BOOLEAN VECTOR SPACES

Stan Gudder
Department of Mathematics
University of Denver
Denver, Colorado 80208
sgudder@math.du.edu

Abstract

This article discusses the basic properties of finite-dimensional Boolean vector spaces and their linear transformations. We first introduce a natural Boolean-valued inner product and discuss orthonormal bases. We show that all bases are orthonormal and have the same cardinality. It is shown that the set of subspaces form an atomistic orthomodular poset. We then demonstrate that an operator that is diagonal relative to one basis is diagonal relative to all bases and that all projections are diagonal. It is proved that an operator is diagonal if and only if any basis consists of eigenvectors of the operator. We characterize extremal states and show that a state is extremal if and only if it is pure. Finally, we introduce tensor products and direct sums of Boolean vector spaces.

1 Introduction

Roughly speaking, a Boolean vector space is a vector space in which the scalars are elements of a Boolean algebra. Although some of our results can be generalized to the infinite dimensional case, in this work we only consider finite-dimensional spaces. There is already a considerable literature on Boolean vector spaces [6, 11, 14, 15, 16], but as far as we know the results presented here are new. There have also been investigations into the related fields of Boolean matrices and matrices over distributive lattices

[1, 2, 3, 7, 8, 9, 10, 12]. These works have applications in graph theory, computer science and fuzzy systems.

Following this introduction, Section 2 presents some preliminary results. We first introduce a natural Boolean-valued inner product and discuss orthonormal bases. One of our surprising results is that all bases are orthonormal. Not so surprising is that all bases have the same cardinality. We then consider linear transformations and operators.

Section 3 discusses subspaces and projections in Boolean vector spaces. It is shown that the set of subspaces forms an atomistic orthomodular poset. Since there is a bijection between subspaces and projections, projections inherit this same structure. Another surprising result is that an operator that is diagonal relative to one basis is diagonal relative to all bases. Also surprising is that all projections are diagonal.

In Section 4 we consider states and diagonality. We first discuss the concepts of eigenvectors and eigenvalues. We then show that an operator is diagonal if and only if every basis consists of eigenvectors of the operator. After defining the concept of a state, we show that a state is extremal if and only if it is pure. We then characterize extremal states.

Finally, Section 5 presents an introduction to tensor products and direct sums of Boolean vector spaces. We leave a deeper study of these concepts to a later investigation.

In this paper, $\mathcal{B}$ will denote an arbitrary but fixed Boolean algebra with least and greatest elements 0 and 1, respectively. The order on $\mathcal{B}$ is denoted by $\leq$ and the meet and join of $a, b \in \mathcal{B}$ are denoted by ab and $a \vee b$, respectively. We write the complement of $a \in \mathcal{B}$ as a' and say that $a, b \in \mathcal{B}$ are **disjoint** if $ab = 0$ or equivalently $a \leq b'$.

We close this section with a motivating example for our work in this field [4, 5]. A **Boolean matrix** is an $n \times m$ matrix with entries in $\mathcal{B}$. We then write $A = [a_{ij}]$ with $a_{ij} \in \mathcal{B}$, $i = 1, \ldots, n$ and $j = 1, \ldots, m$. If A is an $n \times m$ Boolean matrix and B is an $m \times k$ Boolean matrix, we define the product AB to be the $n \times k$ matrix whose (i, j) entry is given by $\vee_{r=1}^{m} a_{ir} b_{rj}$. In particular, we consider elements of $\mathcal{B}^m$ to be $m \times 1$ matrices (column vectors) and for $b = (b_1, \ldots, b_m) \in \mathcal{B}^m$ we have

$$(Ab)_i = \bigvee_{r=1}^{m} a_{ir} b_r$$

$i = 1, \ldots, n$ so that $Ab \in \mathcal{B}^n$. We can thus consider A as a transformation

$A\colon \mathcal{B}^m \to \mathcal{B}^n$. As mentioned earlier, Boolean matrices and their generalization to distributive lattices provide useful tools in various fields such as switching nets, automata theory and finite graph theory.

Our main motivation for studying Boolean vector spaces and matrices comes an analogy to Markov chains [4, 13]. Let G be a finite directed graph whose vertices are labelled $1, 2, \ldots, n$. We think of the vectors of G as sites that a physical system can occupy or possible configurations for a computer. The edges of G designate the allowable transitions between sites or configurations. If there is an edge from vertex i to vertex j, we label it by an element $a_{ji} \in \mathcal{B}$. We think of a_{ji} as the event or proposition that the system (computer) evolves from site (configuration) i to site (configuration) j in one time-step. If there is no edge from i to j, then we set $a_{ji} = 0$. The $n \times n$ Boolean matrix $A = [a_{ij}]$ is the transition matrix in one time-step for the physical system and is determined by the dynamical law for the system. Alternatively, for a computer, A is determined by a program or algorithm and the internal states of the computer. The transition matrix for m time-steps is then naturally given by the matrix product A^m.

Assuming that the system evolves from site i to some specific site j in one time-step, we postulate that $a_{ji}a_{ki} = 0$ for $j \neq k$ and $\vee_{j=1}^{n} a_{ji} = 1$ for $i = 1, 2, \ldots, n$. Thus, each column of A is what we shall later call a consistent unit vector. Suppose that b_i is the event or proposition that the system is at the site i initially. We would then have the consistent unit vector $b = (b_1, \ldots, b_n) \in \mathcal{B}^n$ and $Ab \in \mathcal{B}^n$ describes the system location at one time-step. It is easy to check that Ab is again a consistent unit vector and we interpret $(Ab)_i$ to be the event that the system is at site i at one time-step. In this way, A^m, $m = 1, 2, \ldots$, describes the dynamics of the system and this gives an analog to a traditional Markov chain [13].

2 Preliminary Results

We begin with the definition of a Boolean vector space. Note that our definition is different than that given in [14, 15, 16].

A **Boolean vector space** is a system $(V, \mathcal{B}, +, \cdot\,)$ where V is a nonempty set, $\mathcal{B}$ is a Boolean algebra, $+$ is a binary operation on V and $\cdot$ is a map from $\mathcal{B} \times V$ to V such that

(1) $u + v = v + u$ for all $u, v \in V$

(2) $u + (v + w) = (u + v) + w$ for all $u, v, w \in V$

(3) $a \cdot (b \cdot v) = (ab) \cdot v$ for all $a, b \in \mathcal{B}$ and $v \in V$

(4) $a \cdot (u + v) = a \cdot u + a \cdot v$ for all $a \in \mathcal{B}$ and $u, v \in V$

(5) $(a \vee b) \cdot v = a \cdot v + b \cdot v$ for all $a, b \in \mathcal{B}$ and $v \in V$

(6) there exists $\{v_1, \ldots, v_n\} \subseteq V$ such that every $v \in V$ has a unique representation $v = \sum_{i=1}^{n} a_i \cdot v_i$

We usually denote a Boolean vector space simply by V and we denote the scalar product $a \cdot v$ by av. we call $\{v_1, \ldots, v_n\}$ in (6) a **basis** for V. In general, V has many bases. An example of a Boolean vector space is $L_n(\mathcal{B}) = \mathcal{B}^n$ where

$$\mathcal{B}^n = \mathcal{B} \times \mathcal{B} \times \cdots \times \mathcal{B} \quad (n \text{ factors})$$

In this case we define

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 \vee b_1, \ldots, a_n \vee b_n)$$

and

$$a(b_1, \ldots, b_n) = (ab_1, \ldots, ab_n)$$

The **standard basis** for $L_n(\mathcal{B})$ is $\delta_1 = (1, 0, \ldots, 0), \delta_2 = (0, 1, 0, \ldots, 0), \ldots, \delta_n = (0, \ldots, 0, 1)$. We shall show that any Boolean vector space is isomorphic to $L_n(\mathcal{B})$ for some $n \in \mathbb{N}$.

For the Boolean vector space V we define $u \le v$ if there is a $w \in V$ such that $u + w = v$. We define $0, 1 \in V$ by $0 = \sum 0v_i$ and $1 = \sum 1v_i$. Moreover, if $v = \sum a_i v_i$ we define $v' = \sum a_i' v_i$. If an entity associated with V is independent of the basis of V, we say that the entity is an **invariant**. The next result shows that $0, 1$ and v' are invariants.

Theorem 2.1. *Let V be a Boolean vector space with basis $\{v_1, \ldots, v_n\}$.* (i) *If $u = \sum a_i v_i$ and $v = \sum b_i v_i$, then $u \le v$ if and only if $a_i \le b_i$, $i = 1, \ldots, n$.* (ii) *The relation $\le$ is a partial order relation.* (iii) *$0 \le v \le 1$ for all $v \in V$.* (iv) *For $v \in V$, v' is the smallest element of V satisfying $v + v' = 1$.*

Proof. (i) Let $u \le v$ with $u + w = v$ and let $w = \sum c_i v_i$. Then

$$\sum b_i v_i = \sum a_i v_i + \sum c_i v_i = \sum (a_i \vee c_i) v_i$$

Hence, $b_i = a_i \vee c_i \geq a_i$, $i = 1, \ldots, n$. Conversely, if $a_i \leq b_i$ then $b_i = a_i \vee c_i$ where $c_i = b_i \wedge a_i'$. Letting $w = \sum c_i v_i$ we have that $u + w = v$ so $u \leq v$. (ii) It is clear that $\leq$ is reflexive and transitive. To prove antisymmetry, suppose that $u \leq v$ and $v \leq u$. By (i) we have that $a_i = b_i$, $i = 1, \ldots, n$, so $u = v$. (iii) Since $0 \leq b_i \leq 1$, by (i) we have that $0 \leq v \leq 1$. (iv) Since

$$\sum b_i v_i + \sum b_i' v_i = \sum (b_i \vee b_i') v_i = \sum 1 v_i = 1$$

we have that $v + v' = 1$. If $v + u = 1$ we have $b_i \vee a_i = 1$, $i = 1, \ldots, n$. Hence, $a_i \geq b_i'$, $i = 1, \ldots, n$ so by (i) $v' \leq u$. $\square$

Let V be a Boolean vector space with basis $\{v_1, \ldots, v_n\}$. We define the **inner product** $\langle u, v \rangle = \vee a_i b_i$ where $u = \sum a_i v_i$, $v = \sum b_i v_i$. For example, in $L_n(\mathcal{B})$ we always use the inner product

$$\langle (a_1, \ldots, a_n), (b_1, \ldots, b_n) \rangle = \bigvee a_i b_i$$

The **norm** of $v \in V$ is $\|v\| = \langle v, v \rangle = \vee b_i$. Notice that $\|av\| = a\|v\|$ and

$$\|u + v\| = \|u\| \bigvee \|v\|$$

For Boolean vector spaces V and W a map $T \colon V \to W$ is **linear** if it satisfies $T(av) = aTv$ and $T(u + v) = Tu + Tv$ for all $u, v \in V$ and $a \in \mathcal{B}$. A linear map T is **isometric** if $\langle Tu, Tv \rangle = \langle u, v \rangle$ for all $u, v \in V$. If $T \colon V \to W$ is isometric, then clearly $\|Tv\| = \|v\|$ so T is norm preserving. However, the converse does not hold. For a counterexample, let $T \colon V \to V$ be defined by $Tv = \|v\|\, 1$. Then

$$T(av) = \|av\|\, 1 = a\|v\|\, 1 = aTv$$

and

$$T(u + v) = \|u + v\|\, 1 = \|u\| \bigvee \|v\|\, 1 = \|u\|\, 1 + \|v\|\, 1 = Tu + Tv$$

Hence, T is linear, Moreover,

$$\|Tv\| = |\, \|v\|\, 1\, | = \|v\|$$

so T is norm preserving. However,

$$\langle Tu, Tv \rangle = \langle \|u\|\, 1, \|v\|\, 1 \rangle = \|u\|\, \|v\| \neq \langle u, v \rangle$$

in general. For example, we may have $u, v \neq 0$ with $\langle u, v\rangle = 0$. Thus, T is not isometric.

