

František Katrnoška

LOGICS THAT ARE GENERATED BY IDEMPOTENTS

(submitted by D. Mushtari)

ABSTRACT. The main result of this paper is the generalization of the theorem which represents one of the generally accepted cases concerning the characterization of the logic of idempotents (see [5], [6], [7]). If R is a ring then the R -circulant matrices are introduced and some consequences for the logics of idempotents of the corresponding rings. Some convenient examples are added as well. Certain results of this paper may find applications in the foundation of quantum theory.

1. INTRODUCTION

For a ring R with identity 1, we denote by $U(R)$ the set of all idempotents of R . If, moreover, R is a $*$ -ring with identity, we denote by $P(R)$ the set of all projectors of R .

The following definition will play an important role in the sequel:

Definition 1. Let $(L, \leq, 0, 1, ')$ be a poset with 0 and 1 as the smallest and the greatest element, respectively, and a unary operation $': L \rightarrow L$ (the orthocomplementation) such that

- (i) $p \leq q \Rightarrow q' \leq p', \quad p, q \in L$
- (ii) $(p')' = p, \quad p \in L$
- (iii) $p \vee p' = 1, \quad p \in L$
- (iv) $p \leq q' \Rightarrow p \vee q \text{ exists in } L, \quad p, q \in L$
- (v) $p \leq q \Rightarrow q = p \vee (p' \wedge q), \quad p, q \in L$

Then L will be called a logic or also an orthomodular poset. If L is also a lattice, then L is called an orthomodular lattice.

2000 Mathematical Subject Classification. Primary 06C15, Secondary 15A33.

Key words and phrases. Ring and $*$ -ring with identity, idempotents, projectors of a $*$ -ring.

Suppose now that R is a commutative field. Denote by $\mathcal{M}_{22}(R)$ the set of all $(2, 2)$ -matrices over R . The set $\mathcal{M}_{22}(R)$ is a non-commutative ring with identity. We give now an example.

Example 1 The idempotents of the ring $\mathcal{M}_{22}(R)$ are the following matrices:

$$O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad \text{Tr}(A) = 1, \\ \det(A) = 0, \quad a, b, c, d \in R.$$

The set $U(\mathcal{M}_{22}(R))$ is a logic which is a lattice.

The partial order in this example is defined by setting

$$(A_1 \leq A_2) \Leftrightarrow (A_1 A_2 = A_2 A_1 = A_1, \quad A_1, A_2 \in U(\mathcal{M}_{22}(R)))$$

and the orthocomplementation $': U(\mathcal{M}_{22}(R)) \rightarrow U(\mathcal{M}_{22}(R))$ by $A' = E - A$.

Let R be an associative ring with identity. We will suppose furthermore in this paper that the order in the set $U(R)$ is defined always by setting

$$(1) \quad (p \leq q) \Leftrightarrow (pq = qp = p, \quad p, q \in U(R))$$

and the orthocomplement by

$$(2) \quad p' = 1 - p, \quad p \in U(R).$$

If R is an associative $*$ ring with identity then the partial order and the orthocomplementation are defined also in $P(R)$ in this manner. It is clear that in this case $\{0, 1\} \subset P(R) \subset U(R)$. It is well known (see [5], [6], [7]) that the sets $U(R)$ and $P(R)$ are logics with regard to the conditions (1) and (2). In the next section we give some generalization of this result. First we introduce the following definition:

Definition 2. Let L be a logic. A subset S of L is said to be a sublogic of L if the following conditions are satisfied:

- (i) $0 \in S$.
- (ii) If $p \in S$ then $p' \in S$.
- (iii) If $p, q \in S$ and $p \leq q'$, then $p \vee q \in S$.

Let R be an associative $*$ ring with identity. Then $P(R)$ is a sublogic of the logic $U(R)$ as will be shown in the sequel.

Let L be a logic. We say that $p, q \in L$ are orthogonal ($p \perp q$) if $p \leq q'$. We now introduce a further example of a sublogic of a given logic L .

