CZECH TECHNICAL
UNIVERSITY
IN PRAGUE

F3

Faculty of Electrical Engineering
Department of Cybernetics

Master's Thesis

Combinatorial Methods in the Study of Quantum Structures

Václav Voráček

May 2021
Supervisor: Prof. Ing. Mirko Navara, DrSc.

Acknowledgement

I would like to express my deepest gratitude to my supervisor Prof. Ing. Mirko Navara, DrSc. for his thorough and patient guidance throughout the beginnings of my academic career.

I would like to thank to my family, friends and Hanka for their support.

Declaration

I declare that the presented work was developed independently and that I have listed all sources of information used within it in accordance with the methodical instructions for observing the ethical principles in the preparation of university theses.

Prague, 21.5.2021

....

Abstrakt / Abstract

Při snaze matematicky popsat kvantovou mechaniku vyvstalo mnoho problémů. V této práci se zaměříme na problémy ze dvou různých oblastí. Nejprve se budeme věnovat existenci skrytých proměnných a následně budeme zkoumat kvantové struktury, což jsou algebraické struktury popisující logiku kvantové mechaniky.

V práci je obsažena definitivní odpověď na déle než 25 let otevřenou otázku, jestli je možné přiřadit nenulovým vektorům z $\mathbb{R}^3$ nekonstantně nuly a jedničky tak, že z každé trojice ortogonálních vektorů je lichému počtu z nich přiřazena 1.

Je zde také ukázan příklad ortokomplementovaného diferenčního svazu bez stavů.

Klíčová slova: Bellova-Kochenova-Speckerova věta; ortokomplementovaný diferenční svaz; teorie skrytých proměnných; $\mathbb{Z}_2$-stav; svaz podprostorů $\mathbb{R}^3$

Překlad titulu: Kombinatorické metody ve studiu kvantových struktur

There are challenging problems related to the mathematical description of quantum mechanics. The thesis focuses on such problems from two different areas: The problems related to the existence of hidden variables and problems arising in the study of quantum structures, which are algebraic structures describing the logic of quantum mechanics. In both of these directions, we arrive at novel results.

A definitive answer is provided to a question open for over 25 years, whether there is a non-constant assignment of zeros and ones to the non-zero vectors of $\mathbb{R}^3$ such that from every three pairwise orthogonal vectors, an odd number of them is assigned 1. The answer is negative.

An example of an orthocomplemented difference lattice admitting no states is presented.

Keywords: Bell–Kochen–Specker theorem; orthocomplemented difference lattice; hidden-variable theory; $\mathbb{Z}_2$-state; lattice of subspaces of $\mathbb{R}^3$

Contents

Tables / Figures

Chapter 1
Introduction

1.1 Motivation

We will deal with mathematical questions related to quantum mechanics. In this section, we briefly outline the problems which we specify later.

Chapter 2 is devoted to the introduction to the mathematical aspects of quantum mechanics and to the subsequent extensive motivation of the problems we will tackle.

- One of the fundamental questions in the interpretation of quantum mechanics is the existence of hidden variables.

  In 1935, Einstein conducted a thought experiment in [13], yielding a paradoxical result which is known as EPR paradox. The seemingly absurd situation would occur when we perform measurements on two entangled particles. Quantum mechanics predicts the randomness of the outcome of an experiment. However, for entangled particles, a measurement of one particle will determine the outcome of the same measurement performed on the second particle, which may be arbitrarily distant. Seemingly, there would occur a transfer of information faster than the speed of light.

  A resolution to this paradox would be to assume that the outcomes of the measurements are known beforehand but unknown to us; thus, the measurement will only reveal the hidden variables, and no so-called spooky action at a distance occurs.
- Unlike the classical case, Boolean algebras are not sufficient to describe the logic of quantum mechanics. For example, quantum logic is not distributive; thus, we need more general algebras for their description.

1.2 Goals of the Thesis

- Make a gentle introduction to the mathematical aspect of quantum physics.
- Examine the modifications of Bell–Kochen–Specker theorem.
- Study states on orthocomplemented difference lattices.
- Solve some open problems related to states on quantum structures and Bell–Kochen–Specker theorem.

1.3 State of the Art

Due to the nature of the problems, we will define the concepts, formulate questions and review the literature in every chapter independently.

Chapter 2
Quantum Physics

This chapter aims at a description of the nature of quantum mechanics in terms of linear algebra, which will be used throughout the thesis.

The goal is not to explain physics; we are willing to introduce a (part of a) mathematical formalism used to describe quantum mechanics matters. With this abstraction, we motivate and formulate some of the questions we will study.

The notation commonly used for the mathematical description of quantum mechanics is called a *Bra-Ket* notation (or also a Dirac notation). However, we will use a possibly simpler notation that will be sufficient for our purpose. We will avoid the Bra-Ket notation, as we expect the reader not to be familiar with it, for the cost of restricting ourselves to finite vector spaces. Instead, we will use only the vector space $\mathbb{R}^n$ over the field of real numbers with the standard vector addition and multiplication of a vector by a scalar. We consider a vector to be a one-column matrix, but we will write it in a row to save space. It should not bring any confusion since we will encounter only vectors and square matrices.

We shall note that, although we approach quantum mechanics using so-called matrix mechanics, introduced by Heisenberg, Born and Jordan in [9], it is also possible to explain the phenomenons of quantum physics in terms of partial differential equations. This direction was coined at almost the same time by Schrödinger in [42].

2.1 Mathematical Description of Quantum Mechanics

With every quantum system, may it be a particle, or a set of particles, is tied a Hilbert space describing it. Hilbert space is a complete vector space equipped with an inner product. The dimension of the Hilbert space may be finite or infinite; both cases are important for physics. The Hilbert space represents every possible state (think of position, momentum), which the quantum system may attain. We shall ground this in the following definition:

Definition 2.1. A quantum system is represented by a vector space $H = \mathbb{R}^n$ in the following way:

- A *state* of a system is represented by a unit vector $\mathbf{x} \in H$.
- A *measurement* is represented by a symmetric matrix $\mathbf{A} \in \mathbb{R}^{n \times n}$.
- The outcome of a measurement is one of the eigenvalues of $\mathbf{A}$. The probability of measuring a certain eigenvalue λ_i equals $\mathbf{x}^T \mathbf{P}_i \mathbf{x}$, where $\mathbf{P}_i$ is the projector on the eigenspace of $\mathbf{A}$, corresponding to the eigenvalue λ_i and $\mathbf{x}$ is the state of the system before the measurement.
- After performing a measurement by a matrix $\mathbf{A}$ with outcome λ, the state changes, and it becomes an eigenvector of $\mathbf{A}$ corresponding to the eigenvalue λ.

For the sake of simplicity, we will not explicitly address the case when a measurement matrix has eigenspaces of dimension greater than one. Treating the general case is technical, and we do not need it for our outline of the principles of quantum mechanics; hence we will be silent about the technical details.

Using the spectral theorem, we may rewrite a measurement $\mathbf{A} \in \mathbb{R}^{n \times n}$ as a sum of dyads, $\mathbf{A} = \lambda_1 \mathbf{v}_1 \mathbf{v}_1^T + \lambda_2 \mathbf{v}_2 \mathbf{v}_2^T + \ldots + \lambda_n \mathbf{v}_n \mathbf{v}_n^T$, with pairwise orthogonal eigenvectors $\mathbf{v}_i$, $i = 1, \ldots, n$. Then the process of measurement may be seen as the state collapsing to one of the eigenvectors of $\mathbf{A}$ with probability corresponding to $(\mathbf{x}^T \mathbf{v}_i)^2$ for eigenvector $\mathbf{v}_i$.

We will show a simple illustrative example of the process of performing measurements.

Example 2.1. Let the description of experiment be as follows:

- The system is $H = \mathbb{R}^2$.
- The state of H is $\mathbf{x} = (1, 0)$.
- The measurement is $\mathbf{M} = \frac{1}{4}\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ and its eigenvalues and eigenvectors are:
  - $\mathbf{v}_1 = \frac{\sqrt{2}}{2}(1, 1)$, $\lambda_1 = \frac{3}{4}$.
  - $\mathbf{v}_2 = \frac{\sqrt{2}}{2}(1, -1)$, $\lambda_2 = \frac{1}{4}$.

The probability of measuring the eigenvalue $\frac{3}{4}$ is then $(\mathbf{x}^T \mathbf{v_1})^2 = 0.5$, with state collapsing to eigenstate $\mathbf{v}_1$. Similarly, the probability of measuring $\frac{1}{4}$ is $(\mathbf{x}^T \mathbf{v_2})^2 = 0.5$ and the state would collapse to $\mathbf{v}_2$.

2.2 EPR Paradox

Einstein, although one of its fathers, was skeptical about the completeness of the quantum theory. He considered the probabilistic character of quantum measurements not to be caused by nature but by our inability to determine reality. In a famous paper [13], the authors (Einstein, Podolski, Rosen, hence the EPR paradox) supported their skepticism by performing a thought experiment.

In the experiment, there are two observers, let us call them Alice and Bob. At the start of the experiment, they are at the same place, and both of them are given a particle, which is in an entangled state. We will get to the quantum entanglement later; for now, we may consider the entangled particles to be identical. Now, Bob and Alice walk away from each other several light-years. The paradox arises when Alice measures her particle. The outcome of the measure is random, following the rules described before. However, when Bob makes the exact measurement, he will get a (for him) seemingly random outcome, but in fact, the outcome will be identical to Alice's. This phenomenon is observed whenever they make the measurements, possibly at the same time, while being arbitrarily distant.

The information about the outcome of Alice's measurement is propagated instantly to Bob, which is faster than the speed of light. This was not a satisfactory result, and the authors concluded that the interpretation of quantum mechanics is incomplete.

2.3 Hidden-Variable Theory

A solution to the paradox mentioned above would be an introduction of new variables that describe the system, but we cannot get to know them. The paradox will be resolved if we introduce hidden variables. The paradox was built on quantum entanglement, which requires the particles (loosely speaking) to be very close to each other at some time. Hence, the particles could have agreed on how they would act on different measurements performed in the future, hence on measurement, the particles would act according to the agreement, and no transfer of information, faster than the speed of light, would be necessary.

It may seem plausible to introduce such a concept to get rid of its randomness and innocent at the same time, since there is no apparent difference between events being random and events being deterministic but unknown to us beforehand. Einstein was a great supporter of this interpretation and his famous quote:

`God does not play dice`

originates in this context.

It later turned out that such hidden variables do not describe the world well[1], and the outcomes of measurements are indeed random in their nature.

2.3.1 Informal Historical Overview

In 1932, von Neumann has proven in his book [46] that the hidden-variable theory is wrong. However, it later turned out that he used an absurd assumption.

The flaw was noticed in 1935, in the paper [19], but it remained overlooked until the sixties. Then, in the paper [3], Bell eventually pointed out von Neumann's mistake.

In the year 1964, Bell proposed an experiment yielding different outcomes for the theory with, and without, hidden variables. Later, in the years 1966 and 1967 respectively, Bell in [3], and independently Kochen and Specker in [22], have proven the nonexistence of hidden variables in a more general way, and the theorem is called a *Bell–Kochen–Specker theorem* (abbr. BKS theorem). We will inspect the BKS theorem extensively in the following chapters.

The EPR paradox indicates that there may be occurring some communication between particles which is propagated faster than light. This is addressed by a so-called no-communication theorem, see [39], which states that none of the observers is able to influence the measurement of the other; hence no communication is occurring here.

Nevertheless, a pair of entangled particles may allow us to achieve results that would be impossible if there were some hidden variables. Before showing such examples and ruling out the hidden-variable theory, we shall precisely introduce the quantum entanglement first.

2.4 Quantum Entanglement

In the EPR paradox, Alice and Bob needed to have, in some sense, identical particles. The phenomenon is called quantum entanglement and is described as follows. Let there be two quantum systems, H_A, and H_B. The quantum system containing both, $H_A \in \mathbb{R}^n$ and $H_B \in \mathbb{R}^m$, can be written[2] as $H = H_A \times H_B \in \mathbb{R}^{m+n}$. Sometimes a state $\mathbf{x} \in H$

[1] There still exist several non-local hidden-variable theories, see [8] and its derivations for an example. We will not be precise here.

[2] The operators $\otimes, \times$ are the Kronecker product and Cartesian product respectively.

may be written as $\mathbf{x} = \mathbf{x}_A \otimes \mathbf{x}_B$ for some $\mathbf{x}_A \in H_A, \mathbf{x}_B \in H_B$. In that case, we call the state $\mathbf{x}$ to be separable. However, not all states are separable; in that case, we call them entangled. Before we move on to the examples, we shall summarize this in the upcoming definition.

Definition 2.2. Let $H_A, H_B, H = H_A \times H_B$ be quantum systems. A state $\mathbf{x} \in H$ is called an *entangled* state, if there are no states $\mathbf{x}_A \in H_A, \mathbf{x}_B \in H_B$ such that $\mathbf{x} = \mathbf{x}_A \otimes \mathbf{x}_B$. The systems (particles) H_A, H_B are then called entangled.

Example 2.2. Let $H_A, H_B \in \mathbb{R}^2$ be two quantum systems and $H \in \mathbb{R}^4$ be the composite quantum system.

- A state $(1,0,0,0)$ can be written as $(1,0) \otimes (1,0)$, hence it is a separable state.
- A state $\frac{1}{\sqrt{2}}(1,0,0,1)$ is entangled, since it cannot be written as

$$(a,b) \otimes (c,d) = (a(c,d), b(c,d)) = (ac, ad, bc, bd)$$

  because no element of $\{a,b,c,d\}$ can be zero, but at the same time some of them has to be zero.
- A state $\frac{1}{\sqrt{2}}(1,0,0,1)$ can be written as a linear combination of separable states:

$$\frac{1}{\sqrt{2}}(1,0,0,1) = \frac{1}{\sqrt{2}}((1,0,0,0) + (0,0,0,1)) = \frac{1}{\sqrt{2}}((1,0) \otimes (1,0) + (0,1) \otimes (0,1)).$$

When a state of $H = H_A \times H_B$ is separable, we do not need to merge the systems. Hence, in the first example, we can describe the system H, using the systems H_A, H_B separately.

In the last example, we have shown a decomposition of an entangled state into a linear combination of separable states. When both of the particles represented by H_A, H_B are measured by $\mathbf{M} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, there are two possible outcomes:

- The entangled state $\mathbf{x}$ collapses to state $(1,0) \otimes (1,0)$, and both measurements have outcome 1.
- The entangled state $\mathbf{x}$ collapses to state $(0,1) \otimes (0,1)$, and both measurements have outcome -1.

Both of the cases happen with 50 % probability, but as soon as one of the particles is measured, the second outcome is deterministic.

The entangled particles need not behave the same way. The important property is that a measurement of one particle affects the outcome of a measurement of the entangled one.

2.5 Compatible Measurements

Although generally the process of taking a measurement affects the state, it may happen that two measurements, $\mathbf{A}, \mathbf{B}$, are compatible, and we may perform multiple measurements of one state. To be precise, we say that two measurements, $\mathbf{A}, \mathbf{B}$ are compatible if whenever we make consecutive measurements $\mathbf{A}$, then $\mathbf{B}$, and then again $\mathbf{A}$, the outcome of the first and the last measurement are equal.

Proposition 2.1. For any two measurements $\mathbf{A}$, $\mathbf{B}$, the following properties are equivalent:

- They are compatible.
- They share an eigenbasis.
- The matrices $\mathbf{A}$, $\mathbf{B}$ commute.

Proof.

- (i $\Rightarrow$ ii) After performing the measurement $\mathbf{A}$, the state will collapse to eigenvector $\mathbf{v}_A$ of $\mathbf{A}$. After measurement $\mathbf{B}$, the state will be $\mathbf{v}_B$. If $\mathbf{v}_A \neq \mathbf{v}_B$, then the outcome of measurement $\mathbf{A}$ of state $\mathbf{v}_B$ would not equal to the first outcome with certainty. Hence, they share every eigenvector, and the eigenbases are equal.
- (ii $\Rightarrow$ i) After the first measurement, the state will collapse to a common eigenvector of $\mathbf{A}$, $\mathbf{B}$ and will not be changed by any consecutive measurement of $\mathbf{A}$ or $\mathbf{B}$.
- (ii $\Rightarrow$ iii) The matrices are symmetric and share an eigenbasis. We rewrite them using the spectral theorem with orthogonal[1] matrix $\mathbf{V}$ and diagonal (thus commuting) matrices $\mathbf{\Lambda}_A$, $\mathbf{\Lambda}_B$. Then

$$\mathbf{AB} = \mathbf{V\Lambda}_A\mathbf{V}^T\mathbf{V\Lambda}_B\mathbf{V}^T = \mathbf{V\Lambda}_A\mathbf{\Lambda}_B\mathbf{V}^T = \mathbf{V\Lambda}_B\mathbf{\Lambda}_A\mathbf{V}^T = \mathbf{V\Lambda}_B\mathbf{V}^T\mathbf{V\Lambda}_A\mathbf{V}^T = \mathbf{BA}.$$

- (iii $\Rightarrow$ ii) For an eigenvector $\mathbf{v}$ of $\mathbf{A}$ corresponding to the eigenvalue λ it holds:
  - $\mathbf{Av} = \lambda\mathbf{v}$,
  - $\mathbf{ABv} = \mathbf{BAv} = \lambda\mathbf{Bv}$,

  Hence both vectors, $\mathbf{v}$ and $\mathbf{Bv}$, correspond to the same eigenvalue. We assumed that the eigenspaces are one-dimensional, hence $\mathbf{Bv} = \lambda\mathbf{v}$; thus $\mathbf{v}$ is also an eigenvector of $\mathbf{B}$. This holds for every eigenvector of $\mathbf{A}$; thus, the eigenbases are equal.