Notice that for the basis $\{v_1, \ldots, v_n\}$ we have that $\langle v_i, v_j\rangle = \delta_{ij}$ where δ_{ij} is the Kronecker delta. If a set $\{w_1, \ldots, w_m\} \subseteq V$ satisfies $\langle w_i, w_j\rangle = \delta_{ij}$ we call $\{w_1, \ldots, w_m\}$ an **orthonormal set**. In this way, $\{v_1, \ldots, v_n\}$ is an orthonormal basis. Moreover,

$$v = \sum_{i=1}^{n} \langle v, v_i\rangle v_i$$

for all $v \in V$. The proof of the following lemma is straightforward.

Lemma 2.2. *The inner product satisfies the following conditions.* (i) $\langle u, v\rangle = \langle v, u\rangle$. (ii) $\langle u+v, w\rangle = \langle u, w\rangle \vee \langle v, w\rangle$. (iii) $\langle au, v\rangle = a\langle u, v\rangle$. (iv) $\|v\| = \langle v, v\rangle = 0$ *if and only if* $v = 0$. (v) $\langle u, v\rangle = \langle w, v\rangle$ *for all* $v \in V$ *implies that* $u = w$. (vi) $\langle v, v'\rangle = 0$. (vii) $\langle u, v\rangle \leq \|u\|\,\|v\|$.

Thus, the inner product is **symmetric** (i), **linear** ((ii) and (iii)), **definite** (iv), **nondegenerate** (v) and **complementary** (vi). Condition (vii) is called Schwarz's inequality.

Lemma 2.3. *Let V be a Boolean vector space with basis $\{v_1, \ldots, v_n\}$. There exists an isometric linear bijection $\phi\colon V \to L_n(\mathcal{B})$. Moreover, $(V, \leq, ')$ is a Boolean algebra and $\phi\colon V \to \mathcal{B}^n$ is a Boolean algebra isomorphism.*

Proof. Define $\phi\colon V \to L_n(\mathcal{B})$ by $\phi(v) = (a_1, \ldots, a_n)$ where $v = \sum a_i v_i$. It is clear that ϕ is an isometric, linear bijection. It follows from Theorem 2.1 (i) that ϕ and ϕ^{-1} preserve order. We conclude that $(V, \leq, ')$ is a Boolean algebra and that $\phi\colon V \to \mathcal{B}^n$ is a Boolean isomorphism. $\square$

Theorem 2.4. *If V is a Boolean vector space, then all bases for V are orthonormal and have the same cardinality. Moreover, the inner product is an invariant.*

Proof. Let $\{u_1, \ldots, u_m\}$ and $\{v_1, \ldots, v_n\}$ be bases for V and let $\phi_1\colon V \to L_m(\mathcal{B})$ and $\phi_2\colon V \to L_n(\mathcal{B})$ be the corresponding isometric, linear bijections given by Lemma 2.3. Then $\phi_2 \circ \phi_1^{-1}\colon L_m(\mathcal{B}) \to L_n(\mathcal{B})$ is a linear bijection. It follows from [5] that $m = n$ and that $\phi_2 \circ \phi_1^{-1}$ is isometric. Let $\langle u, v\rangle_i$, $i = 1, 2$, be the inner products relative to $\{u_1, \dots, u_n\}$ and $\{v_1, \dots, v_n\}$, respectively. We then have

$$\begin{aligned} \langle u, v \rangle_1 &= \langle \phi_1(u), \phi_1(v) \rangle = \left\langle \phi_2 \circ \phi_1^{-1} \left[\phi_1(u)\right], \phi_2 \circ \phi_1^{-1} \left[\phi_1(v)\right] \right\rangle \\ &= \langle \phi_2(u), \phi_2(v) \rangle = \langle u, v \rangle_2 \end{aligned}$$

Hence the inner product is an invariant. Denoting this invariant inner product by $\langle u, v \rangle$, again we have

$$\langle u_i, u_j \rangle = \langle u_i, u_j \rangle_1 = \delta_{ij}$$

Therefore, all bases are orthonormal with respect to this invariant inner product. $\square$

Lemma 2.5. *Let V and W be Boolean vector spaces over the same Boolean algebra $\mathcal{B}$.* (i) *If $f \colon V \to \mathcal{B}$ is a linear functional, then there exists a unique $v \in V$ such that $f(u) = \langle v, u \rangle$ for all $u \in V$.* (ii) *If $T \colon V \to W$ is a linear map, there exists a unique linear map $T^* \colon W \to V$ such that*

$$\langle Tv, w \rangle = \langle v, T^* w \rangle$$

for all $v \in V$, $w \in W$.

Proof. (i) Uniqueness follows from the nondegeneracy of the inner product. Let $\{v_1, \dots, v_n\}$ be a basis for V. Since $u = \sum \langle v_i, u \rangle v_i$ we have

$$f(u) = f\left(\sum \langle v_i, u \rangle v_i\right) = \bigvee \langle v_i, u \rangle f(v_i) = \left\langle \sum f(v_i) v_i, u \right\rangle$$

Letting $v = \sum f(v_i) v_i$ completes the proof. (ii) Again, uniqueness follows from the nondegeneracy of the inner product. For a fixed $w \in W$, the map $v \mapsto \langle Tv, w \rangle$ is a linear functional on V. By (i) there exists a unique $w^* \in V$ such that $\langle Tv, w \rangle = \langle v, w^* \rangle$ for all $v \in V$. Define $T^* \colon W \to V$ by $T^* w = w^*$. It is easy to check that T^* is linear. $\square$

We call T^* in Lemma 2.5 (ii) the **adjoint** of T. A linear map $T \colon V \to V$ is called an **operator**. It is easy to check that an operator is isometric if and only if $T^* T = I$ the identity map. A map $F \colon V \times V \to \mathcal{B}$ is **bilinear** if it is linear in both arguments.

Lemma 2.6. *If $F \colon V \times V \to \mathcal{B}$ is bilinear, there exists a unique operator T on V such that $F(u, v) = \langle Tu, v \rangle$ for all $u, v \in V$. Moreover, F is symmetric if and only if $T = T^*$.*

Proof. As before, uniqueness follows from the nondegenercy of the inner product. Since $u \mapsto F(v,u)$ is linear, by Lemma 2.5 (i) there exists a unique $w \in V$ such that $F(v,u) = \langle w,u\rangle$ for all $u \in V$. Define $T\colon V \to V$ by $Tv = w$. Now T is linear because

$$\langle T(av),u\rangle = F(av,u) = aF(v,u) = a\langle Tv,u\rangle = \langle aTv,u\rangle$$

Hence, $T(av) = aTv$ for every $a \in \mathcal{B}$, $v \in V$. Also,

$$\begin{aligned}\langle T(v_1+v_2),u\rangle &= F(v_1+v_2,u) = F(v_1,u)\bigvee F(v_2,u)\\ &= \langle Tv_1,u\rangle \bigvee \langle Tv_2,u\rangle = \langle Tv_1+Tv_2,u\rangle\end{aligned}$$

Hence, $T(v_1+v_2) = Tv_1 + Tv_2$ for all $v_1, v_2 \in V$. Finally, F is symmetric if and only if

$$\langle Tu,v\rangle = \langle Tv,u\rangle = \langle v,T^*u\rangle = \langle T^*u,v\rangle$$

for all $u,v \in V$. This is equivalent to $T = T^*$. □

An operator T is **definite** if $\langle Tv,v\rangle = 0$ implies that $v = 0$. An operator T is **complementary** if $\langle Tv,v'\rangle = 0$ for all $v \in V$

Lemma 2.7. *Let $T\colon V \to V$ be an operator.* (i) *T is definite if and only if $\langle Tv,v\rangle = \|v\|$ for every $v \in V$.* (ii) *T is complementary if and only if $\langle Tu,v\rangle = 0$ whenever $\langle u,v\rangle = 0$.*

Proof. (i) It is clear that $\langle Tv,v\rangle = \|v\|$ implies T is definite. Conversely, suppose T is definite and $\langle Tv,v\rangle \neq \|v\|$ for some $v \in V$. By Schwarz's inequality we have that

$$\langle Tv,v\rangle \le \|Tv\|\,\|v\| \le \|v\|$$

Since $\langle Tv,v\rangle < \|v\|$, there exists an $a \in \mathcal{B}$ such that $a \neq 0$, $\langle Tv,v\rangle \vee a = \|v\|$ and $a\langle Tv,v\rangle = 0$. Since T is definite and $\langle T(av),av\rangle = 0$, we conclude that $av = 0$. But this contradicts the fact that $\|av\| = a\|v\| = a \neq 0$. (ii) If $\langle Tu,v\rangle = 0$ whenever $\langle u,v\rangle = 0$ then T is complementary because $\langle v,v'\rangle = 0$. Conversely, suppose T is complementary and $\langle u,v\rangle = 0$. Let $\{v_1,\ldots,v_n\}$ be a basis for V with $u = \sum a_iv_i$ and $v = \sum b_iv_i$. Then $\vee a_ib_i = \langle u,v\rangle = 0$ so $b_i \le a_i'$, $i = 1,\ldots,n$. Hence, $v \le u'$ and there exists a $w \in V$ such that $v + w = u'$. We then have

$$\langle Tu,v\rangle \le \langle Tu,v\rangle + \langle Tu,w\rangle = \langle Tu,u'\rangle = 0$$

Thus, $\langle Tu,v\rangle = 0$. □

Corollary 2.8. *An operator $T\colon V \to V$ is definite and complementary if and only if $T = I$ the identity operator.*

Proof. It is clear that I is definite and complementary. Conversely, suppose that T is definite and complementary. Since V is a Boolean algebra, for $u, v \in V$ there exist mutually disjoint and hence mutually orthogonal elements $u_1, v_1, v \in V$ such that $u = u_1 + w$, $v = v_1 + w$. Thus

$$\begin{aligned}\langle Tu, v\rangle &= \langle Tu_1, v_1\rangle \bigvee \langle Tw, v_1\rangle \bigvee \langle Tu_1, w\rangle \bigvee \langle Tw, w\rangle \\ &= \langle Tw, w\rangle = \|w\| = \langle w, w\rangle = \langle u, v\rangle\end{aligned}$$

We conclude that $Tu = u$ for all $u \in V$ so that $T = I$. $\square$

The next result shows that a subset of the conditions listed in Lemma 2.2 characterize the inner product.

