:

$$\alpha(e^{(i)} \,.\, e^{(j)}) = \alpha(o) = o = a_i \,.\, a_j = \alpha(e^{(i)}) \,.\, \alpha(e^{(j)}).$$

Also it is immediately obvious

$$\left.\begin{aligned} \alpha(O \,.\, e^{(i)}) &= \alpha(o) = o = O \,.\, \alpha(e^{(i)}) \\ \alpha(1 \,.\, e^{(i)}) &= \alpha(e^{(i)}) = a_i = 1 \,.\, \alpha(e^{(i)}) \end{aligned}\right\} \Rightarrow \alpha(\varepsilon \,.\, e^{(i)}) = \varepsilon \,.\, \alpha(e^{(i)})$$

consequently α is really a homomorphic mapping of $\mathfrak{M}_m$ into $\mathfrak{M}_n$.

2. Let α be a homomorphic mapping of $\mathfrak{M}_m$ into $\mathfrak{M}_n$, $\alpha(o) = o$, and let A have at least two unities in the i-th column, let they are in the k-th and s-th row. Then:

$$\alpha(e^{(k)}) = (a_{k,1}, \dots, a_{k,i-1}, 1, a_{k,i+1}, \dots, a_{k,n})$$

$$\alpha(e^{(s)}) = (a_{s,1}, \dots, a_{s,i-1}, 1, a_{s,i+1}, \dots, a_{s,n})$$

consequently $\alpha(e^{(k)}) \,.\, \alpha(e^{(s)}) \neq o$, because it has the i-th coordinate equal to *1*, but it holds $\alpha(e^{(k)} \,.\, e^{(s)}) = \alpha(o) = o$, which is a contradiction.

The following theorems are clear:

-A1- If A is the B-matrix of the type m/n and if it has in each column and each row just one unity, then A represents the isomorphic mapping of $\mathfrak{M}_m$ onto $\mathfrak{M}_m$.

-A2- If A is the B-matrix of the type m/n, $m < n$ and if it has in each column at most one and in each row just one unity, then the set of images of all vectors from $\mathfrak{M}_m$, i.e. $\alpha(\mathfrak{M}_m)$, forms the B-modul $\mathfrak{M}'_n \subset \mathfrak{M}_n$ which is isomorphic with $\mathfrak{M}_m$.

Furthermore, we shall prove the following theorem:

Theorem 2. If α is a homomorphic mapping of $\mathfrak{M}_m$ into $\mathfrak{M}_n$, where $\alpha(o) = o$, then there exists just one B-matrix A of type m/n representing this mapping.

Proof: In [1] it is proved that the modul $\mathfrak{M}_m$ has just one base, namely $\{e^{(1)}, e^{(2)}, \ldots, e^{(m)}\}$. Each vector from $\mathfrak{M}_m$ may thus be expressed in the only way as a linear combination of base vectors:

$$\varphi \in \mathfrak{M}_m \Rightarrow \varphi = \sum_{i=1}^{m} f_i e^{(i)}.$$

Since α is the homomorphic mapping, it holds:

$$\alpha(\varphi) = \sum_{i=1}^{m} f_i \,.\, \alpha(e^{(i)}).$$

Let us denote $\alpha(e^{(i)}) = a_i$, then a_i are univocally determined rows of a B-matrix A.

Theorems 2 and 1 secure representation of all homomorphic mappings of $\mathfrak{M}_m$ into $\mathfrak{M}_n$, fulfilling $\alpha(o) = o$, by the set of all B-matrices of the type m/n having in each column at most one unity.

There are just $\binom{n}{k} m^{n-k}$ B-matrices of the type m/n, having k zero-columns and $n - k$ columns with just one unity. If we consider also the so called degenerated Boolean algebra (see [4]) having only one element, namely O, then we can formulate the theorem:

Theorem 3. There exist just $s = (m + 1)^n$ homomorphic mappings of a Boolean algebra with 2^m elements into a Boolean algebra with 2^n elements, fulfilling $\alpha(O) = O$.

Corollary: There exist just $r = (m + 1)^m$ endomorphisms of a Boolean algebra with 2^m elements, which image O onto O.

2.

Mappings and all the more homomorphisms, can under certain assumptions be composed. Since this composition is associative, there must exist an associative operations among B-matrices of a certain type corresponding to this composition.

Let $\mathfrak{M}_m$, $\mathfrak{M}_n$, $\mathfrak{M}_p$ be B-moduls, let the B-matrix A_1 of the type m/n represents a mapping α_1 of the B-modul $\mathfrak{M}_m$ into $\mathfrak{M}_n$, let a matrix A_2 of the type n/p represents a mapping α_2 of $\mathfrak{M}_n$ into $\mathfrak{M}_p$ and let us denote by α_3 the composed mapping $\alpha_3 = \alpha_2\alpha_1$ of the modul $\mathfrak{M}_m$ into $\mathfrak{M}_p$. Then the operation $\odot$ corresponding to the composition of mappings is feasible only among matrices of the types m/n, n/p, the resulting matrix is of the type m/p.