∎

Corollary 2.2. Let $\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n$, be pairwise compatible measurements, then the following propositions hold true:

- The measurements $\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n$, together with the matrix $\mathbf{A}_1\mathbf{A}_2 \dots \mathbf{A}_n$, share an eigenbasis.
- The product of outcomes of measurements $\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n$ is an eigenvalue of matrix $\mathbf{A}_1\mathbf{A}_2 \dots \mathbf{A}_n$.

2.6 Quantum Pseudo-Telepathy

Now we shall rule out the hidden-variable model. To be precise, we show a thought experiment yielding different outcomes for the theories with hidden variables and those without them. To eventually decide which model describes nature better, one must experiment with reality, and it disproves the hidden-variable theory.

[1] A matrix $\mathbf{V} \in \mathbb{R}^{n \times n}$ is called *orthogonal*, if it is regular and $\mathbf{V}^T = \mathbf{V}^{-1}$.

We demonstrate the insufficiency of hidden-variable theory by using a phenomenon called quantum pseudo-telepathy.

This phenomenon was first described in [35]; the following example is called a *Peres–Mermin square*.

The phenomenon is called pseudo-telepathy since the result is similar to what we would consider telepathy. However, on the other hand, we have already mentioned the no-communication theorem. Hence no transfer of information is possible, and the phenomenon instead bypasses the need for telepathy rather than enabling it.

Consider a game where Alice and Bob are trying to fill a 3×3 table by values ± 1, where Bob will fill one row and Alice one column. Bob and Alice may agree on a strategy before the game, but they cannot communicate after the game starts.

When the game starts, Bob is given a number $r \in \{1, 2, 3\}$, determining which row to fill. Similarly for Alice, she gets a number $c \in \{1, 2, 3\}$, determining the column. Thus, both of them know their number but do not know the other.

They will win the game if the product of Alice's numbers is -1, the product of Bob's numbers is 1, and they have assigned an equal number to the entry at position r, c.

Example 2.3. If Bob gets $r = 1$, Alice gets $c = 3$, then Bob's assignment $(1, 1, 1)$, together with Alice's assignment of $(1, 1, -1)$ will result in Table 2.1[1], hence it is a winning assignment.

1	1	1	1
		1	
		-1	
		-1	

Table 2.1. Example of a winning assignment

On the other hand, if Bob assigned the numbers $(1, 1, 1)$ with $r = 3$ and Alice would assign $(1, 1, -1)$ with $c = 3$, they would lose, as illustrated in Table 2.2.

		1	
		1	
1	1	$1 \neq -1$	1
		-1	

Table 2.2. Example of a losing assignment

It is impossible for them to win every game, even when they can communicate before the game and share their strategies. If they could always win, it would mean that they can fill the table before the game such that the values in every row multiply to one, while the values in every row will multiply to minus one. Their assignment would then correspond to the values of Table 2.3. E.g., Alice with $c = 2$ would assign values $(M_{1,2}, M_{2,2}, M_{3,2})$ to the second column.

It is not possible to fill such table since the product of all filled numbers should be positive if we are multiplying the values by rows, but at the same time, it should be

[1] The last column and row are the results of multiplication of numbers in the corresponding column or row respectively.

$M_{1,1}$	$M_{1,2}$	$M_{1,3}$	1
$M_{2,1}$	$M_{2,2}$	$M_{2,3}$	1
$M_{3,1}$	$M_{3,2}$	$M_{3,3}$	1
-1	-1	-1	

Table 2.3. General assignment

negative if we multiply the values by columns. This is an apparent contradiction since the multiplication of integers is associative. However, on the other hand, it is possible to fill the table using matrices such that they multiply by rows to the identity matrix and by columns to the negative identity matrix.

We introduce the following matrices. They are called Pauli matrices, and we use their standard names:

$$\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

and remind the identity for Kronecker product and matrix multiplication:

$$(\mathbf{A} \otimes \mathbf{B})(\mathbf{C} \otimes \mathbf{D}) = (\mathbf{AC}) \otimes (\mathbf{BD}).$$

Furthemore, it holds that $\mathbf{X}^2 = \mathbf{Z}^2 = \mathbf{I}_2$ and $\mathbf{XZ} = -\mathbf{ZX}$, where $\mathbf{I}_k \in \mathbb{R}^{k\times k}$ is the identity matrix. The eigenvalues of matrices $\mathbf{X}, \mathbf{Z}$ are ± 1.

Now we can check that for Table 2.4

$\mathbf{I}_2 \otimes \mathbf{Z}$	$\mathbf{Z} \otimes \mathbf{I}_2$	$\mathbf{Z} \otimes \mathbf{Z}$	$\mathbf{I}_4$
$\mathbf{X} \otimes \mathbf{I}_2$	$\mathbf{I}_2 \otimes \mathbf{X}$	$\mathbf{X} \otimes \mathbf{X}$	$\mathbf{I}_4$
$-\mathbf{X} \otimes \mathbf{Z}$	$-\mathbf{Z} \otimes \mathbf{X}$	$\mathbf{ZX} \otimes \mathbf{XZ}$	$\mathbf{I}_4$
$-\mathbf{I}_4$	$-\mathbf{I}_4$	$-\mathbf{I}_4$	

Table 2.4. Table of measurements

The following properties hold:

- The product of matrices in every row is the identity matrix.
- The product of matrices in every column is the negative identity matrix.
- Every pair of matrices in every column commutes.
- Every pair of matrices in every row commutes.
- Every matrix in the table has eigenvalues ± 1.

2.6.1 Winning Strategy

Let us describe the winning strategy for Bob and Alice. They will both have a particle, which is entangled with the other such that the outcomes of the measurements will be the same for both of them. The system of one particle is $\mathbb{R}^4$, so the composite system is $\mathbb{R}^8$, but we will not go into technical details here.

Every element of Table 2.4 corresponds to a measurement. When Bob and Alice want to fill an entry of the table, they perform the measurement associated with the position, and they would assign the outcome of the measurement, which is ± 1. The matrices commute, hence the measurements are compatible, and it does not matter in which order the measurements are made.

This is indeed a winning strategy. According to Corollary 2.2, the product of Alice's numbers will be an eigenvalue of matrix $-\mathbf{I}_4$, which can only be -1. Similarly for Bob, the product of his numbers is 1. Bob and Alice have entangled particles such that their outcome of a common measurement will be the same; hence they would fill the same number in the common position.

Corollary 2.3. Quantum mechanics allows a winning strategy for a game, for which there is no winning strategy in a deterministic world.

2.7 Quantum Logic

In a later chapter of the thesis, we will deal with quantum logic, more precisely, with certain algebraic structures, which could be used to describe the algebra of quantum logic.

We are interested in the study of quantum structures themselves, rather than in their connection with physics; hence we will only briefly review the reasons why the standard logic (represented by a Boolean algebra) is insufficient in quantum mechanics.

2.7.1 Heisenberg Uncertainty Principle

Possibly the most explicit argument on the incompatibility of classical logic and quantum logic is derived from the Heisenberg uncertainty principle. It states that the more precisely we know a particle's position, the less precisely we know its momentum[1]. We show a heavily simplified example that demonstrates the fact that quantum logic is not distributive. It is not meant to prove the non-distributivity; it should instead provide the reader an intuition of why the distributivity may be violated.

We formulate the uncertainty principle as:

$$\Delta x \Delta p \geq \frac{\hbar}{2},$$

Let us introduce the following logical variables, where we use units such that $\frac{\hbar}{2} = 1.5$:

- A: $0 \leq p \leq 1$, i.e., the momentum of a particle is between zero and one.
- B: $-1 \leq p \leq 0$, i.e., the momentum of a particle is between minus one and zero.
- C: $0 \leq x \leq 1$, i.e., the position of a particle is between zero and one.

The uncertainty of position and momentum, respectively, is the length of the interval in which they are known to be.

We recall the distributive law in propositional logic:

$$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C).$$

Plugging in the logical variables[2], we conclude that the formula on the right-hand-side cannot be true, since neither $(A \wedge B)$ nor $(A \wedge C)$ can be measured due to the Heisenberg uncertainty principle. On the other hand, the proposition on the left-hand-side may be true; thus the quantum logics do not follow the distributive law.

[1] But it also may be expressed using different quantities, such as time and energy.

[2] The meaning of logical connectives $\wedge, \vee$ for the logical variables is hopefully intuitive, e.g., $A \vee B$ stands for $-1 \leq p \leq 1$, $A \wedge C$ stands for $(p, x) \in [0, 1]^2$, etc.

2.7.2 Observer Effect

In the classical case, it is expected that the measurement does not change the state of the system. For example, let us consider a car. We are able to measure its momentum and position without affecting it.

It is not the case in quantum mechanics anymore. The act of measuring the position of a particle is tied, e.g., with a photon interacting with the particle. The interaction between the photon and the particle results in a change of the state of the particle. Hence, the measured position is not the current but rather a past position of the measured particle.

We have already discussed the compatibility of measurements in Section 2.5.

It may happen that several measurements are compatible; hence we can imagine measuring them at the same time. On the other hand, this is not possible for every pair of observables.

2.7.3 Quantum Structures

Von Neumann in [46], and later together with Birkhoff in [7], have shown (with the use of heuristic arguments) that the propositions about quantum mechanics are well described by the calculus of linear subspaces of a Hilbert space, which can be represented using a modular ortholattice.

Later, it was shown that it is unnecessary to require the modularity condition, and a weaker one, orthomodularity, suffices. There are also different algebraic structures used to describe the quantum logic, for example, orthomodular posets, orthoalgebras and (lattice) effect algebras. For more information about quantum logic, we refer the reader to books [12, 44] written by physicists, or to [40], written by mathematicians.

We will study even more specific algebras, having potential in being applied in quantum theory, which are orthocomplemented lattices with a symmetric difference, coined in [24].

Chapter 3
Bell–Kochen–Specker Theorem

The Bell–Kochen–Specker theorem (abbr. BKS theorem) is a no-go theorem that invalidates most of the hidden-variable theories in quantum mechanics. It was proven independently by Bell in 1966 in [3] and by Kochen and Specker in 1967 in [22]. Bell's proof is simpler but only rules out hidden variables in four or higher dimensions. On the other hand, the proof of Kochen and Specker addresses even the tree-dimensional case; hence it is a more general result. Admittedly, the theorem is a simple corollary of much more general Gleason's theorem with which we will deal in Section 3.2. Gleason's theorem was proved in 1957 in [14] but was overlooked by the physicists' community.

The theorem resolves the problem whether it is possible that the outcomes of measurements are deterministic but unknown to us beforehand. We have already discussed the hidden-variable theory in Section 2.3.

3.1 Statement

Here, we consider the following setup. Let there be a particle with state $\mathbf{x} \in \mathbb{R}^n$ which we want to measure. We can measure it in n orthogonal directions, and in precisely one of those, the outcome will be 1, and in other directions, the outcome is always 0. Our goal is to disprove the hidden-variable theory, according to which the outcomes of measurements are already known (but not to us), and the measurement only reveals those hidden states. If this was the case, then we could assign zeros and ones to the vectors of $\mathbb{R}^n$ such that precisely one vector in every orthogonal basis would be assigned 1. It turns out that it is not possible for $n \geq 3$. Before going into details, we make of this the upcoming theorem:

Theorem 3.1. There is no mapping $v : \mathbb{R}^n \setminus \{\mathbf{0}\} \to \{0, 1\}$ such that for every orthogonal basis $\mathbf{x}_1, \mathbf{x}_2, \ldots \mathbf{x}_n$ of $\mathbb{R}^n$ the following holds:

$$v(\mathbf{x}_1) + v(\mathbf{x}_2) + \ldots + v(\mathbf{x}_n) = 1,$$

if and only if $n \geq 3$.

Clearly, for any mapping v, every vector $\mathbf{x} \in \mathbb{R}^n$ and scalar $c \in \mathbb{R}, c \neq 0$, it holds that $v(\mathbf{x}) = v(c \cdot \mathbf{x})$; hence we may, without loss of generality, assume that we are assigning values to one-dimensional subspaces, which we call *rays*. We will use rays and vectors interchangeably. We will also refer to mapping v as a *coloring*.

Proof of Theorem 3.1. The case when $n \leq 1$ is trivial. When $n = 2$, no two distinct orthogonal bases share a vector; thus, we may assign one vector of every orthogonal basis 0 and 1 to the other arbitrarily.

The case when $n = 3$ is complicated, and we dedicate Subsection 4.3.1 to it. For now, assume that the theorem holds for $n = 3$, and we show that it holds for any dimension $m \geq 4$.

Assume to the contrary that there is a coloring v in $\mathbb{R}^m$. There is also an orthogonal basis $\{\mathbf{x}_1, \mathbf{x}_2, \dots \mathbf{x}_m\}$. Without loss of generality, $v(\mathbf{x}_i) = 1 \iff i = 1$.

Consider the set $Y = \operatorname{span}(\{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3\})$. Every its orthogonal basis $\{\mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3\}$ must satisfy $v(\mathbf{y}_1) + v(\mathbf{y}_2) + v(\mathbf{y}_3) = 1$ since $\{\mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3, \mathbf{x}_4, \mathbf{x}_5, \dots \mathbf{x}_m\}$ is an orthogonal basis of $\mathbb{R}^m$. Clearly, Y is isomorphic to $\mathbb{R}^3$, and we found a coloring of $\mathbb{R}^3$ which we assumed to be impossible. ■

Although the argument uses the fact that for $n = 3$ there is no coloring, it is clear that an almost identical argument would conclude that there is no coloring of $\mathbb{R}^m, m > n$, if we show that there is no coloring of $\mathbb{R}^n$.

Remark 3.2. Whenever $v : \mathbb{R}^n \setminus \{\mathbf{0}\} \to \{0, 1\}$ is a coloring, then also v' defined as $v'(\mathbf{x}) = v(\mathbf{U}\mathbf{x})$ for an orthogonal matrix $\mathbf{U}$ is a coloring since a transformation by an orthogonal matrix preserves the dot product and hence preserves the orthogonality relation.

Example 3.1. Let us have the following rays:

- $\mathbf{x} = (1, 1, 1)$,
- $\mathbf{y} = (0, 1, 1)$,
- $\mathbf{z} = (1, 1, 0)$.

We are also given the information that for every coloring v, $v(\mathbf{x}) + v(\mathbf{y}) + v(\mathbf{z}) = 1$.

A mapping $v : \mathbb{R}^n \setminus \{\mathbf{0}\} \to \{0, 1\}$ defined as $v'(\mathbf{x}) = v(\mathbf{U}\mathbf{x})$ is also a coloring, where $\mathbf{U}$ is a matrix representing the reflection by the plane orthogonal to the x-axis. Thus also

$$\begin{aligned} 1 &= v'(\mathbf{x}) + v'(\mathbf{y}) + v'(\mathbf{z}) \\ &= v(\mathbf{U}\mathbf{x}) + v(\mathbf{U}\mathbf{y}) + v(\mathbf{U}\mathbf{z}) \\ &= v((-1, 1, 1)) + v((0, 1, 1)) + v((-1, 1, 0)). \end{aligned}$$

Similarly, for every coloring v it holds that $v(\mathbf{x}') + v(\mathbf{y}') + v(\mathbf{z}') = 1$, where $\mathbf{x}' = \mathbf{U}\mathbf{x}$, $\mathbf{y}' = \mathbf{U}\mathbf{y}$, $\mathbf{z}' = \mathbf{U}\mathbf{z}$ for any orthogonal matrix $\mathbf{U}$.

The original proofs by Bell and Kochen–Specker were based on a construction of a set of vectors that cannot be colored. We discuss this approach more in Section 3.3. The original proof by Kochen and Specker is very similar to the one we present in Section 3.4.

3.2 Gleason's Theorem

We will be dealing with finite sets of points which are not colorable; thus they serve as a proof of BKS theorem. However, the theorem was actually proven by Gleason in [14] in 1957. He has proven an even more general[1] result, known as Gleason's theorem:

Theorem 3.3. Let $n \geq 3$; the only mapping $v : \mathbb{R}^n \to [0, 1]$ such that for any orthonormal basis $\{\mathbf{x}_1, \mathbf{x}_2, \dots \mathbf{x}_n\}$ it holds that $v(\mathbf{x}_1) + v(\mathbf{x}_2) + \dots + v(\mathbf{x}_n) = 1$ is in the form $v(\mathbf{x}) = \mathbf{x}^T \mathbf{A} \mathbf{x}$ where $\mathbf{A}$ is an arbitrary symmetric positive semi-definite matrix with unit

[1] We do not show it in its full generality.

trace.

The BKS theorem is then a trivial consequence. However, the proof of Gleason's theorem is known to be notoriously hard. On the other hand, there must be a finite set of points that is not colorable. This is a corollary of Gödel's completeness theorem. Such sets were consequently found and we will show some later.

