VILNIUS UNIVERSITY

Haroldas Giedra

PROOF SYSTEM FOR LOGIC OF CORRELATED KNOWLEDGE

Doctoral Dissertation
Physical Sciences, Informatics (09P)

Vilnius, 2014

The dissertation work was carried out at the Institute of Mathematics and Informatics of Vilnius University in 2009 - 2013.

Scientific Supervisor:

Assoc. Prof. Dr. Habil. Regimantas Ričardas Pliuškevičius (Vilnius University, Physical Sciences, Informatics - 09P)

VILNIAUS UNIVERSITETAS

Haroldas Giedra

ĮRODYMŲ SISTEMA KORELIATYVIŲ ŽINIŲ LOGIKAI

Daktaro disertacija
Fiziniai mokslai, informatika (09P)

Vilnius, 2014

Disertacija rengta 2009 - 2013 metais Vilniaus universiteto Matematikos ir informatikos institute.

Mokslinis vadovas:

Doc. habil. dr. Regimantas Ričardas Pliuškevičius (Vilniaus universitetas, fiziniai mokslai, informatika - 09P).

Acknowledgements

I would like express my special thanks to Prof. Regimantas Pliuškevičius, Prof. Aida Pliuškevičienė, Assoc. Prof. Jūratė Sakalauskaitė and Dr. Romas Alonderis for their sincere knowledge sharing, collaboration, consultancy and indispensable support.

I am sincerely thankful to Prof. Gintautas Dzemyda, Prof. Albertas Čaplinskas, Prof. Antanas Žilinskas and Danutė Rimeišienė for their honest help and support in all areas during PhD studies from the beginning.

I greatly appreciate the time and effort of the reviewers Dr. Adomas Birštūnas and Dr. Julius Andrikonis for their professional opinion and attitude, notes and advices reviewing the PhD thesis.

I wish to thank to my Parents that gave me life and grow me up.

And I am thankful to all people of Lithuania for opportunity to work in science.

Haroldas Giedra
Vilnius

Table of Contents

Notation

LCK - logic of correlated knowledge.
HS-LCK - Hilbert style proof system for logic of correlated knowledge.
GS-LCK - Gentzen style sequent calculus for logic of correlated knowledge.
GS-LCK-PROC - proof search procedure in the sequent calculus GS-LCK.
$\mathbb{C}$ - set of complex numbers.
$|\psi\rangle$ - quantum bit.
H - Hilbert space.
cod - codification function.
msg - message assignment function.
$chan$ - channel assignment function.
res - measurement assignment function.
a_i - agent.
O_{a_i} - set of possible observations of agent a_i.
I - group of agents.
o - joint observation.
O_I - set of joint observations of group of agents I.
r - result of observation.
o^r - atomic formula of joint observation and result.
p - atomic proposition.
$s \overset{I}{\sim} t$ - relational atom.
$s : A$ - labelled formula.
S - sequent.
Γ, Δ - multisets of formulas in a sequent.
$TableLK$ - table of the applications of the rules $(K_I \Rightarrow)$ and $(K_N \Rightarrow)$.
$TableRK$ - table of the applications of the rule $(\Rightarrow K_I)$.
$n(K_I)$ - number of the knowledge operators K_I in the negative part of the sequent.

Chapter 1

Introduction

1.1 Research Area and Problems

In quantum mechanics we have quantums systems consisting of elementary particles (e.g. electrons). Information about such systems can be handled, using logical calculi. In 1936 von Neumann co-authored a paper with G. Birkhoff [8] introducing the ideas of quantum logic. However some important impossibility results were obtained [2, 40]. D. Aerts, C. Randall and D. Foulis showed that quantum logic rises problems when trying to describe compound systems consisting of more than one elementary particle that can exhibit quantum entanglement. Also they showed that tensor products of quantum logic do not exist.

Several other approaches were obtained to reason about quantum systems. One of the latest is logic of correlated knowledge introduced by Alexandru Baltag and Sonja Smets in 2010 [5]. Logic of correlated knowledge abstracts away from Hilbert spaces, which are used in quantum mechanics and quantum logic, and suggests to accomodate correlation models to quantum systems and quantum entanglement. However, we do not have yet automated proof system for logic of correlated knowledge, which would allow us to reason about quantum systems automatically, using computers.

