International Journal of Theoretical Physics, Vol. 34, No. 8, 1995

Orthomodular Posets of Idempotents in Finite Rings of Matrices

Jürgen Flachsmeyer[1]

Received October 24, 1994

The idempotents, resp. Hermitian idempotents, of a unital ring, resp. involutive unital ring, form an orthomodular poset. We study these orthomodular posets for rings of matrices over the integers modulo m or over Galois fields. In analogy to the Hilbert space situation we look for idempotent matrices (projections) corresponding to splitting subspaces of finite-dimensional vector spaces.

1. IDEMPOTENTS OF A UNITAL RING

For a real or complex Hilbert space $\mathbf{H}$ let $Hilb(\mathbf{H})$ be the corresponding complete atomistic ortholattice of all Hilbert subspaces $E \subseteq \mathbf{H}$. In a canonical way this lattice is isomorphic to the lattice of all Hermitian idempotents of the Banach algebra $\mathbf{B(H)}$ of all bounded (= continuous) linear operators A: $\mathbf{H} \to \mathbf{H}$. We have

$$Hilb(\mathbf{H}) \leftrightarrow Proj(\mathbf{H})$$

$$E\ (= imP) \leftrightarrow P\colon \mathbf{H} \to \mathbf{H}$$

whereby $P \in \mathbf{B(H)}$ with $P^2 = P$ and $P = P^*$. Instead of the algebra $\mathbf{B(H)}$ one can start with any involutive unital ring $\mathcal{R}^*$ (Birkhoff, 1967) or even with any arbitrary unital ring $\mathcal{R}$ (Flachsmeyer, 1982; Katrnoška, 1990) to get by their Hermitian idempotents, respectively idempotents, an orthomodular poset. Let us recall the statements in full.

Theorem A. 1.1. Let $\mathcal{R}$ be an arbitrary ring with unit. Then the set $Idem(\mathcal{R}) = \{x\colon x \in \mathcal{R}, x^2 = x\}$ of all idempotents is an orthomodular poset with respect to the order

$$x \le y\colon \Leftrightarrow x \cdot y = y \cdot x = x$$

[1] FB Mathematik/Informatik, Ernst-Moritz-Arndt-Universität, 17489 Greifswald, Germany.

0020-7748/95/0800-1359$07.50/0

and the orthocomplement

$$x^{\perp} = 1 - x$$

1.2. If $x \leq y$, then $inf(y, x^{\perp})$ exists and $inf(y, x^{\perp}) = y - x$.

1.3. Orthogonality in $Idem(\mathcal{R})$ means

$$x \perp y \Leftrightarrow x \cdot y = y \cdot x = 0$$

1.4. If $x \perp y$, then $sup(x, y)$ exists and $sup(x, y) = x + y$.

2.1. If * is a ring involution on $\mathcal{R}$, then the set $HermIdem(\mathcal{R}) = \{x\colon x \in \mathcal{R}, x^2 = x \text{ and } x^* = x\}$ of all Hermitian idempotents is an orthomodular poset with respect to the above-mentioned order and the orthocomplemention.

2.2. For $x, y \in HermIdem(\mathcal{R})$ and $x \leq y$ the difference $y - x$ belongs to $HermIdem(\mathcal{R})$ and is the infimum of y and $x^{\perp}$.

2.3. If $x \perp y$, then $x + y$ belongs to $HermIdem(\mathcal{R})$ and is the supremum of x and y.

Remark. In generalization of 1.2 and 1.4 the following properties in $HermIdem(\mathcal{R})$ are fulfilled:

1.5. If x, y commute, i.e., $xy = yx$, then the infimum and the supremum exist and

$$\inf(x, y) = xy$$

$$\sup(x, y) = x + y - xy$$

Corollary. For a commutative unital ring $\mathcal{R}$ the orthomodular poset $Idem(\mathcal{R})$ is a Boolean algebra.

The argumentation is as follows. By the commutativity $Idem(\mathcal{R})$ is an ortholattice and it is also distributive. Namely,

$$x \wedge (y \vee z) = x(y \vee z) = x(y + z - yz) = xy + xz - xyz$$

$$(x \wedge y) \vee (x \wedge z) = xy \vee yz = xy + yz - xyz$$

2. THE BOOLEAN ALGEBRA OF IDEMPOTENTS OF THE RING $\mathbf{Z}_m$

Let $\mathbf{Z}_m$ be the ring of the rests $0, 1, 2, \ldots, m - 1$ of the integers *mod* m. Now, $\mathbf{Z}_m$ is a commutative unital ring, therefore $Idem(\mathbf{Z}_m)$ has to be a finite Boolean algebra. How does one get it?

