Ivan Chajda; Helmut Länger

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

Mathematica Bohemica, Vol. 147 (2022), No. 2, 141–153

Persistent URL: `http://dml.cz/dmlcz/150322`

ORTHOGONALITY AND COMPLEMENTATION IN THE LATTICE OF SUBSPACES OF A FINITE VECTOR SPACE

Ivan Chajda, Olomouc, Helmut Länger, Wien

Received March 3, 2020. Published online April 26, 2021.
Communicated by Sándor Radeleczki

Abstract. We investigate the lattice $\mathbf{L}(\mathbf{V})$ of subspaces of an m-dimensional vector space $\mathbf{V}$ over a finite field $\mathrm{GF}(q)$ with a prime power $q = p^n$ together with the unary operation of orthogonality. It is well-known that this lattice is modular and that the orthogonality is an antitone involution. The lattice $\mathbf{L}(\mathbf{V})$ satisfies the chain condition and we determine the number of covers of its elements, especially the number of its atoms. We characterize when orthogonality is a complementation and hence when $\mathbf{L}(\mathbf{V})$ is orthomodular. For $m > 1$ and $p \nmid m$ we show that $\mathbf{L}(\mathbf{V})$ contains a $(2^m + 2)$-element (non-Boolean) orthomodular lattice as a subposet. Finally, for q being a prime and $m = 2$ we characterize orthomodularity of $\mathbf{L}(\mathbf{V})$ by a simple condition.

Keywords: vector space; lattice of subspaces; finite field; orthomodular lattice; modular lattice; Boolean lattice; complementation

MSC 2020: 06C15, 15A03, 12D15, 06C05

1. Introduction

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 whether something similar holds for vector spaces over finite fields. An attempt in

Support of the research by the Austrian Science Fund (FWF), project I 4579-N, and by the Czech Science Foundation (GAČR), project 20-09869L entitled "The many facets of orthomodularity", as well as by ÖAD, project CZ 02/2019 entitled "Function algebras and ordered structures related to logic and data fusion", and, concerning the first author, by IGA, project PřF 2021 030, is gratefully acknowledged.

DOI: 10.21136/MB.2021.0042-20

this direction was done by Eckmann and Zabey (see [4]). An interesting structure in such a lattice is the sublattice of closed subspaces. Unfortunately, this lattice need not be a sublattice of the lattice of all subspaces and, moreover, this lattice even need not be orthomodular. These facts imply that these lattices in general cannot be used in the logic of quantum mechanics (see [4]). However, subspaces of finite-dimensional vector spaces turn out to be closed. It comes out that in such a case the lattice of subspaces sometimes has a nice structure and hence may be used in the axiomatization of logics similarly as lattices of topologically closed subspaces of Hilbert spaces over the complex numbers are used in the logic of quantum mechanics.

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.

The paper is organized in the following way. 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

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

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, see e.g. Theorems 15 and 16 in [3]. Moreover, this lattice is *paraorthomodular* (see [5] for this concept and for several corresponding results) because it satisfies the condition

$$U \subseteq W \text{ and } U^\perp \cap W = \{\vec{0}\} \text{ imply } U = W,$$

see [3] for the proof. It is well-known that every bounded modular lattice with an antitone involution which is, moreover, a complementation is already orthomodular. Recall from [1] that an *orthomodular lattice* is a bounded lattice $(L, \vee, \wedge, ', 0, 1)$ with an antitone involution which is a complementation such that

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

$(x, y \in L)$. 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 Hasse diagram (see Figure 1).

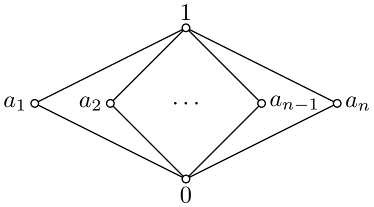

Figure 1.