The proof of Gleason's theorem has since been simplified and made more elementary, but still there is no space here to write it down. See [40] for the proof.

The theorem is actually an equivalence. The direction that any positive semi-definite matrix with unit trace defines the desired mapping is indeed easy.

Proof of one direction of Theorem 3.3. Take any orthonormal basis $\{\mathbf{x}_1, \mathbf{x}_2, \dots \mathbf{x}_m\}$ and stack the vectors (by columns) to a matrix $\mathbf{X}$. The product $\mathbf{X}^T\mathbf{X}$ is an identity matrix since by the definition of orthonormal basis:

$$(\mathbf{X}^\mathbf{T}\mathbf{X})_{i,j} = \mathbf{x}_i^T\mathbf{x}_j = \begin{cases} 1 & \text{whenever } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Thus $\mathbf{X}$ is an orthogonal matrix, $\mathbf{X}^{-1} = \mathbf{X}^T$ and $\mathbf{X}\mathbf{X}^T = \mathbf{I}_m$. We further use the cyclic property of trace:

$$\sum_{i=1}^{m} v(\mathbf{x}_i) = \sum_{i=1}^{m} \mathbf{x}_i^T\mathbf{A}\mathbf{x}_i = \mathrm{tr}(\mathbf{X}^T\mathbf{A}\mathbf{X}) = \mathrm{tr}(\mathbf{A}\mathbf{X}\mathbf{X}^T) = \mathrm{tr}(\mathbf{A}) = 1.$$

We conclude the proof by remarking that $\mathbf{x}^T\mathbf{A}\mathbf{x} \geq 0$ for any $\mathbf{x} \in \mathbb{R}^n$ and positivie semi-definite matrix $\mathbf{A}$; thus $0 \leq v(\mathbf{x}) \leq 1$. ∎

3.3 BKS Constructions

The original proof of Kochen and Specker consisted of a set of 117 vectors for which there was no coloring. We do not list here the original construction, but we present a gadget approach 3.4 to BKS constructions, and their idea was similar.

Later, Peres [36] found a non-colorable set of 33 vectors. We use the set to prove the BKS theorem in Subsection 4.3.1. Later, a set of 31 vectors that cannot be colored was found by Conway and Kochen [38], see Figure 3.1. The set consists of points (dots in the figure) with integer coordinates on the surface of a cube $[-2, 2]^3$.

3.4 Gadget Structures in BKS Graphs

In this section, we describe an approach to proving the BKS theorem. For convenience, we represent the set of rays using a graph with vertices corresponding to rays and edges denoting the orthogonality relation; thus, we will use vertices and corresponding rays interchangeably.

The proof of the BKS theorem is a trivial consequence of the existence of a BKS graph.

Definition 3.1. A *BKS graph* is a graph $G = (V, E)$ satisfying the following properties:

- For every vertex $v \in V$ there is a corresponding ray $\mathbf{v}$ in $\mathbb{R}^3$ and if there is an edge $(x, y) \in E$ it holds that $\mathbf{x}$ is orthogonal to $\mathbf{y}$.

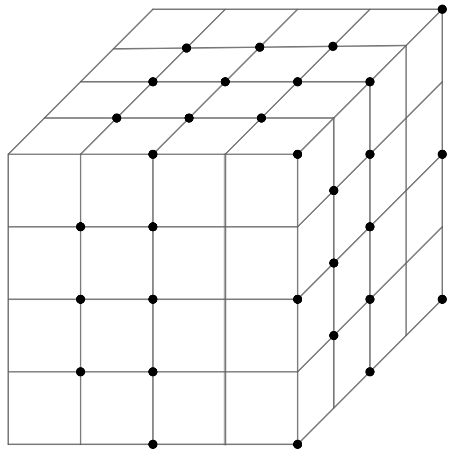

Figure 3.1. Conway–Kochen set

- The set of rays corresponding to the vertices is not colorable. That is, there is no mapping $v : V \to \{0,1\}$ such that for every edge $(x,y) \in E$, $v(x)+v(y) \leq 1$, and for every triangle[1] x, y, z it holds that $v(x)+v(y)+v(z) = 1$.

Recently, in [41], it was shown that every BKS graph has a colorable subgraph with two distinguished vertices x, y which are not connected by an edge, and in every possible coloring v it holds that $v(x)+v(y) \leq 1$. More interestingly, they also showed that we could construct a BKS graph from such subgraphs. It is not that surprising since the original proof of Kochen and Specker adopted a similar construction, but they did not describe the technique in general. The results of [41] are also more general since their constructions work in arbitrary dimensions. We prove the results only in three dimensions. Let us first show a construction of how to obtain a gadget from a BKS graph.

Definition 3.2. A graph $G = (V,E)$ is called a *gadget* if it is colorable and there are vertices $x, y \in V$ such that $(x,y) \notin V$ and no coloring satisfies $v(x) = v(y) = 1$.

Theorem 3.4. Let a graph $G = (V,E)$ be a BKS graph. Then it contains a gadget as a subgraph.

Proof. The graph is not colorable. We will remove one edge from E at a time until the removal of the next edge (x,y) would result in a colorable graph. We remove the edge, and the resulting graph is a gadget. Every coloring necessarily satisfies $v(x) = v(y) = 1$, otherwise it would be a valid coloring even before the removal. Since $v(x) = 1$, it must be contained in a triangle, thus there is a triangle a,b,x and in every coloring it necessarily holds that $v(b) = 0$. Thus $v(y)+v(b) \leq 1$ and they are not orthogonal, so it is indeed a gadget. ∎

[1] A triangle is a complete subgraph on 3 vertices.

The construction may be interesting from a graph-theoretical perspective. However, on the other hand, the set of vertices, i.e., rays, remains the same, and the action of deleting an edge makes no sense. According to [41], every known BKS graph contains an **induced** subgraph that is a gadget. This is a much more interesting and stronger result, but in general, it was not shown yet that it is possible for every BKS graph.

We proceed with a construction that produces a BKS graph from gadgets. We show it on an example.

Let us first present a gadget captured in Figure 3.2.

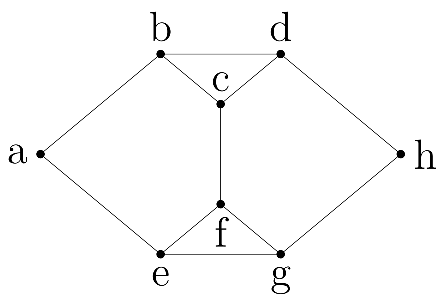

Figure 3.2. Gadget "Specker's bug"

Rays corresponding to vertices:

- $\mathbf{a} = (1, -1, 1)$
- $\mathbf{b} = (1, 1, 0)$
- $\mathbf{c} = (0, 0, 1)$
- $\mathbf{d} = (-1, 1, 0)$
- $\mathbf{e} = (0, 1, 1)$
- $\mathbf{f} = (1, 0, 0)$
- $\mathbf{g} = (0, 1, -1)$
- $\mathbf{h} = (1, 1, 1)$

Proposition 3.5. The graph in Figure 3.2 is a gadget with distinguished vertices a, h.

Proof. First we show that there is a coloring, then we show that there is no coloring v, $v(a) = v(h) = 1$.

The mapping v defined as

$$v(x) = \begin{cases} 1 & \text{if } x \in \{e, d\}, \\ 0 & \text{otherwise}, \end{cases}$$

is clearly a coloring.

For the other part, we proceed by contradiction. Assume to the contrary that there is a coloring v such that $v(a) = v(h) = 1$. Then $v(b) = v(d) = 0$ and $v(c) = 1$. Similarly, $v(e) = v(g)$ and $v(f) = 1$; thus $1 = v(c) = v(f)$ which is a contradiction since they are connected by an edge.

■

Now consider the four rays[1]:

- $\mathbf{a}$
- $\mathbf{h}$
- $\mathbf{a} \times \mathbf{h}$
- $(\mathbf{a} \times \mathbf{h}) \times \mathbf{h}$

If $v(\mathbf{a}) = 1$, then $v(\mathbf{h}) = v(\mathbf{a} \times \mathbf{h}) = 0$ and $v((\mathbf{a} \times \mathbf{h}) \times \mathbf{h}) = 1$. Thus, we are able to construct a graph with two distinguished vectors s, t such that whenever $v(s) = 1$,

[1] Operator $\times$ stands for cross product. It produces a vector orthogonal to both operands.

then also $v(t) = 1$. See the graph in Figure 3.3 for an extended graph from Figure 3.2 with omitted/renamed labels for brevity. We call such a graph a 11-gadget[1].

Definition 3.3. A graph $G = (V, E)$ is called a 11-*gadget* if it contains two vertices $s, t \in V$ such that in any coloring $v(s) = 1 \Rightarrow v(t) = 1$. We will also use a term 11_θ-gadget, where the θ stands for the angle between rays corresponding to vertices s, t. We will also call the distinguished vertices s and t.

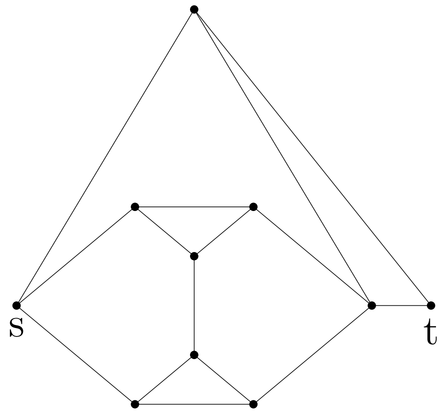

Figure 3.3. 11-gadget

We can chain the 11-gadgets in the sense of Figure 3.4. The resulting graph is again a 11-gadget since $v(s_1) = 1 \Rightarrow v(t_2) = 1$ for any coloring v.

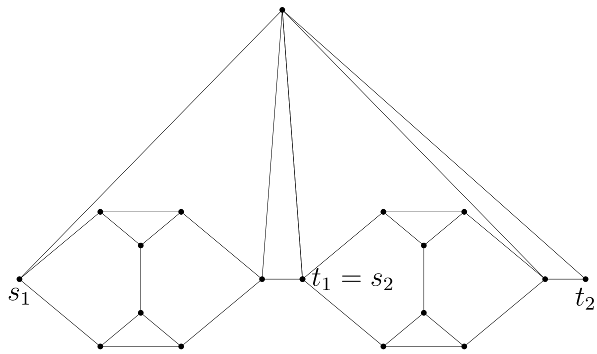

Figure 3.4. Chain of 11-gadgets

In this particular example, the rays corresponding to s_1, $s_2 = t_1$, t_2 are in a common plane; thus the rays s_1 and t_2 make double the angle of the rays s_1 and t_1. The angle may be smaller if the rays do not lie in a common plane.

Remark 3.6. Let us have two 11_θ-gadgets with s, t being s_1, s_2 and t_1, t_2 respectively. We may chain them so that $t_1 = s_2$; thus $v(s_1) = 1 \Rightarrow v(t_2) = 1$. The chain forms a $11_{\theta'}$-gadget, where θ' is an arbitrary number from interval $(0, 2\theta]$ and is a 11-gadget.

Now we have all the tools needed to construct a BKS graph from a chain of 11_θ gadgets. Take any orthogonal basis **a**, **b**, **c** and use the just constructed 11-gadget such that

[1] Here 11 stands for "one-one", not for eleven.

$v(\mathbf{a}) = 1 \Rightarrow v(\mathbf{b}) = 1$, $v(\mathbf{b}) = 1 \Rightarrow v(\mathbf{c}) = 1$, $v(\mathbf{c}) = 1 \Rightarrow v(\mathbf{a}) = 1$. Then the resulting graph will be a BKS graph.

Thus, we obtained a proof of the BKS theorem.

3.5 Computational Aspects of Searching for BKS Graphs

There is a research direction aiming at finding the smallest possible BKS graph. At the time of writing, the smallest known BKS graph contains 31 vertices; we have already presented the construction in Figure 3.1.

Recently, it was shown that no graph with 21 or fewer vertices is a BKS graph, see [45]. The lower bounds on the number of vertices of a BKS graph are obtained by an exhaustive generation of graphs and verifying that they are indeed not BKS graphs. We decompose the general approach to verify that there is no BKS graph with a given number of vertices into three problems, each of which is computationally demanding.

3.5.1 Exhaustive Generation of Graphs

The state-of-the-art approach generates all graphs up to a given size that does not violate the necessary conditions for a graph to be a BKS graph, see 3.5.2. The process of enumerating all possible graphs with a given number of vertices is intractable even for small graphs with, e.g., 15 vertices since the graphs generally have a huge automorphism group. A solution to this problem is the isomorphism-free exhaustive generation, see [30]. Unfortunately, no algorithm with polynomial time complexity is known for the graph-isomorphism problem; thus, the isomorphism-free generation is computationally extensive.

3.5.2 Embeddability of Graphs

Given a graph, it is not immediate if its vertices can be assigned rays of $\mathbb{R}^3$ such that the edges follow the orthogonality relation. Therefore, we call a graph *embeddable* if there is such an assignment.

There are known some necessary but not sufficient graph-theoretical properties of the smallest possible BKS graph. For instance, it is 4-colorable and contains no cycle of length 4.

To eventually decide if a graph $G = (V, E)$ is embeddable, it is necessary to solve a system of polynomial equations with three variables v_1, v_2, v_3 for every vertex $v \in V$ determining the ray. There is one equation for every edge and one for every vertex.

- $v_1^2 + v_2^2 + v_3^2 = 1$ for every vertex $v \in V$.
- $u_1 v_1 + u_2 v_2 + u_3 v_3 = 0$ for every edge $(u, v) \in E$.

That is a hard problem, see [1].

3.5.3 Coloring Verification

The last problem is to verify if a graph is colorable in the BKS sense or not. Unfortunately, this is again an *NP*-hard problem. The problem can be reduced to the 3-coloring problem, which is known to be *NP*-hard even if the graph is embeddable, we refer to [1].

Chapter 4
Modifications of Bell–Kochen–Specker Theorem

We review a handful of notable variants of the Bell–Kochen–Specker theorem. The variants were often proposed by physicists but enjoyed great attention even in the mathematical community.

4.1 Rational Measurements

The physicists' community questioned the assumption of BKS theorem, which allowed real measurements. They argued about the fact that the measurements are not exact; hence it does not make sense to consider the measurements to be real. An additional motivation to the consideration of the rational version of BKS theorem is the discrete nature of quantum physics.

It is an easy corollary of [15] that the set of unit vectors with rational coordinates in three dimensions is $\{0,1\}$-colorable. It is subject to debate if this result nullifies the BKS theorem or not; see [18, 31] for the respective arguments.

We will prove the theorem using analogical tools to those in [15]; hence also to those in [18, 31]. We also use red/blue colors instead of zeros and ones for the sake of brevity.

Theorem 4.1. The set $M = \{\boldsymbol{x} \mid \boldsymbol{x}^T\boldsymbol{x} = 1, \boldsymbol{x} \in \mathbb{Q}^3\}$ can be colored in a way that for every three pairwise orthogonal vectors precisely one of them is colored red and the remaining two are colored blue.

Before we proceed with the proof, we note that if we scale every vector of M by an arbitrary non-zero scalar, not necessarily the same for every vector, the new set would be colorable if and only if the original set was colorable, since two scaled vectors are orthogonal if and only if they were orthogonal before scaling. This leads us to the observation that we can see the set M as the set of precisely those one-dimensional subspaces of $\mathbb{R}^3$ that intersect with the unit rational sphere. First, we choose a convenient representative for every vector of M.

Definition 4.1. We call a triplet of integers x, y, z *Pythagorean*, if they are not all zeros and there is an integer n such that $x^2 + y^2 + z^2 = n^2$. Let the set of all Pythagorean triplets be P, and we will treat them as vectors in $\mathbb{R}^3$.

Lemma 4.2. There is the following correspondence between Pythagorean triples and rational unit vectors:

- For every vector $(a, b, c) \in M$ there is a real α such that $\alpha(a, b, c) \in P$.
- For every triplet $(x, y, z) \in P$ there is a real β such that $\beta(x, y, z) \in M$.

Proof.

- By definition of M, we may rewrite

$$(a, b, c) = \left(\frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3}\right)$$

for integers p_i, q_i, $i \in \{1, 2, 3\}$, and it also holds that:

$$\left(\frac{p_1}{q_1}\right)^2 + \left(\frac{p_2}{q_2}\right)^2 + \left(\frac{p_3}{q_3}\right)^2 = 1.$$

Thus we choose $\alpha = q_1 q_2 q_3$ and indeed

$$(p_1 q_2 q_3)^2 + (q_1 p_2 q_3)^2 + (q_1 q_2 p_3)^2 = (q_1 q_2 q_3)^2.$$

- We divide the equation $x^2 + y^2 + z^2 = n^2$ by n^2 and get

$$\left(\frac{x}{n}\right)^2 + \left(\frac{y}{n}\right)^2 + \left(\frac{z}{n}\right)^2 = 1,$$

hence $(\frac{x}{n}, \frac{y}{n}, \frac{z}{n})$ is a unit vector and has rational coordinates and therefore is contained in M.

■

Of course, the second claim of Lemma 4.2 is not needed to prove the theorem, and we list it only for the sake of completeness. Lemma 4.2 allows us to identify vectors of M with their scaled versions from P.

