Orthogonality and complementation in the lattice of subspaces of a finite vector space

Ivan Chajda and Helmut Länger

Palacký
University
Olomouc

2020

The lattice of subspaces of a given vector space was studied by several authors from various points of view. In particular, for (possibly infinite-dimensional) vector spaces over the field of complex numbers such lattices serve as an algebraic axiomatization of the logic of quantum mechanics. It was shown that such lattices are orthomodular and, if the vector space has finite dimension, even modular. The question arises if something similar holds for vector spaces over finite fields.

Throughout the paper we consider finite-dimensional vector spaces $\mathbf{V}$ over a finite field $\mathrm{GF}(q)$. Assume $\dim \mathbf{V} = m > 1$ and $q = p^n$ for some prime p.

First we derive some conditions which are satisfied by the lattice $\mathbf{L}(\mathbf{V})$ of subspaces of $\mathbf{V}$ together with the unary operation of orthogonality and we obtain a certain relationship between m and q. Then we characterize those $\mathbf{V}$ for which $\mathbf{L}(\mathbf{V})$ is orthomodular. The lattice $\mathbf{L}(\mathbf{V})$ turns out to be orthomodular if and only if orthogonality is a complementation. We show that $\mathbf{L}(\mathbf{V})$ contains Boolean subalgebras of size 2^m and that in case $p \nmid m$, $\mathbf{L}(\mathbf{V})$ contains a $(2^m + 2)$-element (non-Boolean) orthomodular lattice as a subposet.

In the whole paper let $\mathbb{N}$ denote the set of all positive integers. Let V denote the universe of $\mathbf{V}$. Without loss of generality assume $V = (\mathrm{GF}(q))^m$. For $\vec{a} = (a_1, \ldots, a_m), \vec{b} = (b_1, \ldots, b_m) \in V$ and $M \subseteq V$ put

$$\begin{aligned}
\vec{a}\vec{b} &:= \sum_{i=1}^{m} a_i b_i, \\
\vec{a} \perp \vec{b} &:\Leftrightarrow \vec{a}\vec{b} = 0, \\
M^\perp &:= \{\vec{x} \in V \mid \vec{x} \perp \vec{y} \text{ for all } \vec{y} \in M\}, \\
\langle M \rangle &:= \text{ linear subspace of } \mathbf{V} \text{ generated by } M, \\
L(\mathbf{V}) &:= \text{ set of all linear subspaces of } \mathbf{V}, \\
\mathbf{L}(\mathbf{V}) &:= (L(\mathbf{V}), +, \cap, {}^\perp, \{\vec{0}\}, V).
\end{aligned}$$

If not stated explicitly otherwise, whenever we consider a unary operation on $L(\mathbf{V})$, this will be $^\perp$. As usual, by a *basis* of $\mathbf{V}$ we mean a linearly independent generating set of $\mathbf{V}$. It is well-known that any m linearly independent vectors of V form a basis of $\mathbf{V}$. Moreover, it is well-known that $\mathbf{L}(\mathbf{V})$ is a modular lattice with an antitone involution.

Recall that an *orthomodular lattice* is a bounded lattice $(L, \vee, \wedge, ', 0, 1)$ with an antitone involution which is a complementation such that

$$x \leq y \text{ implies } y = x \vee (x' \wedge y)$$

$(x, y \in L)$. The above arguments show that $\mathbf{L}(\mathbf{V})$ is orthomodular if and only if $^{\perp}$ is a complementation. Hence we want to investigate when $^{\perp}$ is a complementation. For $n > 1$ let $\mathbf{M}_n$ denote the modular lattice with the following Hasse diagram (see Fig. 1):

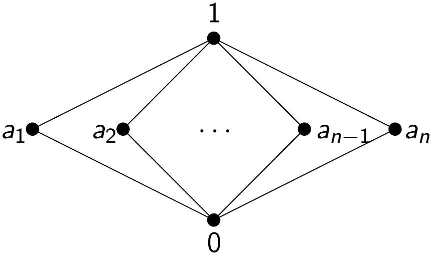

Fig. 1

Theorem 1

The lattice $\mathbf{L(V)}$ *is orthomodular if and only if* V *does not contain a non-trivial self-orthogonal vector.*

Example 1

Assume $(q, m) = (3, 2)$. *Then the Hasse diagram of* $\mathbf{L(V)}$ *looks as follows* $($*see Fig. 2*$)$*:*

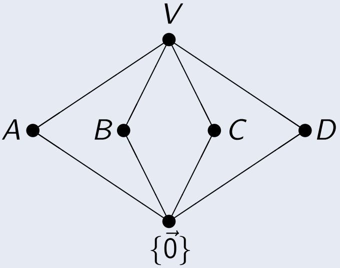

Fig. 2

where

$$\begin{aligned} A &:= \{(0,0),(0,1),(0,2)\}, \\ B &:= \{(0,0),(1,0),(2,0)\}, \\ C &:= \{(0,0),(1,1),(2,2)\}, \\ D &:= \{(0,0),(1,2),(2,1)\}. \end{aligned}$$

Hence $(L(\mathbf{V}),+,\cap) \cong \mathbf{M}_4$. Moreover,

U	A	B	C	D
$U^\perp$	B	A	D	C

and hence $\mathbf{L}(\mathbf{V})$ is orthomodular. This is in accordance with the fact that V has no non-trivial self-orthogonal vector.