Theorem 1. *The lattice* $\mathbf{L}(\mathbf{V})$ *is orthomodular if and only if* V *does not contain a nontrivial self-orthogonal vector.*

Proof. We use the fact that $\mathbf{L}(\mathbf{V})$ is orthomodular if and only if $^{\perp}$ is a complementation. Since

$$\dim(U + U^{\perp}) + \dim(U \cap U^{\perp}) = \dim U + \dim U^{\perp} = m$$

for all $U \in L(\mathbf{V})$, we have $U + U^{\perp} = V$ if and only if $U \cap U^{\perp} = \{\vec{0}\}$. Hence $^{\perp}$ is a complementation if and only if $U \cap U^{\perp} = \{\vec{0}\}$ for all $U \in L(\mathbf{V})$. If $^{\perp}$ is not a complementation then there exist some $U \in L(\mathbf{V})$ and some $\vec{a} \in V \setminus \{\vec{0}\}$ with $\vec{a} \in U \cap U^{\perp}$. But then $\vec{a}$ is a nontrivial self-orthogonal vector of V. If, conversely, V possesses a nontrivial self-orthogonal vector $\vec{b}$ then $\vec{b} \neq \vec{0}$ and $\vec{b} \in \langle\{\vec{b}\}\rangle \cap \langle\{\vec{b}\}\rangle^{\perp}$, and hence $\langle\{\vec{b}\}\rangle \cap \langle\{\vec{b}\}\rangle^{\perp} \neq \{\vec{0}\}$, i.e. $^{\perp}$ is not a complementation. □

If V does not contain a nontrivial self-orthogonal vector then $\mathbf{L}(\mathbf{V})$ is orthomodular because $^{\perp}$ is an orthocomplementation and $\mathbf{L}(\mathbf{V})$ is modular. This is the case in the following example.

Example 2. Assume $(q, m) = (3, 2)$. Then the Hasse diagram of $\mathbf{L}(\mathbf{V})$ looks as in Figure 2,

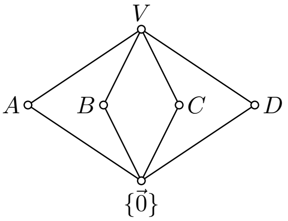

Figure 2.

where

$$A := \{(0,0),(0,1),(0,2)\}, \quad B := \{(0,0),(1,0),(2,0)\},$$
$$C := \{(0,0),(1,1),(2,2)\}, \quad D := \{(0,0),(1,2),(2,1)\}.$$

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 nontrivial self-orthogonal vector.

On the contrary, we have the following situation.

Example 3. 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 nontrivial self-orthogonal vector of V.

It turns out that V contains a nontrivial self-orthogonal vector in case $m \geqslant 4$.

Proposition 4. *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.*

Proof. By Theorem 1, we must show that there exists a unique $m(q) \in \{2,3,4\}$ such that V contains a self-orthogonal vector $\vec{a} = (a_1,\ldots,a_m)$ if and only if $m \geqslant m(q)$. Obviously,

$$m(q) = \min\{k \in \mathbb{N} \colon \text{ there exist } a_1,\ldots,a_k \in (\mathrm{GF}(q)) \setminus \{0\} \text{ with } a_1^2 + \ldots + a_k^2 = 0\}$$

and because of Lagrange's four-squares theorem saying that every non-negative integer is the sum of four squares, there exist $a,b,c,d \in \mathbb{Z}$ with $a^2+b^2+c^2+d^2 = p$. Hence (a,b,c,d) is a nontrivial self-orthogonal vector of V. This shows $m(q) \leqslant 4$. For even q, $(1,1,0,\ldots,0)$ is a nontrivial self-orthogonal vector of V. □

Example 5. Assume $(q, m) = (2, 2)$. Then the Hasse diagram of $\mathbf{L}(\mathbf{V})$ looks as in Figure 3,

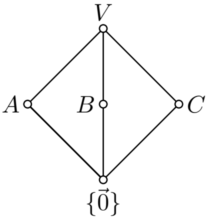

Figure 3.

where

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

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 nontrivial self-orthogonal vector of V.

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

Theorem 6. *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* $m(q) \leqslant 3$.

Proof. In both cases we construct a suitable nontrivial self-orthogonal vector of V.

(i) If $4 \mid p-1$ then

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = 1$$

and hence there exists some $a \in \mathbb{Z}$ with $a^2 \equiv -1 \pmod{p}$. This shows that $(a,1)$ is a nontrivial self-orthogonal vector of V.

(ii) If $16 \mid (p+5)(p-1)$ then

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{(p-1)/2}(-1)^{(p+1)(p-1)/8} = (-1)^{(p+5)(p-1)/8} = 1$$

and hence there exists some $b \in \mathbb{Z}$ with $b^2 \equiv -2 \pmod{p}$. This shows that $(b,1,1)$ is a nontrivial self-orthogonal vector of V. □

For small numbers q we can compute $m(q)$ as follows.