Example 2 Let L be a logic containing a subset $\{p_i : i \in N\}$ such that $p_i \not\leq p_j$, $p_i \not\leq p'_j$ for $i \neq j$. We denote by S the following subset of L :

$$S = \{0, 1\} \cup \{p_i, p'_i : i \in N\}.$$

It can be shown that S is a sublogic of L .

2. CHARACTERIZATION OF SOME LOGICS OF IDEMPOTENTS

In this section we introduce first of all some conditions which guarantee that a subset S of a logic L is a sublogic of L . We introduce at the same time some examples and also certain consequences and conclusions which immediately follow.

Theorem 1. *Let R be an associative ring with identity and let S be a subset of $U(R)$. The conjunction of the following conditions is sufficient for S to be a sublogic of $U(R)$:*

- (i) $0 \in S$.
- (ii) If $p \in S$ then $p' \in S$.
- (iii) If $p_1, p_2 \in S$ and if $p_1 p_2 = p_2 p_1$ then $p_1 p_2 \in S$ and $p_1 + p_2 - p_1 p_2 \in S$.

Proof. Suppose that S fulfils the conditions (i)–(iii) of the theorem. Define the partial order \leq and the orthocomplementation according to the conditions (1) and (2). Clearly $\{0, 1\} \subset S$. S is a partially ordered set.

- a) If $p \in S$ then $p \cdot p = p^2 = p$. Therefore $p \leq p$.
- b) Suppose that $p_1 \leq p_2$ and $p_2 \leq p_1$, $p_1, p_2 \in S$. Then it follows that

$$p_1 = p_1 p_2 = p_2 p_1 = p_2.$$

- c) Let $p_1, p_2, p_3 \in S$ and suppose, moreover, that $p_1 \leq p_2$ and $p_2 \leq p_3$. Then we have

$$p_1 p_2 = p_2 p_1 = p_1, \quad p_2 p_3 = p_3 p_2 = p_2.$$

From this follows $p_1 = p_1 p_2 = p_1 \cdot p_2 p_3 = p_1 p_2 \cdot p_3 = p_1 p_3$. Therefore $p_1 \leq p_3$. The relation \leq is also transitive.

Now we will prove the properties (i)–(v) of Definition 1.

- (i): Suppose that $p \leq q$ if $p, q \in S$. Then $pq = qp = p$ and we have

$$q'p' = (1 - q)(1 - p) = 1 - p - q + pq = 1 - p - q + p = 1 - q = q'.$$

Therefore $q' \leq p'$.

- (ii): Let $p \in S$. Due to condition (ii) of Theorem 1, it follows that

$$(p')' = 1 - p' = 1 - (1 - p) = p.$$

We prove property (iv) first, because property (iii) follows immediately from (iv) as a consequence. Suppose that $p \leq q'$, $p, q \in S$. Then $p(1 - q) = (1 - q)p = p$. From this it follows that $pq = qp = 0$ and by (iii) of this theorem we have $p + q - pq = p + q \in S$. We prove now that $p + q = p \vee q$. Indeed, $p(p + q) = (p + q)p = p$, $q(p + q) = (p + q)q = q$.

Therefore we have $p + q \geq p$ and $p + q \geq q$. If $r \geq p, r \geq q$, $r \in S$, then $rp = pr = p$, $rq = qr = q$. Therefore we have $r(p + q) = (p + q)r = p + q$. Also $p + q = p \vee q \in S$.

- (iii): If $p \in S$ then $p' \in S$ and $p \leq (p')'$. By (iv), $p \vee p' = p + p' = p + (1 - p) = 1$. If $p, q \in S$ and if $pq = qp$, then it can be shown that $p \wedge q = pq$. The proof is easy.

(v): Suppose that $p \leq q, p, q \in S$. Then $pq = qp = p$. Because $p', q \in S$ and $p'q = qp'$, it follows that $q \wedge p' \in S$, $q \wedge p' = q(1-p) = (1-p)q = q-p$. At the same time, $p \wedge (q \wedge p') = p(q-p) = pq-p^2 = 0$. Therefore we have $p \vee (q \wedge p') = p+q \wedge p' = p+(q-p) = q$.