Lemma 4.3. For every Pythagorean triplet $(x, y, z) \in P$, it holds that at most one of its coordinates is odd.

Proof. Looking for a contradiction. Let there be two or three odd numbers among $(x, y, z) \in P$, then $x^2 + y^2 + z^2 \equiv m \pmod 4$, $m \in \{2, 3\}$, but quadratic residues modulo 4 are only $0, 1$; a contradiction. ■

Note that whenever a vector $\boldsymbol{p} \in P$ contains an odd element at position i, then, by a simple corollary of the uniqueness of prime factorization, there is no scalar α such that $\alpha\boldsymbol{p} \in P$ has an odd element at coordinate $j \neq i$, where $i, j \in \{1, 2, 3\}$.

Proof of Theorem 4.1. We prove the theorem by giving an explicit coloring. Employing the Lemma 4.2, every vector $\boldsymbol{x} \in M$ is a scaled vector $\boldsymbol{p} \in P$. Without loss of generality, the greatest common divisor of elements of $\boldsymbol{p}$ is 1. Then the vector $\boldsymbol{p}$ has precisely one odd element by Lemma 4.3. We color $\boldsymbol{x}$ by red if and only if the odd element of $\boldsymbol{p}$ is in its last position. We note that whenever two vectors are orthogonal, then their corresponding Pythagorean vectors contain the odd element at different positions. Otherwise, their inner product is odd and therefore non-zero; thus, no two vectors colored red are orthogonal, and among every three pairwise orthogonal vectors, there is one red, which concludes the proof. ∎

Clearly, we can obtain an even stronger result that the set M can be colored by three colors such that every pair of orthogonal vectors is colored differently. This is indeed the original result of Godsil and Zaks from [15].

Remark 4.4. The choice of a set representing rational measurements M may seem to be arbitrary; for instance, a vector $(1, 1, 1)$ is not a vector from M, although it could be considered rational. If we consider vectors with integer coordinates, we can find a non-colorable set, e.g., Conway's set.

4.2 Higher Dimensions

Now we inspect the proofs of BKS theorem in higher dimensions. The original construction from the proof of BKS theorem proved the nonexistence of hidden variables in three dimensions, and after a trivial modification, the theorem rules out the hidden variables even in higher dimensions. It is not a mathematical curiosity; the three dimensions do not correspond to the dimensionality of the surrounding world. It corresponds to the dimensionality of the quantum system. In the introductory chapter, we have already made use of the 8-dimensional Hilbert space. Even infinite-dimensional Hilbert spaces are considered in practice, hence proving the BKS theorem in any dimension would be valuable for physics.

The proofs of BKS theorem in higher dimensions are interesting for their simplicity, while they are almost as strong as those in three dimensions for the physicists. We shall show two proofs, one with 18 vectors of $\mathbb{R}^4$, and the other with 21 vectors of $\mathbb{C}^6$. For the latter, we emphasize that although we defined the coloring in $\mathbb{R}^n$, its definition in $\mathbb{C}^n$ is analogical, and we did not consider it only for the sake of simplicity.

4.2.1 Cabello's Proof of BKS Theorem in Four Dimensions

Probably the most elegant proof of the BKS theorem is the Cabello's proof in four dimensions [11]. It considers 18 vectors. We stacked them in the following matrix:

$$\begin{pmatrix}
0001 & 0001 & 1\bar{1}1\bar{1} & 1\bar{1}1\bar{1} & 0010 & 1\bar{1}\bar{1}1 & 11\bar{1}1 & 11\bar{1}1 & 111\bar{1} \\
0010 & 0100 & 1\bar{1}\bar{1}1 & 1111 & 0100 & 1111 & 111\bar{1} & \bar{1}111 & \bar{1}111 \\
1100 & 1010 & 1100 & 10\bar{1}0 & 1001 & 100\bar{1} & 1\bar{1}00 & 1010 & 1001 \\
1\bar{1}00 & 10\bar{1}0 & 0011 & 010\bar{1} & 100\bar{1} & 01\bar{1}0 & 0011 & 010\bar{1} & 01\bar{1}0
\end{pmatrix} \tag{1}$$

For typographical reasons, we used $\bar{1}$, instead of -1, and every element of the matrix corresponds to a vector in four dimensions. E.g., the element $01\bar{1}0$ in the bottom-right corner corresponds to the vector $(0, 1, -1, 0)$.

Let us assume that there is a BKS coloring of the 18 vectors. Matrix (1) has two significant properties:

- Each of its nine columns contains an orthogonal basis of $\mathbb{R}^4$; thus, the sum of the values of a state in every column is 1, and the sum of the values of a state over all elements of the matrix is odd.

- Every vector is contained in the table precisely twice; hence the sum of the values of a state of all 36 elements of the matrix is even.

Therefore, we arrived at an apparent contradiction.

For the reader's convenience, we identified the vectors with letters $a \ldots r$ and rewrote the table using the letters to make it easier to verify that every vector was used twice.

$$\begin{pmatrix} a & a & j & j & b & k & l & l & d \\ b & m & k & i & m & i & d & c & c \\ g & f & g & p & h & n & o & f & h \\ o & p & e & q & n & r & e & q & r \end{pmatrix} \tag{2}$$

Corollary 4.5. There is no coloring of $\mathbb{R}^4$.

4.2.2 Proof With 7 Contexts in $\mathbb{C}^6$

The smallest possible BKS set in terms of contexts (number of bases used) is in six dimensions. It contains 7 contexts and 21 vectors. It was proposed in [23], where they also claimed that it is the smallest BKS set possible in terms of contexts. We do not list the vectors explicitly here because they are rather complicated. Instead, we refer the reader to the paper for details. Therefore, we only present a hypergraph representing the set of vectors in Figure 4.1. Every dot in the figure corresponds to a vector, and every straight line connects six dots which correspond to six vectors forming an orthogonal basis.

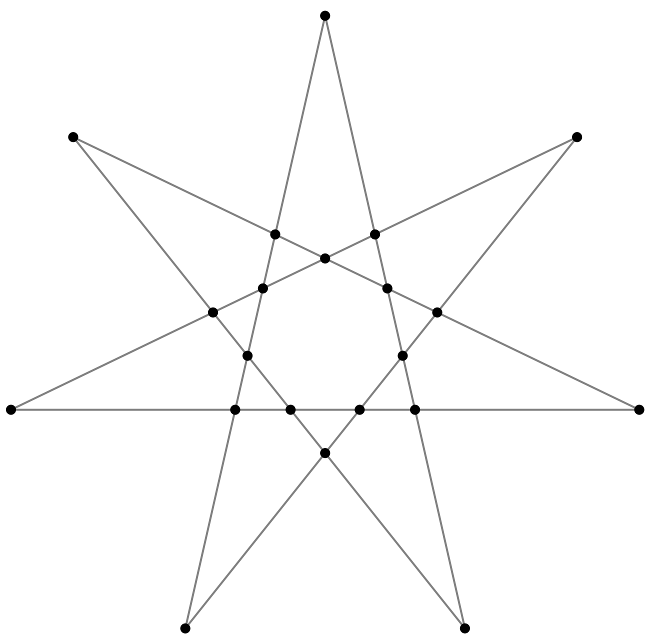

Figure 4.1. BKS set in 6 dimensions.

The argument is similar to the one in four dimensions. There are seven orthogonal bases, and every vector is contained in precisely two bases; thus, the sum of the doubles of all values of a state should be even and odd at the same time.

Corollary 4.6. There is no coloring of $\mathbb{C}^6$.

4.3 Statistical Argument

Although all the mentioned approaches constructed a set of vectors, for which there was no $\{0,1\}$-coloring, there are also constructions showing that there can be $\{0,1\}$-coloring of $\mathbb{R}^3$, but it would contradict quantum mechanics in another way.

The following construction is from Yu and Oh [49]. The set $S = \{-1,0,1\}^3 \subset \mathbb{R}^3$ contains 27 elements. One of them is zero which we discard, and for every other vector $\mathbf{x} \in S$, also $-\mathbf{x} \in S$, so there are 13 rays in S.

Lemma 4.7. At most one vector from the collection:

- $\mathbf{a} = 111$
- $\mathbf{b} = \bar{1}11$
- $\mathbf{c} = 1\bar{1}1$
- $\mathbf{d} = 11\bar{1}$

may be assigned 1.

Proof. We show that every assignment of two ones would lead to a contradiction. We abuse the symmetry; hence it is sufficient to inspect the following two cases.

- $v(\bar{1}11) = v(111) = 1$.
  - $v(101) = v(10\bar{1}) = 0$; hence $v(010) = 1$.
  - $v(110) = v(1\bar{1}0) = 0$; hence $v(001) = 1$, a contradiction.
- $v(\bar{1}11) = v(1\bar{1}1) = 1$.
  - $v(101) = v(10\bar{1}) = 0$; hence $v(010) = 1$.
  - $v(011) = v(01\bar{1}) = 0$; hence $v(100) = 1$, a contradiction.

∎

Thus in every possible assignment, $v(\mathbf{a}) + v(\mathbf{b}) + v(\mathbf{c}) + v(\mathbf{d}) \leq 1$.

On the other hand, every of these rays corresponds to a projector to themselves and quantum mechanics predicts[1], that the expected value of $v(\mathbf{h_1}) + v(\mathbf{h_2}) + v(\mathbf{h_3}) + v(\mathbf{h_4})$ should be an eigenvalue of

$$\frac{\mathbf{a}\mathbf{a}^T}{\mathbf{a}^T\mathbf{a}} + \frac{\mathbf{b}\mathbf{b}^T}{\mathbf{b}^T\mathbf{b}} + \frac{\mathbf{c}\mathbf{c}^T}{\mathbf{c}^T\mathbf{c}} + \frac{\mathbf{d}\mathbf{d}^T}{\mathbf{d}^T\mathbf{d}} = \frac{4}{3}\mathbf{I}_3.$$

It can only be $4/3$, but $4/3 \not\leq 1$; thus, the hidden variable theory is not compatible with quantum mechanics.

[1] We are not capable of describing this quantum mechanics prediction; we paraphrased the original paper here.

4.3.1 Proof of BKS Theorem in Three Dimensions

We use the Yu–Oh set to arrive at a contradiction. The resulting configuration is known as Peres configuration [36], and it has 33 vectors. We do not provide the original argument. We show a possibly clearer one, consisting of two steps, one of which was already presented in Lemma 4.7.

Consider again the set of rays $S = (\{-1,0,1\}^3 \setminus \{(0,0,0)\}) \subset \mathbb{R}^3$ containing 13 elements as discussed before. We will use the same notation for ray description as before, additionally we use 2 as $\sqrt{2}$ for brevity; e.g., $1\bar{2}0$ corresponds to the vector $(1, -\sqrt{2}, 0)$.

We take three copies of the set and rotate every copy by 45° with respect to the axes x,y,z to obtain sets S_x, S_y and S_z respectively. Note that the vectors 100, 010, 001 are contained in all of the sets S_x, S_y, S_z; thus their union contains[1] $13 + 10 + 10 = 33$ elements.

When a vector is rotated about an axis, its component remains unchanged in the axis direction. For the remaining directions, they will rotate as follows:

$$11 \to 20 \to 1\bar{1} \to 0\bar{2} \to \bar{1}\bar{1} \to \bar{2}0 \to \bar{1}1 \to 02 \to 11.$$

We will employ Lemma 4.7; thus we list the needed vectors and their respective images after rotation. We write $\mathbf{a}_x$ for the image of $\mathbf{a}$ after rotation about x axis; similarly for other vectors and axes. We will also use $\mathbf{e}_i$ for the i-th standard basis vector.

	S	S_x	S_y	S_z
a	111	120	210	201
b	$\bar{1}11$	$\bar{1}20$	012	021
c	$1\bar{1}1$	102	$2\bar{1}0$	$0\bar{2}1$
d	$11\bar{1}$	$10\bar{2}$	$01\bar{2}$	$20\bar{1}$

Table 4.1. Rotated rays

We recall Lemma 4.7, that for any $v : \mathbb{R}^3 \to \{0,1\}$ it holds that

- $v(\mathbf{a}) + v(\mathbf{b}) + v(\mathbf{c}) + v(\mathbf{d}) \leq 1$.

Therefore, according to Remark 3.2 it also holds that:

- $v(\mathbf{a}_x) + v(\mathbf{b}_x) + v(\mathbf{c}_x) + v(\mathbf{d}_x) \leq 1$,
- $v(\mathbf{a}_y) + v(\mathbf{b}_y) + v(\mathbf{c}_y) + v(\mathbf{d}_y) \leq 1$,
- $v(\mathbf{a}_z) + v(\mathbf{b}_z) + v(\mathbf{c}_z) + v(\mathbf{d}_z) \leq 1$,
- $v(\mathbf{e}_1) + v(\mathbf{e}_2) + v(\mathbf{e}_3) = 1$.

However, we can form the following orthogonal bases:

- $\{\mathbf{a}_x, \mathbf{c}_y, \mathbf{e}_3\}$,
- $\{\mathbf{b}_x, \mathbf{a}_y, \mathbf{e}_3\}$,
- $\{\mathbf{c}_x, \mathbf{d}_z, \mathbf{e}_2\}$,
- $\{\mathbf{d}_x, \mathbf{a}_z, \mathbf{e}_2\}$,
- $\{\mathbf{b}_y, \mathbf{c}_z, \mathbf{e}_1\}$,
- $\{\mathbf{d}_y, \mathbf{b}_z, \mathbf{e}_1\}$.

[1] It is clear that it contains at most 33 elements. We will not argue why is it exactly 33.

Thus, the sum of values of elements in the bases is 6; let us write:

$$\begin{aligned}
6 &= \overbrace{v(\mathbf{a}_x)+v(\mathbf{c}_y)+v(\mathbf{e}_3)}^{=1}+\overbrace{v(\mathbf{b}_x)+v(\mathbf{a}_y)+v(\mathbf{e}_3)}^{=1}+\overbrace{v(\mathbf{c}_x)+v(\mathbf{d}_z)+v(\mathbf{e}_2)}^{=1}\\
&+\overbrace{v(\mathbf{d}_x)+v(\mathbf{a}_z)+v(\mathbf{e}_2)}^{=1}+\overbrace{v(\mathbf{b}_y)+v(\mathbf{c}_z)+v(\mathbf{e}_1)}^{=1}+\overbrace{v(\mathbf{d}_y)+v(\mathbf{b}_z)+v(\mathbf{e}_1)}^{=1}\\
&=\underbrace{v(\mathbf{a}_x)+v(\mathbf{b}_x)+v(\mathbf{c}_x)+v(\mathbf{d}_x)}_{\leq 1}+\underbrace{v(\mathbf{a}_y)+v(\mathbf{b}_y)+v(\mathbf{c}_y)+v(\mathbf{d}_y)}_{\leq 1}\\
&+\underbrace{v(\mathbf{a}_z)+v(\mathbf{b}_z)+v(\mathbf{c}_z)+v(\mathbf{d}_z)}_{\leq 1}+2\underbrace{(v(\mathbf{e}_1)+v(\mathbf{e}_2)+v(\mathbf{e}_3))}_{=1}\\
&\leq 5
\end{aligned}$$

That is absurd; thus, the set $S_x \cup S_y \cup S_z$ cannot be colored in the BKS sense.

4.4 $\mathbb{Z}_2$-Valued Assignment

Peres in [37] coined in a multiplicative version of BKS theorem. Consequently, there were attempts to clarify if it is possible to assign (nontrivially) zeros and ones to vectors of $\mathbb{R}^n$ such that in any orthogonal basis, an odd number of vectors is assigned 1. The answer from [34] is that for $n \geq 4$ it is impossible. The question for $n = 3$ was open and arises in many contexts, see [17, 24, 26, 28–29, 33–34]. In Chapter 6 we give a definitive answer that it is not possible.

Chapter 5
Orthocomplemented Difference Lattices

In this chapter, we will study orthocomplemented difference lattices (abbr. ODLs). They were introduced and consequently studied by Matoušek and Pták in their works [24–29]. The aim of this chapter is to study states on ODLs. We give an example of an ODL with no real-valued state; we also study $\mathbb{Z}_2$-states. The novelty of this chapter lies in Section 5.5. The rest of the chapter is heavily based on the abovementioned papers, but we make use of different techniques. In particular, we use the connection between Boolean algebras and ODLs to provide proofs that are often algorithmic.

5.1 Definitions

We provide the definition of an orthocomplemented difference lattice and inspect the independence of the axioms of the symmetric difference operator. The orthocomplemented lattices were already heavily studied, see, e.g., [4, 21]; therefore, we do not dive into the details of the axioms.