Example 7. The following table shows the values of $m(q)$ for small q and a corresponding nontrivial self-orthogonal vector of minimal dimension.

q	$m(q)$	Nontrivial self-orthogonal vector of minimal dimension
2	2	$(1,1)$
3	3	$(1,1,1)$
4	2	$(1,1)$
5	2	$(1,2)$
7	3	$(1,2,3)$
8	2	$(1,1)$
9	2	$(1,x)$
11	3	$(1,1,3)$
13	2	$(2,3)$
16	2	$(1,1)$
17	2	$(1,4)$

Here we used $\mathrm{GF}(9) \cong \mathbb{Z}_3/(x^2+1)$ and neither $\mathrm{GF}(9) \cong \mathbb{Z}_3/(x^2+x-1)$ nor $\mathrm{GF}(9) \cong \mathbb{Z}_3/(x^2-x-1)$.

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 number of covers in $\mathbf{L}(\mathbf{V})$. For this reason, we introduce the numbers a_n as follows:

Put $a_0 := 1$ and

$$a_n := \prod_{i=1}^{n}(q^i - 1) \quad \text{for all } n \in \mathbb{N}.$$

Recall from [2] that a *lattice* with 0 is called *atomistic* if every of its elements is a join of atoms.

Proposition 8. *Let $d \in \{0,\dots,m\}$ and $\mathbf{V}$ be an m-dimensional vector space over $\mathrm{GF}(q)$. Then the following statements 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*

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

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

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

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

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

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

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

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

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

Proof. Let us recall Theorem 23 in [3]. It says that if $d \leqslant e \leqslant m$ then every d-dimensional subspace of $\mathbf{V}$ is included in $a_{m-d}/(a_{m-e}a_{e-d})$ e-dimensional subspaces of $\mathbf{V}$. Now (i) and (ii) are well-known, (iii) is Theorem 1 in [3], (iv) is the special case $e := d + 1$ of Theorem 23 in [3], (v) is a special case of (iii) when considering the number of $(d - 1)$-dimensional linear subspaces of a d-dimensional vector space over GF(q), (vi) is the special case $d := 0$ of (iv), and (vii) follows from (vi). □

Of course, the lattice $\mathbf{L}(\mathbf{V}) = (L(\mathbf{V}), +, \cap, \{\vec{0}\}, V)$ is complemented in each case even when $^\perp$ is not a complementation.

There is a natural question if conditions (i)–(vii) of Proposition 8 determine an m-dimensional vector space $\mathbf{V}$ over GF(q). In other words, we have the following problem: Let m and n be positive integers, $m > 2$, $q = p^n$ with a prime p and $\mathbf{L} = (L, \vee, \wedge)$ a lattice satisfying the following conditions:

(1) $\mathbf{L}$ is complemented,
(2) $\mathbf{L}$ is modular,
(3) $\mathbf{L}$ is atomistic,
(4) $\mathbf{L}$ has height m,
(5) $\mathbf{L}$ has $1 + q + q^2 + \ldots + q^{m-1}$ atoms,
(6) every element of L of height $d > 0$ covers $1 + q + q^2 + \ldots + q^{d-1}$ elements,
(7) every element of L of height $d < m$ is covered by $1 + q + q^2 + \ldots + q^{m-d-1}$ elements.

Does this imply $\mathbf{L} \cong \mathbf{L}(\mathbf{V}) = (L(\mathbf{V}), +, \cap)$ for some m-dimensional vector space $\mathbf{V}$ over GF(q)?

The positive answer to this question follows from the known results collected in [6], Chapter IV.5. All the concepts used here are taken from [6]. Namely, having a vector space $\mathbf{V} = (V, +, \cdot)$, the lattice $\mathbf{L}(\mathbf{V}) = (L(\mathbf{V}), +, \cap, \{\vec{0}\}, V)$ is known to be isomorphic to $\mathbf{L}(\mathbf{V}')$ where $\mathbf{V}'$ is the projective space derived from $\mathbf{V}$ in the canonical way. However, $\mathbf{V}'$ can be coordinatized and hence $\mathbf{L}(\mathbf{V}) \cong \mathbf{L}(\mathbf{V}')$ is an Arguesian lattice since $\mathbf{V}'$ satisfies Desargues's law. Thus, for $\mathbf{L}$ satisfying (1)–(7) it holds:

(8) $\mathbf{L}$ is a finite simple complemented Arguesian lattice of height greater than 2 (the complementation not necessarily coincides with ${}^{\perp}$).