Theorem 2.9. *A map $F\colon V \times V \to \mathcal{B}$ coincides with the inner product if and only if F is bilinear, definite and complementary.*

Proof. Applying Lemma 2.2, the inner product is bilinear, definite and complementary. Conversely, suppose that $F\colon V \times V \to \mathcal{B}$ is a definite, complementary bilinear form. By Lemma 2.6, there exists an operator $T\colon V \to V$ such that $F(u, v) = \langle Tu, v\rangle$ for all $u, v \in V$. It follows that T is definite and complementary. Applying Corollary 2.8, we have $T = I$. Hence, $f(u, v) = \langle u, v\rangle$. $\square$

We can also characterize the norm on V.

Theorem 2.10. *A map $f\colon V \to \mathcal{B}$ coincides with the norm if and only if f is linear and satisfies $f(v_i) = 1$, $i = 1, \ldots, n$, for some basis $\{v_1, \ldots, v_n\}$*

Proof. Clearly, the norm is linear and satisfies the given condition. Conversely, suppose $f\colon V \to \mathcal{B}$ is linear and satisfies the condition. By Lemma 2.5 (i) there exists a $v \in V$ such that $f(u) = \langle v, u\rangle$ for all $u \in V$. We then have

$$\langle v, v_i\rangle = f(v_i) = 1, \quad i = 1, \ldots, m$$

Hence, $v = 1$ so that $f(u) = \langle 1, u\rangle = \|u\|$ for all $u \in V$. $\square$

We now give another simple characterization of the norm.

Lemma 2.11. *The norm $\|v\|$ is the unique $a \in \mathcal{B}$ such that $v = au$ for some u with $\|u\| = 1$.*

Proof. To show that a is unique, we have

$$a = a\|u\| = \|au\| = \|v\|$$

To show that u exists, let $\{v_1, \ldots, v_n\}$ be a basis with $v = \sum a_i v_i$. Define u by

$$u = a_1 v_1 + \cdots + a_{n-1} v_{n-1} + \left(a_n \bigvee \|v\|'\right) v_n$$

We then have that $\|u\| = 1$ and $v = \|v\|u$. □

Although, the vector u in Lemma 2.11 is not unique, it does satisfy $v \leq u \leq v + \|v\|'1$ and any u satisfying these inequalities will suffice.

3 Subspaces and Projections

In the previous section we saw that all bases of a Boolean vector space have the same cardinality. We call this cardinality the **dimension** of the space. If a Boolean vector space V has dimension n, we can construct Boolean vector spaces of any lower dimension inside V. If $\{v_1, \ldots, v_n\}$ is a basis for V, let $m \leq n$ and define

$$W = \operatorname{span}\{v_1, \ldots, v_m\} = \left\{\sum_{i=1}^{m} a_i v_i \colon a_i \in \mathcal{B}\right\}$$

Then W is a Boolean vector space of dimension m with basis $\{v_1, \ldots, v_m\}$. This is an example of a subspace of V. We shall later give a general definition of a subspace of a Boolean vector space and show that they are essentially of this form.

Theorem 3.1. *Let V be a Boolean vector space with $\dim V = n$. An orthonormal set $\{v_1, \ldots, v_m\} \subseteq V$ is a basis for V if and only if $m = n$.*

Proof. We have already shown that a basis has n elements. Conversely, let $\{v_1, \ldots, v_n\}$ be an orthonormal set in V. By Lemma 2.3, there exists an isometric, linear bijection $\phi \colon V \to L_n(\mathcal{B})$. It follows that $\{\phi(v_1), \ldots, \phi(v_n)\}$ is an orthonormal set in $L_n(\mathcal{B})$ and it is shown in [5] that this set must be a basis for $L_n(\mathcal{B})$. We conclude that $\{v_1, \ldots, v_n\}$ is a basis for V. □

A vector $v \in V$ is **consistent** if there exists a basis $\{v_1, \ldots, v_n\}$ for V such that $\langle v, v_i\rangle\langle v, v_j\rangle = 0$, $i \neq j$. A subset of V is **consistent** if all of its elements are consistent. It is clear that a basis for V is consistent.

Lemma 3.2. *Consistency is an invariant.*

Proof. Suppose v is consistent and $\langle v, v_i\rangle\langle v, v_j\rangle = 0$, $i \neq j$, for a basis $\{v_1, \ldots, v_n\}$. If $\{w_1, \ldots, w_n\}$ is another basis we have for $i \neq j$ that

$$\begin{aligned}
\langle v, w_i\rangle\langle v, w_j\rangle &= \left\langle v, \sum_k \langle w_i, v_k\rangle v_k \right\rangle \left\langle v, \sum_r \langle w_j, v_r\rangle v_r \right\rangle \\
&= \bigvee_k \langle w_i, v_k\rangle\langle v, v_k\rangle \bigvee_r \langle w_j, v_r\rangle\langle v, v_r\rangle \\
&= \bigvee_{k,r} \langle w_i, v_k\rangle\langle w_j, v_r\rangle\langle v, v_k\rangle\langle v, v_r\rangle \\
&= \bigvee_k \langle w_i, v_k\rangle\langle w_j, v_k\rangle\langle v, v_k\rangle \\
&\leq \bigvee_k \langle w_i, v_k\rangle\langle v_k, w_j\rangle \\
&= \left\langle \sum_k \langle w_i, v_k\rangle v_k, w_j \right\rangle = \langle w_i, w_j\rangle = 0 \qquad \square
\end{aligned}$$

Notice that in Lemma 3.2 we have derived the useful **Parseval's identity**. This states that if $\{v_1, \ldots, v_n\}$ is a basis for V then for $u, v \in V$ we have $\vee\langle u, v_i\rangle\langle v_i, v\rangle = \langle u, v\rangle$.

Theorem 3.3. *If $\{u_1, \ldots, u_m\}$ is a consistent orthonormal set in a Boolean vector space V with $\dim V = n$, then $m \leq n$ and $\{u_1, \ldots, u_m\}$ can be extended to a basis for V.*

Proof. Let $\phi\colon V \to L_n(\mathcal{B})$ be the isometric, linear bijection given by Lemma 2.3. Since $\phi(v_i) = \delta_i$, we have for $i \neq j$ that

$$\begin{aligned}
\langle \phi(u_k), \delta_i\rangle\langle \phi(u_k)\delta_j\rangle &= \langle \phi(u_k), \phi(v_i)\rangle\langle \phi(u_k), \phi(v_j)\rangle \\
&= \langle u_k, v_i\rangle\langle u_k, v_j\rangle = 0
\end{aligned}$$

for $k = 1, \dots, m$. It follows that $\{\phi(u_1), \dots, \phi(u_m)\}$ is a consistent orthonormal set in $L_n(\mathcal{B})$. It follows from [5] that $m \leq n$ and that $\{\phi(u_1), \dots, \phi(u_m)\}$ can be extended to a basis for $L_n(\mathcal{B})$. We conclude that $\{u_1, \dots, u_m\}$ can be extended to a basis for V. $\square$

A **subspace** of a Boolean vector space V is a subset of V of the form $\mathcal{M} = \operatorname{span}\{v_1, \dots, v_m\}$ where $\{v_1, \dots, v_m\}$ is a consistent orthonormal set in V. Then $\mathcal{M}$ is a Boolean vector space with the same operations as in V and $\dim \mathcal{M} = m$. Moreover, $\{v_1, \dots, v_m\}$ is a basis for $\mathcal{M}$ that can be extended to a basis for V. By convention, we call $\{0\}$ a subspace of V with basis $\emptyset$.

Example 1. *This example shows that the intersection of two subspaces need not be a subspace. Let $\mathcal{M}$ and $\mathcal{N}$ be the following subspaces of $L_2(\mathcal{B})$.*

$$\mathcal{M} = \{b(1,0) \colon b \in \mathcal{B}\}, \quad \mathcal{N} = \{b(a,a') \colon b \in \mathcal{B}\}$$

where $a \neq 0, 1$. Now $(a,0) = a(a,a')$ so $(a,0) \in \mathcal{M} \cap \mathcal{N}$ and hence, $\mathcal{M} \cap \mathcal{N} \neq \{0\}$ The elements of $\mathcal{M} \cap \mathcal{N}$ have the form $b(a,a')$ where $b \leq a$ so

$$\mathcal{M} \cap \mathcal{N} = \{(b,0) \colon b \leq a\}$$

Hence, $\mathcal{M} \cap \mathcal{N}$ contains no unit vectors so $\mathcal{M} \cap \mathcal{N}$ is not a subspace.

For a subset $\mathcal{M} \subseteq V$ we define

$$\mathcal{M}^\perp = \{v \in V \colon \langle v, u \rangle = 0 \quad \text{for all } u \in \mathcal{M}\}$$

Example 2. *This example shows that $\mathcal{M}^\perp$ need not be a subspace. In $L_2(\mathcal{B})$ let $\mathcal{M} = \{(a,a)\}$ where $a \neq 0, 1$. Then $(c,d) \in \mathcal{M}^\perp$ if and only if $c, d \leq a'$. But then $c \vee d \leq a' < 1$ so $\mathcal{M}^\perp$ contains no unit vectors. Hence, $\mathcal{M}^\perp$ is not a subspace.*

If $\mathcal{M}$, $\mathcal{N}$ are subspaces of V we write $\mathcal{M} \perp \mathcal{N}$ if $\langle u, v \rangle = 0$ for every $u \in \mathcal{M}$, $v \in \mathcal{N}$. Of course, $\mathcal{M} \perp \mathcal{N}$ implies $\mathcal{M} \cap \mathcal{N} = \{0\}$. It is not know whether the converse holds.

We denote the set of subspaces of V by $\mathcal{S}(V)$ and endow $\mathcal{S}(V)$ with the set-inclusion partial order $\subseteq$. We denote the greatest lower bound and least upper bound in $(\mathcal{S}(V), \subseteq)$ by $\mathcal{M} \wedge \mathcal{N}$ and $\mathcal{M} \vee \mathcal{N}$, respectively, when they exist.