Let the matrix A_1 has elements δ_{is}, let rows of the matrix A_2 be p-dimensional B-vectores $k_1, k_2, \ldots, k_n$ and let us denote the rows of the resulting matrix A_3 by $f_1, f_2, \ldots, f_m$, which are again p-dimensional B-vectors. Let the modul $\mathfrak{M}_m$ has base $\{e^{(1)}, \ldots, e^{(m)}\}$, modul $\mathfrak{M}_n$ has base $\{e_*^{(l)}, \ldots, e_*^{(n)}\}$. Then: $\alpha_2(e_*^{(i)}) = k_i$, $\alpha_1(e^{(i)}) = c_i$, where $c_i = (\delta_{i1}, \dots, \delta_{in})$. The composed mapping $\alpha_3 = \alpha_2\alpha_1$ then images vectors $e^{(i)}$ onto the rows of the resulting matrix A_3, thus:

$$f_i = \alpha_3(e^{(i)}) = \alpha_2(\alpha_1(e^{(i)})) = \alpha_2(c_i) = \alpha_2\Big(\sum_{s=1}^{n} \delta_{is}e_*^{(s)}\Big) = \sum_{s=1}^{n} \delta_{is}\alpha_2(e_*^{(s)}) = \sum_{s=1}^{n} \delta_{is}k_s$$

and thus $f_i = \sum_{s=1}^{n} \delta_{is}k_s$ is the formula for the determination of rows of the resulting B-matrix A_3. Symbolically we write $A_3 = A_1 \odot A_2$.

Example 2.

$$A_1 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \qquad A_2 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \qquad A_3 = A_1 \odot A_2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$$

The operation $\odot$ is a partial associative operation on the set of all B-matrices. This operations is everywhere defined on the set of all square B-matrices of the type m/m. The set of all square matrices of the type m/m forms an algebra $\mathfrak{A}$ with four operations, denoted by symbols $+, \cdot, \odot, \mathsf{T}$, where $+, \cdot$ are addition and multiplication, defined in definition 3. With respect to this operations, $\mathfrak{A}$ forms a distributive lattice. With respect to operation $\odot$, $\mathfrak{A}$ is a semigroup. The operation T is a unary operation of the transposition of B-matrices in a way usual in the matrix-calcul.

Further we consider the set of all square B-matrices of the type m/m, having in each row and in each column just one unity. These matrices represent isomorphisms $\mathfrak{M}_m$ onto $\mathfrak{M}_m$, the composition of two isomorphisms is again an isomorphism, consequently the set of these matrices, let us denote it by $\mathfrak{A}_1$, is closed with respect to the operation $\odot$. $\mathfrak{A}_1$ is a subsemigroup of the semigroup $\mathfrak{A}$, but $\mathfrak{A}_1$ is even a group. The inverse element to a matrix $A \in \mathfrak{A}_1$ is the transposed matrix $A^{\mathsf{T}} \in \mathfrak{A}_1$, unity of this group is the so called identical matrix I, representing the identical isomorphism (having unities just in the diagonal). The matrices of the algebra $\mathfrak{A}_1$ are called B-regular.

In the algebra $\mathfrak{A}$ it is possible to cancellate by B-regular elements. The matrix J is agressive with respect to operation $\odot$ for B-regular matrices. For matrices, which are not B-regular, there holds only the following inequality (in the sense of the lattice ordering):

$$B \in \mathfrak{A} \qquad J \geqq J \odot B \geqq B.$$

For the right multiplication by the element J even this inequality does not hold. Also the relation $A \odot A^{\mathsf{T}} = A^{\mathsf{T}} \odot A$ holds only for B-regular matrices.

Let us denote by $\mathfrak{A}_2$ the set of all B-matrices of the type m/m, having in each column at least one unity. With respect to the addition, $\mathfrak{A}_2$ is closed. Matrices from $\mathfrak{A}_2$ represent all semihomomorphic mappings of $\mathfrak{M}_m$ into $\mathfrak{M}_m$, fulfilling:

$$\alpha(o) = o \qquad \alpha(j) = j.$$

Again, it is clear that $\mathfrak{A}_2$ is a subsemigroup of the semigroup $\mathfrak{A}$ and the group $\mathfrak{A}_1$ is a subsemigroup of $\mathfrak{A}_2$. With respect to the operation T, however, $\mathfrak{A}_2$ is no more closed.

It is possible to construct further subalgebras of $\mathfrak{A}$ and to investigate by means of this metod the properties of mappings of Boolean algebras. The aim of this paper was, however, only to show some advantages of matrix representation in the investigation of homomorphisms in finite Boolean algebras.

REFERENCES

[1] Metelka Josef: *Vektorielles Modell der endlichen Booleschen Algebren* (1966, Acta Universitatis Palackianae Olomucensis).

[2] Birkhoff Garret: *Lattice Theory* (Amer. Math. Society, New York 1940).

[3] Whitesitt J. Eldon: *Boolean Algebra and its Aplications.*

[4] Rieger Lad.: *Algebraic Methods of Mathematical Logic* (Academia Prague 1967).

I. Chajda
Přerov, třída Lidových milicí 290
Czechoslovakia