1.2 Actuality

The states of quantum systems are determined by performing measurements on particles. The informational processes of such measurements can be handled using proof system. Also calculations of quantum computing are executed by changing the states of the quantum register, which consists of quantum bits or quantum particles, until the result of computing is obtained. The process of the changes of the states can be analysed and managed using logical calculus. Automated proof system for logic of correlated knowledge would allow to do this in automated way, using computers.

1.3 Aim of the Research

The main aim of the research is to create proof system for logic of correlated knowledge, satisfying the properties of soundness, completeness and termination.

1.4 Tasks of the Research

The tasks for reaching the main aim of the research are:

- Create sequent calculus GS-LCK for logic of correlated knowledge.
- Prove soundness of GS-LCK.
- Prove invertibility of rules.
- Prove admissibility of weakening.
- Prove admissibility of contraction.
- Prove admissibility of cut.
- Prove completeness of GS-LCK.
- Create proof search procedure for GS-LCK.
- Prove the termination of proof search procedure.

1.5 Research Methodology

As a main method to create automated proof system, sequent calculus is used. Gerhard Gentzen introduced sequent calculi in 1934 [15]. Sequent calculus allows to perform automated proof search if cut rule is admissible. We are using the ideas of semantic internalization, suggested by Sara Negri in [30], to get admissibility of cut rule and other properties of the sequent calculus GS-LCK. Also the Hilbert style proof system suggested by Alexandru Baltag and Sonja Smets in [5] is used to prove the completeness of GS-LCK.

1.6 Scientific Novelty

The following new results have been obtained in the research:

- Sequent calculus GS-LCK for logic of correlated knowledge has been created.
- Soundness, completeness and admissibility of weakening, contraction and cut of GS-LCK have been proved.
- Terminating proof search procedure for GS-LCK has been created.
- Decidability of logic of correlated knowledge has been proved.

1.7 Defending Statements

- Sequent calculus GS-LCK for logic of correlated knowledge has been created, which satisfy the properties:
  - Soundness.
  - Invertibility of rules.
  - Admissibility of weakening, contraction and cut.
  - Completeness.
- Procedure GS-LCK-PROC has been created, which performs terminating proof search in sequent calculus GS-LCK.
- Logic of correlated knowledge is decidable.

Chapter 2

Quantum mechanics

Quantum mechanics is a branch of physics which deals with physical phenomena at nanoscopic scales where the action is on the order of the Planck constant. It provides a mathematical description of much of the dual particle-like and wave-like behavior and interactions of energy and matter.

In 1900, Max Planck introduced quantum hypothesis, which was the birth of quantum mechanics [29]. Planck made the assumption that energy was made of individual units, or quanta. Albert Einstein theorized that not just the energy, but the radiation itself was quantized in the same manner. In 1924, Louis de Broglie proposed that there is no fundamental difference in the makeup and behavior of energy and matter. On the atomic and subatomic level either may behave as if made of either particles or waves. This theory became known as the principle of wave-particle duality: elementary particles of both energy and matter behave, depending on the conditions, like either particles or waves. Werner Heisenberg proposed that precise, simultaneous measurement of two complementary values - such as the position and momentum of a subatomic particle - is impossible. Contrary to the principles of classical physics, their simultaneous measurement is inescapably flawed: the more precisely one value is measured, the more flawed will be the measurement of the other value. This theory became known as the uncertainty principle, which prompted Albert Einstein's famous comment, "God does not play dice".