Example 3. *The example shows that $\mathcal{M} \wedge \mathcal{N}$ need not exist. Let $\mathcal{M}$, $\mathcal{N}$ be the following subspaces of $L_3(\mathcal{B})$:*

$$\mathcal{M} = \{c(1,0,0) + d(0,1,0) = (c,d,0) \colon c,d \in \mathcal{B}\}$$
$$\mathcal{N} = \{c(a,a',0) + d(a',0,a) \colon c,d \in \mathcal{B}\}$$

where $a \neq 0,1$. Define the subspace

$$\mathcal{M}_1 = \{c(1,0,0) = (c,0,0) \colon c \in \mathcal{B}\}$$
$$\mathcal{N}_1 = \{c(a,a',0) \colon c \in \mathcal{B}\}$$

Now it is clear that $\mathcal{N}_1 \subseteq \mathcal{M}, \mathcal{N}$ and $\mathcal{M}_1 \subseteq \mathcal{M}$. Moreover, since

$$a(a,a',0) + a'(a',0,a) = (1,0,0)$$

we see that $\mathcal{M}_1 \subseteq \mathcal{N}$. Since $\dim(\mathcal{M}_1) = \dim(\mathcal{N}_1) = 1$ and $\dim(\mathcal{M}) = \dim(\mathcal{N}) = 2$ there are no elements of $\mathcal{S}(V)$ strictly between them. Since $\mathcal{M}_1$ and $\mathcal{N}_1$ are incomparable, $\mathcal{M} \wedge \mathcal{N}$ does not exist.

Let $\mathcal{M}$ be a subspace of V with basis $\{v_1, \ldots, v_m\}$. Extend this basis of $\mathcal{M}$ to a basis $\{v_1, \ldots, v_n\}$ of V. It is then clear that $\mathcal{M}^\perp \in \mathcal{S}(V)$ and $\mathcal{M}^\perp = \operatorname{span}\{v_{m+1}, \ldots, v_n\}$. Let $(S, \leq, 0, {}^\perp)$ be a partially ordered set where $0 \leq a$ for all $a \in S$ and ${}^\perp \colon S \to S$. We say that ${}^\perp$ is an **orthocomplementation** on S if $a^{\perp\perp} = a$ for all $a \in S$, $a \leq b$ implies $b^\perp \leq a^\perp$ and $a \wedge a^\perp = 0$ for all $a \in S$. We call $(S, \leq, 0, {}^\perp)$ an **orthomodular poset** if ${}^\perp$ is an orthocomplementation, $a \vee b$ exists whenever $a \leq b^\perp$ and $a \leq b$ implies $b = a \vee (b \wedge a')$. An element $b \in S$ is an **atom** if $b \neq 0$ and $a \leq b$ implies $a = 0$ or $a = b$. We say that $(S, \leq, 0, {}^\perp)$ is **atomistic** if for every $a \in S$ we have

$$a = \bigvee \{b \colon b \leq a, b \text{ an atom}\}$$

Notice that the atoms in $\mathcal{S}(V)$ are the one-dimensional subspaces in $\mathcal{S}(V)$.

Theorem 3.4. *The system $\left(\mathcal{S}(V), \subseteq, \{0\}, {}^\perp\right)$ forms an atomistic orthomodular poset.*

Proof. It is clear that $\mathcal{M} \subseteq \mathcal{N}$ implies $\mathcal{N}^\perp \subseteq \mathcal{M}^\perp$, $\mathcal{M} = \mathcal{M}^{\perp\perp}$ and $\mathcal{M} \wedge \mathcal{M}^\perp = \{0\}$. Now suppose $\mathcal{M} \subseteq \mathcal{N}^\perp$. Let $\{u_1, \ldots, u_m\}$ be a basis for $\mathcal{M}$ and $\{v_1 \ldots, v_n\}$ be a basis for $\mathcal{N}$. Then

$$\{u_1, \ldots, u_m, v_1, \ldots, v_n\}$$

is a consistent orthonormal set and it follows that

$$\mathcal{R} = \operatorname{span}\{u_1, \ldots, u_m, v_1, \ldots, v_n\} \in \mathcal{S}(V)$$

Clearly, $\mathcal{M}, \mathcal{N} \subseteq \mathcal{R}$. Suppose $\mathcal{P} \in \mathcal{S}(V)$ with $\mathcal{M}, \mathcal{N} \subseteq \mathcal{P}$. Then $\{u_1, \ldots, u_m\} = \mathcal{P}$ and $\{v_1, \ldots, v_n\} \subseteq \mathcal{P}$. Hence, $\mathcal{R} \subseteq \mathcal{P}$ so $\mathcal{R} = \mathcal{M} \vee \mathcal{N}$. Next, suppose that $\mathcal{M} \subseteq \mathcal{N}$. Then $\mathcal{M} \subseteq \mathcal{N}^{\perp\perp} = (\mathcal{N}^{\perp})^{\perp}$ so $\mathcal{M} \vee \mathcal{N}^{\perp}$ exists. It follows that $\mathcal{N} \wedge \mathcal{M}^{\perp} = (\mathcal{N}^{\perp} \vee \mathcal{M})^{\perp}$ exists. Since $\mathcal{M} \subseteq \mathcal{M} \vee \mathcal{N}^{\perp} = (\mathcal{N} \wedge \mathcal{M}^{\perp})^{\perp}$, we have that $\mathcal{M} \vee (\mathcal{N} \wedge \mathcal{M}^{\perp})$ exists and $\mathcal{M} \vee (\mathcal{N} \wedge \mathcal{M}^{\perp}) \subseteq \mathcal{N}$. To prove the reverse inclusion, let $\{u_1, \ldots, u_m\}$ be a basis for $\mathcal{M}$. Since $\mathcal{M} \subseteq \mathcal{N}$ and $\mathcal{N}$ is a Boolean vector space we can extend this basis to a basis $\{u_1, \ldots, u_m, u_{m+1}, \ldots, u_n\}$ for $\mathcal{N}$. We now show that $\{u_{m+1} \ldots, u_n\}$ is a basis for $\mathcal{N} \wedge \mathcal{M}^{\perp}$. Since $\{u_{m+1}, \ldots, u_n\} \subseteq \mathcal{N} \wedge \mathcal{M}^{\perp}$, $\operatorname{span}\{u_{m+1}, \ldots, u_n\} \subseteq \mathcal{N} \wedge \mathcal{M}^{\perp}$. Conversely, if $v \in \mathcal{N} \wedge \mathcal{M}^{\perp}$ then

$$v = \sum_{i=1}^{n} \langle v, u_i \rangle u_i = \sum_{i=m+1}^{n} \langle v, u_i \rangle u_i \in \operatorname{span}\{u_{m+1}, \ldots, u_n\}$$

Hence, $\{u_{m+1}, \ldots, u_n\}$ is a basis for $\mathcal{N} \wedge \mathcal{M}^{\perp}$. Applying our previous work in this proof we conclude that

$$\mathcal{M} \vee (\mathcal{N} \wedge \mathcal{M}^{\perp}) = \operatorname{span}\{u_1, \ldots, u_n\} = \mathcal{N}$$

To show that $\mathcal{S}(V)$ is atomistic, let $\mathcal{M} \in \mathcal{S}(V)$. Let $\{v_1 \ldots, v_m\}$ be a basis for $\mathcal{M}$ and let $\widehat{v}_1, \ldots, \widehat{v}_m$ be the one-dimensional subspaces generated by $v_1, \ldots, v_m$, respectively. Then $\widehat{v}_1, \ldots, \widehat{v}_m$ are atoms with $\widehat{v}_i \subseteq \mathcal{M}$, $i = 1, \ldots, m$. If $\mathcal{N} \in \mathcal{S}(V)$ with $\widehat{v}_i \subseteq \mathcal{N}$, $i = 1, \ldots, m$, then $\mathcal{M} \subseteq \mathcal{N}$. Hence, $\mathcal{M} = \vee_{i=1}^{m} \widehat{v}_i$. Now suppose that $\mathcal{R} \in \mathcal{S}(V)$ and $\mathcal{P} \subseteq \mathcal{R}$ for every atom $\mathcal{P} \in \mathcal{S}(V)$ with $\mathcal{P} \subseteq \mathcal{M}$. Then $\widehat{v}_i \subseteq \mathcal{R}$, $i = 1, \ldots, m$, so that $\mathcal{M} \subseteq \mathcal{R}$. Hence,

$$\mathcal{M} = \bigvee \{\mathcal{P} \in \mathcal{S}(V) \colon \mathcal{P} \subseteq \mathcal{M}, \quad \mathcal{P} \text{ an atom}\} \qquad \square$$

Example 4. *If $\mathcal{M}, \mathcal{N} \in \mathcal{S}(V)$ and $\mathcal{M} \cap \mathcal{N} \in \mathcal{S}(V)W$, then clearly $\mathcal{M} \cap \mathcal{N} = \mathcal{M} \wedge \mathcal{N}$. The converse does not hold. That is, if $\mathcal{M} \wedge \mathcal{N}$ exists, then $\mathcal{M} \cap \mathcal{N}$ need not be a subspace. In Example 1, $\mathcal{M} \cap \mathcal{N}$ is not a subspace but $\mathcal{M} \wedge \mathcal{N} = \{0\}$.*

Example 5. *This example shows that the distributive law does not hold in $\mathcal{S}(V)$ even when $\vee$ and $\wedge$ exist. Let $\mathcal{M}, \mathcal{N}, \mathcal{P}$ be the following subspaces in $L_2(\mathcal{B})$:*

$$\mathcal{M} = \{b(1,0) \colon b \in \mathcal{B}\}, \quad \mathcal{N} = \{b(0,1) \colon b \in \mathcal{B}\}, \quad \mathcal{P} = \{b(a,a') \colon b \in \mathcal{B}\}$$

where $a \neq 0, 1$. Then $\mathcal{M} \wedge \mathcal{P} = \mathcal{N} \wedge \mathcal{P} = \{0\}$ and $\mathcal{M} \vee \mathcal{N} = \mathcal{S}(V)$. Hence,

$$\mathcal{P} \wedge (\mathcal{M} \vee \mathcal{N}) = \mathcal{P} \neq \{0\} = (\mathcal{P} \wedge \mathcal{M}) \vee (\mathcal{P} \wedge \mathcal{N})$$

For $v \in V$ we define the **dual vector** v^* to be the linear functional $v^* \colon V \to \mathcal{B}$ given by $v^*(u) = \langle v, u \rangle$. For $u, v \in V$ we define the **outer-product** uv^* to be the operator $uv^* \colon V \to V$ given by $uv^*(w) = \langle v, w \rangle u$. Let $\mathcal{M}$ be a subspace of V with basis $\{v_1, \ldots, v_m\}$. We define the **projection** onto $\mathcal{M}$ to be the operator $P_{\mathcal{M}} \colon V \to V$ given by $P_{\mathcal{M}} = \sum_{i=1}^{m} v_i v_i^*$. Thus $P_{\mathcal{M}}(u) = \sum \langle v_i, u \rangle v_i$ for all $u \in V$. Of course, the range of $P_{\mathcal{M}}$ is $\mathcal{M}$ and it is easy to show that $P_{\mathcal{M}} = P_{\mathcal{M}}^* = P_{\mathcal{M}}^2$. The next lemma shows that $P_{\mathcal{M}}$ is an invariant.