On the contrary, we have the following situation.

Example 2

Assume $(q, m) = (5, 2)$. Then $\mathbf{L}(\mathbf{V})$ is not orthomodular since $U^{\perp} = U$ for

$$U = \{(0, 0), (1, 3), (2, 1), (3, 4), (4, 2)\}.$$

This is in accordance with the fact that $(1, 2)$ is a non-trivial self-orthogonal vector of V.

It turns out that V contains a non-trivial self-orthogonal vector in case $m \geq 4$.

Proposition 2

There exists a unique $m(q) \in \{2, 3, 4\}$ such that $\mathbf{L}(\mathbf{V})$ is orthomodular if and only if $m < m(q)$. We have $m(q) = 2$ for even q.

Example 3

Assume $(q, m) = (2, 2)$. *Then the Hasse diagram of* $\mathbf{L}(\mathbf{V})$ *looks as follows* (*see Fig. 3*)*:*

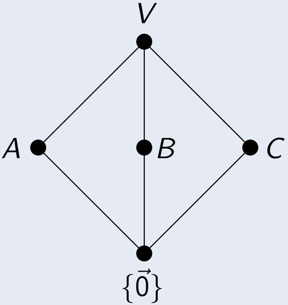

Fig. 3

where

$$A := \{(0,0),(0,1)\},$$
$$B := \{(0,0),(1,0)\},$$
$$C := \{(0,0),(1,1)\}.$$

Hence $(L(\mathbf{V}),+,\cap) \cong \mathbf{M}_3$. Moreover,

U	A	B	C
$U^\perp$	B	A	C

and hence $\mathbf{L}(\mathbf{V})$ is not orthomodular. This is in accordance with the fact that $(1,1)$ is a non-trivial self-orthogonal vector of V.

In some cases, we can find a smaller upper bound for $m(q)$.

Theorem 3

Let $\mathbf{V}$ *be an* m*-dimensional vector space over the field* $\mathrm{GF}(q)$.

(i) *If* $4 \mid p-1$ *then* $m(q)=2$,

(ii) *If* $16 \mid (p+5)(p-1)$ *then* $m(q) \leq 3$.

Our next task is the description of $\mathbf{L}(\mathbf{V}) = (L(\mathbf{V}), +, \cap, \{\vec{0}\}, V)$. We determine the number of d-dimensional linear subspaces of $\mathbf{V}$ as well as the numbers of covers in $\mathbf{L}(\mathbf{V})$. For this reason, we introduce the numbers a_n as follows:
Put $a_0 := 1$ and

$$a_n := \prod_{i=1}^{n} (q^i - 1)$$

for all $n \in \mathbb{N}$.
Recall that a *lattice* with 0 is called *atomistic* if every of its elements is a join of atoms.

Proposition 4

Let $d \in \{0, \ldots, m\}$ *and* $\mathbf{V}$ *be an* m*-dimensional vector space over* $\mathrm{GF}(q)$*. Then the following hold:*

(i) $\mathbf{L}(\mathbf{V})$ *is an atomistic modular lattice,*

(ii) *For every element* $U \in L(\mathbf{V})$*, all maximal chains between* $\{\vec{0}\}$ *and* U *have the same length* (Chain condition),

(iii) $\mathbf{V}$ *has exactly* $a_m/(a_d a_{m-d})$ d*-dimensional linear subspaces.*

(iv) *If* $d < m$ *then every* d*-dimensional linear subspace of* $\mathbf{V}$ *is contained in exactly*

$$\frac{q^{m-d}-1}{q-1} = 1 + q + q^2 + \cdots + q^{m-d-1}$$

$(d+1)$*-dimensional linear subspaces of* $\mathbf{V}$*.*

(v) *If* $d > 0$ *then every* d*-dimensional linear subspace of* $\mathbf{V}$ *contains exactly*