Conversely, assume $\mathbf{L}$ to satisfy (8). Then $\mathbf{L}$ is modular, of finite height and complemented, i.e. it is a geometric lattice and hence it is coordinatizable over a division ring, that is, over a skew field (see [6], Theorem 15). But this skew field is finite since so is $\mathbf{L}$. Hence $\mathbf{L}$ satisfies (1)–(7) since finite skew fields are fields by Wedderburn's theorem. Altogether, $\mathbf{L}$ is a finite simple complemented modular lattice of height greater than 2 and either its height is greater than 3 or $\mathbf{L}$ is Arguesian.

The following concept will be used in the sequel.

Definition 9. An m-element subset $\{\vec{b}_1,\ldots,\vec{b}_m\}$ of an m-dimensional vector space $\mathbf{V}$ over $\mathrm{GF}(q)$ is called an *orthogonal basis* of $\mathbf{V}$ if

$$\vec{b}_i\vec{b}_j \begin{cases} \neq 0 & \text{if } \ i=j,\\ = 0 & \text{otherwise.}\end{cases}$$

Example 10. Let $\mathbf{V}$ be an m-dimensional vector space over $\mathrm{GF}(q)$. Then

- ▷ $\{(1,0,\ldots,0),(0,1,0,\ldots,0),\ldots,(0,\ldots,0,1)\}$ is an orthogonal basis of $\mathbf{V}$ for arbitrary p,
- ▷ $\{(0,1,\ldots,1),(1,0,1,\ldots,1),\ldots,(1,\ldots,1,0)\}$ is an orthogonal basis of $\mathbf{V}$ if and only if $p \mid m-2$.

Lemma 11. *Let* $B=\{\vec{b}_1,\ldots,\vec{b}_m\}$ *be an orthogonal basis of* $\mathbf{V}$ *and* $I \subseteq \{1,\ldots,m\}$. *Then*

(i) B *is a basis of* $\mathbf{V}$,

(ii) $\langle\{\vec{b}_i\colon\ i\in I\}\rangle^{\perp} = \langle\{\vec{b}_i\colon\ i\in\{1,\ldots,m\}\setminus I\}\rangle$.

Proof. Assume $a_1,\ldots,a_m \in \mathrm{GF}(q)$ and put $\vec{a} := a_1\vec{b}_1+\ldots+a_m\vec{b}_m$.

(i) If $\vec{a}=\vec{0}$ then $a_i\vec{b}_i\vec{b}_i = \vec{a}\vec{b}_i = \vec{0}\vec{b}_i = 0$ for all $i=1,\ldots,m$ and hence $a_1=\ldots=a_m=0$ showing the independence of $\vec{b}_1,\ldots,\vec{b}_m$.

(ii) The following statements are equivalent:

$$\begin{aligned} \vec{a} &\in \langle\{\vec{b}_i\colon\ i\in I\}\rangle^{\perp},\\ \vec{a}\vec{b}_i &= 0 \text{ for all } i\in I,\\ a_i\vec{b}_i\vec{b}_i &= 0 \text{ for all } i\in I,\\ a_i &= 0 \text{ for all } i\in I,\\ \vec{a} &\in \langle\{\vec{b}_i\colon\ i\in\{1,\ldots,m\}\setminus I\}\rangle. \end{aligned}$$

□

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 $k \leqslant m$.

Lemma 12. *Let $\{\vec{b}_1, \dots, \vec{b}_m\}$ be an orthogonal basis of $\mathbf{V}$. Then the subalgebra of $\mathbf{L}(\mathbf{V})$ generated by $\{\langle\{\vec{b}_1\}\rangle, \dots, \langle\{\vec{b}_m\}\rangle\}$ is isomorphic to $\mathbf{2^m}$. Since $\mathbf{2^m}$ contains subalgebras isomorphic to $\mathbf{2^i}$ for every $i = 1, \dots, m$, this is also true for $\mathbf{L}(\mathbf{V})$.*