Lemma 3.5. *The projection $P_{\mathcal{M}}$ is independent of the basis of $\mathcal{M}$.*

Proof. Let $\{v_1, \ldots, v_m\}$ and $\{w_1, \ldots, v_m\}$ be bases for $\mathcal{M}$.Then by Parseval's identity we have

$$\begin{aligned}
P_{\mathcal{M}}(u) &= \sum_i \langle v_i, u \rangle v_i = \sum_i \left\langle \sum_j \langle v_i, w_j \rangle w_j, u \right\rangle \sum_k \langle v_i, w_k \rangle w_k \\
&= \bigvee_i \bigvee_j \langle v_i, w_j \rangle \langle w_j, u \rangle \sum \langle v_i, w_k \rangle w_k \\
&= \sum_k \bigvee_j \bigvee_i \langle w_j, v_i \rangle \langle v_i, w_k \rangle \langle w_j, u \rangle w_k \\
&= \sum_k \bigvee_j \langle w_j, w_k \rangle \langle w_j, u \rangle w_k = \sum_k \langle w_k, u \rangle w_k
\end{aligned}$$

□

An operator $T \colon V \to V$ is **diagonal** if $\langle Tv_i, v_j \rangle = 0$, $i \neq j$, $i, j = 1, \ldots, n$, for some basis $\{v_1, \ldots, v_n\}$ for V. We now have the following surprising result.

Lemma 3.6. *Diagonality is an invariant.*

Proof. Let $\{v_1, \ldots, v_n\}$ and $\{w_1, \ldots, v_n\}$ be bases for V and suppose that

$\langle Tv_i, v_j\rangle = 0$ for $i \neq j$. By Parseval's identity we have for $i \neq j$ that

$$\begin{aligned}
\langle Tw_i, w_j\rangle &= \left\langle T\sum_k \langle w_i, v_k\rangle v_k, \sum_r \langle w_j, v_r\rangle v_r \right\rangle \\
&= \bigvee_{k,r} \langle w_i, v_k\rangle\langle w_j, v_r\rangle\langle Tv_k, v_r\rangle \\
&= \bigvee_{k} \langle w_i, v_k\rangle\langle v_k, w_j\rangle\langle Tv_k, v_k\rangle \\
&\leq \bigvee_{k} \langle w_i, v_k\rangle\langle v_k, w_j\rangle = \langle w_i, w_j\rangle = 0
\end{aligned}$$

□

Corollary 3.7. *Every projection is diagonal.*

Proof. Let $\{v_1, \dots, v_m\}$ be a basis for the subspace $\mathcal{M}$. Then for $i \neq j$ we have

$$\begin{aligned}
\langle P_{\mathcal{M}} v_i, v_j\rangle &= \left\langle \sum_k \langle v_k, v_i\rangle v_k, , v_j \right\rangle = \bigvee_k \langle v_i, v_k\rangle\langle v_k, v_j\rangle \\
&= \langle v_i, v_j\rangle = 0
\end{aligned}$$

□

Example 6. *We have seen that a projection P satisfies $P = P^* = P^2$. However, these conditions are not sufficient for P to be a projection. For instance, on $L_2(\mathcal{B})$ let P be the matrix*

$$P = \begin{bmatrix} 1 & a \\ a & 1 \end{bmatrix}$$

where $a \neq 0$. Then $P = P^* = P^2$ but P is not a projection because P is not diagonal.

Lemma 3.8. (i) *If T is diagonal, then $T = T^*$.* (ii) *If S and T are diagonal operators on V then $ST = TS$.*

Proof. (i) Suppose $T\colon V \to V$ is diagonal and $\{v_1, \dots, v_n\}$ is a basis for V. Then for $i \neq j$ we have

$$\langle T^* v_i, v_j\rangle = \langle v_i, Tv_j\rangle = 0$$

Hence, for $i \neq j$ we have $\langle T^* v_i, v_j\rangle = \langle Tv_i, v_j\rangle$. Moreover,

$$\langle T^* v_i, v_i\rangle = \langle v_i, Tv_i\rangle = \langle Tv_i, v_i\rangle$$

We conclude that $T^* v_i = Tv_i$ for $i = 1, \ldots, n$, so that $T^* = T$. (ii) For a basis $\{v_1, \ldots, v_n\}$ of V we have

$$\begin{aligned}\langle STv_i, v_j\rangle = \langle Tv_i, Sv_j\rangle &= \bigvee_k \langle Tv_i, v_k\rangle\langle v_k, Sv_j\rangle \\ &= \langle Sv_j, v_j\rangle\langle Tv_i, v_i\rangle\delta_{ij}\end{aligned}$$

By symmetry we have

$$\langle TSv_i, v_j\rangle = \langle Tv_j, v_j\rangle\langle Sv_i, v_i\rangle\delta_{ij}$$

Hence, $\langle STv_i, v_j\rangle = \langle TSv_i, v_j\rangle$ for all i, j, so that $ST = TS$. □

We denote the set of projections on V by $\mathcal{P}(V)$. Since there is a one-to-one correspondence between subspaces and projections, we can transfer the order and $^\perp$ on $\mathcal{S}(V)$ to $\mathcal{P}(V)$. We thus define $P_\mathcal{M} \leq P_\mathcal{N}$ if $\mathcal{M} \subseteq \mathcal{N}$ and define $P_\mathcal{M}^\perp = P_{\mathcal{M}^\perp}$. In this way $\mathcal{P}(V)$ becomes an atomistic, orthomodular poset.

Lemma 3.9. *On $\mathcal{P}(V)$ we have that $P \leq Q$ if and only if $PQ = P$. Moreover, $P^\perp$ is the unique projection satisfying $PP^\perp = 0$ and $P + P^\perp = I$.*

Proof. Let $P = P_\mathcal{M}$ and $Q = P_\mathcal{N}$ for $\mathcal{M}, \mathcal{N} \in \mathcal{S}(V)$. If $P_\mathcal{M} \leq P_\mathcal{N}$ then $\mathcal{M} \subseteq \mathcal{N}$. If $v \in \mathcal{M}$ then $P_\mathcal{M} P_\mathcal{N} v = P_\mathcal{M} v$. If $v \in \mathcal{M}^\perp$ then

$$P_\mathcal{M} P_\mathcal{N} v = P_\mathcal{N} P_\mathcal{M} v = 0 = P_\mathcal{M} v$$

Hence, $P_\mathcal{M} P_\mathcal{N} = P_\mathcal{M}$. Conversely, suppose that $P_\mathcal{M} P_\mathcal{N} = P_\mathcal{M}$. If $\{v_1, \ldots, v_m\}$ is a basis for $\mathcal{M}$ then

$$P_\mathcal{N} v_i = P_\mathcal{N} P_\mathcal{M} v_i = P_\mathcal{M} v_i = v_i$$

Hence, $v_i \in \mathcal{N}$, $i = 1, \ldots, n$, and we conclude that $\mathcal{M} \subseteq \mathcal{N}$. Thus, $P_\mathcal{M} \leq P_\mathcal{N}$. For the second statement, again let $P = P_\mathcal{M}$. It is clear that $P_\mathcal{M} P_\mathcal{M}^\perp = P_\mathcal{M} P_{\mathcal{M}^\perp} = 0$ and $P_\mathcal{M} + P_\mathcal{M}^\perp = I$. For uniqueness, suppose $P_\mathcal{N}$ satisfies, $P_\mathcal{M} P_\mathcal{N} = 0$ and $P_\mathcal{M} + P_\mathcal{N} = I$. If $v \in \mathcal{N}$ then

$$P_\mathcal{M} v = P_\mathcal{M} P_\mathcal{N} v = 0$$

which implies that $v \in \mathcal{M}^\perp$. Hence, $\mathcal{N} \subseteq \mathcal{M}^\perp$. If $v \in \mathcal{M}^\perp$ then

$$v = P_{\mathcal{M}}v + P_{\mathcal{N}}v = P_{\mathcal{N}}v \in \mathcal{N}$$

Hence, $\mathcal{M}^\perp \subseteq \mathcal{N}$ so that $\mathcal{N} = \mathcal{M}^\perp$. Therefore, $P_{\mathcal{N}} = P_{\mathcal{M}^\perp} = P_{\mathcal{M}}^\perp$. □

Corollary 3.10. *For $P, Q \in \mathcal{P}(V)$ if $PQ \in \mathcal{P}(V)$ then $P \wedge Q$ exists and $PQ = P \wedge Q$.*

Proof. Since $P(PQ) = PQ$ and $Q(PQ) = Q(QP) = PQ$ we have $PQ \leq P, Q$. If $R \in \mathcal{P}(V)$ and $R \leq P, Q$ then $R(PQ) = RQ = R$. Hence, $R \leq PQ$ so that $PQ = P \wedge Q$. □

It is not known whether the converse holds. That is, if $P \wedge Q$ exists then $PQ \in \mathcal{P}(V)$ is unknown.

4 States and Diagonality

An **eigenvector** for an operator T is a unit vector v such that $Tv = av$ for some $a \in \mathcal{B}$. We then call a an **eigenvalue corresponding to** v and we call (a, v) an **eigenpair** for T. In general, $a\underline{v} = b\underline{v}$ for $v \neq 0$ does not imply $a = b$. However, if $\|v\| = 1$, then $a\underline{v} = b\underline{v}$ implies

$$a = a\|v\| = \|av\| = \|bv\| = b$$

Hence, if (a, v) and (b, v) are eigenpairs then $a = b$. Thus, the eigenvalue corresponding to an eigenvector is unique.

Theorem 4.1. *The following statements are equivalent.* (i) *T is diagonal in V.* (ii) *Any basis for V consists of eigenvectors of T.* (iii) *Any consistent unit vector is an eigenvector of T.* (iv) *There is a basis for V consisting of eigenvectors of T.*

Proof. (i)⇒(ii) Let T be diagonal and suppose $\{v_1, \ldots, v_n\}$ is a basis for V. Letting $a_i = \langle Tv_i, v_i \rangle$ we have for $i \neq j$ that

$$\langle Tv_i, v_j \rangle = 0 = \langle a_i v_i, v_j \rangle$$

Moreover, $\langle Tv_i, v_i \rangle = \langle a_i v_i, v_i \rangle$. Hence, $Tv_i = a_i v_i$ so $\{v_1, \ldots, v_n\}$ consists of eigenvectors of T. (ii)⇒(iii) Since any consistent unit vector can be extended to a basis for V, (iii) follows from Statement (ii). (iii)⇒(iv) Since the elements of any basis are consistent (iv) follows from Statement (iii). (iv)$\Rightarrow$(i) Let $\{v_1, \ldots, v_n\}$ be a basis of eigenvectors of T and suppose $Tv_i = a_i v_i$, $i = 1, \ldots, n$. For $i \neq j$, we have

$$\langle Tv_i, v_j \rangle = \langle a_i v_i, v_j \rangle = a_i \langle v_i, v_j \rangle = 0$$

Hence, T is diagonal. $\square$

Example 7. *Eigenvectors corresponding to distinct eigenvalues of a diagonal operator need not be orthogonal. In $L_2(\mathcal{B})$, let $v_1 = (a, a')$, $v_2 = (a', a)$ where $a \neq 0, 1$. Let $b_1 \neq b_2 \in \mathcal{B}$ and let $c_1 = b_1 a + b_2 a'$, $c_2 = b_1 a' + b_2 a$. The operator T given by the matrix*

$$T = \begin{bmatrix} c_1 & 0 \\ 0 & c_2 \end{bmatrix}$$

has many eigenpairs including (c_1, δ_1), (c_2, δ_2), (b_1, v_1), (b_2, v_2). In general $b_1 \neq c_1$ but $\langle v_1, \delta_1 \rangle = a \neq 0$.