So it was proved that the conditions (i)–(iii) of the Theorem 1 are sufficient for S to be a logic. It remains to prove that S is really a sublogic of $U(R)$, i.e., that operations on S coincide with those inherited from $U(R)$. Condition (ii) of Definition 2 is condition (ii) of Theorem 1. To prove condition (iii) of Definition 2, suppose that $p, q \in S$ and $p \leq q'$. Then $pq = qp = 0$ and $p+q = p \vee q \in S$. The proof is complete. \square

Remark 1. If $U(R)$ is a logic such that for each $p, q \in U(R)$ from $pq = qp$ it follows that $pq = 0$. Then each sublogic S of $U(R)$ satisfies condition (iii) of Theorem 1. In particular, if $p, q \in S$ and $pq = qp = 0$, then $p \leq q'$ and, by (iii) of Definition 2, $p \vee q = p+q = p+q-pq \in S$.

As a consequence, for the logic $U(\mathcal{M}_{22}(R))$ of all idempotents of the ring of all $(2, 2)$ -matrices over the a commutative field R , each sublogic S of $U(\mathcal{M}_{22}(R))$ satisfies condition (iii) of Theorem 1.

Example 3 Let R be an associative $*$ -ring with identity. Then the set $P(R)$ fulfils the conditions (i)–(iii) of Theorem 1. Therefore $P(R)$ is a sublogic of the logic $U(R)$.

Now we introduce an example which has undeniable connections with the foundation of the set of all states of the spin of an electron.

Example 4 Let H_2 be a two-dimensional Hilbert space over the complex numbers. The space H_2 among others corresponds to the set of all states of the spin of one electron. Let S be the set of $(2, 2)$ -matrices of the following forms:

$$O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad M_1 = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix},$$

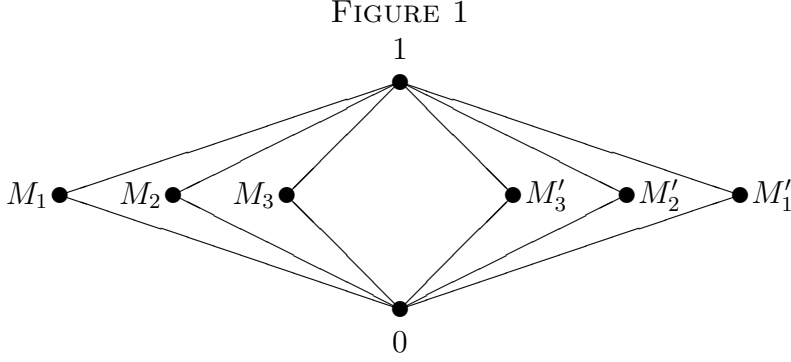
$$M_2 = \begin{bmatrix} \frac{1}{2} & \frac{-i}{2} \\ \frac{i}{2} & \frac{1}{2} \end{bmatrix}, \quad M_3 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad M'_i = E - M_i, \quad i = 1, 2, 3.$$

It can be shown that the set S satisfies conditions (i)–(iii) of Theorem 1. Therefore $(S, \leq, 0, E, ')$ is a sublogic of the logic $U(\mathcal{M}_{22}(C))$ of all $(2, 2)$ -matrices over the field C of all complex numbers. This sublogic S is an orthomodular lattice. The picture of $(S, \leq, 0, E, ')$ is introduced in Fig. 1.

Notice that there exists a connection between the matrices $M_i, i = 1, 2, 3$ and the Pauli matrices $\sigma_i, i = 1, 2, 3$. The Pauli matrices are:

$$\sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

As $M_i = \frac{1}{2}(E + \sigma_i), i = 1, 2, 3$, and the matrices $S_i = \frac{1}{2}\sigma_i, i = 1, 2, 3$ correspond to the projections of the spin on the i th axis.



Open Problem 1. *Though it is clear that each sublogic S of the logic $U(R)$ satisfies conditions (i) and (ii) of Theorem 1, it remains an open question whether any sublogic S of $U(R)$ has to satisfy also condition (iii).*

It is very important to determine some condition for a given sublogic S of $U(R)$ to be a Boolean algebra. The following proposition gives a sufficient condition.