Theorem 1. 1. The Boolean algebra of all idempotents of the ring $\mathbf{Z}_m$ is isomorphic to $\mathbf{2}^k$, where k is the number of the distinct prime factors of m:

$$Idem(\mathbf{Z}_m) \simeq \mathbf{2}^k, \qquad m = p_1^{\nu_1} p_2^{\nu_2} \cdots p_k^{\nu_k}, \quad 2 \leq p_1 < p_2 < \cdots < p_k \leq m$$

where p_ν are primes.

2. One obtains the nontrivial complemented pairs of $Idem(\mathbf{Z}_m)$ as follows:

Let A, B be any nontrivial splitting of the set $\{1, 2, \ldots, k\}$, i.e., $A \neq \emptyset$, $B \neq \emptyset$, $A \cap B = \emptyset$, $A \cup B = \{1, 2, \ldots, k\}$.

Define $a := \Pi\, p_\alpha^{\nu_\alpha}$ $(\alpha \in A)$, $b := \Pi\, p_\beta^{\nu_\beta}$ $(\beta \in B)$.

Then a, b are relatively prime, $(a, b) = 1$; therefore there exist integers u, v with $a \cdot u + b \cdot v = 1$.

By $\bar{a} := au \bmod m$ and $\bar{b} := bv \bmod m$ one has a complemented pair $\bar{a}$, $\bar{b}$ in $Idem(\mathbf{Z}_m)$.

Proof. For $\bar{a}$, $\bar{b}$ it remains to show that in $Idem(\mathbf{Z}_m)$ the following are satisfied: $\bar{a} \wedge \bar{b} = 0$ and $\bar{a} \vee \bar{b} = 1$. According to 1.5 of the Remark this means

$$\bar{a} \cdot \bar{b} = 0 \qquad \text{and} \qquad \bar{a} + \bar{b} - \bar{a} \cdot \bar{b} = 1 \text{ in } \mathbf{Z}_m$$

But this holds by definition of $\bar{a}$ and $\bar{b}$. ∎

Table I shows the situation for some m.

3. HOW MANY IDEMPOTENT MATRICES EXIST OVER $\mathbf{Z}_m$?

For a given model m and a given format number n we ask for the number of idempotent, resp. Hermitian idempotent, matrices of size $n \times n$ over the basic ring $\mathbf{Z}_m$,

$$card(Idem(Mat(n \times n, \mathbf{Z}_m)))$$

$$card(HermIdem(Mat(n \times n, \mathbf{Z}_m)))$$

We will take the involution in the ring $Mat(n \times n, \mathbf{Z}_m)$ of matrices over $\mathbf{Z}_m$

Table I.

m	2	3	4	5	7	8	9	11	13	16	17	19	23	25	27	29
$Idem(\mathbf{Z}_m)$									1							
									0							

<table>
<tr><td>m</td><td colspan="2">6</td><td colspan="2">10</td><td colspan="2">12</td><td colspan="2">14</td><td colspan="2">20</td><td colspan="2">21</td><td colspan="2">22</td><td colspan="2">24</td><td colspan="2">26</td></tr>
<tr><td>Idem(Z_m)</td><td>3</td><td>4</td><td>5</td><td>6</td><td>4</td><td>9</td><td>7</td><td>8</td><td>5</td><td>16</td><td>7</td><td>15</td><td>11</td><td>12</td><td>9</td><td>16</td><td>13</td><td>14</td></tr>
<tr><td></td><td colspan="2">0</td><td colspan="2">0</td><td colspan="2">0</td><td colspan="2">0</td><td colspan="2">0</td><td colspan="2">0</td><td colspan="2">0</td><td colspan="2">0</td><td colspan="2">0</td></tr>
</table>

m		30			42			60	
$Idem(\mathbf{Z}_m)$		1			1			1	
	16	21	25	7	15	22	16	21	25
	6	10	15	21	28	36	36	40	45
		0			0			0	

Table II.

lot m	$Idem(\mathfrak{R})$ card	$HermIdem(\mathfrak{R})$ card	m	$Idem\mathfrak{R}$ card	$HermIdem(\mathfrak{R})$ card
$n = 2$			$n = 2$		
2	8	4	14	464	40
3	14	6	15	448	36
4	26	6	16	386	18
5	32	6	17	308	18
6	112	24	18	880	56
7	58	10	19	382	22
8	98	10	20	832	36
			$n = 3$		
9	110	14	2	58	10
10	256	24	3	236	20
11	134	14	4	898	34
12	364	36	5	1552	52
13	184	14			

as the matrix transpose: $A \mapsto A^{\top}$. We are far from a general sufficient answer. With the help of computers we counted the list in Table II.