Proof. Let S denote the subuniverse of $\mathbf{L}(\mathbf{V})$ generated by $\{\langle\{\vec{b}_1\}\rangle, \dots, \langle\{\vec{b}_m\}\rangle\}$. Using Lemma 11 it is easy to see that $S = \{\langle\{\vec{b}_i\colon\ i \in I\}\rangle\colon\ I \subseteq \{1, \dots, m\}\}$ and that $I \mapsto \langle\{\vec{b}_i\colon\ i \in I\}\rangle$ is an isomorphism from

$$(2^{\{1,\dots,m\}}, \cup, \cap, I \mapsto \{1, \dots, m\} \setminus I, \emptyset, \{1, \dots, m\})$$

to $\mathbf{S} := (\mathbf{S}, +, \cap, {}^\perp, \{\vec{\mathbf{0}}\}, \mathbf{V})$. This shows $\mathbf{S} \cong \mathbf{2^m}$. The rest of the proof is clear. □

As shown by Proposition 4, if the dimension of $\mathbf{V}$ is small enough then $\mathbf{L}(\mathbf{V})$ is an orthomodular lattice. Now we show when $\mathbf{L}(\mathbf{V})$ contains an orthomodular lattice isomorphic to a horizontal sum of Boolean algebras also for an arbitrary dimension of $\mathbf{V}$ that is not a multiple of p.

Let $\mathbf{L}_i = (L_i, \vee_i, \wedge_i, {}'^i, 0, 1)$ $(i = 1, 2)$ be nontrivial orthomodular lattices satisfying $L_1 \cap L_2 = \{0, 1\}$. Then their *horizontal sum* $\mathbf{L}_1 + \mathbf{L}_2 = (L, \vee, \wedge, {}', 0, 1)$ is defined by

$$\begin{aligned}
L &:= L_1 \cup L_2,\\
x \vee y &:= \begin{cases} x \vee_i y & \text{if } i \in \{1,2\} \text{ and } x, y \in L_i,\\ 1 & \text{otherwise,}\end{cases}\\
x \wedge y &:= \begin{cases} x \wedge_i y & \text{if } i \in \{1,2\} \text{ and } x, y \in L_i,\\ 0 & \text{otherwise,}\end{cases}\\
x' &:= x'^i \qquad\quad \text{if } i \in \{1,2\} \text{ and } x \in L_i
\end{aligned}$$

$(x, y \in L)$. It is well-known that the horizontal sum of two orthomodular lattices is again an orthomodular lattice.

Theorem 13. *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 $m = 2$.*

Proof. Put

$$N := \{1, \dots, m\}, \quad \vec{e}_i := (0, \dots, 0, 1, 0, \dots, 0) \text{ with 1 at place } i \text{ for all } i \in N,$$
$$U_I := \langle\{\vec{e}_i \colon i \in I\}\rangle \text{ for all } I \subseteq N, \quad W := \langle\{(1, \dots, 1)\}\rangle,$$
$$S := \{U_I \colon I \subseteq N\} \cup \{W, W^\perp\}.$$

From Lemma 12 we have that $\{U_I \colon I \subseteq N\}$ is a subuniverse of $\mathbf{L}(\mathbf{V})$ and $I \mapsto U_I$ is an isomorphism from $(2^N, \cup, \cap, I \mapsto N \setminus I, \emptyset, N)$ to $(\{U_I \colon I \subseteq N\}, +, \cap, {}^\perp, \{\vec{0}\}, V)$. Clearly, $U_I \nsubseteq W$, $W^\perp \nsubseteq U_I$ for all $I \in 2^N \setminus \{\emptyset, N\}$. This shows that in $(S, \subseteq, {}^\perp, \{\vec{0}\}, V)$ the following statements hold for all $I \in 2^N \setminus \{\emptyset, N\}$:

$$W \vee U_I = V, \qquad W \wedge U_I = \{\vec{0}\},$$
$$W^\perp \vee U_I = V, \quad W^\perp \wedge U_I = \{\vec{0}\}.$$