Definition 5.1. An orthocomplemented difference lattice is a sextuplet $(L,\leq,\triangle,',\mathbf{0},\mathbf{1})$, where $\leq$ is a binary relation on L; $\triangle$ and $'$ are mappings $\triangle : L \times L \to L$ and $' : L \to L$; the elements $\mathbf{0}, \mathbf{1} \in L$ are the least and the greatest elements respectively, and the following axioms hold:

- The tuple $(L, \leq,', \mathbf{0}, \mathbf{1})$ forms an orthocomplemented lattice; that is for every elements $a, b, c \in L$ the following properties hold:
  - $(L, \leq)$ is a poset, i.e.,
    - $a \leq a$. (reflexivity)
    - If $a \leq b$ and $b \leq a$, then $a = b$. (antisymmetry)
    - If $a \leq b$ and $b \leq c$, then $a \leq c$. (transitivity)
  - There is the supremum (denoted as $a \vee b$) and the infimum (denoted as $a \wedge b$), which is the least upper bound resp. the greatest lower bound; that is:
    - If $a \leq c$ and $b \leq c$, then $a \vee b \leq c$. (supremum)
    - If $c \leq a$ and $c \leq b$, then $c \leq a \wedge b$. (infimum)

    Thus, $(L, \leq)$ is a lattice.
  - Lattice $(L, \leq,', \mathbf{0}, \mathbf{1})$ is orthocomplemented; i.e., it holds:
    - $a' \vee a = \mathbf{1}$, $a' \wedge a = \mathbf{0}$. (complement law)
    - $a'' = a$. (involution law)
    - If $a \leq b$, then $b' \leq a'$. (order reversing)

- The $\triangle$ operator axiomatically introduces the symmetric difference operation in the following way, that for arbitrary elements $a, b, c \in L$ it holds:
  - $a \triangle (b \triangle c) = (a \triangle b) \triangle c$. (associativity)
  - $a \triangle \mathbf{1} = a'$.
  - $\mathbf{1} \triangle a = a'$.
  - $a \triangle b \leq a \vee b$.

The orthocomplemented lattice $(L, \leq, ', \mathbf{0}, \mathbf{1})$ is called the *support* of the ODL $(L, \leq, \triangle, ', \mathbf{0}, \mathbf{1})$. The term "orthocomplemented" suggests that an orthogonality relation is present here; we introduce it as follows:

Definition 5.2. Let L be an ODL. Elements $a, b \in L$ are *orthogonal* if $a \leq b'$.

Whenever $a \leq b'$ then also $b \leq a'$; thus, the definition properly introduces a symmetric binary relation.

We shall present some examples of ODLs. Any Boolean algebra with the standard symmetric difference is an ODL. The converse is not true, and some ODLs are not Boolean algebras.

For example, we take an ODL which is a Boolean algebra, and remove all inequality relations that are not necessary; thus, the only remaining inequality relations will be $\mathbf{0} \leq a$ and $a \leq \mathbf{1}$ for any $a \in L$. The resulting algebra is not a Boolean algebra whenever it has more than four elements.

When no ambiguity may occur, we write just L instead of the whole sextuplet when considering an ODL.

For the sake of simplicity, we assume that L is finite. This assumption plays a role only in a few cases to make the proofs more accessible. Notably, the assumption allows us to develop the theory of ODLs without considering the controversial axiom of choice.

First, we shall inspect the axioms of symmetric difference. They are chosen such that the symmetric difference would have similar properties to the standard symmetric difference known from Boolean algebras. At first, we show that all four axioms of $\triangle$ are independent.

Proposition 5.1. The set of axioms of $\triangle$ is independent.

Proof. We show examples of $\triangle$ such that they satisfy all but one axiom.

We define $\triangle$ on a four-element orthocomplemented lattice $L = \{\mathbf{0}, x, x', \mathbf{1}\}$ where the complemention and order are standard.

- The $\triangle$ operator defined by Table 5.1 satisfies every axiom but the first. The first is violated since $\mathbf{1} = (x \triangle x') \triangle \mathbf{1} \neq x \triangle (x' \triangle \mathbf{1}) = \mathbf{0}$.

$\triangle$	$\mathbf{0}$	x	x'	$\mathbf{1}$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$
x	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	x'
x'	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	x
$\mathbf{1}$	$\mathbf{1}$	x'	x	$\mathbf{0}$

Table 5.1. Example of $\triangle$ violating only the first axiom

- The independence of the second axiom is a trivial consequence of the independence of the third axiom, which we show in the sequel.
- The $\triangle$ operator defined by Table 5.2 satisfies every axiom but the third. It is immediate that the third is violated and that the second and fourth are satisfied. It is more involved to show that the defined $\triangle$ is indeed associative; we split the proof into multiple cases:
  - If any of the elements a, b, c is $\mathbf{0}$, then it holds since $\mathbf{0} \triangle e = e \triangle \mathbf{0} = e$ for any element $e \in L$.
  - If the element c is x or x', then it holds since $e \triangle c = c$ for any element $e \in L$.
  - Otherwise $c = \mathbf{1}$ and it suffices to show that $a \triangle b' = (a \triangle b)'$ which can be verified in the table without much effort.

$\triangle$	$\mathbf{0}$	x	x'	$\mathbf{1}$
$\mathbf{0}$	$\mathbf{0}$	x	x'	$\mathbf{1}$
x	x	x	x'	x'
x'	x'	x	x'	x
$\mathbf{1}$	$\mathbf{1}$	x	x'	$\mathbf{0}$

Table 5.2. Example of $\triangle$ violating only the third axiom

- The independence of the last axiom will be resolved later, see Corollary 5.12.

■

5.2 Basic Properties

The motivation behind introducing the symmetric difference on orthocomplemented lattices is to obtain a natural class of algebras containing Boolean algebras while being more general. This section shows certain nontrivial properties that hold for Boolean algebras and hold for ODLs. We first show that De Morgan's laws hold due to properties of the orthocomplemented lattice; then, we proceed with properties specific to the symmetric difference operator.

Proposition 5.2. (De Morgan's laws) Let L be an ODL; the following identities hold for every pair of elements $a, b \in L$:

- $(a \vee b)' = a' \wedge b'$.
- $(a \wedge b)' = a' \vee b'$.

Proof. Employing the order-reversing property, we get:

- $a \leq a \vee b \Rightarrow (a \vee b)' \leq a'$.
- $b \leq a \vee b \Rightarrow (a \vee b)' \leq b'$.
- $(a \vee b)' \leq a' \wedge b'$.

Similarly for a', b':

- $a' \wedge b' \leq a' \Rightarrow a \leq (a' \wedge b')'$,
- $a' \wedge b' \leq b' \Rightarrow b \leq (a' \wedge b')'$,
- $a \vee b \leq (a' \wedge b')' \Rightarrow a' \wedge b' \leq (a \vee b)'$.

Taking the last inequalities of both series, together with the antisymmetric property of $\leq$, we arrive at $(a \vee b)' = a' \wedge b'$, which concludes the first claim of the proposition.

For the second one, we note that the complementation operator $'$ is bijective; thus, to take the complements of both sides of the equations is an equivalent operation, and the second claim immediately follows from the first one. ∎

Proposition 5.3.

(i) $a \triangle \mathbf{0} = a$, $\mathbf{0} \triangle a = a$.
(ii) $a \triangle a = \mathbf{0}$.
(iii) $a \triangle b = b \triangle a$.
(iv) $a \triangle b' = a' \triangle b = (a \triangle b)'$.
(v) $a' \triangle b' = a \triangle b$.
(vi) $a \triangle b = \mathbf{0} \iff a = b$.
(vii) $(a \wedge b') \vee (b \wedge a') \leq a \triangle b \leq (a \vee b) \wedge (a' \vee b')$.

Proof.

(i)

- $a \triangle \mathbf{0} = a \triangle (\mathbf{1} \triangle \mathbf{1}) = (a \triangle \mathbf{1}) \triangle \mathbf{1} = a' \triangle \mathbf{1} = a'' = a$.
- $\mathbf{0} \triangle a = (\mathbf{1} \triangle \mathbf{1}) \triangle a = \mathbf{1} \triangle (\mathbf{1} \triangle a) = \mathbf{1} \triangle a' = a'' = a$.

(ii) $a \triangle a = a \triangle (\mathbf{1} \triangle a') = (a \triangle \mathbf{1}) \triangle a' = a' \triangle a'$, moreover we know:

- $a \geq a \triangle a$,
- $a' \geq a' \triangle a' = a \triangle a$,

hence $a \triangle a \leq a \wedge a' = \mathbf{0}$; thus $a \triangle a = \mathbf{0}$.

(iii) $a \triangle b = \mathbf{0} \triangle (a \triangle b) \triangle \mathbf{0} = (b \triangle b) \triangle (a \triangle b) \triangle (a \triangle a) = b \triangle ((b \triangle a) \triangle (b \triangle a)) \triangle a = b \triangle a$.
(iv) $a \triangle b' = a \triangle (\mathbf{1} \triangle b) = (a \triangle \mathbf{1}) \triangle b = a' \triangle b = \mathbf{1} \triangle (a \triangle b) = (a \triangle b)'$.
(v) $a \triangle b = a \triangle b \triangle \mathbf{0} = a \triangle b \triangle \mathbf{1} \triangle \mathbf{1} = \mathbf{1} \triangle a \triangle b \triangle \mathbf{1} = a' \triangle b'$.
(vi) The right-to-left direction is already proven. For the converse, we have:

$$a = a \triangle \mathbf{0} = a \triangle (b \triangle b) = (a \triangle b) \triangle b = \mathbf{0} \triangle b = b.$$

(vii) These properties follow from the preceding ones and from the axioms:

- $a \triangle b \leq a \vee b$.
- $a \triangle b = a' \triangle b' \leq a' \vee b'$.
- $(a \triangle b)' = a \triangle b' \leq a \vee b'$.
- $(a \triangle b)' = a' \triangle b \leq a' \vee b$.

We negate the latter two identities and simplify them using De Morgan's laws. Then we obtain:

$$(a \wedge b') \vee (a' \wedge b) \leq a \triangle b \leq (a \vee b) \wedge (a' \vee b')$$

∎

As discussed in Section 2.7, the underlying algebra for quantum logics should follow the orthomodular law. We show that it is indeed the case for ODLs.

Let us show that the orthomodular law (see [40]) is satisfied for any ODL L. The orthomodular law is a weakened version of the modular law:

- If $a \leq c$, then $a \vee (b \wedge c) = (a \vee b) \wedge c$,

  which we enforce only for $b = a'$, hence the orthomodular law is:

- If $a \leq c$, then $a \vee (a' \wedge c) = c$.

Definition 5.3. Let L be an orthocomplemented lattice for which the orthomodular law holds then L is an *orthomodular lattice* (abbr. OML).

Proposition 5.4. The support of any ODL L is an OML.

Proof. We verify that the orthomodular law holds for every pair of elements $a, c \in L$ such that $a \leq c$. We show equality using two inequalities.

The first is obvious; $a \vee (a' \wedge c) \leq c \vee (a' \wedge c) = c$. For the second, we need to employ the properties of symmetric difference. Using the Claim (vii) of Proposition 5.3, we get:

$$a' \wedge c = (a \wedge c') \vee (a' \wedge c) \leq a \triangle c \leq (a \vee c) \wedge (a' \vee c') = a' \wedge c,$$

where we used the fact $a \leq c$, hence $c' \leq a'$ and $a \wedge c' \leq c \wedge a'$; thus $a \triangle c = a' \wedge c$ and finally:

$$c = a \triangle a \triangle c = a \triangle (a' \wedge c) \leq a \vee (a' \wedge c),$$

which is the other direction; the proof is completed. ∎

In the proof of Porposition 5.4 we note an interesting fact that if $a \leq c$, then $a \triangle c$ may be defined in only one way. We later show that there are many pairs of elements for which the symmetric difference may be defined uniquely. Before that, we will briefly focus on OMLs.

5.3 Intermezzo about Orthomodular Lattices

Orthomodular lattices were extensively studied as quantum logics, see [4, 21, 40]. According to Proposition 5.4, ODLs are OMLs with a defined symmetric difference on them; therefore, we will represent them using Greechie diagrams.

5.3.1 Greechie Diagrams

A common representation for an OML is a hypergraph representation called a Greechie diagram, coined in [16]. We remind the reader that a hypergraph is a pair $H = (V, E)$, where V is a set of vertices and E is a set of edges such that for every edge $e \in E$, $e \subseteq V$; see [5] for more details. Thus, hypergraphs are a generalization of undirected graphs where the edges may contain an arbitrary number of vertices.

An orthomodular lattice can be seen as a union of Boolean algebras; thus, a convenient representation is to use hypergraphs whose vertices correspond to the least non-zero elements of the OML, which are called *atoms*; and every edge corresponds to the set of atoms of a maximal Boolean subalgebra of the OML. A maximal Boolean subalgebra of an OML is called a *block*; see [4, 21, 40].

Not every hypergraph represents an OML in this sense. However, there is quite a large class of hypergraphs, called Greechie diagrams, which represent OMLs. Not every OML is representable by a Greechie diagram.

Definition 5.4. Let $H = (V, E)$ be a hypergraph. It represents an OML if the following conditions hold:

- Every edge contains at least 2 vertices.
- If an edge contains precisely 2 vertices, it does not intersect with any other edge.
- No two edges have more than one vertex in common.
- The length of every cycle[1] is at least 5.

We call such hypergraph a *Greechie diagram*.

We show several examples of Greechie diagrams in Figure 5.1, where dots correspond to vertices and maximal straight line segments correspond to edges. The hypergraph in the figure, as well as every its induced[2] subhypergraph, corresponds to an orthomodular lattice.

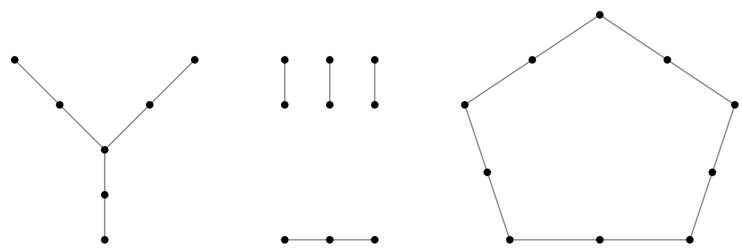

Figure 5.1. Example of an orthomodular lattice represented by a Greechie diagram

5.4 Boolean Algebras as Subalgebras of Orthocomplemented Difference Lattices

OMLs can be seen as unions of Boolean algebras; thus, ODLs can be seen as unions of Boolean algebras endowed with a symmetric difference operator. We note that the axiomatic symmetric difference of ODLs necessarily corresponds to the standard symmetric difference of Boolean algebras in every Boolean subalgebra of the ODL.

[1] A cycle of length $n \geq 3$ is an alternating sequence of distinct edges and vertices (with the exception that the first and the last vertex are equal) $v_1, e_1, v_2, e_2, \dots v_n e_n v_1$ such that every vertex is contained in the neighboring edges.

[2] A hypergraph $H_2 = (V_2, E_2)$ is an induced subhypergraph of $H = (V, E)$ if $V_2 \subseteq V$, $E_2 \subseteq E$ and $\forall e \in E, e \subseteq V_2 \Rightarrow e \in E_2$.

Proposition 5.5. Let L be an ODL and $x, y \in L$ its elements. The following conditions are equivalent:

- x and y are contained in a Boolean subalgebra of L,
- $x = (x \wedge y) \vee (x \wedge y')$,
- $x = (x \vee y) \wedge (x \vee y')$.

Proposition 5.6. Let L be an ODL and $x, y \in L$ its elements contained in a block, then:

$$(x \wedge y') \vee (x' \wedge y) = x \mathbin{\triangle} y = (x \vee y) \wedge (x' \vee y').$$

Proof. A simple corollary of the property (vii) of Proposition 5.3:

$$(x \wedge y') \vee (x' \wedge y) \leq x \mathbin{\triangle} y \leq (x \vee y) \wedge (x' \vee y'),$$

and the fact that x, y are contained in a Boolean subalgebra. ∎

The connection between ODLs and Boolean algebras is even tighter. In some sense, the symmetric difference operator of any ODL corresponds to a Boolean algebra. We will be more precise later.

Proposition 5.7. Let L be an ODL; the cardinality of L is 2^n for some natural n.

Proof. We first introduce[1] a $\Delta : \mathcal{P}(L) \to L$ operator as a shortcut for the symmetric difference of multiple elements, that is e.g., $\Delta(\{x, y, z\}) = x \mathbin{\triangle} y \mathbin{\triangle} z$. The $\triangle$ operator is commutative and associative; thus the definition is unambiguous. We further note that $\mathbf{0}$ is the neutral element w.r.t. $\triangle$ operator; therefore $\Delta(\emptyset) = \mathbf{0}$.

Now, we show that there exists a set $M \subseteq L$ such that for every element $e \in L$ there is a subset $S \subseteq M$ such that $\Delta(S) = e$ and at the same time, for no two distinct subsets $S_1, S_2 \subseteq M$ it holds that $\Delta(S_1) = \Delta(S_2)$. We call the latter property that M is an *independent* set.

We sketch an algorithm which constructs such M. It starts with $M = \emptyset$ and repeats the following process until termination:

- Find an element $e \in L$ such that there is no subset $S \subseteq M$ such that $\Delta(S) = e$.
  - If there is no such element, we terminate the algorithm.
  - Otherwise, set $M := M \cup \{e\}$.

Let us comment on the correctness of the algorithm. The details are omitted for the sake of brevity.

- The algorithm terminates since L is a finite set.
- When the algorithm terminates, then for every element $e \in L$ there is a subset $S \subseteq M$ such that $\Delta(S) = e$.
- The construction ensures that M is an independent set.

[1] The set $\mathcal{P}(L)$ is the power set of L. That is the set of all subsets of L.