$$\frac{q^{d}-1}{q-1} = 1 + q + q^2 + \cdots + q^{d-1}$$

$(d-1)$*-dimensional linear subspaces of* $\mathbf{V}$*.*

(vi) *The lattice* $\mathbf{L}(\mathbf{V})$ *has exactly*

$$\frac{q^{m}-1}{q-1} = 1 + q + q^2 + \cdots + q^{m-1}$$

atoms, namely the one-dimensional linear subspaces of $\mathbf{V}$*.*

(vii) *If* $m = 2$ *then* $(L(\mathbf{V}), +, \cap) \cong \mathbf{M}_{q+1}$*.*

Denote by $\mathbf{2}^k$ the finite Boolean lattice (Boolean algebra) having just k atoms. In what follows we will check when $\mathbf{L}(\mathbf{V})$ for an m-dimensional vector space $\mathbf{V}$ over $\mathrm{GF}(q)$ contains a subalgebra isomorphic to $\mathbf{2}^k$ for some $k \leq m$.

Theorem 5

Let $\mathbf{V}$ be an m-dimensional vector space over the field $\mathrm{GF}(q)$ for $q = p^n$ with p prime and assume $p \nmid m$. Then there exists a subset S of V such that $(S, \subseteq, {}^{\perp}, \{\vec{0}\}, V)$ is an orthomodular lattice isomorphic to the horizontal sum of the Boolean algebras $\mathbf{2}^m$ and $\mathbf{2}^2$. The presented set S is a subuniverse of $\mathbf{L}(\mathbf{V})$ if and only if $m = 2$.

The following example shows a lattice of the form $\mathbf{L}(\mathbf{V})$ that is not orthomodular, but contains a non-Boolean but orthomodular lattice as a subposet.

Example 4

Assume $(q, m) = (2, 3)$. *Then the Hasse diagram of* $\mathbf{L}(\mathbf{V})$ *looks as follows* (*see Fig. 4*)*:*

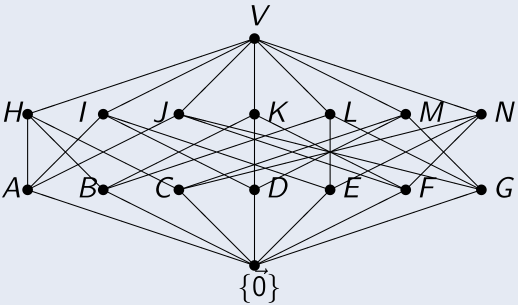

Fig. 4

where

$$
\begin{aligned}
A &:= \{(0,0,0),(0,0,1)\},\\
B &:= \{(0,0,0),(0,1,0)\},\\
C &:= \{(0,0,0),(0,1,1)\},\\
D &:= \{(0,0,0),(1,0,0)\},\\
E &:= \{(0,0,0),(1,0,1)\},\\
F &:= \{(0,0,0),(1,1,0)\},\\
G &:= \{(0,0,0),(1,1,1)\},\\
H &:= \{(0,0,0),(0,0,1),(0,1,0),(0,1,1)\},\\
I &:= \{(0,0,0),(0,0,1),(1,0,0),(1,0,1)\},\\
J &:= \{(0,0,0),(0,0,1),(1,1,0),(1,1,1)\},\\
K &:= \{(0,0,0),(0,1,0),(1,0,0),(1,1,0)\},\\
L &:= \{(0,0,0),(0,1,0),(1,0,1),(1,1,1)\},\\
M &:= \{(0,0,0),(0,1,1),(1,0,0),(1,1,1)\},\\
N &:= \{(0,0,0),(0,1,1),(1,0,1),(1,1,0)\}.
\end{aligned}
$$

Moreover,

U	A	B	C	D	E	F	G
$U^\perp$	K	I	M	H	L	J	N

Since $C + C^\perp = M \neq V$, $^\perp$ is not a complementation and hence $\mathbf{L}(\mathbf{V})$ is not orthomodular. This is in accordance with the fact that $(1, 1, 0)$ is a non-trivial self-orthogonal vector of V. We have $p \nmid m$. Hence we can apply Theorem 5.

The set S of Theorem 5 equals $\{\{\vec{0}\}, A, B, D, G, H, I, K, N, V\}$ and the Hasse diagram of the orthomodular lattice $(S, \subseteq, {}^{\perp}, \{\vec{0}\}, V)$ is visualized in Fig. 5:

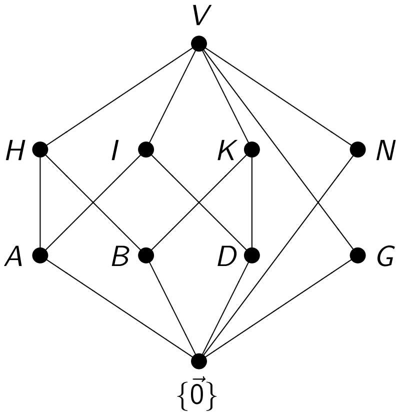

Fig. 5

Since $D + G = M \notin S$, S is not a subuniverse of $\mathbf{L}(\mathbf{V})$. One can easily see that this lattice is the horizontal sum of the Boolean lattices $\mathbf{2}^3$ and $\mathbf{2}^2$.