Moreover, $\dim W = 1$ and $\dim W^\perp = m - 1$. Since $p \nmid m$ we have $W \nsubseteq W^\perp$. In case $m = 2$ we have for $i = 1, 2$

$$\begin{aligned} W \vee U_{\{i\}} &= W + U_{\{i\}} = V, \\ W \wedge U_{\{i\}} &= W \cap U_{\{i\}} = \{\vec{0}\}, \\ W^\perp \vee U_{\{i\}} &= W + U_{\{i\}} = V, \\ W^\perp \wedge U_{\{i\}} &= W \cap U_{\{i\}} = \{\vec{0}\} \end{aligned}$$

and hence S is a subuniverse of $\mathbf{L}(\mathbf{V})$. If, however, $m > 2$ then

$$W + U_{\{1\}} \subsetneqq V = W \vee U_{\{1\}}$$

since $\dim(W + U_{\{1\}}) = 2 < m$. This shows that in this case S is not a subuniverse of $\mathbf{L}(\mathbf{V})$. □

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

Example 14. Assume $(q, m) = (2, 3)$. Then the Hasse diagram of $\mathbf{L}(\mathbf{V})$ looks as in Figure 4, where

$$\begin{aligned} A &:= \{(0,0,0), (0,0,1)\}, \\ B &:= \{(0,0,0), (0,1,0)\}, \\ C &:= \{(0,0,0), (0,1,1)\}, \\ D &:= \{(0,0,0), (1,0,0)\}, \\ E &:= \{(0,0,0), (1,0,1)\}, \\ F &:= \{(0,0,0), (1,1,0)\}, \\ G &:= \{(0,0,0), (1,1,1)\}, \end{aligned}$$

$$\begin{aligned} H &:= \{(0,0,0),(0,0,1),(0,1,0),(0,1,1)\}, \\ I &:= \{(0,0,0),(0,0,1),(1,0,0),(1,0,1)\}, \\ J &:= \{(0,0,0),(0,0,1),(1,1,0),(1,1,1)\}, \\ K &:= \{(0,0,0),(0,1,0),(1,0,0),(1,1,0)\}, \\ L &:= \{(0,0,0),(0,1,0),(1,0,1),(1,1,1)\}, \\ M &:= \{(0,0,0),(0,1,1),(1,0,0),(1,1,1)\}, \\ N &:= \{(0,0,0),(0,1,1),(1,0,1),(1,1,0)\}. \end{aligned}$$

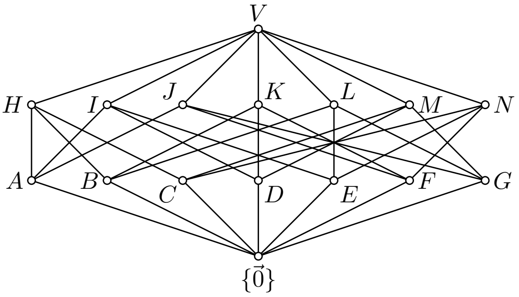

Figure 4.

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 $\mathbf{L(V)}$ is not orthomodular. This is in accordance with the fact that $(1,1,0)$ is a nontrivial self-orthogonal vector of V. We have $p \nmid m$. Hence we can apply Theorem 13. The set S of Theorem 13 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 Figure 5.

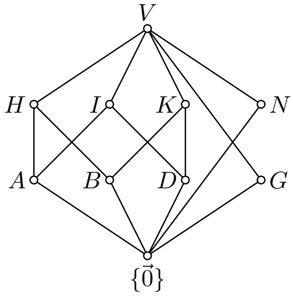

Figure 5.

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

If V does not contain a nontrivial self-orthogonal vector then $\mathbf{L(V)}$ is orthomodular because ${}^\perp$ is an orthocomplementation and $\mathbf{L(V)}$ is modular. This is the case in the following example.

Example 15. In Example 2 we have $p \nmid m$. Hence we can apply Theorem 13. The set S of Theorem 13 coincides with $L(\mathbf{V})$ and is therefore trivially a subuniverse of $\mathbf{L(V)}$.

In the rest of paper, we will investigate the lattice $\mathbf{L(V)}$ for two-dimensional vector spaces $\mathbf{V}$ over $\mathrm{GF}(q)$. For $n > 1$ let $\mathbf{MO_n}$ denote the modular ortholattice with atoms $a_1, a_2, \ldots, a_n, a_1^\perp, a_2^\perp, \ldots, a_n^\perp$ and the Hasse diagram (see Figure 6)

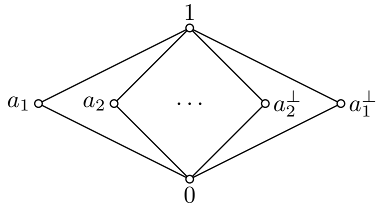

Figure 6.