Thus, the subsets of the final M are in a one-to-one correspondence with the elements of L; consequently, L contains 2^n elements for a natural n. ■

Inspired by the proof, we may consider the (ordered) set M to serve as a basis of L, where the elements of L have unique coordinates with respect to M; the coordinates will be either 0 or 1; thus, it is a vector space over $\mathbb{Z}_2$.

Corollary 5.8. Let L be an ODL. Then the set L is a vector space over the field $\mathbb{Z}_2$ with the operators $+$, $\cdot$ defined as follows:

- For $a, b \in L$, $a + b = a \bigtriangleup b$.
- For $a \in L$, $0 \cdot a = \mathbf{0}$ and $1 \cdot a = a$.

We demonstrate this in the following example.

Example 5.1. Let L be an ODL with 32 elements and $M = (a, b, c, d, e) \subset L$ be an independent set. Then there is an element $x \in L, x = a \bigtriangleup c \bigtriangleup e$ and x will have coordinates $(1, 0, 1, 0, 1)$.

This way, we may introduce a bijective mapping between an ODL and a Boolean algebra such that the symmetric differences will coincide.

Proposition 5.9. Let L be an ODL and its number of elements be 2^n. Let $B = \{0, 1\}^n$ be a Boolean algebra. There is a bijective mapping $f : L \to B$ such that $f(\mathbf{0}) = \mathbf{0}$, $f(\mathbf{1}) = \mathbf{1}$ and $a \bigtriangleup b = f^{-1}(f(a) \bigtriangleup_B f(b))$ for $a, b \in L$, where $\bigtriangleup_B$ is the standard symmetric difference in Boolean algebra B.

Proof. The proposition is a simple corollary of the proof of Proposition 5.7. The only thing we are to show is that there exists an ordered basis M such that $\mathbf{1} = \Delta(M)$.

We construct M as in the proof of Proposition 5.7 and it either satisfies the property and we are done; otherwise there is a non-empty subset $S \subset M$ such that $\Delta(S) = \mathbf{1}$ and there is an element $e \in S$. Then the set $N = M \setminus \{e\} \cup \{\Delta(M \setminus \{e\}) \bigtriangleup \mathbf{1}\}$ is the desired basis.

Example 5.2. We show an example application of Proposition 5.9 on ODL L captured in Figure 5.2. Let there also hold that $b \bigtriangleup d = g$ which fully defines the $\bigtriangleup$ operator. It can be seen that L contains 16 elements, that is $\mathbf{0}, \mathbf{1}$, together with seven atoms and their complements. A desired mapping is the following:

- $a \sim (1, 0, 0, 0)$,
- $b \sim (0, 1, 0, 0)$,
- $c \sim (0, 0, 1, 1)$,
- $d \sim (0, 1, 0, 1)$,
- $e \sim (0, 0, 1, 0)$,
- $f \sim (0, 1, 1, 0)$,
- $g \sim (0, 0, 0, 1)$,
- $a' \sim (0, 1, 1, 1)$,
- $b' \sim (1, 0, 1, 1)$,
- $c' \sim (1, 1, 0, 0)$,
- $d' \sim (1, 0, 1, 0)$,
- $e' \sim (1, 1, 0, 1)$,
- $f' \sim (1, 0, 0, 1)$,
- $g' \sim (1, 1, 1, 0)$.

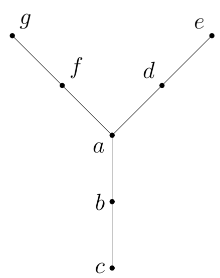

Figure 5.2. Example of an ODL

Remark 5.10. According to Proposition 5.9, there is a bijective mapping between any ODL and binary strings of certain length. The mapping may be interpreted as assigning coordinates to the elements of L which is a vector space according to Corollary 5.8.

It is not clear which OMLs may be endowed with a symmetric difference. In Proposition 5.7, we have shown that every ODL necessarily contains 2^n elements. Even this is not sufficient for OML to be extendable to ODL, we provide another simple necessary condition in the upcoming proposition.

Proposition 5.11. Let L be an ODL, then there is no atom $c \in L$ contained in precisely two blocks.

Proof. Assume to the contrary that there is such an atom in blocks B_1, B_2. Consider two arbitrary atoms $a \in B_1 \setminus B_2$, $b \in B_2 \setminus B_1$. It holds that $a \leq c'$ and $b \leq c'$; then also $a \triangle b \leq c'$. The element c' is contained only in blocks B_1, B_2, so must be $a \triangle b$. Without loss of generality, let $a \triangle b = d \in B_1$. Then $a \triangle d = b$, but Boolean subalgebra is closed under the symmetric difference; a contradiction. ■

Note that if the symmetric difference did not have the last axiom, i.e., $a \triangle b \leq a \vee b$, $a, b \in L$ for an ODL L, then if L has 2^n elements, any mapping $m : L \to \{0,1\}^n$ would introduce a valid symmetric difference in the sense of Proposition 5.9. But it is a simple corollary of 5.11 that not every OML with 2^n elements can be endowed with a symmetric difference.

Corollary 5.12. The set of axioms of the $\triangle$ operator is independent.

5.5 Stateless Orthocomplemented Difference Lattice

We proceed with the main result of this chapter, which is an example of a stateless ODL. We first define a state, then we show an OML and endow it with a partial symmetric difference; then we conclude that it admits no state, and finally, we show that such a symmetric difference exists.

Definition 5.5. Let L be an ODL. A mapping $s : L \to [0,1]$ is called a *state* if the following holds:

- $s(x) + s(y) = s(x \vee y)$, whenever x and y are orthogonal.
- $s(\mathbf{1}) = 1$.
- $s(x) + s(y) \geq s(x \triangle y)$.

Although Proposition 5.9 suggests that from an ODL, we may obtain the associated Boolean algebra, here we are interested in the converse. We take an OML with 2^n elements and associate every element with a binary string of length n, which determines the symmetric difference.

In Figure 5.3, there is the OML L which we will endow with a symmetric difference operator. It contains two blocks with 7 atoms, three blocks with 3 atoms, and 3960[1]

[1] $3960 = (2^{13} - 2 - 3(2^3 - 2) - 2(2^7 - 2))/2$

blocks with two atoms, which are not shown in the figure for obvious reasons. The blocks are represented by horizontal lines. The vertical dotted lines indicate the symmetric difference in a way that if three vertices (atoms), e.g., a_1, b_1, c_1 are connected by a dotted line then $a_1 \triangle b_1 \triangle c_1 = \mathbf{1}$; thus, $a_1 \triangle b_1 = c_1'$.

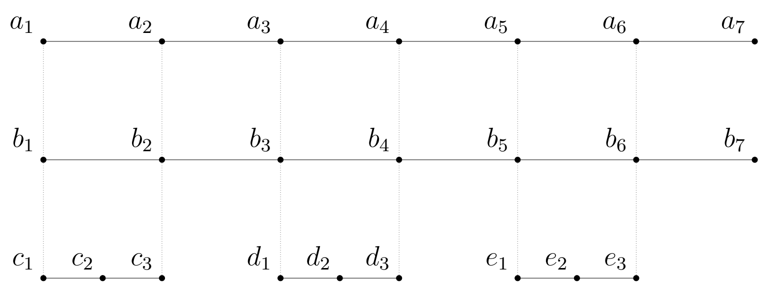

Figure 5.3. Example of a stateless orthocomplemented difference lattice

For now, we assume that such a symmetric difference exists and we show that the ODL does not admit any state. We rewrite the symmetric differences from the figure explicitly:

- $a_1 \triangle b_1 = c_1' = c_2 \vee c_3$,
- $a_2 \triangle b_2 = c_3' = c_1 \vee c_2$,
- $a_3 \triangle b_3 = d_1' = d_2 \vee d_3$,
- $a_4 \triangle b_4 = d_3' = d_1 \vee d_2$,
- $a_5 \triangle b_5 = e_1' = e_2 \vee e_3$,
- $a_6 \triangle b_6 = e_3' = e_1 \vee e_2$.

Assume that there exists a state s; then it satisfies:

- $s(a_1) + s(b_1) \geq s(a_1 \triangle b_1) = s(c_2 \vee c_3) = s(c_2) + s(c_3)$,
- $s(a_2) + s(b_2) \geq s(a_2 \triangle b_2) = s(c_1 \vee c_2) = s(c_1) + s(c_2)$,
- $s(c_1) + s(c_2) + s(c_3) = 1$.

Together we have:

- $s(a_1) + s(a_2) + s(b_1) + s(b_2) \geq s(c_1) + 2s(c_2) + s(c_3) \geq 1$.

Similarly we get:

- $s(a_3) + s(a_4) + s(b_3) + s(b_4) \geq 1$,
- $s(a_5) + s(a_6) + s(b_5) + s(b_6) \geq 1$.

Summing them up:

- $\sum_{i=1}^{6}(s(a_i) + s(b_i)) \geq 3$.

On the other hand, we know:

- $\sum_{i=1}^{7}(s(a_i) + s(b_i)) = 2$.

That is, together with the non-negativity of s, a contradiction.

We show that an ODL with such a symmetric difference indeed exists. We introduce a mapping $f : L \to \{0,1\}^{13}$ which assigns a binary string to every element of L. Those binary strings will then determine the symmetric difference in the sense of Proposition 5.9. It is sufficient to show the assignment of atoms since according to Proposition 5.6, the value of f on every non-atom is determined.

- $f(a_1) = (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$
- $f(a_2) = (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$
- $f(a_3) = (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$
- $f(a_4) = (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$
- $f(a_5) = (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$
- $f(a_6) = (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$
- $f(a_7) = (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$

- $f(b_1) = (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$
- $f(b_2) = (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$
- $f(b_3) = (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$
- $f(b_4) = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$
- $f(b_5) = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$
- $f(b_6) = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$
- $f(b_7) = (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$

- $f(c_1) = (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$
- $f(c_2) = (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$
- $f(c_3) = (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$

- $f(d_1) = (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$
- $f(d_2) = (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$
- $f(d_3) = (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$

- $f(e_1) = (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$
- $f(e_2) = (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$
- $f(e_3) = (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$

For the remaining two-atom blocks, we can go through them one-by-one and assign an arbitrary binary string $\mathbf{s}$, which is unassigned yet, to one atom, and the string $\mathbf{1} \triangle \mathbf{s}$ to the other.

We shall verify that the intersection of any two blocks is trivial; i.e., $\{\mathbf{0}, \mathbf{1}\}$.

First, we see that the binary strings corresponding to elements of a block with atoms a_i (resp. b_i) are constant in the last seven (resp. the first seven) entries. Clearly, the only elements with this property from the blocks with atoms c_i, d_i, e_i are $\mathbf{0}, \mathbf{1}$.

The verification, that the intersection of blocks with atoms a_i and b_i is trivial, is similar. The common element has to be constant in the first seven elements and in the last seven elements at the same time. Thus, it is constant and can only be $\mathbf{0}$ or $\mathbf{1}$.

The remaining verification is immediate.

We emphasize that the resulting structure is indeed an ODL; the axioms of the symmetric difference operator are satisfied.

Corollary 5.13. There exists a stateless ODL.

We note that this is not just a mathematical curiosity. We motivated the study of ODLs by their possible ability to describe quantum logic. Arguably, an ODL that possesses no states clearly cannot describe any nontrivial system's logic. However, an example of a stateless OML from [16] led to a positive result showing that the state space of OMLs can be an arbitrary convex compact set, see [43] for the precise meaning.

It is possible that a certain adaptation of the construction from [43] could be applied for ODLs, however, the generalization from OMLs to ODLs is not immediate. It is only clear that the state space of any ODL is compact and convex.

Proposition 5.14. Let L be an ODL. Then the set of all possible states S is compact and convex in the following sense; for every $s_1, s_2 \in S$ a mapping $s : L \to [0, 1]$ defined as $s(x) = \alpha s_1(x) + (1 - \alpha)s_2(x)$ for every $x \in L$ is a state, i.e., $s \in S$ for any $\alpha \in [0, 1]$.

The proof is straightforward and can be found in [20].

5.6 $\mathbb{Z}_2$-States on Orthocomplemented Difference Lattices

In the final section, we inspect $\mathbb{Z}_2$-valued states. We show that there is a close relationship between the symmetric difference and such states. We start with listing definitions and interesting properties.

5.6.1 Definitions

Definition 5.6. Let L be an ODL, and $x, y \in L$, $x \leq y$ be two of its elements, we call the set $\{z \mid x \leq z \leq y, z \in L\}$ an *interval*, and denote it by $[x, y]$.

When no ambiguity can occur, for the sake of brevity, we may write $s(M)$, where M is a subset of L, and by this we mean $s(M) = \{s(x) \mid x \in M\}$.

Proposition 5.15. Let L be an ODL and $x \in L$ its element, then the interval $[\mathbf{0}, x]$ is closed under $\triangle$.

Proof. For any two elements $a, b \in L$ such that $a \leq x, b \leq x$ it holds that $a \vee b \leq x$ and $a \triangle b \leq a \vee b \leq x$. ∎

Corollary 5.16. Every interval has 2^n elements.

Corollary 5.16 allows us to prove the fact that no atom is contained in exactly two blocks.

Alternative proof of Proposition 5.11. Take an atom a which belongs to exactly two blocks and compute the cardinality of the interval below its coatom, $[0, a']$. It is composed of two intervals in the blocks, with 2^j, 2^k elements for some $j, k \geq 2$, respectively, overlapping in another Boolean subalgebra with 2^l elements, where $l < j, k$. Thus the cardinality of $[0, a']$ is

$$2^j + 2^k - 2^l = 2^l \left(2^{j-l} + 2^{k-l} - 1\right).$$

The number in the bracket is odd and it is not 1, thus not a power of 2. ∎

Definition 5.7. Let L be an ODL. A mapping $s : L \to \mathbb{Z}_2$ is called a *$\mathbb{Z}_2$-valued state* (abbr. $\mathbb{Z}_2$-state, or just state) if the following holds:

- $s(x) \oplus s(y) = s(x \vee y)$, whenever x, and y are orthogonal.
- $s(\mathbf{1}) = 1$.

5.6.2 Properties of Orthocomplemented Difference Lattices Related to $\mathbb{Z}_2$-States

Definition 5.8. Let L be an ODL. Then:

- L is called $\mathbb{Z}_2$-*rich* if for every two elements $x, y \in L$ such that $y \not\leq x$, there is a $\mathbb{Z}_2$-state s such that $s([\mathbf{0}, x]) = \{0\}$, and $s([y, \mathbf{1}]) = \{1\}$.
- L is called $\mathbb{Z}_2$-*complete* if for every two elements $x, y \in L$ such that $\mathbf{0} \neq y$, $x \neq \mathbf{1}$, $x \neq y$, there is a $\mathbb{Z}_2$-state s such that $s(x) = 0$, $s(y) = 1$.
- L is called $\mathbb{Z}_2$-*full* if for every two elements $x, y \in L, x \neq y$, there is a $\mathbb{Z}_2$-state s such that $s(x) \neq s(y)$.

In the literature, e.g., in [26], there is a different definition of $\mathbb{Z}_2$-fullness, which corresponds to our $\mathbb{Z}_2$-completeness. We will later show that the properties are indeed equivalent and that our definition of $\mathbb{Z}_2$-fullness is arguably more transparent.

Let us briefly comment on the properties. All of them require L to have for any pair of elements $x, y \in L$ a $\mathbb{Z}_2$-state, which distinguishes them in some sense whenever it is not an apparent contradiction.

The property of $\mathbb{Z}_2$-fullness is the weakest since it requires a state distinguishing the elements in an arbitrary way. Clearly, if an ODL L is $\mathbb{Z}_2$-rich or $\mathbb{Z}_2$-complete, then it is also $\mathbb{Z}_2$-full.

The relation between $\mathbb{Z}_2$-richness, and $\mathbb{Z}_2$-completeness is not immediate. For a pair of elements x, y such that $\mathbf{0} \neq y$, $x \neq \mathbf{1}$ and $y < x$, the property of $\mathbb{Z}_2$-completeness requires a state s satisfying $s(y) = 1$, $s(x) = 0$, while the $\mathbb{Z}_2$-richness does not.

At first sight, the property of $\mathbb{Z}_2$-completeness might seem to be more restrictive than the property of $\mathbb{Z}_2$-fullness, since we do not only require that, for every pair of elements, there is a state that distinguishes them, but furthermore, it allows us to choose the valuation on them. However, we shall show they are indeed equivalent.

Theorem 5.17. The properties of $\mathbb{Z}_2$-fullness a $\mathbb{Z}_2$-completeness are equivalent.

Proof. The direction $\mathbb{Z}_2$-complete $\Rightarrow$ $\mathbb{Z}_2$-full is immediate. For the other direction, for any $x, y \in L$, satisfying $\mathbf{0} \neq y, x \neq \mathbf{1}, x \neq y$, we give a construction of a state that fulfils the property of $\mathbb{Z}_2$-completeness for x, y, i.e., $s(x) = 0, s(y) = 1$, given L is $\mathbb{Z}_2$-full. We consider the three following $\mathbb{Z}_2$-states. If one of them satisfies $0 = s_i(x) \neq s_i(y) = 1$, we are done. Otherwise, the values on x, y are as follows:

- state s_1, distinguishing x, y, i.e., $s_1(x) \neq s_1(y)$, thus $s_1(x) = 1$, and $s_1(y) = 0$.
- state s_2, distinguishing $x, \mathbf{1}$, i.e., $s_2(x) \neq s_2(\mathbf{1}) = 1$, thus $s_2(x) = 0$, and hence $s_2(y) = 0$.
- state s_3, distinguishing $\mathbf{0}, y$, i.e., $0 = s_3(\mathbf{0}) \neq s_3(y)$, thus $s_3(y) = 1$, and hence $s_3(x) = 1$.