We conclude this section with a few remarks on the order structure of $Idem(\mathfrak{R})$ and $HermIdem(\mathfrak{R})$. Also with the help of computers we identified some of them and obtained their Greechie diagrams.

Remark. 1. $HermIdem(Mat(2 \times 2, \mathbf{Z}_6))$ is the amalgam of two Boolean algebras $\mathbf{2}^4$ with the Greechie diagram given in Fig. 1.

2. In $Idem(Mat(3 \times 3, \mathbf{Z}_2))$ the nontrivial elements are atoms, resp. antiatoms (28 of each sort). This orthoposet fails to be a lattice. The two atoms

$$\begin{pmatrix} 100 \\ 000 \\ 000 \end{pmatrix} \quad \begin{pmatrix} 110 \\ 000 \\ 000 \end{pmatrix}$$

have the following two antiatoms as common successors

$$\begin{pmatrix} 100 \\ 010 \\ 000 \end{pmatrix} \quad \begin{pmatrix} 100 \\ 010 \\ 010 \end{pmatrix}$$

Another argumentation that this orthoposet cannot be a lattice follows from

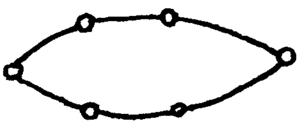

Fig. 1.

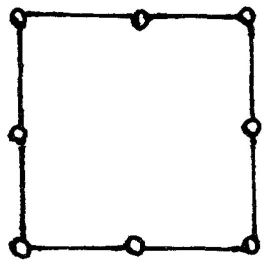

Fig. 2.

Greechie's amalgam theorem (Beran, 1985). *Idem*(*Mat*(3 × 3, $\mathbf{Z}_2$)) consists of 28 copies of the maximal Boolean subalgebra $\mathbf{2}^3$. Each atom is covered by three copies of $\mathbf{2}^3$.

Each maximal Boolean subalgebra belongs to a quadrangles loop with the Greechie diagram shown in Fig. 2. Therefore the lattice structure is not valid. The orthoposet with the shown Greechie diagram is known as Janowitz poset $\mathbf{J}_{18}$ (Janowitz, 1968; Beran, 1985, pp. 148ff).

In Fig. 3 we draw an order diagram of $\mathbf{J}_{18}$ restricting to the 8 atoms and their antiatoms. This shows that the atoms 1 and 5 have the common successors $3^{\perp}$ and $7^{\perp}$, analogously for 3, 7 and $1^{\perp}$, $5^{\perp}$.

4. THE ORTHOMODULAR POSET OF SPLITTING SUBSPACES

Let $\mathbf{F}$ be any commutative field and $\mathbf{V} = \mathbf{F}^n$ the finite-dimensional standard vector space over this field, $n = \dim \mathbf{V}$, $n \geq 1$.

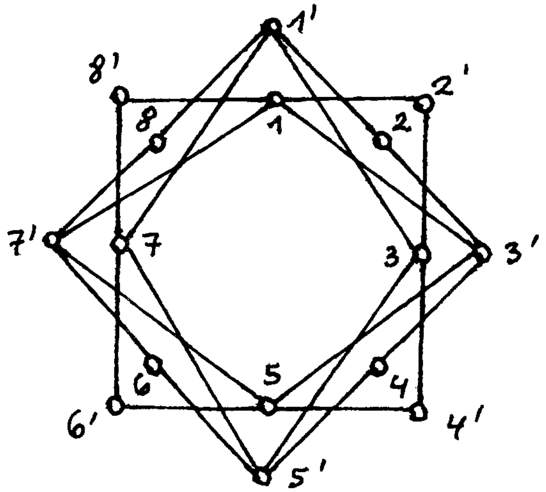

Fig. 3.