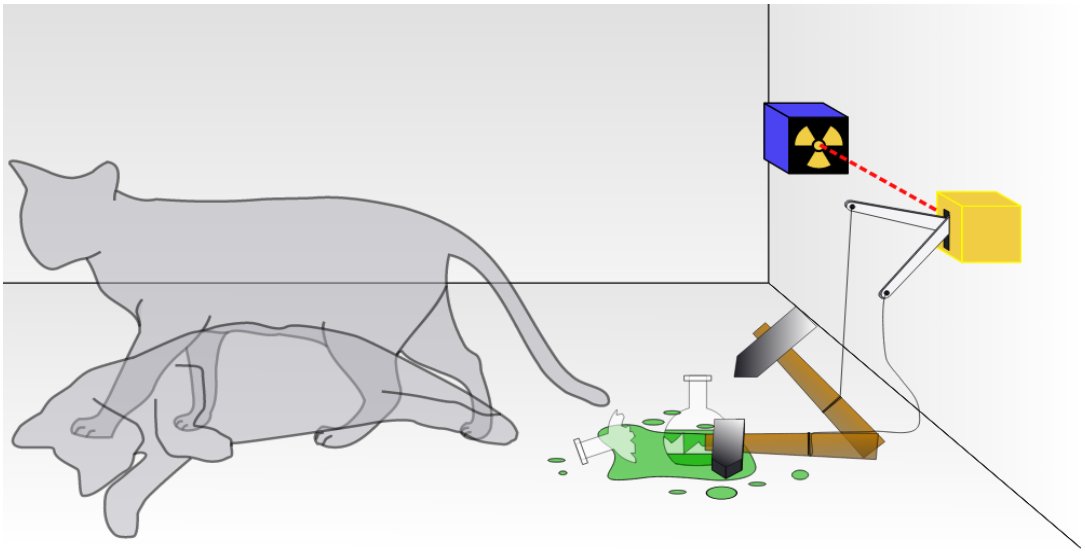
Early quantum theory was significantly formulated in the mid-1920s. Werner

Heisenberg, Max Born and Pascual Jordan introduced matrix mechanics. Erwin Schrödinger formulated Schrödinger equation, which describes how the quantum state of a physical system changes with time [50]. Wolfgang Pauli and Satyendra Nath Bose proposed results in statistics of subatomic particles.

By 1930, quantum mechanics had been further unified and formalized by the work of David Hilbert, Paul Dirac and John von Neumann [48] with a greater emphasis placed on measurement in quantum mechanics, the statistical nature of our knowledge of reality, and philosophical speculation about the role of the observer.

The two major interpretations of quantum theory's implications for the nature of reality are the Copenhagen interpretation and the many-worlds theory. Niels Bohr proposed the Copenhagen interpretation of quantum theory, which asserts that a particle is whatever it is measured to be (for example, a wave or a particle), but that it cannot be assumed to have specific properties, or even to exist, until it is measured. In short, Bohr was saying that objective reality does not exist. This translates to a principle called superposition that claims that while we do not know what the state of any object is, it is actually in all possible states simultaneously, as long as we don't look to check.

To illustrate this theory, we can use the famous and somewhat cruel analogy of Schrodinger's Cat. First, we have a living cat and place it in a thick lead box. At this stage, there is no question that the cat is alive.



We then throw in a vial of cyanide and seal the box. We do not know if the cat is alive or if it has broken the cyanide capsule and died. Since we do not know, the cat is both dead and alive, according to quantum law - in a superposition of states. It is only when we break open the box and see what condition the cat is that the superposition is lost, and the cat must be either alive or dead.

Broadly speaking, Quantum mechanics incorporates four classes of phenomena:

- Quantization of certain physical properties
- Wave-particle duality
- Principle of uncertainty
- Quantum entanglement

It covers fields like:

- Mathematical formulation of quantum mechanics
- Interpretations of quantum mechanics
- Quantum field theory
- Quantum states
- Quantum information
- Quantum computers
- Supersymmetry
- Quantum gravity
- String theory

Our work is mostly related to quantum states, especially to superposition and quantum entanglement.

2.1 Quantum states

State of a physical system at a given time is basically all information that identifies the particular state the system is in. For quantum mechanical systems the classical phase space is not suitable for describing any state of the system. There is a more complicated mathematical structure for representing the states of quantum mechanical systems. This has to be so, because new concepts not

met in classical systems, such as superposition, arise in quantum mechanics and mathematical apparatus should be appropriate to handle these.

It appears that, any state of a quantum mechanical system can be mathematically represented as a ray in a Hilbert space.