Proposition 1. *Let R be an associative ring with identity and let S be a subset of $U(R)$ which satisfies conditions (i)–(iii) of Theorem 1 and, moreover,*

(iv) *all elements of S are pairwise commutative.*

Then the sublogic $(S, \leq, 0, 1, ')$ is a Boolean algebra.

Proof. With regard to condition (iv) it follows that S is a lattice, i.e., for each $p, q \in S$, there exist the elements $p \vee q$ and $p \wedge q$ in S . It is well known that each distributive orthomodular lattice is a Boolean algebra (see [3]), it suffices to prove distributivity of S . If $p, q, r \in S$, then

$$p \wedge (q \vee r) = p(q \vee r) = p(q + r - qr) = pq + pr - pqr.$$

On the other hand, we have

$$(p \wedge q) \vee (p \wedge r) = (pq) \vee (qr) = pq + qr - pqr.$$

Therefore $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$. Similarly, it can be shown that

$$p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r), \quad p, q, r \in S.$$

Therefore the distributivity laws are valid and $(S, \leq, 0, 1, ')$ is a Boolean algebra. \square

Example 5 Let R be an associative commutative ring with identity. Then $P(R)$ is a Boolean subalgebra of the logic $U(R)$ (which is also a Boolean algebra). The proof follows at once from Theorem 1 and it is a consequence of Proposition 1.

In the general case, it is difficult to establish all Boolean subalgebras of a given logic $U(R)$. In some special cases it is possible. At the conclusion of this section we introduce an example of a Boolean subalgebra of the logic $U(R)$. For this purpose we give the following definition:

Definition 3. Let R be an associative ring with identity. We say that B is the Boolean subalgebra of $U(R)$ generated by the elements $p_i \in U(R)$, $i = 1, 2, \dots, n$ if it is the smallest Boolean subalgebra of $U(R)$ containing p_i , $i = 1, 2, \dots, n$.

We show now an example of a Boolean subalgebra $B \subset U(R)$ which is generated by two elements of $U(R)$.

Example 6 Let R be an associative ring with identity and suppose that $p, q \in U(R) \setminus \{0, 1\}$, $p \neq q$, and $pq = qp$. Then the set

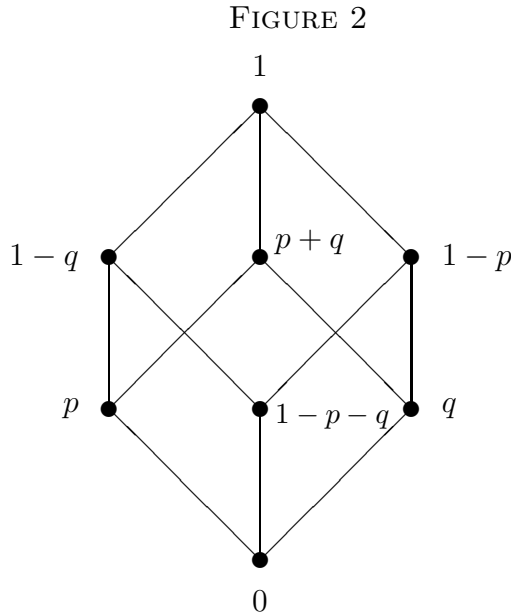
$$B_{p,q} = \{0, p, q, 1-p, 1-q, pq, 1-pq, p-pq, q-pq, p+q-2pq, 1-(p+q-2pq), \\ 1-p+pq, 1-q+pq, 1-p-q+pq, p+q-pq, 1\}$$

is a Boolean subalgebra of the logic $U(R)$. This Boolean subalgebra $B_{p,q}$ is generated by the elements p, q .

In particular, if the elements p, q are orthogonal, then $B_{p,q}$ is of the following form:

$$B_{p,q} = \{0, p, 1-p, q, 1-q, p+q, 1-p-q, 1\}.$$

This Boolean subalgebra of $U(R)$ is illustrated in Fig. 2.