The standard inner product $\langle \cdot\ ,\ \cdot \rangle$: $\mathbf{V} \times \mathbf{V} \to \mathbf{F}$ is defined by $\langle x, y \rangle := \sum_{i=1}^{n} x_i \cdot y_i$ for vectors $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n)$ of $\mathbf{V}$. This inner product is a symmetric bilinear form on $\mathbf{V}$. Two vectors are called *orthogonal* (with respect to the standard inner product)

$$x \perp y \text{ iff their inner product is } zero\text{: } \langle x, y \rangle = 0$$

It may be that there are nonzero *isotropic* vectors in $\mathbf{V}$, i.e., $x \perp x$ without $x = 0$. The natural base $b_1 = (1, 0, 0, \ldots, 0), \ldots, b_n = (0, 0, \ldots, 0, 1)$ forms an orthogonal base of $\mathbf{V}$. For any subset $A \subseteq \mathbf{V}$ let

$$A^{\perp} := \{x\colon x \in \mathbf{V} \text{ with } x \perp a \text{ for all } a \in A\}$$

Lemma. The correspondence $A \mapsto A^{\perp}$ in the power set $Pow(\mathbf{V})$ of the vector space V has the following properties.

1. $\emptyset^{\perp} = \mathbf{V} = \{0\}^{\perp}$, $\mathbf{V}^{\perp} = \{0\}$.
2. $A \subseteq B \Rightarrow B^{\perp} \subseteq A^{\perp}$.
3. $A^{\perp}$ is always a linear subspace.
4. $A \subseteq A^{\perp\perp}$; moreover, $A^{\perp\perp} = span\ A$. Every linear subspace F is orthogonal closed: $F^{\perp\perp} = F$.
5. For linear subspaces E, F of $\mathbf{V}$,

$$(E + F)^{\perp} = E^{\perp} \cap F^{\perp} \qquad \text{and} \qquad (E \cap F)^{\perp} = E^{\perp} + F^{\perp}$$

Proof. Properties 1–3 are straightforward.

Ad 4. $A \subseteq A^{\perp\perp}$ is straightforward. $A^{\perp\perp}$ is linear; therefore $spanA \subseteq A^{\perp\perp}$. Now we assume an element $b \in A^{\perp\perp} \setminus spanA$. Take a vector base B of $spanA$. Now, $B \cup \{b\}$ can be extended to a vector base $\overline{B}$ of $\mathbf{V}$. Define a linear functional f: $\mathbf{V} \to \mathbf{F}$ by setting $f(b) = 1$ and $f = 0$ on $\overline{B} \setminus \{b\}$. There is a unique representation vector $y \in \mathbf{V}$ for f, i.e., $f(\cdot) = \langle \cdot, y \rangle$. This y belongs to $(spanA)^{\perp}$ and therefore to $A^{\perp}$. But

$$\langle y, b \rangle = 1 \quad \text{implies } b \text{ not orthogonal to } y, \quad \text{i.e.,} \quad b \notin A^{\perp\perp}$$

By this contradiction it must be that $A^{\perp\perp} = spanA$.

Ad 5. $E \subseteq E + F$ and $F \subseteq E + F$ imply $(E + F)^{\perp} \subseteq E^{\perp} \cap F^{\perp}$.

For the converse let $x \in E^{\perp} \cap F^{\perp}$ and $u \in E$, $v \in F$.

Then $x \perp u$ and $x \perp v$ and therefore $x \perp (u + v)$, i.e., $x \in (E + F)^{\perp}$. Thus $E^{\perp} \cap F^{\perp} \subseteq (E + F)^{\perp}$.

The other equation can be proven by application of $(E + F)^{\perp} = E^{\perp} \cap F^{\perp}$ and the orthogonal closedness of linear subspaces. Namely, $(E \cap F)^{\perp} = (E^{\perp\perp} \cap F^{\perp\perp})^{\perp} = ((E^{\perp} + F^{\perp}))^{\perp\perp} = E^{\perp} + F^{\perp}$. ■

Now we consider the set $Linsub(\mathbf{V})$ of all linear subspaces of the finite-dimensional vector space $\mathbf{V} = \mathbf{F}^n$ over the field $\mathbf{F}$ with respect to the partial order of inclusion and the unary operation $^{\perp}$ of orthogonality. The poset

($Linsub(\mathbf{F}^n)$, $\subseteq$) is a complete atomic modular lattice which is sometimes called the $(n-1)$-dimensional projective geometry $\mathbf{PG}_{n-1}(\mathbf{F})$ over the field $\mathbf{F}$.

One has the following result.