A Hilbert space is a vector space over the field of complex numbers $\mathbb{C}$, with vectors denoted by $|\psi\rangle$ (Dirac's ket notation). A ket $|\psi\rangle$ is represented as a $n \times 1$ matrix (or a n element vector), where n is the dimension of the Hilbert space, and its corresponding bra $\langle\psi|$ is the transpose conjugate of the ket. It has an inner product $\langle\psi|\varphi\rangle$ (may be seen as matrix multiplication) that maps an ordered pair of vectors to $\mathbb{C}$, with the properties:

- Positivity: $\langle\psi|\psi\rangle > 0$ for $|\psi\rangle \neq 0$
- Linearity: $\langle\varphi|(a|\psi_1\rangle + b|\psi_2\rangle) = a\langle\varphi|\psi_1\rangle + b\langle\varphi|\psi_2\rangle$
- Skew symmetry: $\langle\varphi|\psi\rangle = \langle\psi|\varphi\rangle^*$

A ray in a Hilbert space is an equivalent class of vectors that differ by multiplication by a nonzero complex scalar. That is, a ray is represented by a given vector and all its (complex) multiples. Superposition and quantum entanglement will be formalized in Hilbert spaces in the next sections.

2.1.1 Superposition

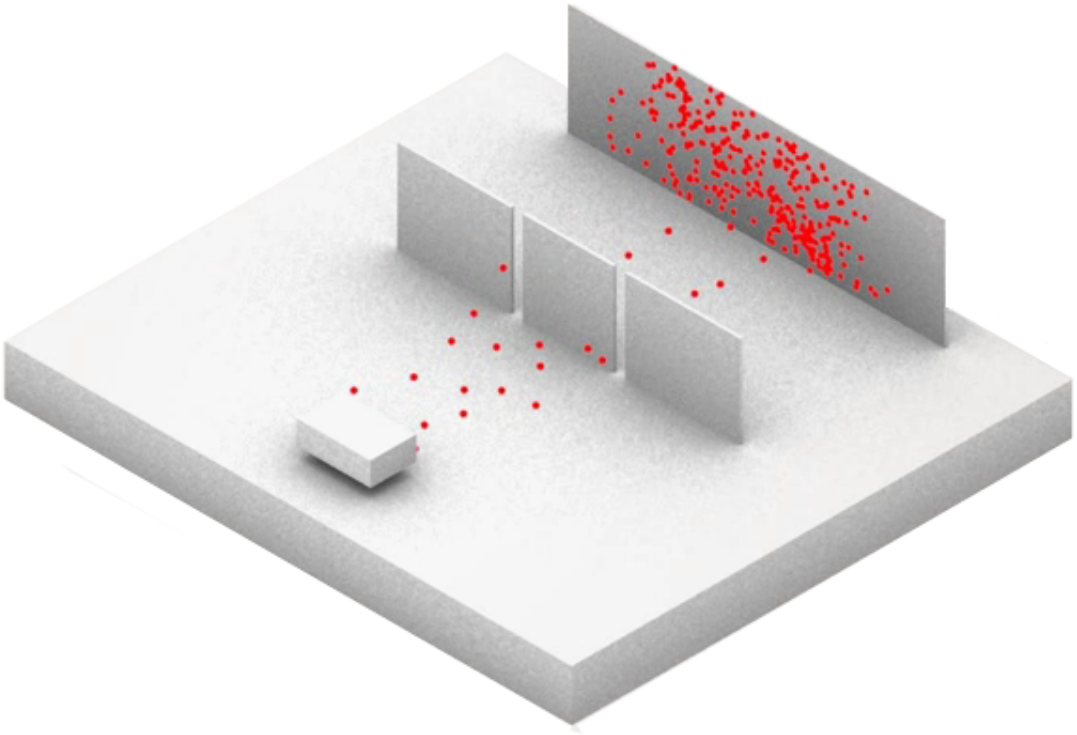
Quantum superposition is a fundamental principle of quantum mechanics that holds that a physical system, such as an electron, exists partly in all its particular theoretically possible states (or, configuration of its properties) simultaneously, but when measured or observed, it gives a result corresponding to only one of the possible configurations.

Mathematically, it refers to a property of solutions to the Schrödinger equation. Since the Schrödinger equation is linear, any linear combination of solutions to a particular equation will also be a solution of it.