Proposition 16. *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 $M := \{(x,y) \in \mathbb{N}^2 \colon\ x \leqslant y \leqslant \frac{1}{2}p\}$. Then*

(i) *If there exists some $(x,y) \in M$ with $p \mid (x^2+y^2)$ then $\mathbf{L(V)}$ is not orthomodular.*
(ii) *If $q = p$ then $\mathbf{L(V)}$ is orthomodular if and only if $p \nmid (x^2+y^2)$ for all $(x,y) \in M$.*
(iii) *If $\mathbf{L(V)}$ is orthomodular then $\mathbf{L(V)} \cong \mathbf{MO_{(q+1)/2}}$.*

Proof. (i) If there exists some $(x,y) \in M$ with $p \mid (x^2+y^2)$ then (x,y) is a nontrivial self-orthogonal vector of V and hence $\mathbf{L(V)}$ is not orthomodular according to Theorem 1.

(ii) Assume $q = p$. Then $\mathrm{GF}(q) \cong \mathbb{Z}_p$. According to Theorem 1, $\mathbf{L(V)}$ is orthomodular if and only if V does not contain a nontrivial self-orthogonal vector. Now $(a,b) \in \mathbb{Z}_p^2$ is a nontrivial self-orthogonal vector if and only if $(a,b) \neq (0,0)$ and $a^2+b^2 = 0$ in $\mathbb{Z}_p$. If (a,b) is a nontrivial self-orthogonal vector then $a \neq 0$ and $b \neq 0$ in $\mathbb{Z}_p$. Since modulo p all nonzero elements of $\mathbb{Z}_p$ are given by 1 if $p = 2$ and by $\pm1, \pm2, \pm3, \ldots, \pm\frac{1}{2}(p-1)$ otherwise, all squares of nonzero elements are given modulo p by 1 if $p = 2$ and by $1^2, 2^2, 3^2, \ldots, (\frac{1}{2}(p-1))^2$ otherwise.

(iii) This follows from (vii) of Proposition 8. □

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

Example 17. For $m=2$ we have

q	$(L(\mathbf{V}),+,\cap)$	$\mathbf{L}(\mathbf{V})$	Nontrivial 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	$(1,4)$

Here we used $\mathrm{GF}(9)\cong\mathbb{Z}_3/(x^2+1)$ and neither $\mathrm{GF}(9)\cong\mathbb{Z}_3/(x^2+x-1)$ nor $\mathrm{GF}(9)\cong\mathbb{Z}_3/(x^2-x-1)$.

Acknowledgement. The authors are grateful to Gábor Czédli for his valuable remarks.

References

[1] *L. Beran*: Orthomodular Lattices. Algebraic Approach. Mathematics and Its Applications 18 (East European Series). D. Reidel, Dordrecht, 1985. zbl MR doi

[2] *G. Birkhoff*: Lattice Theory. American Mathematical Society Colloquium Publications 25. AMS, Providence, 1979. zbl MR doi

[3] *I. Chajda, H. Länger*: The lattice of subspaces of a vector space over a finite field. Soft Comput. *23* (2019), 3261–3267. zbl doi

[4] *J.-P. Eckmann, P. C. Zabey*: Impossibility of quantum mechanics in a Hilbert space over a finite field. Helv. Phys. Acta *42* (1969), 420–424. zbl MR

[5] *R. Giuntini, A. Ledda, F. Paoli*: A new view of effects in a Hilbert space. Stud. Log. *104* (2016), 1145–1177. zbl MR doi

[6] *G. Grätzer*: General Lattice Theory. Birkhäuser, Basel, 2003. zbl MR doi

Authors' addresses: *Ivan Chajda*, Palacký University Olomouc, Faculty of Science, Department of Algebra and Geometry, 17. listopadu 12, 771 46 Olomouc, Czech Republic, e-mail: `ivan.chajda@upol.cz`; *Helmut Länger*, TU Wien, Fakultät für Mathematik und Geoinformation, Institut für Diskrete Mathematik und Geometrie, Wiedner Hauptstraße 8-10, 1040 Wien, Austria, and Palacký University Olomouc, Faculty of Science, Department of Algebra and Geometry, 17. listopadu 12, 771 46 Olomouc, Czech Republic, e-mail: `helmut.laenger@tuwien.ac.at`.