Lemma 4.2. *If T is a diagonal operator on V with eigenpair (a, v), then there exists a consistent unit vector u such that $u \leq v$ and (a, u) is an eigenpair.*

Proof. Let $\{v_1, \ldots, v_n\}$ be a basis for V and suppose $v = \sum b_i v_i$. Define $c_i \in \mathcal{B}$, $i = 1, \ldots, n$, by $c_1 = b_1$, $c_2 = b_2 b_1', \ldots, c_n = b_n b_1' \cdots b_{n-1}'$. It is easy to check that $u = \sum c_i v_i$ is a consistent unit vector and clearly $u \leq v$. Since $Tv = av$ we have that

$$\sum a b_i v_i = av = \sum b_i T v_i = \sum_i b_i \sum_j \langle T v_i, v_j \rangle v_j = \sum b_i \langle T v_i, v_i \rangle v_i$$

Hence, $a b_i = \langle T v_i, v_i \rangle b_i$, $i = 1, \ldots, n$. Therefore,

$$\langle T v_i, v_i \rangle c_i = \langle T v_i, v_i \rangle b_i b_1' \cdots b_{i-1}' = a b_i b_1' \cdots b_{i-1}' = a c_i$$

We conclude that

$$Tu = \sum c_i T v_i = \sum c_i \langle T v_i, v_i \rangle v_i = a \sum c_i v_i = av$$

Hence, (a, u) is an eigenpair. $\square$

Theorem 4.3. *If T is a diagonal operator on V, then a is an eigenvalue of T if and only if $a = \langle Tv, v\rangle$ for some consistent unit vector v.*

Proof. If a is an eigenvalue for T then $Tu = au$ for some unit vector u. By Lemma 4.2, there is a consistent unit vector v such that $Tv = av$. Hence,

$$\langle Tv, v\rangle = \langle av, v\rangle = a\langle v, v\rangle = a$$

Conversely, suppose $a = \langle Tv_1, v_1\rangle$ for some consistent unit vector v_1. We can extend v_1 to a basis $\{v_1, v_2, \ldots, v_n\}$ for V. Then

$$Tv_1 = \sum \langle Tv_1, v_i\rangle v_i = \langle Tv_1, v_1\rangle v_1 = av_1$$

Hence, a is an eigenvalue of T. $\square$

Example 8. *Let T be the operator on $L_2(\mathcal{B})$ given by the matrix*

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

Then for any $a \in \mathcal{B}$ we have $T(a, a') = (a, 0) = a(a, a')$. Hence, every $a \in \mathcal{B}$ is an eigenvalue of T.

We denote the set of operators on the Boolean vector space V by $\mathcal{O}(V)$. A **state** on $\mathcal{O}(V)$ is map $s\colon \mathcal{O}(V) \to [0, 1] \subseteq \mathbb{R}$ that satisfies

(1) $s(I) = 1$ (**unital**)

(2) if $ST^* = 0$ or $S^*T = 0$, then $s(S + T) = s(S) + s(T)$ (**additive**)

(3) if u and v are orthogonal, consistent unit vectors, then $s(uv^*) = 0$ (**diagonal**)

(4) $s\left[T(uv^*)\right] \leq s(uv^*)$ for all $T \in \mathcal{O}(V)$, $u, v \in V$. (**outer bounded**)

We denote the set of states on $\mathcal{O}(V)$ by $\widehat{\mathcal{O}}(V)$. Notice that $\widehat{\mathcal{O}}(V)$ is convex. That is, if $\lambda_i \in \mathbb{R}$ with $\lambda_i \geq 0$, $\sum \lambda_i = 1$ and $s_i \in \widehat{\mathcal{O}}(V)$, $i = 1, \ldots, n$, then $\sum \lambda_i s_i \in \widehat{\mathcal{O}}(V)$.

Example 9. *Let μ be a finitely additive probability measure on $\mathcal{B}$ and let w_1 be a consistent unit vector in V. Then $s(T) = \mu(\langle Tw_1, w_1\rangle)$ is a state on $\mathcal{O}(V)$. Indeed, s clearly satisfies Conditions (1) and (2). To verify (3), let u and v be orthogonal, consistent unit vectors. Extending w_1 to a basis $\{w_1, \ldots, w_n\}$ for V we have*

$$\begin{aligned}\langle uv^*(w_1), w_1\rangle &= \langle\langle v, w_1\rangle u, w_1\rangle = \langle v, w_1\rangle\langle w_1, u\rangle\\ &\leq \bigvee \langle v, w_1\rangle\langle w_i, u\rangle = \langle v, u\rangle = 0\end{aligned}$$

Hence, $s(uv^*) = 0$. To verify (4) we have by Schwarz's equality that

$$\begin{aligned}s\left[T(uv^*)\right] &= \langle T(uv^*)w_1, w_1\rangle = \langle uv^*(w_1), T^*w_1\rangle\\ &\leq \|uv^*(w_1)\| = \langle uv^*(w_1), vu^*(w_1)\rangle\\ &= \langle\langle v, w_1\rangle u, \langle u, w_1\rangle v\rangle = \langle v, w_1\rangle\langle u, w_1\rangle\langle u, v\rangle\\ &\leq \langle v, w_1\rangle\langle u, w_1\rangle = \langle\langle v, w_1\rangle u, w_1\rangle = \langle uv^*(w_1), w_1\rangle\\ &= s(uv^*)\end{aligned}$$

A state s is **extremal** if $s = \lambda s_1 + (1-\lambda)s_2$ for $\lambda \in (0,1)$, $s_1, s_2 \in \widehat{\mathcal{O}}(V)$, then $s_1 = s_2$. A state is **pure** if there is a one-dimensional projection vv^* such that $s(vv^*) = 1$. Notice by Condition (2) that $s(T) = s(0+T) = s(0) + s(T)$ so $s(0) = 0$ for any state s.

Lemma 4.4. *Extremal states are pure.*

Proof. Suppose $s\colon \mathcal{O}(V)$ is a state that is not pure. Since I is a projection with $s(I) = 1$ there exists $P \in \mathcal{P}(V)$ such that $\dim(P) > 1$, $s(P) = 1$ and $s(Q) \neq 1$ for any $Q \in \mathcal{P}(V)$ with $Q < P$. Let $\{v_1, \ldots, v_n\}$ be a basis for V where $\{v_1, \ldots, v_m\}$ is a basis for P and let $P_i = v_iv_i^*$. We then have that $P = \sum_{i=1}^m P_i$. Since $P_iP_j^* = P_iP_j = 0$ for $i \neq j$, we have that $1 = s(P) = \sum_{i=1}^m s(P_i)$ and $s(P_i), s(P_j) \neq 0$ for at least two indices i, j. We can assume without loss of generality that $s(P_i) \neq 0$ for $i = 1, \ldots, r$ where $r \geq 2$. Now $s_i\colon \mathcal{O}(V) \to [0,1]$ defined by $s_i(T) = s(TP_i)/s(P_i)$, $i = 1, \ldots, r$ is a state. Indeed, Condition (1) clearly holds. To verify Condition (2), suppose $ST^* = 0$. Then $(SP_i)(TP_i)^* = SP_iT^*$ and for any $u, v \in V$ we have

$$\begin{aligned}\langle SP_iT^*u, v\rangle &= \langle S\langle T^*u, v_i\rangle v_i, v\rangle = \langle T^*u, v_i\rangle\langle Sv_i, v\rangle\\ &= \langle T^*u, v_i\rangle\langle v_i, S^*v\rangle \leq \bigvee_i \langle T^*u, v_i\rangle\langle v_i, S^*v\rangle\\ &= \langle T^*u, S^*v\rangle = \langle ST^*u, v\rangle = 0\end{aligned}$$

Hence,

$$\begin{aligned}s_i(S+T) &= \frac{1}{s(P_i)}\, s(SP_i+TP_i) = \frac{1}{s(P_i)}\, s(SP_i) + \frac{1}{s(P_i)}\, s(TP_i)\\ &= s_i(S)+s_i(T)\end{aligned}$$

To verify Condition (3), let u and v be orthogonal, consistent unit vectors. Since

$$(uv^*P_i)(uv^*P_j)^* = uv^*P_iP_jvu^* = 0$$

for $i \neq j$ we have

$$\sum_{i=1}^n s(uv^*P_i) = s\left(uv^*\sum_{i=1}^n P_i\right) = s(uv^*) = 0$$

Hence,

$$s_i(uv^*) = \frac{1}{s(P_i)}\, s(uv^*P_i) = 0$$

To verify Condition (4), we have

$$uv^*P_i = (uv^*)(v_iv_i^*) = \langle v, v_i\rangle uv_i^*$$

Letting $u_1 = \langle v, v_i\rangle u$ we have that $uv^*P_i = u_1v_i^*$. Hence,

$$\begin{aligned}s_i\left[T(uv^*)\right] &= \frac{1}{s(P_i)}\, s\left[T(uv^*)P_i\right] = \frac{1}{s(P_i)}\, s\left[T(u_1v_i^*)\right]\\ &\le \frac{1}{s(P_i)}\, s(u_1v^*) = \frac{1}{s(P_i)}\, s(uv^*P_i) = s_i(uv^*)\end{aligned}$$

Finally, Condition (4) gives $s(TP_i) \le s(P_i)$ so $s_i(T) \le 1$. We conclude that s_i is a state, $i = 1, \ldots, r$. Since

$$(TP_i)(TP_j)^* = TP_iP_jT^* = 0$$

for $i \neq j$, we have

$$s(T) = s\left(\sum_{i=1}^n TP_i\right) = \sum_{i=1}^n s(TP_i)$$

By Condition (4) we have $s(TP_i) \leq s(P_i) = 0$, $i = r+1, \dots, n$. Hence,

$$s(T) = \sum_{i=1}^{r} s(TP_i) = \sum_{i=1}^{r} s(P_i)s_i(T)$$

We conclude that

$$s = \sum_{i=1}^{r} s(P_i)s_i$$

where $\sum_{i=1}^{r} s(P_i) = 1$. Since $s_i(P_i) = 1$ and $s_i(P_j) = 0$ for $i \neq j$, we have that the s_i are different, $i = 1, \dots, r$. Hence, s is not extremal. $\square$

Theorem 4.5. *If $s\colon \mathcal{O}(V) \to [0,1]$ is an extremal state, there exists a unique finitely additive probability measure μ on $\mathcal{B}$ and a consistent unit vector $v_1 \in V$ such that $s(T) = \mu\left(\langle Tv_1, v_1\rangle\right)$.*