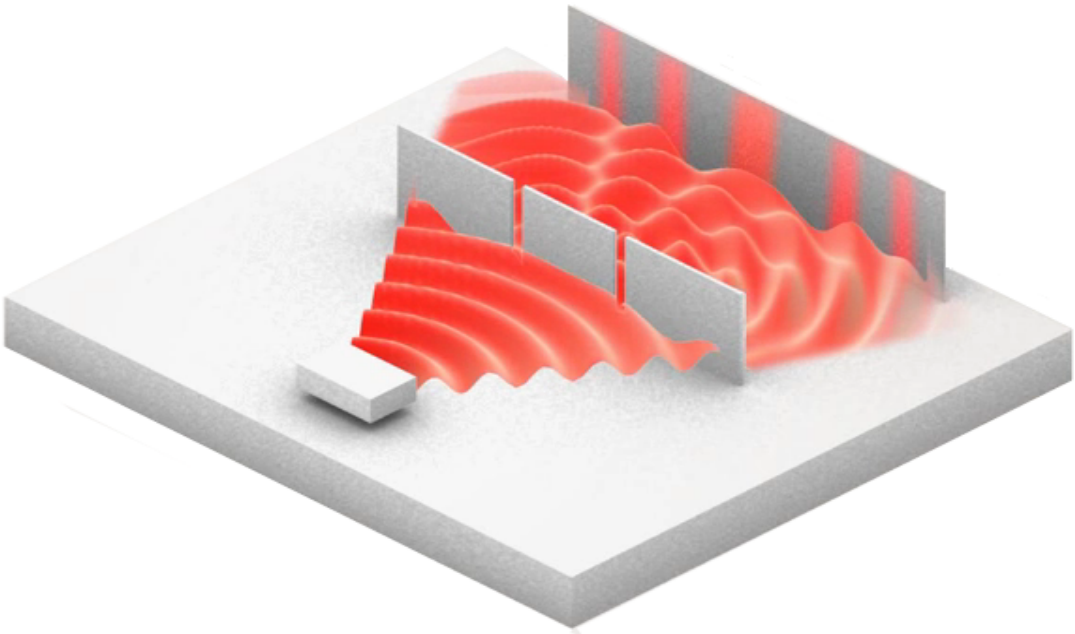
An example of a directly observable effect of superposition is interference peaks from an electron wave in a double-slit experiment.

In the double-slit experiment a beam of electrons one at a time is directed through two narrow, closely spaced slits. Behind them there is a screen which can detect where the electrons that made it through the slits end up.

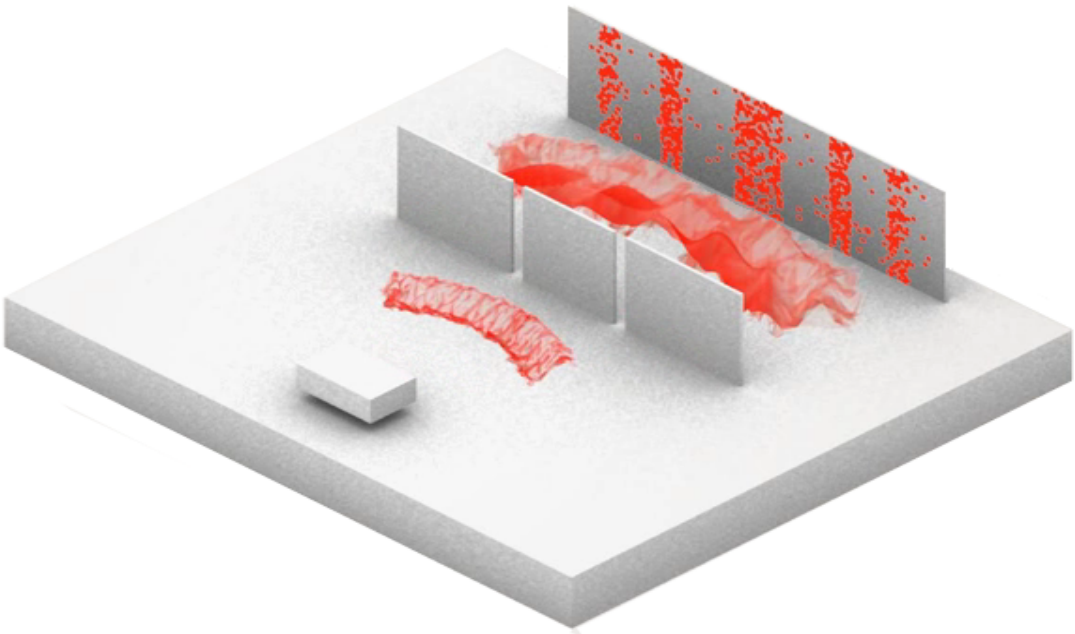
1. Single objects (not electrons) are sent on two slits. Objects touch the screen randomly.