Theorem 2. ($Linsub(\mathbf{F}^n)$, $\subseteq$, $^\perp$), n natural number ≥ 1, is a unit closed SOP (semiorthoposet) in the sense of Gudder (1994) in which the Morgan rules hold:

$$(E \vee F)^\perp = E^\perp \wedge F^\perp$$

$$(E \wedge P)^\perp = E^\perp \vee F^\perp$$

This SOP in general contains strongly inconsistent elements, which means that there can be a linear subspace F for which $F = F^\perp$.

Proof. The first part is the content of the lemma. The supremum $E \vee F$ equals $E + F$ and the infimum $E \wedge F$ equals $E \cap F$. For the existence of strongly inconsistent elements see, for example, the case $\mathbf{F} = GF(2) = \mathbf{Z}_2$. Then $Linsub(\mathbf{F}^2)$ contains only the following three 1-dimensional subspaces:

$$E = \{00, 01\}$$

$$F = \{00, 10\}$$

$$G = \{00, 11\}$$

One has $E^\perp = F$, $F^\perp = E$, and $G = G^\perp$.

The Hasse diagram of $Linsub(\mathbf{F}^2)$ is the same as that of the subgroup lattice of the Klein four-group D_2. ■

Now we consider such linear subspaces F of $\mathbf{V} = \mathbf{F}^n$ which split $\mathbf{V}$ into the sum of F and its orthogonal $F^\perp$, i.e., $\mathbf{V} = F + F^\perp$. In the notation of Gudder these are the *sharp* elements of the SOP $Linsub(\mathbf{F}^n)$. Because of the lemma the splitting property $\mathbf{V} = F + F^\perp$ is equivalent to $F \cap F^\perp = \{0\}$. The equivalence of $\mathbf{V} = F + F^\perp$ and $F \cap F^\perp = \{0\}$ is also a consequence of closedness of the SOP $Linsub(\mathbf{F}^n)$. Let $Splittlinsub(\mathbf{F}^n)$ be the set of all the splitting linear subspaces F of $\mathbf{F}^n$. The following holds for this set.

Theorem 3. ($Splittlinsub(\mathbf{F}^n)$, $\subseteq$, $^\perp$) is an orthomodular poset (OMP) which is isomorphic to $HermIdem(Mat(n \times n, \mathbf{F}))$ by the isomorphism

$$F \leftrightarrow P \quad (\text{projector } P\colon \mathbf{F}^n \to \mathbf{F}^n \text{ with } imP = F, \ker P = F^\perp)$$

($Splittlinsub(\mathbf{F}^n)$, $\subseteq$, $^\perp$) is in general not a sublattice of ($Linsub(\mathbf{F}^n)$, $\subseteq$).

Proof. Let $\mathbf{S} = Splittlinsub(\mathbf{F}^n)$. Then $\{0\}$, $\mathbf{F}^n$ belong to $\mathbf{S}$. Thus $\mathbf{S}$ is with respect to the inclusion a bounded poset and $^\perp\colon \mathbf{S} \to S$ is an orthocomplementation on it. This orthoposet is in the case $\mathbf{F} = GF(2)$ and $\mathbf{V} = \mathbf{F}^3$ not a sublattice of $(Linsub(\mathbf{F}^3), \subseteq)$. Namely the pairs

$$E = \{000, 100\}, \qquad E^{\perp} = \{000, 001, 010, 011\}$$

and

$$F = \{000, 111\}, \qquad F^{\perp} = \{000, 011, 101, 110\}$$

are splitting, but $E^{\perp} \cap F^{\perp} = \{000, 011\}$ is not splitting because $(E^{\perp} \cap F^{\perp})^{\perp} = \{000, 011, 100, 111\}$.

Now we have to argue for the isomorphism between $Splittlinsub(\mathbf{F}^n)$ and $HermIdem(Mat(n \times n, \mathbf{F}))$. Let $(F, F^{\perp})$ be a pair of splitting subspaces. To this pair corresponds a projection pair $(P, Id - P)$, where P is defined by

$$Px = u \text{ iff } x = u + v \qquad \text{with} \qquad u \in F, \quad v \in F^{\perp}$$

P: $\mathbf{F}^n \to \mathbf{F}^n$ belongs to the unital ring $Linop(\mathbf{F}^n)$ of all linear operators on $\mathbf{F}^n$. This ring is endowed with an involution according to the standard scalar product: $Linop \ni A \mapsto A^*$ defined by

$$\langle A^*x, y\rangle = \langle x, Ay\rangle \qquad \text{for all} \quad x, y \in \mathbf{F}^n$$