Proof. Define $\mu\colon \mathcal{B} \to [0,1]$ by $\mu(a) = s(aI)$. Then $\mu(1) = s(I) = 1$ and $ab = 0$ implies

$$(aI)(bI)^* = abI = 0$$

so that

$$\mu(a \vee b) = s\left((a \vee b)I\right) = s(aI + bI) = s(aI) + s(bI) = \mu(a) + \mu(b)$$

Hence, μ is a countably additive probability measure on $\mathcal{B}$. By Lemma 4.4, s is a pure state so $s(v_1v_1^*) = 1$ for some consistent unit vector v_1. Extend v_1 to a basis $\{v_1, \dots, v_n\}$ for V. Since $(v_iv_i^*)(v_1v_1^*) = 0$ for $i \neq 1$ we have

$$1 = s(v_iv_i^* + v_1v_1^*) = s(v_iv_i^*) + s(v_1v_1^*) = s(v_iv_i^*) + 1$$

Hence, $s(v_iv_i^*) = 0$ for $i \neq 1$. Moreover, since s is diagonal we have that $s(v_iv_j^*) = 0$ for all $i \neq j$. By Condition (4) we have that $s(av_iv_i^*) = s(aIv_iv_i^*) \leq s(v_iv_i^*) = 0$ for $i \neq 1$ and similarly $s(av_iv_j^*) = 0$ for $i \neq j$ and all $a \in \mathcal{B}$. We conclude that for any $a \in \mathcal{B}$ we have

$$s(av_iv_j^*) = \mu\left(\langle av_iv_j^*v_1, v_1\rangle\right)$$

whenever i and j are not both 1. Moreover, for any $a \in \mathcal{B}$ we have

$$s(av_1v_1^*) = s\left(a\sum_{i=1}^{n} v_iv_i^*\right) = s(aI) = \mu(a) = \mu\left(\langle av_1v_1^*v_1, v_1\rangle\right)$$

For $T \in \mathcal{O}(V)$ it is well-known that we can write $T = \sum t_{ij} v_i v_j^*$, $t_{ij} \in \mathcal{B}$. By additivity we have

$$\begin{aligned} s(T) &= s\left(\sum t_{ij} v_i v_j^*\right) = s(t_{11} v_1 v_1^*) = \mu\left(\langle t_{11} v_1 v_1^* v_1, v_1\rangle\right) \\ &= \mu\left(\langle T v_1, v_1\rangle\right) \end{aligned}$$

For uniqueness we have for all $a \in \mathcal{B}$ that

$$\mu(a) = \mu\left(\langle aI v_1, v_1\rangle\right) = s(aI) \qquad \square$$

Corollary 4.6. *A state is pure if and only if it is extremal.*

Proof. By Lemma 4.4 extremal states are pure. Conversely, suppose $s\colon \mathcal{O}(V) \to [0,1]$ is pure. Then there exists a consistent unit vector $v \in V$ such that $s(vv^*) = 1$. To show that s is extremal, assume that $s = \lambda s_1 + (1-\lambda)s_2$ where $0 < \lambda < 1$ and s_1, s_2 are states. Then

$$\lambda s_1(vv^*) + (1-\lambda)s_2(vv^*) = s(vv^*) = 1$$

Hence, $s_1(vv^*) = s_2(vv^*) = 1$. By Theorem 4.5, there exists a probability measure μ on $\mathcal{B}$ such that

$$s_1(T) = s_2(T) = \mu\left(\langle Tv, v\rangle\right) = s(T)$$

for every $T \in \mathcal{O}(V)$. Hence, $s_1 = s_2 = s$ so s is extremal. $\square$

The next result shows that every state is a finite convex combination of extremal (pure) states.

Corollary 4.7. *If s is a state on $\mathcal{O}(V)$ with $\dim(V) = n$, then there exists a consistent orthonormal set $\{v_1, \ldots, v_m\}$, $m \le n$, in V, $\lambda_i \in \mathbb{R}$ with $\lambda_k > 0$, $\sum_{i=1}^m \lambda_i = 1$ and finitely additive probability measure μ_i on $\mathcal{B}$, $i = 1, \ldots, m$ such that*

$$s(T) = \sum_{i=1}^m \lambda_i \mu_i\left(\langle T v_i, v_i\rangle\right)$$

for all $T \in \mathcal{O}(V)$.

Proof. Let $\{v_1, \ldots, v_n\}$ be a basis for V. Without loss of generality, we can assume that $s(v_i v_i^*) \ne 0$ for $i = 1, \ldots, m$ and $s(v_j v_j^*) = 0$ for $j = m+1, \ldots, n$. As in the proof of Lemma 4.4, the maps $s_i\colon \mathcal{O}(V) \to [0,1]$ given by $s_i(T) =$

$s\left[T(v_iv_i^*)\right]/s(v_iv_i^*)$, $i=1,\ldots,m$ are pure states on $\mathcal{O}(V)$. Moreover, as in the proof of Lemma 4.4, we have

$$s(T)=\sum_{i=1}^m\left[T(v_iv_i^*)\right]=\sum_{i=1}^m s(v_iv_i^*)s_i(T)$$

where $s(v_iv_i^*)>0$ and $\sum s(v_iv_i^*)=1$. By Theorem 4.5, there exist finitely additive probability measures μ_i on $\mathcal{B}$ such that $s_i(T)=\mu_i\left(\langle Tv_i,v_i\rangle\right)$, $i=1,\ldots,m$. Letting $\lambda_i=s(v_iv_i^*)$, $i=1,\ldots,m$, completes the proof. $\square$

Denoting the set of diagonal operators on V by $\mathcal{D}(V)$ the theory of states on $\mathcal{D}(V)$ is much simpler. We define a **state** on $\mathcal{D}(V)$ to be a functional $s\colon\mathcal{D}(V)\to[0,\infty)$ such that $s(I)=1$ and $s(S+T)=s(S)+s(T)$ whenever $ST=0$. For any $D\in\mathcal{D}(V)$ there exists a unique $D'\in\mathcal{D}(V)$ such that $DD'=0$ and $D+D'=I$. Hence,

$$1=s(I)=s(D+D')=s(D)+s(D')$$

so that $s(D)\le 1$. We conclude that $s\colon\mathcal{D}(V)\to[0,1]$ for any state on $\mathcal{D}(V)$. We define pure and extremal states on $\mathcal{D}(V)$ as before. A simplified version of the proof of Lemma 4.4 shows that extremal states on $\mathcal{D}(V)$ are pure. Moreover, the proof of Theorem 4.5 carries over to show that an extremal state s on $\mathcal{D}(V)$ has the form

$$s(D)=\mu\left(\langle Dv,v\rangle\right)$$

as before. Also, Corollaries 4.6 and 4.7 hold for states on $\mathcal{D}(V)$. Finally, any state on $\mathcal{D}(V)$ has a unique extension to a state on $\mathcal{O}(V)$.

5 Tensor Products and Direct Sums

Let V_1,V_2 be Boolean vector spaces over $\mathcal{B}$. For $v_1\in V_1$, $v_2\in V_2$ define $v_1\otimes v_2\colon V_1\times V_2\to\mathcal{B}$ by

$$v_1\otimes v_2\colon(u_1,u_2)=\langle v_1,u_1\rangle\langle v_2,u_2\rangle$$

Then $v_1\otimes v_2$ is a bilinear form. If $F,G\colon V_1\times V_2\to\mathcal{B}$ are bilinear forms, we define the bilinear form $F+G\colon V_1\times V_2\to\mathcal{B}$ by

$$(F+G)(u_1,u_2)=F(u_1,u_2)\vee G(u_1,u_2)$$

and the bilinear form $aF\colon V_1 \times V_2 \to \mathcal{B}$ $a \in \mathcal{B}$, by

$$(aF)(u_1, u_2) = aF(u_1, u_2)$$

We now define the **tensor product** $V_1 \otimes V_2$ by

$$\begin{aligned} &V_1 \otimes V_2 \\ &= \left\{ \sum_{i=1}^{r} \sum_{j=1}^{s} a_{ij} v_i \otimes u_j \colon a_{ij} \in \mathcal{B}, v_i \in V_1, u_j \in V_2, i = 1, \ldots, r, j = 1, \ldots, s \right\} \end{aligned}$$

It is clear that

$$\begin{aligned} a(v_1 \otimes v_2) &= (av_1) \otimes v_2 = v_1 \otimes (av_2) \\ (v_1 + w_1) \otimes v_2 &= v_1 \otimes v_2 + w_1 \otimes v_2 \\ v_1 \otimes (v_2 + w_2) &= v_1 \otimes v_2 + v_1 \otimes w_2 \end{aligned}$$

Theorem 5.1. *$V_1 \otimes V_2$ is a Boolean vector space.*

Proof. The first five axioms for a Boolean vector space are clear. To show that $V_1 \otimes V_2$ has a basis, let $\{x_1, \ldots, x_m\}$ be a basis for V_1 and $\{u_1, \ldots, y_n\}$ a basis for V_2. It is clear that $x_i \otimes y_j$, $i = 1, \ldots, m$, $j = 1, \ldots, n$, generates $V_1 \otimes V_2$. To show uniqueness, suppose

$$\sum_{i,j} a_{ij} x_i \otimes y_j = \sum_{i,j} b_{ij} x_i \otimes y_j$$

We then have

$$\begin{aligned} a_{rs} &= \sum_{i,j} a_{ij} \langle x_i, x_r \rangle \langle u_j, y_s \rangle = \sum a_{ij} x_i \otimes y_j (x_r, y_s) \\ &= \sum_{i,j} b_{ij} x_i \otimes y_j (x_r, y_s) = \sum b_{ij} \langle x_i, x_r \rangle \langle y_j, y_s \rangle = b_{rs} \end{aligned}$$ □

The theory of the tensor product of a finite number of Boolean vector spaces carries over in a straightforward way and we shall mainly concentrate on two Boolean vector spaces. Let U, V, W be Boolean vector spaces. A **bimorphism** $\phi\colon U \times V \to W$ satisfies $\phi(u_1 + u_2, v) = \phi(u_1, v) + \phi(u_2, v)$, $\phi(u, v_1 + v_2) = \phi(u, v_1) + \phi(u, v_2)$ and $\phi(au, v) = \phi(u, av) = a\phi(u, v)$ for all $a \in \mathcal{B}$.