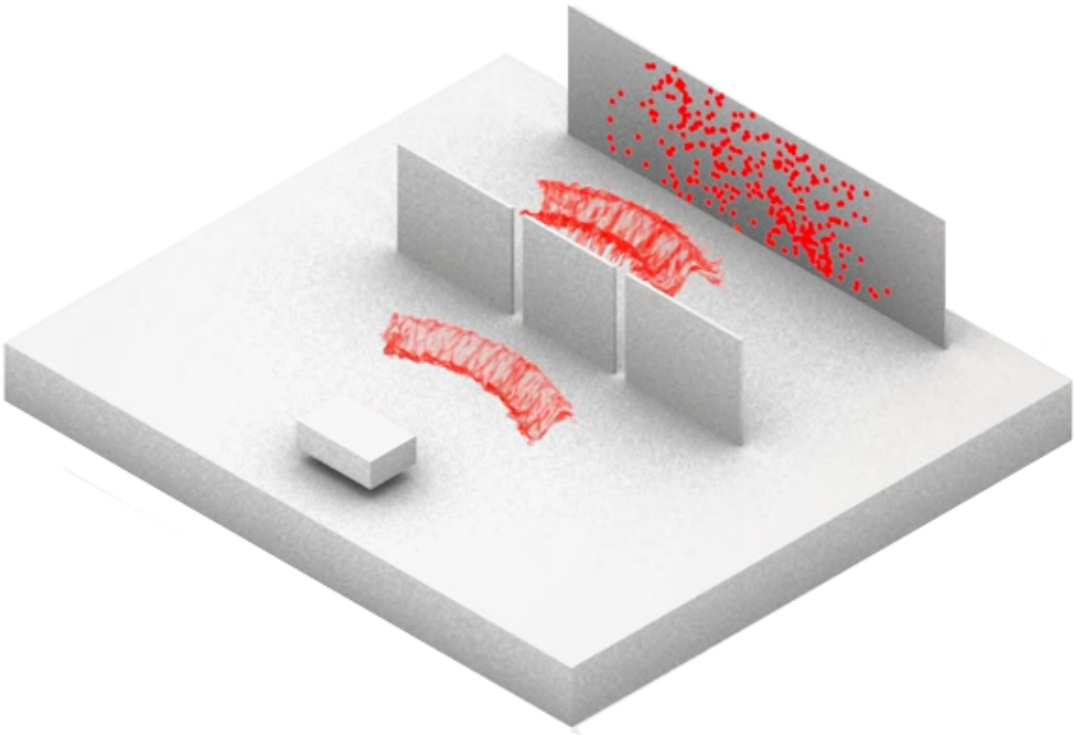
2. A wave is sent on two slits which make it interfere. This results in fringes on the screen.



3. A quantum object - electron is sent on two slits. The wave suddenly reduces into a particle when touching the screen, and more likely at the positions where the wave was more intense. At the end, one observes impacts as for particles, and interference fringes as for waves.



4. If an observer measures through which slit the wave goes, then the wave reduces and goes only through one of the two slits now. No interference can occur anymore, so no fringes appear on the screen. The observer has modified the experiment.



Thus it has been demonstrated that all matter possesses both particle and wave characteristics. Even if the source intensity is turned down so that only one particle (electron) is passing through the apparatus at a time, the same interference pattern develops over time. The quantum particle acts as a wave when passing through the double slits, but as a particle when it is detected. This is a typical feature of quantum complementarity: a quantum particle will act as a wave when we do an experiment to measure its wave-like properties, and like a particle when we do an experiment to measure its particle-like properties.

Directly observable effect of superposition is also a quantum logical qubit state. A qubit can be interpreted as the spin state of an electron. Electron spin can be viewed as a unit three-dimensional vector associated with the particle, representing an axis of rotation. Arrowhead is labeled as N (North) to highlight the fact that spin can also be seen as a magnetic property.

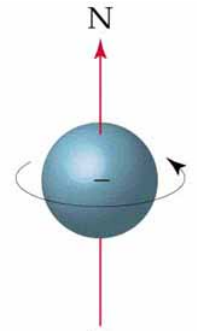


Figure 2.1: Spin of the electron

We fix an electron's position in space. In order to prepare an electron in a particular direction, the electron is surrounded in a powerful magnetic field.