Now, a mapping $s : L \to \mathbb{Z}_2$ defined as $s(e) = s_1(e) \oplus s_2(e) \oplus s_3(e), e \in L$ is the desired state. To see it, we shall verify that s is indeed a state, and $0 = s(x) \neq s(y) = 1$. We start with the latter,

- $s(x) = s_1(x) \oplus s_2(x) \oplus s_3(x) = 1 \oplus 0 \oplus 1 = 0$.
- $s(y) = s_1(y) \oplus s_2(y) \oplus s_3(y) = 0 \oplus 0 \oplus 1 = 1$.

That holds true. For the verification that s is truly a state, we first list the properties of state and prove them for s in the sequel.

- $s(x) \oplus s(y) = s(x \vee y)$, whenever x, and y are orthogonal:

$$\begin{aligned} s(x) \oplus s(y) &= \overbrace{s_1(x) \oplus s_2(x) \oplus s_3(x)}^{s(x)} \oplus \overbrace{s_1(y) \oplus s_2(y) \oplus s_3(y)}^{s(y)} \\ &= \underbrace{s_1(x) \oplus s_1(y)}_{s_1(x\vee y)} \oplus \underbrace{s_2(x) \oplus s_2(y)}_{s_2(x\vee y)} \oplus \underbrace{s_3(x) \oplus s_3(y)}_{s_3(x\vee y)} \\ &= s(x \vee y), \end{aligned}$$

- $s(\mathbf{1}) = 1$:

$$s(\mathbf{1}) = s_1(\mathbf{1}) \oplus s_2(\mathbf{1}) \oplus s_3(\mathbf{1}) = 1 \oplus 1 \oplus 1 = 1.$$

∎

We shall also clarify why the $\mathbb{Z}_2$-richness is more restrictive than $\mathbb{Z}_2$-fullness, and they are indeed not equivalent. See [29] for a study of $\mathbb{Z}_2$-rich OMLs and in particular for an example of $\mathbb{Z}_2$-full OML that is not $\mathbb{Z}_2$-rich.

Proposition 5.18. The property of $\mathbb{Z}_2$-richness is strictly stronger than $\mathbb{Z}_2$-fullness.

We may naturally obtain $\mathbb{Z}_2$-states from symmetric differences in the following sense:

Proposition 5.19. Let L be an ODL. According to Proposition 5.9, there is a bijection $f : L \to \{0,1\}^n$ which induces the symmetric difference. A mapping $s : L \to \{0,1\}$ defined as $s(x) = f(x)_i$ for any $x \in L$ is a $\mathbb{Z}_2$-state[1].

Proof. The condition that $s(\mathbf{1}) = 1$ is satisfied since $f(\mathbf{1}) = \mathbf{1}$. We note that $s(x) \oplus s(y) = s(x \triangle y)$ for any $x, y \in L$. The second condition of a $\mathbb{Z}_2$-state is $s(x) \oplus s(y) = s(x \vee y)$ whenever $x \leq y'$. Then it holds that $x \triangle y = (x \wedge y') \vee (x' \wedge y) = x \vee y$ and we are done. ∎

Proposition 5.19 suggests that we can always find $\mathbb{Z}_2$-states on ODLs. This contrasts with OMLs, where it is possible to construct such algebras that do not admit any non-constant group-valued states, see [32, 48]. Furthermore, since we assigned a unique binary string to every element of the ODL, then for every pair of states, there is a position in which the respective binary strings differ; thus, we can construct a $\mathbb{Z}_2$-state which distinguishes them.

Corollary 5.20. Every ODL is $\mathbb{Z}_2$-full.

Corollary 5.21. Let L be an ODL. A mapping $s : L \to \{0,1\}$ satisfying $s(\mathbf{1}) = 1$ and $s(x) \oplus s(y) = s(x \triangle y)$ is a $\mathbb{Z}_2$-state.

It is not immediately clear if every $\mathbb{Z}_2$-state is in the form from Corollary 5.21. Therefore, we first show that it is necessary for elements in a common block. Then we

[1] $f(x)_i$ stands for the i-th element of the binary string $f(x)$.

show that there are other $\mathbb{Z}_2$-states not following the rule in general.

Proposition 5.22. Let L be an ODL and $x, y \in L$ be contained in a common block, then $s(x) \oplus s(y) = s((x \wedge y') \vee (x' \wedge y)) = s(x \triangle y)$ for any $\mathbb{Z}_2$-state on L.

Proof. Note that elements $x \wedge y'$, $x' \wedge y$, and $x \wedge y$ are pairwise orthogonal, clearly:

- $x \wedge y' \leq (x' \wedge y)' = x \vee y'$,
- $x \wedge y' \leq (x \wedge y)' = x' \vee y'$,
- $x' \wedge y \leq (x \wedge y)' = x' \vee y'$.

As a consequence, for every $\mathbb{Z}_2$-state it holds:

- $s(x \wedge y) \oplus s(x \wedge y') = s(x)$,
- $s(x \wedge y) \oplus s(x' \wedge y) = s(y)$,
- $s(x) \oplus s(y) = s(x' \wedge y) \oplus s(x \wedge y') = s((x' \wedge y) \vee (x \wedge y')) = s(x \triangle y)$.

The proof is concluded. ∎

Proposition 5.23. There is an ODL L with elements $x, y \in L$ such that there is a $\mathbb{Z}_2$-state violating $s(x \triangle y) = s(x) \oplus s(y)$.

Proof. Take the ODL which is a union of three two-atom blocks. It admits 2^3 different $\mathbb{Z}_2$-states. On the other hand, there are only four states satisfying the property $s(x \triangle y) = s(x) \oplus s(y)$ for all pairs x, y. ∎

5.6.3 Lattice of Subspaces of $\mathbb{R}^3$

It was a long-standing open question if the lattice of subspaces of $\mathbb{R}^3$ ($L(\mathbb{R}^3)$) admits a non-constant $\mathbb{Z}_2$-state. We have already encountered this question in the context of hidden-variable theory and BKS theorem in Section 4.4.

It is also connected to the ODLs. In the papers focusing on ODLs it was often formulated as an open question, see e.g., [24, 26, 28–29]. It is the case because $L(\mathbb{R}^3)$ is a natural infinite OML with 3 atoms in every block. According to Corollary 5.20, the study of $\mathbb{Z}_2$-states on it is closely related to the question whether it is possible to endow the lattice with a symmetric difference.

In the upcoming chapter we show that there is no non-constant $\mathbb{Z}_2$-state on $L(\mathbb{R}^3)$.

Corollary 5.24. The lattice of subspaces of $\mathbb{R}^3$ is not ODL-embeddable[1].

[1] Vaguely speaking, there is no ODL which has $L(\mathbb{R}^3)$ as a sublattice. For the precise definition of ODL-embeddability, we refer to [25].

Chapter 6
$\mathbb{Z}_2$-Coloring of the Lattice of Subspaces of $\mathbb{R}^3$

Throughout the thesis, we have encountered the question about the existence of non-constant $\mathbb{Z}_2$-states on the lattice of subspaces of $\mathbb{R}^3$ ($L(\mathbb{R}^3)$) in different contexts. Once with the connection to BKS theorem in Section 4.4, and then in the context of ODLs in Subsection 5.6.3.

In this chapter, we give a definitive answer that the only $\mathbb{Z}_2$-state on $L(\mathbb{R}^3)$ is the constant one. The elements of $L(\mathbb{R}^3)$ are subspaces of $\mathbb{R}^3$; the order is induced by inclusion.

The chapter is almost identical to a part of the paper [47].

We adopt the notation from BKS constructions; thus, we call the state a *coloring* and list the definitions in the spirit of Theorem 3.1.

Definition 6.1.

- A $\mathbb{Z}_2$-*coloring* is a mapping $m : \mathbb{R}^3 \setminus \{\mathbf{0}\} \to \{0, 1\}$ such that, for every three pairwisely orthogonal vectors, $\mathbf{u}, \mathbf{v}, \mathbf{w}$, it holds that $m(\mathbf{u}) \oplus m(\mathbf{v}) \oplus m(\mathbf{w}) = 1$, where $\oplus$ denotes addition modulo 2.
- Two rays, $\mathbf{u}$, $\mathbf{v}$, are called *isochromatic* if $m(\mathbf{u}) = m(\mathbf{v})$ for all $\mathbb{Z}_2$-colorings m.

6.1 Basic Construction

At first, a construction of 21 rays is shown. It contains three non pairwisely-orthogonal rays, $\mathbf{u}$, $\mathbf{r}$, $\mathbf{o}$ such that in every coloring m, $m(\mathbf{u}) \oplus m(\mathbf{r}) \oplus m(\mathbf{o}) = 1$. In Section 6.2, we shall show that this property of three rays is sufficient for every coloring to be constant.

Figure 6.1 shows a hypergraph $H = (V, E)$ that represents a set of rays used in the proof of the main theorem. Vertices (dots) of the hypergraph represent rays. Its edges (smooth curves) represent orthogonality relations in such a way that two vertices contained in an edge are orthogonal. E.g., ray $\mathbf{a}$ is orthogonal to rays $\mathbf{b}, \mathbf{c}, \mathbf{f}, \mathbf{g}$.

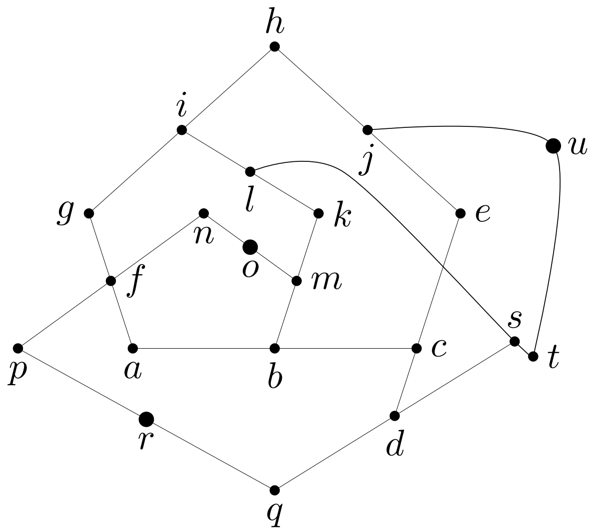

Figure 6.1. Orthogonality diagram

We shall show that there exist rays with these orthogonality relations. We do so by the following explicit construction that ensures the orthogonality relations drawn by *straight lines* in the figure. Each line represents three binary orthogonality relations, ensured by the choice of vectors or by choosing one vector as the cross product of the remaining two *orthogonal* vectors. The construction uses two non-zero real parameters, x, y, which will be specified later.[1]

- $\mathbf{a} = (1,0,0)$
- $\mathbf{b} = (0,1,0)$
- $\mathbf{c} = (0,0,1)$
- $\mathbf{d} = (x,1,0)$
- $\mathbf{e} = \mathbf{c} \times \mathbf{d} = (-1,x,0)$
- $\mathbf{f} = (0,1,y)$
- $\mathbf{g} = \mathbf{a} \times \mathbf{f} = (0,-y,1)$
- $\mathbf{h} = \mathbf{e} \times \mathbf{g}$
- $\mathbf{i} = \mathbf{g} \times \mathbf{h}$
- $\mathbf{j} = \mathbf{e} \times \mathbf{h}$
- $\mathbf{k} = \mathbf{b} \times \mathbf{i}$
- $\mathbf{l} = \mathbf{i} \times \mathbf{k}$
- $\mathbf{m} = \mathbf{b} \times \mathbf{k}$
- $\mathbf{n} = \mathbf{f} \times \mathbf{m}$
- $\mathbf{o} = \mathbf{m} \times \mathbf{n}$
- $\mathbf{p} = \mathbf{f} \times \mathbf{n}$
- $\mathbf{q} = \mathbf{d} \times \mathbf{p}$
- $\mathbf{r} = \mathbf{p} \times \mathbf{q}$
- $\mathbf{s} = \mathbf{d} \times \mathbf{q}$
- $\mathbf{t} = \mathbf{s} \times \mathbf{l}$
- $\mathbf{u} = \mathbf{j} \times \mathbf{t}$

It remains to ensure the orthogonality relations drawn by *round curves* in the figure. The last line of the table contains the respective two cross products whose arguments need not be orthogonal. We shall achieve their orthogonality, $\mathbf{s} \perp \mathbf{l}$, $\mathbf{j} \perp \mathbf{t}$, by adjusting the parameters x, y. This requires to solve the following system of two polynomial equations:

$$\mathbf{l} \cdot \mathbf{s} = 0\,,$$
$$\mathbf{t} \cdot \mathbf{j} = 0\,.$$

It has real roots, e.g., the following:

$$y = \frac{1}{3}\sqrt{1 + \sqrt[3]{163 - 9\sqrt{57}} + \sqrt[3]{163 + 9\sqrt{57}}} \doteq 1.14\,,$$
$$x = -\sqrt{\frac{y^2 + \sqrt{4y^8 + 16y^6 + 25y^4 + 16y^2 + 4}}{2y^2 + 2}} \doteq -1.61\,.$$

[1] We evaluate the coordinates of the vectors only in simple cases; then the complexity of expressions grows rapidly and they are omitted here.

We remark that all the constructed vectors, $\mathbf{a}, \mathbf{b}, \ldots, \mathbf{u}$, are non-zero; this can be checked by a computer.

Suppose that there is a coloring, m. Then we sum its values over all vertices of all 13 edges:

$$s = \bigoplus_{e \in E} \bigoplus_{\mathbf{v} \in e} m(\mathbf{v}) \equiv 13 \equiv 1 \qquad (\mathrm{mod}\ 2)$$

Vertices from $F = \bigcup E \setminus \{\mathbf{r}, \mathbf{u}, \mathbf{o}\}$ are contained twice in the latter sum, thus their coloring does not influence the result. Only vertices $\mathbf{r}, \mathbf{u}, \mathbf{o}$ are contained in a single edge. We may rewrite the sum as

$$s = 2\Bigg(\bigoplus_{\mathbf{v} \in F} m(\mathbf{v})\Bigg) \oplus m(\mathbf{r}) \oplus m(\mathbf{u}) \oplus m(\mathbf{o}) = m(\mathbf{r}) \oplus m(\mathbf{u}) \oplus m(\mathbf{o}) = 1\,.$$

It remains to prove that the rays $\mathbf{r}, \mathbf{u}, \mathbf{o}$ are not all pairwisely orthogonal. We shall verify that $\mathbf{r} \not\perp \mathbf{o}$. According to [16], the hypergraphs representing orthomodular lattices cannot contain cycles of lengths 3 or 4.[1] As $\mathbf{r}, \mathbf{o}$ already have distance 3 in our hypergraph, they can be neither identified, nor connected by an edge, without breaking this rule; hence $\mathbf{r} \neq \mathbf{o}$, $\mathbf{r} \not\perp \mathbf{o}$.

Remark 6.1. We give a detailed argument for readers not familiar with the properties of hypergraphs of orthomodular lattices (Greechie diagrams). Suppose that $\mathbf{r} \perp \mathbf{o}$. Then $\mathbf{r} \times \mathbf{n}$ would be both $\mathbf{o}$ and $\mathbf{p}$, but these are distinct.

We do not verify that there are no other orthogonality relations not drawn in the figure, but this is not needed in the sequel. We could say more about the rays $\mathbf{r}, \mathbf{u}, \mathbf{o}$: they are distinct, not coplanar, etc.

However, the hypergraph techniques have limitations; the fact that $\mathbf{o} \neq \mathbf{u}$ does not follow from the hypergraph. Nevertheless, it was checked for our particular case by computer algebra.

6.2 Application to the Coloring Problem

The coloring is independent of the choice of a coordinate system. For any orthonormal matrix $\mathbf{U} \in \mathbb{R}^{3\times 3}$, if m is a coloring, then $m' : \mathbb{R}^3 \setminus \{\mathbf{0}\} \to \{0, 1\}$, defined by $m'(\mathbf{x}) = m(\mathbf{U}\mathbf{x})$, is also a coloring because the multiplication by an orthonormal matrix preserves the dot product.

Rotations and reflextions are represented by orthonormal matrices. For any two pairs of rays, $(\mathbf{u}, \mathbf{v}), (\mathbf{u}', \mathbf{v}')$, such that $\angle(\mathbf{u}, \mathbf{v}) = \angle(\mathbf{u}', \mathbf{v}')$, i.e., $\frac{|\mathbf{u}\cdot\mathbf{v}|}{\|\mathbf{u}\|\|\mathbf{v}\|} = \frac{|\mathbf{u}'\cdot\mathbf{v}'|}{\|\mathbf{u}'\|\|\mathbf{v}'\|}$, there exists an orthonormal matrix $\mathbf{U}$ such that $\mathbf{U}\mathbf{u} = \mathbf{u}'$ and $\mathbf{U}\mathbf{v} = \mathbf{v}'$.

Corollary 6.2. If some pair of rays with angle θ is isochromatic, then every pair of rays with angle θ is isochromatic.