Example 7 Let F be a commutative field. Denote by $\mathcal{M}_{22}(F)$ the ring of all $(2, 2)$ -matrices over F . Then the logic $U(\mathcal{M}_{22}(F))$ has only the following Boolean subalgebras:

$$B_0 = \{0, 1\}, \quad B_p = \{0, p, p', 1\}, \quad p \in U(\mathcal{M}_{22}(F)).$$

From the physical point of view it is very important to establish at least some Boolean subalgebras of given logics because then it is possible to use the methods of classical physics for the solution of problems which concern certain physical systems. One possibility is shown in the next section.

3. ON RINGS OF CIRCULANTS

It is well known that the circulants have been applied to data smoothing, signal and image processing and also to algebraic coding theory. It could be possible to apply the circulants also in quantum theory to problems which require the use of coding theory. From the references devoted to the theory of circulants we may recommend the books by Davis [4] and by Marcus and Minc [11]. However, these books deal only with circulants over the field of all complex numbers. The approach built up in this paper is more general. Namely, we suppose, that the circulants are defined over any commutative ring. First of all we introduce a generalization of the notion of generalized Latin square.

Definition 4. *Let R be an associative ring. By a generalized R -Latin square of order n we mean a square matrix of order n such that the sums of all rows and of all columns are identical and are equal to some element $s \in R$.*

Definition 5. *Let R be an associative and commutative ring. By an R -circulant of order n we mean a square matrix of order n over R which has the form $C = \text{circ}(c_1, c_2, \dots, c_n)$, $c_i \in R, i = 1, 2, \dots, n$, i.e.,*

$$C = \begin{bmatrix} c_1 & c_2 & c_3 & \dots & c_{n-2} & c_{n-1} & c_n \\ c_n & c_1 & c_2 & \dots & c_{n-3} & c_{n-2} & c_{n-1} \\ c_{n-1} & c_n & c_1 & \dots & c_{n-4} & c_{n-3} & c_{n-2} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ c_3 & c_4 & c_5 & \dots & c_n & c_1 & c_2 \\ c_2 & c_3 & c_4 & \dots & c_{n-1} & c_n & c_1 \end{bmatrix}.$$

We will always suppose that the ring R is commutative. Denote by $L_n(R)$, resp. $C_n(R)$, the set of all generalized R -Latin squares, resp. R -circulants, of order n .

It is clear that $C_n(R) \subset L_n(R)$.

Proposition 2. *The set $L_n(R)$ is a non-commutative ring, while the set $C_n(R)$ is a commutative ring.*

Proof. The proof is easy, although quite long. □

Corollary *Let R be an associative commutative ring with identity, then $U(C_n(R))$ is a Boolean subalgebra of the logic $U(L_n(R))$.*

The determination of all elements of $U(C_n(R))$ is generally difficult. It depends namely on further properties of the ring R . In some cases this task is possible. We introduce now such an example.

Example 8 Let R be a commutative field. Then the Boolean algebra $U(C_n(R)) = \{O, E, M, M'\}$, where

$$O = \begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{bmatrix}, \quad E = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{bmatrix}, \quad M = \frac{1}{n} \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots \\ 1 & 1 & \dots & 1 \end{bmatrix}, \quad M' = E - M.$$

If R is not a commutative field, then the form of $U(C_n(R))$ remains an open problem.

At the end of this paper we introduce some remarks.

- A) Let R be an associative commutative ring with identity e and denote by C the circulant of the form $C = \text{circ}(0, e, 0, \dots, 0)$. Then the circulant $A = \text{circ}(a_1, a_2, \dots, a_n)$, $a_i \in R$, $i = 1, 2, \dots, n$, can be expressed in the form

$$A = \sum_{k=1}^{n-1} a_{k+1} C^k.$$

If R is the field of all complex numbers, then the circulants C^k , $k = 1, 2, \dots, n$, are permutation matrices. This particular result is contained in [4] and in [11].

In the following remarks B and C we assume that R is the field of all real numbers.