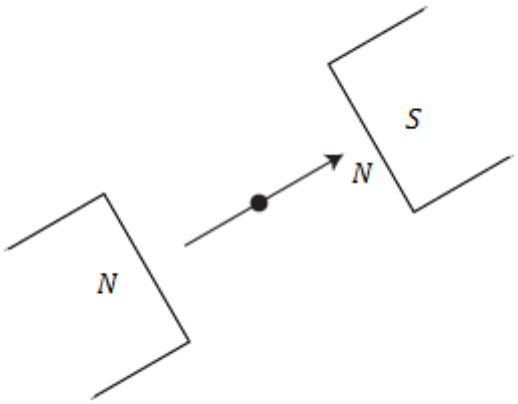


Figure 2.2: Preparation of the electron in a particular direction

The magnetic field forces the electron's spin to end up in the desired direction after a certain amount of time. In fact the spin vector precesses around the desired position, radiating energy and spiralling in. The stronger the field, the quicker this all happens.

Suppose that an electron has been prepared in some unknown direction and we want to be able to measure, or detect the electron's spin. We could again surround the electron with a known magnetic field.

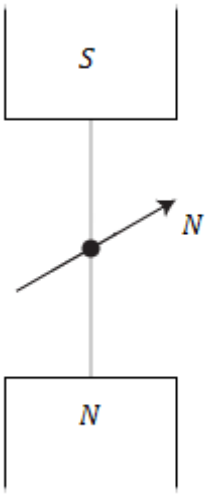


Figure 2.3: Detection of the direction of the electron

What actually happens is that, whatever angle the electron is initially prepared at, when we come to apply the magnetic field only one of two things happen:

- No photon is emitted by the electron.
- Exactly one photon is emitted.

If a photon is emitted, then its associated frequency corresponds to the amount of energy that would be radiated if the electron had been prepared in the North - down position.

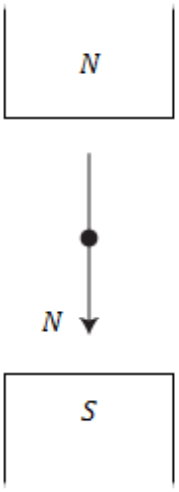


Figure 2.4: Result of the detection of the electron's direction

Note that the actual result - that is, one photon emitted or no photon emitted - doesn't depend on either the prepared angle or the detection angle. In fact, the outcomes of any experiment are probabilistic. This probability depends on the angle. Qualitively, the smaller the angle (between prepared and detection states) the less likely that a photon is emitted. So, information about the prepared angle can be statistically recovered from repeated experiments, but to re-iterate, only one of two outcomes can occur per detection.

The state of the electron can be represented as spin up $|\uparrow\rangle$ and spin down $|\downarrow\rangle$ or equivalently $|0\rangle$ and $|1\rangle$ in Dirac's ket notation.

$$|0\rangle \rightarrow \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$|1\rangle \rightarrow \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

This forms an orthonormal basis for 2-d Hilbert space $\{|0\rangle, |1\rangle\}$. Then the qubit can be represented as a ray in this space. A qubit state is a linear superposition of the basis states [6].

Definition 1 (Qubit). *The qubit is a linear combination of basis states $|0\rangle$ and $|1\rangle$:*

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where α and β are probability amplitudes and $\alpha, \beta \in \mathbb{C}$, $\mathbb{C}$ - set of complex numbers.

When we measure this qubit in the standard basis, the probability of outcome $|0\rangle$ is $|\alpha|^2$ and the probability of outcome $|1\rangle$ is $|\beta|^2$. Because the absolute squares of the amplitudes equate to probabilities, it follows that α and β must be constrained by the equation:

$$|\alpha|^2 + |\beta|^2 = 1$$

Simply because this ensures you must measure either one state or the other, the total probability of all possible outcomes must be 1.

Example of a qubit:

$$|\psi\rangle = \frac{3}{5}i|0\rangle + \frac{4}{5}|1\rangle$$

This qubit state encodes that the particle is in the state where it is an amount $3i/5$ in up and an amount $4/5$ in down. The probability for up is $|3i/5|^2 = 9/25$, the probability for down is $|4/5|^2 = 16/25$. Total probability is $9/25 + 16/25 = 1$.