Theorem 5.2. *(Universality) There exists a bimorphism $\tau\colon V_1 \times V_2 \to V_1 \otimes V_2$ such that any element $F \in V_1 \otimes V_2$ has the form $F = \sum a_{ij}\tau(v_i, u_j)$ and if $\phi\colon V_1 \times V_2 \to W$ is a bimorphism there exists a unique linear map $\psi\colon V_1 \otimes V_2 \to W$ such that $\phi = \psi \circ \tau$.*

Proof. Define $\tau(v_1, v_2) = v_1 \otimes v_2$. Then τ is clearly a bimorphism and any $F \in V_1 \otimes V_2$ has the form

$$F = \sum a_{ij} v_i \otimes v_j = \sum a_{ij}\tau(v_1, u_j)$$

Let $\phi\colon V_1 \times V_2 \to W$ be a bimorphism. Let $\{x_1, \ldots, x_m\}$ be a basis for V_1 and $\{u_1, \ldots, u_n\}$ be a basis for V_2. Define $\psi\colon V_1 \otimes V_2 \to W$ by $\psi(x_i \otimes y_j) = \phi(x_i, y_j)$ and extend by linearity. Then ψ is linear and

$$\begin{aligned}
\psi \circ \tau(v_1, v_2) &= \psi\left(\sum a_i x_i \otimes \sum b_j y_j\right) = \psi\left(\sum a_i b_j x_i \otimes y_j\right) \\
&= \sum a_i b_j \psi(x_i \otimes y_j) = \sum_{i,j} a_i b_j \phi(x_i, y_j) \\
&= \psi\left(\sum a_i x_i, \sum b_j y_j\right) = \phi(v_1, v_2)
\end{aligned}$$

Hence, $\phi = \psi \circ \tau$. To show that ψ is unique, suppose $\psi_1\colon V_1 \otimes V_2 \to W$ is linear and $\phi = \psi_1 \circ \tau$. Then

$$\psi_1(x_i \otimes y_j) = \psi_1 \circ \tau(x_i, y_j) = \phi(x_i, y_j) = \psi(x_i \otimes y_j)$$

Since $x_i \otimes y_j$, $i = 1, \ldots, m$, $j = 1, \ldots, n$, is a basis for $V_1 \otimes V_2$, $\psi_1 = \psi$. ∎

Example 10. *We show that $L_m(\mathcal{B}) \otimes L_n(\mathcal{B}) \approx L_{mn}(\mathcal{B})$. Let $\{u_1, \ldots, u_m\}$ be a basis for $L_m(\mathcal{B})$ and $\{v_1, \ldots v_n\}$ be a basis for $L_n(\mathcal{B})$. We write $u_i = (a_{1i}, \ldots, a_{mi})$, $i = 1, \ldots, m$, and $v_j = (b_{1j}, \ldots, b_{nj})$, $j = 1, \ldots, n$. Define $\phi\colon L_m(\mathcal{B}) \otimes L_n(\mathcal{B}) \to L_{mn}(\mathcal{B})$ by*

$$\phi(u_i \otimes v_j) = (a_{1i}b_{1j}, \ldots, a_{1i}b_{nj}, a_{2i}b_{1j}, \ldots, a_{2i}b_{nj}, \ldots, a_{mi}b_{1j}, \ldots, a_{mi}b_{nj})$$

for $i = 1, \ldots, m$, $j = 1, \ldots, n$, and extend by linearity. Since $\{u_1, \ldots, u_m\}$ and $\{v_1, \ldots, v_n\}$ are consistent orthonormal sets, it is straightforward to show that $\mathcal{A} = \{\phi(u_i \otimes v_j)\colon i = 1, \ldots, m, j = 1, \ldots, n\}$ is a consistent orthonormal set in $L_{mn}(\mathcal{B})$. Since $\mathcal{A}$ has cardinality m, n, it follows that $\mathcal{A}$ is a basis for $L_{mn}(\mathcal{B})$. Hence, ϕ is an isomorphism.

Example 11. *If $u_1, u_2 \in U$, $v_1, v_2 \in V$ we show that*

$$\langle u_1 \otimes v_1, u_2 \otimes v_2 \rangle = \langle u_1, u_2 \rangle \langle v_1, v_2 \rangle$$

Let $\{x_1, \ldots, x_m\}$ be a basis for U and $\{y_1, \ldots, y_n\}$ be a basis for V. Letting $u_1 = \sum a_i x_i$, $v_1 = \sum b_j y_j$, $u_2 = \sum c_r x_r$, $v_2 = \sum d_s y_s$ we have

$$\begin{aligned}
\langle u_1 \otimes v_1, u_2 \otimes v_2 \rangle &= \left\langle \sum a_i x_i \otimes \sum b_j y_j, \sum c_r x_r \otimes \sum d_s y_s \right\rangle \\
&= \bigvee_{i,j,r,s} a_i b_j c_r d_s \langle x_i \otimes y_j, x_r \otimes y_s \rangle \\
&= \bigvee_{i,j} a_i b_j c_i d_j = \bigvee_i a_i c_i \bigvee b_j d_n \\
&= \langle u_1, u_2 \rangle \langle v_1, v_2 \rangle
\end{aligned}$$

Let V and W be Boolean vector spaces over $\mathcal{B}$. Define $V \oplus W = (V \times W, +, \cdot)$ where

$$\begin{aligned}
(v_1, w_1) + (v_2, w_2) &= (v_1 + v_2, w_1 + w_2) \\
a \cdot (v, w) &= (av, aw), \quad a \in \mathcal{B}
\end{aligned}$$

We call $V \oplus W$ the **direct sum** of V and W.

Theorem 5.3. *$V \oplus W$ is a Boolean vector space.*

Proof. It is clear that $V \oplus W$ satisfies the first five axioms for a Boolean vector space. To show that $V \oplus W$ has a basis, let $\{x_1, \ldots, x_m\}$ and $\{y_1, \ldots, y_n\}$ be bases for V and W, respectively. Then

$$\{(x_i, 0), (0, y_j) \colon i = 1, \ldots, m, j = 1, \ldots, n\}$$

is a basis for $V \oplus W$. Indeed, if $v = \sum a_i x_i$ and $w = \sum b_j y_j$, then

$$\begin{aligned}
(v, w) &= \left(\sum a_i x_i, \sum b_j y_j\right) = \left(\sum a_i x_i, 0\right) + \left(0, \sum b_j y_j\right) \\
&= \sum a_i (x_i, 0) + \sum b_j (0, y_j)
\end{aligned}$$

To show uniqueness, suppose $(v, w) = \sum c_i (x_i, 0) + \sum d_j (0, y_j)$. Then

$$\left(\sum a_i x_i, \sum b_j y_j\right) = \left(\sum c_i x_i, \sum d_j y_j\right)$$

so that $\sum a_i x_i = \sum c_i x_i$ and $\sum b_j y_j = \sum d_j y_j$. It follows that $a_i = c_i$ and $b_j = d_j$ for $i = 1, \ldots, m$, $j = 1, \ldots, n$. □

Notice that $\langle (v_1,w_1),(v_2,w_2)\rangle = \langle v_1,v_2\rangle + \langle w_1,w_2\rangle$. The maps $\phi_V\colon V\to V\oplus W$ and $\phi_W\colon W\to V\oplus W$ given by $\phi_V(v)=(v,0)$ and $\phi_W(w)=(0,w)$ are isometries and $\phi_V(V)$, $\phi_V(W)$ are orthogonal subspaces of $V\oplus W$.

Let V_i, $i=1,2,\ldots$, be Boolean vector spaces. We define

$$V_1\oplus V_2\oplus\cdots = (V_1\times V_2\times\cdots,+,\cdot)$$

where $(v_1,v_2,\ldots)+(w_1,w_2,\ldots)=(v_1+w_1,v_2+w_2,\ldots)$ and $c\cdot(v_1,v_2,\ldots)=(cv_1,cv_2,\ldots)$. Now $V_1\oplus V_2\oplus\cdots$ satisfies the first five axioms for a Boolean vector space but we don't have a finite basis. However, we have a countable basis in the following sense. Let $\left\{v_i^j\right\}$ be a basis for V_j. Then

$$\left\{(v_i^1,0,\ldots),(0,v_i^2,0,\ldots),\cdots\right\}$$

forms a basis for $V_1\oplus V_2\oplus\cdots$ in the sense that

$$\begin{aligned}(w_1,w_2,\ldots)&=(w_1,0,\ldots)+(0,w_2,0,\ldots)+\cdots\\ &=\sum c_i^1(v_i^1,0,\ldots)+\sum c_i^2(0,v_i^2,0,\ldots)+\cdots\end{aligned}$$

where the coefficients are unique.

If V is a Boolean vector space, we define the **Fock space**

$$\mathcal{F}(V)=\mathcal{B}\oplus V\oplus(V\otimes V)\oplus(V\otimes V\otimes V)\oplus\cdots$$

Let $\{v_1,\ldots,v_n\}$ be a basis for V. The subspace of $V\otimes V$ generated by the consistent orthonormal set

$$\{v_i\otimes v_i, v_i\otimes v_j+v_j\otimes v_i\colon i,j=1,\ldots,n\}$$

is called the **symmetric subspace** of $V\otimes V$ and is denoted by $V\circledS V$. In a similar way, we have symmetric subspaces of $V\otimes V\otimes V, V\otimes V\otimes V\otimes V,\ldots$. the **symmetric Fock space** is

$$\mathcal{F}_S(V)=\mathcal{B}\oplus V\oplus(V\circledS V)\oplus(V\circledS V\circledS V)\oplus\cdots$$

We leave the study of these Fock spaces to a later paper.

References

[1] T. S. Blyth, On eigenvectors of Boolean matrices, *Proc. Roy. Soc. Edinburgh* **67** (1967), 196–204.

[2] K. Cechlárová, Powers of matrices over distributive lattices – a review, *Fuzzy Sets Sys.* **138** (2003), 627–641.

[3] Y. Givéon, Lattice matrices, *Inf. Contr.* **7** (1964), 477–484.

[4] S. Gudder, Quantum Markov chains, *J. Math. Phys.* **49** (2008), 072105-1–072105-14.

[5] S. Gudder and F. Latrémolère, Boolean inner-product spaces and Boolean matrices (to appear).

[6] P. V. Jagannadham, Linear transformations on Boolean vector spaces, *Math. Ann.* **16** (1966), 240–247.

[7] R. D. Luce, A note on Boolean matrix theory, *Proc. Amer. Math. Soc.* **3** (1952), 382–388.

[8] D. E. Ruthford, Inverses of Boolean matrices, *Proc. Glasgow Math. Soc.* **6** (1963), 49–53.

[9] D. E. Ruthford, The eigenvalue problem for Boolean matrices, *Proc. Roy. Soc. Edinburgh* **67** (1963/1985), 25–38.

[10] D. E. Ruthford, Orthogonal Boolean matrices, *Proc. Roy. Soc. Edinburgh* **67** (1964/1965), 126–135.

[11] R. L. Sindak, Eigenvectors and maximal vectors in Boolean vector spaces, *Proc. Amer. Math. Soc.* **47** (1975), 323–328.

[12] L. A. Skornyakov, Invertible matrices over distributive structures, (Russian) *Sibirsk. Mat. Zh.* **27** (1986), 182–185, (English translation) *Siberian Math. J.* **27** (1986), 289–292.

[13] D. Stirzaker *Stochastic Processes and Models*, Oxford University Press, Oxford, 2005.

[14] N. V. Subrahmanyam, Boolean vector spaces I, *Math. Z.*, **83** (1964), 422–433.

[15] N. V. Subrahmanyam, Boolean vector spaces II, *Math. Z.*, **87** (1965), 401–419.

[16] N. V. Subrahmanyam, Boolean vector spaces III, *Math. Z.*, **100** (1967), 295–313.