In the rest, we will investigate the lattice $\mathbf{L}(\mathbf{V})$ for two-dimensional vector spaces $\mathbf{V}$ over $\mathrm{GF}(q)$.

For $n > 1$ let $\mathbf{MO}_n$ denote the modular ortholattice with the following Hasse diagram (see Fig. 6):

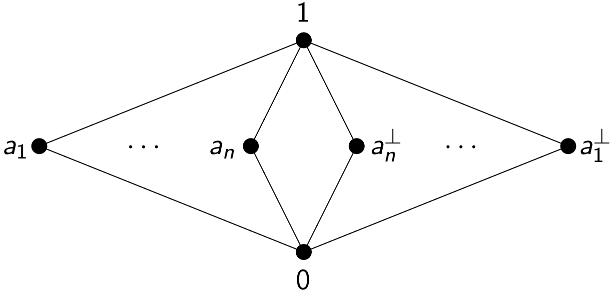

Fig. 6

Proposition 6

Let $\mathbf{V}$ *be a* 2*-dimensional vector space over the field* $\mathrm{GF}(q)$ *for some* $q = p^n$, *without loss of generality assume* $V = (\mathrm{GF}(q))^2$, *and put* $M := \{(x, y) \in \mathbb{N}^2 \mid x \leq y \leq p/2\}$. *Then*

(i) *If there exists some* $(x, y) \in M$ *with* $p \mid (x^2 + y^2)$ *then* $\mathbf{L}(\mathbf{V})$ *is not orthomodular,*

(ii) *if* $q = p$ *then* $\mathbf{L}(\mathbf{V})$ *is orthomodular if and only if* $p \nmid (x^2 + y^2)$ *for all* $(x, y) \in M$.

(iii) *if* $\mathbf{L}(\mathbf{V})$ *is orthomodular then* $\mathbf{L}(\mathbf{V}) \cong \mathbf{MO}_{(q+1)/2}$.

For small q we list all 2-dimensional vector spaces $\mathbf{V}$ over $\mathrm{GF}(q)$ and indicate for which of them $\mathbf{L}(\mathbf{V})$ is orthomodular.

Example 5

For $m = 2$ we have

q	$(L(\mathbf{V}), +, \cap)$	$\mathbf{L}(\mathbf{V})$	*non-trivial self-orthogonal vector*
2	$\cong \mathbf{M}_3$	*not orthomodular*	$(1,1)$
3	$\cong \mathbf{M}_4$	$\cong \mathbf{MO}_2$	
4	$\cong \mathbf{M}_5$	*not orthomodular*	$(1,1)$
5	$\cong \mathbf{M}_6$	*not orthomodular*	$(1,2)$
7	$\cong \mathbf{M}_8$	$\cong \mathbf{MO}_4$	
8	$\cong \mathbf{M}_9$	*not orthomodular*	$(1,1)$
9	$\cong \mathbf{M}_{10}$	*not orthomodular*	$(1,x)$
11	$\cong \mathbf{M}_{12}$	$\cong \mathbf{MO}_6$	
13	$\cong \mathbf{M}_{14}$	*not orthomodular*	$(2,3)$
16	$\cong \mathbf{M}_{17}$	*not orthomodular*	$(1,1)$
17	$\cong \mathbf{M}_{18}$	*not orthomodular*	$(1,4)$

References I

- L. Beran, Orthomodular Lattices. Algebraic Approach. Reidel, Dordrecht 1985. ISBN 90-277-1715-X.
- G. Birkhoff, Lattice Theory. AMS, Providence, R. I., 1979. ISBN 0-8218-1025-1.
- I. Chajda and H. Länger, The lattice of subspaces of a vector space over a finite field. Soft Comput. **23** (2019), 3261–3267.
- I. Chajda and H. Länger, Lattices of subspaces of vector spaces with orthogonality. J. Algebra Appl. (2020), 2050041 (13 pages).
- J.-P. Eckmann and Ph. Ch. Zabey, Impossibility of quantum mechanics in a Hilbert space over a finite field. Helv. Phys. Acta **42** (1969), 420–424.

References II

- R. Giuntini, A. Ledda and F. Paoli, A new view of effects in a Hilbert space. Studia Logica **104** (2016), 1145–1177.
- G. Grätzer, General Lattice Theory. Birkhäuser, Basel 2003. ISBN 978-3-7643-6996-5.
- N. Zierler, On the lattice of closed subspaces of Hilbert space. Pacific J. Math. **19** (1966), 583–586.

The end!

Thanks for your attention!!