[1] More exactly, cycles of lengths 3 or 4 may occur under special circumstances. This requires lattices of height more than 3, which is not the case of the lattice of subspaces of $\mathbb{R}^3$ (dimension at least 4 is needed). See [21] for details.

Theorem 6.3. If two different rays are isochromatic, then the only coloring is the constant one.

Proof. Let $\mathbf{u}, \mathbf{v}$ be isochromatic rays, $\theta = \angle(\mathbf{u}, \mathbf{v}) \neq 0$. We define $\mathbf{S}$ as the set of all rays $\mathbf{w}$ such that $\angle(\mathbf{u}, \mathbf{w}) = \theta$. All rays from $\mathbf{S}$ are isochromatic and their mutual angles span the whole interval $[0, \min(\pi/2, 2\theta)]$. By Corollary 6.2, every pair of rays with angle in $[0, \min(\pi/2, 2\theta)]$ is isochromatic. We repeat this procedure, extending the result to larger angles, and after $\lfloor \log_2 \frac{\pi}{2\theta} \rfloor$ repetitions we obtain that all rays are isochromatic. ■

Theorem 6.4. If there are three different rays $\mathbf{u}, \mathbf{v}, \mathbf{w}$ that are not all pairwisely orthogonal and a constant $c \in \mathbb{Z}_2$ such that every coloring m satisfies $m(\mathbf{u}) \oplus m(\mathbf{v}) \oplus m(\mathbf{w}) = c$, then every coloring is constant.

Proof. We split the proof into two cases. The first is when the three rays are coplanar. Then there is a ray $\mathbf{n}$ orthogonal to all of $\mathbf{u}, \mathbf{v}, \mathbf{w}$. (It need not be unique in singular cases, which are allowed here.) The rotation by $\pi/2$ about $\mathbf{n}$ maps $\mathbf{u} \mapsto \mathbf{u}'$, $\mathbf{v} \mapsto \mathbf{v}'$, $\mathbf{w} \mapsto \mathbf{w}'$ and is represented by an orthonormal matrix $\mathbf{U}$. We take an arbitrary coloring m and construct a coloring m', defined as $m'(\mathbf{x}) = m(\mathbf{U}\mathbf{x})$. The values on $\mathbf{u}, \mathbf{v}, \mathbf{w}$ are summing up to c in any coloring; hence also for m', then

$$c = m'(\mathbf{u}) \oplus m'(\mathbf{v}) \oplus m'(\mathbf{w}) = m(\mathbf{U}\mathbf{u}) \oplus m(\mathbf{U}\mathbf{v}) \oplus m(\mathbf{U}\mathbf{w}) = m(\mathbf{u}') \oplus m(\mathbf{v}') \oplus m(\mathbf{w}').$$

We say that rotation and reflection *preserve* coloring. Now we may continue with the equations:

$$\begin{aligned} m(\mathbf{u}) \oplus m(\mathbf{u}') \oplus m(\mathbf{n}) &= 1\,, \\ m(\mathbf{v}) \oplus m(\mathbf{v}') \oplus m(\mathbf{n}) &= 1\,, \\ m(\mathbf{w}) \oplus m(\mathbf{w}') \oplus m(\mathbf{n}) &= 1\,, \\[1em] \underbrace{m(\mathbf{u}) \oplus m(\mathbf{v}) \oplus m(\mathbf{w})}_{c} & \\ \oplus\ \underbrace{m(\mathbf{u}') \oplus m(\mathbf{v}') \oplus m(\mathbf{w}')}_{c} & \\ \oplus\ m(\mathbf{n}) \oplus m(\mathbf{n}) \oplus m(\mathbf{n}) &= 1\,, \\ m(\mathbf{n}) &= 1\,. \end{aligned}$$

We determined the value of m at a single ray, $\mathbf{n}$. As colorings are preserved by rotations, the same arguments apply to the images of $\mathbf{n}$ (and all rays used in the construction) under any rotation. Due to the spherical symmetry, $\mathbf{n}$ can be mapped to any other ray by some rotation, and m attains the constant value 1 at all rays.

The other case is when the rays, $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w}$ are not coplanar. If the vectors are not pairwisely orthogonal, they contain a non-orthogonal pair. Without loss of generality, we assume that it is $(\mathbf{v}, \mathbf{w})$, i.e., $\mathbf{v} \not\perp \mathbf{w}$. The reflection w.r.t. the plane $\mathrm{span}(\{\mathbf{u}, \mathbf{v}\})$ maps $\mathbf{u}$ and $\mathbf{v}$ to themselves, but maps $\mathbf{w}$ to $\mathbf{w}' \neq \mathbf{w}$. It preserves colorings, thus each coloring m satisfies

$$m(\mathbf{u}) \oplus m(\mathbf{v}) \oplus m(\mathbf{w}) = c,$$
$$m(\mathbf{u}) \oplus m(\mathbf{v}) \oplus m(\mathbf{w}') = c,$$
$$m(\mathbf{w}) = m(\mathbf{w}')$$

for two different rays $\mathbf{w}, \mathbf{w}'$. A direct application of Theorem 6.3 finishes the proof. ∎

Theorem 6.5. There is no non-constant $\mathbb{Z}_2$-coloring of a sphere in $\mathbb{R}^3$.

Proof. This is a straightforward consequence of Theorem 6.4, applied to rays $\mathbf{u}, \mathbf{r}, \mathbf{o}$ from the construction described in Section 6.1. ∎

Remark 6.6. The rays $\mathbf{u}, \mathbf{r}, \mathbf{o}$, constructed in Section 6.1, are not coplanar. However, the proof of this fact (cf. Rem. 6.1) is more complicated than the proof of the "coplanar" part of Theorem 6.4, which, possibly, could find application elsewhere. We proved that there are two distinct sufficient properties (see Theorems 6.3, 6.4) for the coloring to be constant. Our collection of vectors satisfies the first one[1], and by taking the union of our collection with its reflected copy about the plane $\mathrm{span}(\{\mathbf{u}, \mathbf{o}\})$, we arrive at a set of 40 vectors[2], satisfying the second[3] property. We proved Theorem 6.4 in a more general form than needed and for c not necessarily equal to 1.

[1] There are three different vectors, not pairwisely orthogonal, summing up to a constant in every coloring.
[2] Two of the 21 vectors belong to the plane of symmetry, the remaining 19 are reflected. Thus we use $2 + 2 \cdot 19$ vectors in total.
[3] There is a pair of distinct isochromatic vectors.

Chapter 7
Conclusions

7.1 Summary

We started with reviewing the mathematical aspects of quantum mechanics. Then we progressed to study Bell–Kochen–Specker theorem, which rules out the hidden-variable theory of quantum mechanics. Subsequently, we introduced orthocomplemented difference lattices. They are structures that could be used to describe the logic of quantum mechanics. Finally, we showed that there is no non-constant measure on the lattice of subspaces of $\mathbb{R}^3$.

7.2 Contribution

We list the two main results of the thesis:

- We constructed an orthocomplemented difference lattice admitting no state.
- We showed that there is no non-constant measure on the lattice of subspaces of $\mathbb{R}^3$.

References

[1] Arends, F., Ouaknine, J., and Wampler, C. W. On searching for small Kochen–Specker vector systems. 23–34.

[2] Bell, J. S. On the Einstein–Podolsky–Rosen paradox. *Physics Physique Fizika 1*, 3 (1964), 195–200.

[3] Bell, J. S. On the problem of hidden variables in quantum mechanics. *Reviews of Modern Physics 38* (1966), 447–452.

[4] Beran, L. *Orthomodular Lattices: Algebraic Approach*, vol. 18. Springer Science & Business Media, 2012.

[5] Berge, C. *Hypergraphs: Combinatorics of Finite Sets*, vol. 45. Elsevier, 1984.

[6] Birkhoff, G. *Lattice Theory*, vol. 25. American Mathematical Soc., 1940.

[7] Birkhoff, G., and von Neumann, J. The logic of quantum mechanics. *Annals of Mathematics* (1936), 823–843.

[8] Bohm, D. A suggested interpretation of the quantum theory in terms of hidden variables. I. *Physical review 85* (1952), 166–179.

[9] Born, M., Heisenberg, W., and Jordan, P. Zur Quantenmechanik. II. *Zeitschrift für Physik 35*, 8 (1926), 557–615.

[10] Brassard, G., Cleve, R., and Tapp, A. Cost of exactly simulating quantum entanglement with classical communication. *Physical Review Letters 83*, 9 (1999), 1874–1877.

[11] Cabello, A., Estebaranz, J., and García-Alcaine, G. Bell–Kochen–Specker theorem: A proof with 18 vectors. *Physics Letters A 212*, 4 (1996), 183–187.

[12] Cohen, D. W. *An Introduction to Hilbert Space and Quantum Logic*. Springer Science & Business Media, 2012.

[13] Einstein, A., Podolsky, B., and Rosen, N. Can quantum-mechanical description of physical reality be considered complete? *Physical Review 47* (1935), 777–780.

[14] Gleason, A. Measures on the closed subspaces of a Hilbert space. *Indiana University Mathematics Journal 6* (1957), 885–893.

[15] Godsil, C. D., and Zaks, J. Colouring the sphere. *University of Waterloo research report* (1988).

[16] Greechie, R. J. Orthomodular lattices admitting no states. *Journal of Combinatorial Theory, Series A 10*, 2 (1971), 119–132.

[17] Harding, J., Jager, E., and Smith, D. Group-valued measures on the lattice of closed subspaces of a Hilbert space. *International Journal of Theoretical Physics 44*, 5 (2005), 539–548.

[18] Havlicek, H., Krenn, G., Summhammer, J., and Svozil, K. Colouring the rational quantum sphere and the Kochen–Specker theorem. *Journal of Physics A: Mathematical and General 34*, 14 (2001), 3071–3077.

[19] Hermann, G. Die naturphilosophischen Grundlagen der Quantenmechanik. *Naturwissenschaften 23*, 42 (1935), 718–721.

[20] Hroch, M., and Pták, P. States on orthocomplemented difference posets (extensions). *Letters in Mathematical Physics 106*, 8 (2016), 1131–1137.

[21] Kalmbach, G. *Orthomodular Lattices*, vol. 18. Academic Press, 1983.

[22] Kochen, S., and Specker, E. The problem of hidden variables in quantum mechanics. *Indiana University Mathematics Journal 17* (1968), 59–87.

[23] Lisoněk, P., Badziąg, P., Portillo, J. R., and Cabello, A. Kochen–Specker set with seven contexts. *Physical Review A 89* (Apr 2014), 042101.

[24] Matoušek, M. Orthocomplemented lattices with a symmetric difference. *Algebra Universalis 60*, 2 (2009), 185–215.

[25] Matoušek, M., and Pták, P. Orthocomplemented posets with a symmetric difference. *Order 26*, 1 (2009), 1–21.

[26] Matoušek, M., and Pták, P. Symmetric difference on orthomodular lattices and $\mathbb{Z}_2$-valued states. *Commentationes Mathematicae Universitatis Carolinae 50*, 4 (2009), 535–547.

[27] Matoušek, M., and Pták, P. On identities in orthocomplemented difference lattices. *Mathematica Slovaca 60*, 5 (2010), 583–590.

[28] Matoušek, M., and Pták, P. Orthomodular posets related to $\mathbb{Z}_2$-valued states. *International Journal of Theoretical Physics 53*, 10 (2014), 3323–3332.

[29] Matoušek, M., and Pták, P. Orthomodular lattices that are $\mathbb{Z}_2$-rich. *Ricerche di Matematica 67* (2018), 321–329.

[30] McKay, B. D. Isomorph-free exhaustive generation. *Journal of Algorithms 26*, 2 (1998), 306–324.

[31] Meyer, D. A. Finite precision measurement nullifies the Kochen–Specker theorem. *Physical Review Letters 83*, 19 (1999), 3751–3754.

[32] Navara, M. An orthomodular lattice admitting no group-valued measure. *Proceedings of the American Mathematical Society 122*, 1 (1994), 7–12.

[33] Navara, M. Mathematical questions related to non-existence of hidden variables. *Foundations of Probability and Physics 5*, American Institute of Physics Conference Proceedings, vol. 1101 (2009), 119–126.

[34] Navara, M., and Pták, P. For $n \geq 5$ there is no nontrivial $\mathbb{Z}_2$-measure on $L(\mathbb{R}^n)$. *International Journal of Theoretical Physics 43*, 7 (2004), 1595–1598.

[35] Peres, A. Incompatible results of quantum measurements. *Physics Letters A 151*, 3-4 (1990), 107–108.

[36] Peres, A. Two simple proofs of the Kochen–Specker theorem. *Journal of Physics A: Mathematical and General 24*, 4 (1991), 175–178.

[37] Peres, A. Generalized Kochen–Specker theorem. *Foundations of Physics 26*, 6 (1996), 807—812.

[38] Peres, A. *Quantum Theory: Concepts and Methods*, vol. 57. Springer Science & Business Media, 2006.

[39] Peres, A., and Terno, D. R. Quantum information and relativity theory. *Reviews of Modern Physics 76*, 1 (2004), 93–123.

[40] Pták, P., and Pulmannová, S. *Orthomodular Structures as Quantum Logics.* Springer Netherlands, 1991.

[41] Ramanathan, R., Rosicka, M., Horodecki, K., Pironio, S., Horodecki, M., and Horodecki, P. Gadget structures in proofs of the Kochen–Specker theorem. *Quantum 4* (2020), 308.

[42] Schrödinger, E. An undulatory theory of the mechanics of atoms and molecules. *Physical Review 28* (1926), 1049–1070.

[43] Shultz, F. W. A characterization of state spaces of orthomodular lattices. *Journal of Combinatorial Theory, Series A 17*, 3 (1974), 317–328.

[44] Svozil, K. *Quantum Logic.* Springer Science & Business Media, 1998.

[45] Uijlen, S., and Westerbaan, B. A Kochen–Specker system has at least 22 vectors. *New Generation Computing 34*, 1-2 (2016), 3–23.

[46] von Neumann, J. *Mathematische Grundlagen der Quantenmechanik.* Springer, Berlin, 1932.

[47] Voráček, V., and Navara, M. Generalised Kochen–Specker theorem in three dimensions. *Foundations of Physics, submitted* (2021).

[48] Weber, H. There are orthomodular lattices without non-trivial group-valued states: A computer-based construction. *Journal of Mathematical Analysis and Applications 183*, 1 (1994), 89–93.

[49] Yu, S., and Oh, C. H. State-independent proof of Kochen–Specker theorem with 13 rays. *Physical Review Letters 108*, 3 (2012), 030402.

Appendix A
Master's Thesis Assignment

MASTER'S THESIS ASSIGNMENT

I. Personal and study details

Student's name:	**Voráček Václav**	Personal ID number:	**466379**
Faculty / Institute:	**Faculty of Electrical Engineering**		
Department / Institute:	**Department of Cybernetics**		
Study program:	**Open Informatics**		
Specialisation:	**Computer Vision and Image Processing**		

II. Master's thesis details

Master's thesis title in English:

Combinatorial Methods in the Study of Quantum Structures

Master's thesis title in Czech:

Kombinatorické metody ve studiu kvantových struktur

Guidelines:

Examine the state spaces (spaces of probability measures) of event structures used in quantum mechanics, using mathematical and computational tools. Concentrate on the existence of states with particular properties, studied in previous works. States with values in other groups than the reals should be considered, too. Emphasis should be put on results related to the (non-)existence of hidden variables, i.e., states attaining only two values. Try to solve some of the open problems or find improvements of known proofs.

Bibliography / sources:

[1] Bell, J.S.: On the Einstein–Podolsky–Rosen paradox. Physics 1 (1964), 195–200.
[2] Bell, J.S.: On the problem of hidden variables in quantum mechanics. Reviews of Modern Physics 38 (1966), 447–452.
[3] Kochen, S., Specker, E.: The problem of hidden variables in quantum mechanics. Indiana Univ. Math. J. 17 (1968), 59–87.
[4] Navara, M., Pták, P.: For n ≥ 5 there is no nontrivial Z2-measure on L(Rn). International Journal of Theoretical Physics 43, 7 (2004), 1595–1598.
[5] Harding, J., Jager, E., Smith, D.: Group-valued measures on the lattice of closed subspaces of a Hilbert space. International Journal of Theoretical Physics 44 (2005), 539–548.
[6] Navara, M.: Mathematical questions related to non-existence of hidden variables. American Institute of Physics Conference Proceedings 1101 (2009), 119–126.

Name and workplace of master's thesis supervisor:

prof. Ing. Mirko Navara, DrSc., Machine Learning, FEE

Name and workplace of second master's thesis supervisor or consultant:

Date of master's thesis assignment: **01.01.2021** Deadline for master's thesis submission: **21.05.2021**

Assignment valid until: **30.09.2022**

prof. Ing. Mirko Navara, DrSc. Supervisor's signature	prof. Ing. Tomáš Svoboda, Ph.D. Head of department's signature	prof. Mgr. Petr Páta, Ph.D. Dean's signature

III. Assignment receipt

The student acknowledges that the master's thesis is an individual work. The student must produce his thesis without the assistance of others, with the exception of provided consultations. Within the master's thesis, the author must state the names of consultants and include a list of references.

.	
Date of assignment receipt	Student's signature