The considered projection P is a Hermitian idempotent. Conversely, a Her-

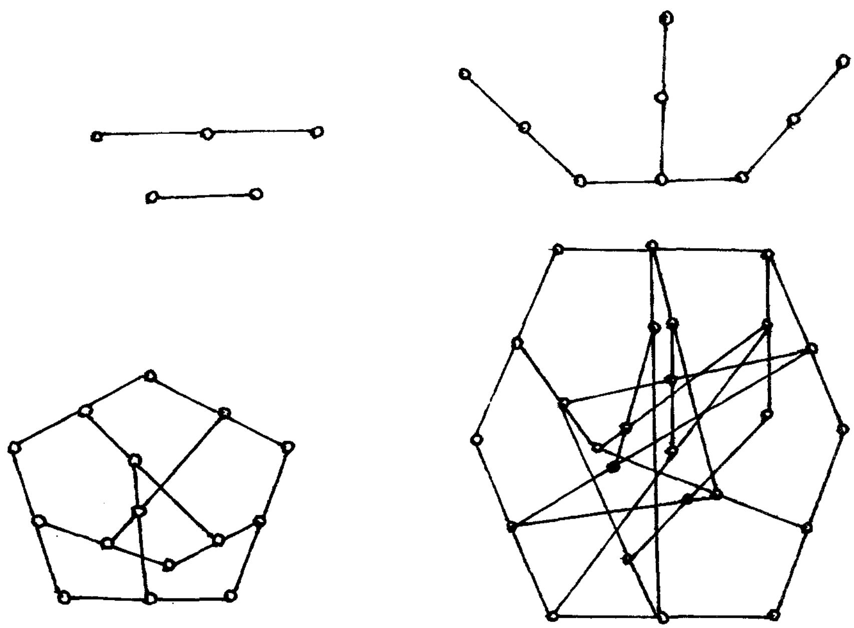

Fig. 4.

mitian idempotent $Q \in Linop(\mathbf{F}^n)$ is determined by a splitting pair $(F, F^{\perp})$. One has only to take $F := imQ$. Then $\ker Q \perp F$ because for $x \in \ker Q$

$$\langle x, Qz \rangle = \langle Q^* x, z \rangle = \langle Qx, z \rangle = 0 \qquad \text{for all} \quad z \in \mathbf{F}^n$$

Thus $\ker Q \subseteq F^{\perp}$. But for $y \in F^{\perp}$ one has $\langle y, Qz \rangle = 0$ for any z. Then $\langle Qy, z \rangle = 0$. This implies $Qy = 0$, i.e., $F^{\perp} \subseteq \ker Q$. Thus $(imQ, \ker Q)$ is an orthocomplemented pair. Moreover it splits, because $x \in imQ \cap \ker Q$ implies $Qx = 0$ and $x = Qz$. Now $Q^2 = Q$ and therefore $Qx = Q^2 z = Qz = x$, i.e., $x = 0$. Via the standard base in $\mathbf{F}^n$ each Hermitian idempotent linear operator corresponds to a Hermitian idempotent matrix over $\mathbf{F}$. ■

Remark. For the first Galois fields $\mathbf{F} = GF(2)$, $GF(3)$, $GF(4)$, $GF(5)$ we identified the orthoposets of $SplittingLinsub(\mathbf{F}^3)$ [$\cong HermIdem(Mat(3 \times 3, \mathbf{F}))$] by the Greechie diagrams given in Fig. 4.

REFERENCES

Beran, L. (1985). *Orthomodular Lattices–Algebraic Approach*, Reidel, Dordrecht.

Birkhoff, G. (1967). *Lattice Theory*, American Mathematical Society, Providence, Rhode Island.

Flachsmeyer, J. (1982). Note on orthocomplemented posets, in *Proceedings Conference on Topology and Measure III*, Part 1 (Greifswald), pp. 65–75.

Greechie, R. J. (1969). An orthomodular poset with a full set of states not embeddable in Hilbert space, *Caribbean Journal of Science and Mathematics*, **1**, 15–26.

Gudder, S. P. (1994). Semi-orthoposets, preprint.

Harding, J. (1994). Decompositions in quantum logic, preprint.

Janowitz, M. F. (1968). A note on generalized orthomodular lattices, *Journal of Natural Sciences and Mathematics*, **8**, 89–94.

Kalmbach, G. (1983). *Orthomodular Lattices*, Academie Press, London.

Katrnoška, F. (1990). Logics of idempotents of rings, in *Proceedings of the Second Winter School on Measure Theory*, Liptovský Ján, pp. 100–104.