- B) A very important class of matrices (especially from the statistical point of view) is the class of the double stochastic matrices. Recall that a matrix S is called *double stochastic* if the sums of all elements of each row and also of each column of S are always equal to 1 and if all elements of S are non-negative real numbers. Thus $S \in L_n(R)$ for some $n \in N$. The set $S_n(R)$, $n \in N$ of all double stochastic matrices of order n is of course not a ring, it is only a semigroup with identity with respect to multiplication (i.e., a non-commutative monoid). (See Birkhoff [3] and Ward and Dilworth [15].)
- C) The square matrix U whose elements are either one or zero and which has exactly one nonzero entry in each row and each column is called *permutation matrix*. If U is a permutation matrix of order n , then $U \in S_n(R)$. We remark that Birkhoff's theorem states that the set $S_n(R)$ forms a convex polyhedron with permutation matrices of order n as vertices (see [10, p. 1089], [11], and [14]).
- D) Let us also mention a characterization of an arbitrary logic with the help of *orthomodular fans*, i.e., triples $\{(L \setminus \{0, 1\}), ', G\}$ where L is a logic, the unary operation $': (L \setminus \{0, 1\}) \rightarrow (L \setminus \{0, 1\})$ is a restriction of the orthocomplementation on the set $L \setminus \{0, 1\}$ and G is the set

$$G = \{(p, q, r) \in (L \setminus \{0, 1\})^3 : p + q + r = 1\}.$$

A characterization of logics by fans and further details are given by P. Ovchinnikov in the paper [13].

E) As introduced above (see Example 1), the logic $U(\mathcal{M}_{22}(R))$ is an orthomodular lattice. In contrast to this, the logic $U(\mathcal{M}_{nn}(R))$ with $n \geq 3$ is not a lattice. This fact follows immediately from [12, Prop. 1]. Moreover, notice that all blocks of the logic $U(\mathcal{M}_{22}(R))$ have only the following form: $\mathcal{B}_A = \{0, E, A, E - A\}$, $A \in U(\mathcal{M}_{22}(R))$.

Acknowledgements. The author would like to Mirko Navara for help in the preparation of this paper.

REFERENCES

- [1] Beltrametti, Cassinelli: The Logic of Quantum Mechanics. Addison Wesley, Massachusetts (1981).
- [2] Beran, L.: Orthomodular Lattices, Algebraic Approach. Academia, Prague, Reidel, Dordrecht (1984).
- [3] Birkhoff, G.: Lattice Theory. Amer. Math. Soc., Providence, Rhode Island (1973).
- [4] Davis, P.: Circulant Matrices. London (1970).
- [5] Flachsmeier, J.: Note on orthocomplemented posets. Proc. Conf. Topology and Measure, Greifswald (1982), 65–75.
- [6] Kalinin, V. V.: Orthomodular partially ordered sets with dimension (in Russian). Algebra and Logics 15 (1976), No. 5, 535–557.
- [7] Katrnoška, F.: Logics and States of Physical Systems (in Czech). Thesis, Czech Technical University, Prague (1980).
- [8] Katrnoška, F.: Logics of idempotents of rings. Topology, Measure and Fractals, Vol. 66, Akad. Verlag, Berlin (1992), 131–136.
- [9] Katrnoška, F.: On some rings and their M -Bases of idempotents. Proc. of 3rd Scf. Colloq. Prague (2001), 140–149.
- [10] Louck, J.D.: Doubly stochastic matrices in quantum mechanics. Found. Phys. 27 (1997), 1085–1104.
- [11] Marcus, M., Minc, H.: A Survey of Matrix Theory and Matrix Inequalities. Allyn and Bacon, Inc., Boston, 1964.
- [12] Mushtari, D.: Logics of projectors in Banach spaces (in Russian). Izvestija Vuzov (Mat.) 8 (1989), 44–52.
- [13] Ovchinnikov, P.: Another combinatorial characterization of orthomodular posets. Kazan Tracts in Math. Vol. 4. Measures on Projections and Orthomodular Posets. Kazan Math. Soc. (1998), 87–94.
- [14] Svozil, K.: Quantum Logic. Springer, Berlin/Heidelberg, 1998.
- [15] Ward, M., Dilworth, R.P.: Residuated Lattices. *Trans. Amer. Math. Soc.* 45 (1939), 335–354.

INSTITUTE OF CHEMICAL TECHNOLOGY

DEPARTMENT OF MATHEMATICS

TECHNICKÁ 5, 166 28 PRAGUE 6, CZECH REPUBLIC