2.1.2 Quantum entanglement

Quantum entanglement is a special connection between pairs or groups of quantum systems, or any objects described by quantum mechanics. An entangled system has a quantum state which cannot be factored out into the product of states of its local constituents - individual particles. The system cannot be expressed as a direct product of quantum states that make up the system. If entangled, one constituent cannot be fully described without considering the other(s). Like the quantum states of individual particles, the state of an entangled system is expressible as a sum, or superposition, of basis states, which are eigenstates of some observable(s).

Consider two noninteracting systems A and B, with respective Hilbert spaces H_A and H_B. The Hilbert space of the composite system is the tensor product:

$$H_A \otimes H_B$$

If the first system is in state $|\psi\rangle_A$ and the second in state $|\varphi\rangle_B$, then the state of the composite system is:

$$|\psi\rangle_A \otimes |\varphi\rangle_B$$

States of the composite system which can be represented in this form are called separable states, or product states.

Not all states are separable states. Fix a basis $\{|i\rangle_A\}$ for H_A and a basis $\{|j\rangle_B\}$ for H_B. The most general state in $H_A \otimes H_B$ is of the form:

$$|\psi\rangle_{AB} = \sum_{i,j} c_{ij}|i\rangle_A \otimes |j\rangle_B$$

This state is separable if there exist c_i^A, c_j^B so that $c_{ij} = c_i^A c_j^B$, yielding $|\psi\rangle_A = \sum_i c_i^A |i\rangle_A$ and $|\varphi\rangle_B = \sum_j c_j^B |j\rangle_B$. It is inseparable if for all c_i^A, c_j^B we have $c_{ij} \neq c_i^A c_j^B$. If a state is inseparable, it is called an entangled state.

For example, given two basis vectors $\{|0\rangle_A, |1\rangle_A\}$ of H_A and two basis vectors $\{|0\rangle_B, |1\rangle_B\}$ of H_B, the following is an entangled state:

$$\frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B)$$

If the composite system is in this state, it is impossible to attribute to either system A or system B a definite pure state. The above example is one of four Bell states, which are entangled pure states of the $H_A \otimes H_B$ space, but which cannot be separated into pure states of each H_A and H_B.

Suppose Alice is an observer for system A, and Bob is an observer for system B. If in the entangled state given above Alice makes a measurement in the $\{|0\rangle, |1\rangle\}$ eigenbasis of A, there are two possible outcomes, occurring with equal probability [32]:

- Alice measures 0, and the state of the system collapses to $|0\rangle_A |1\rangle_B$. Entanglement is broken when the entangled particles decohere through interaction with the environment, for example, when a measurement is made [33].

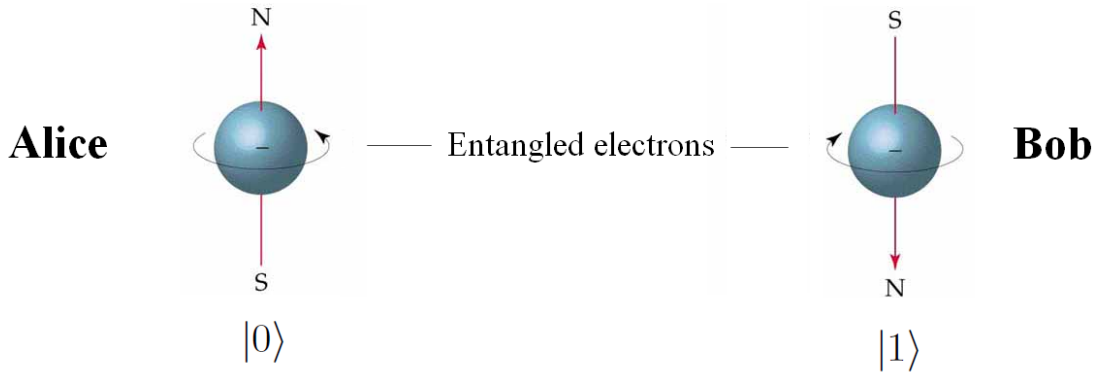


Figure 2.5: Possible outcome (1) of the measurement

Any subsequent measurement performed by Bob, in the same basis, will always return 1.

- Alice measures 1, and the state of the system collapses to $|1\rangle_A|0\rangle_B$.

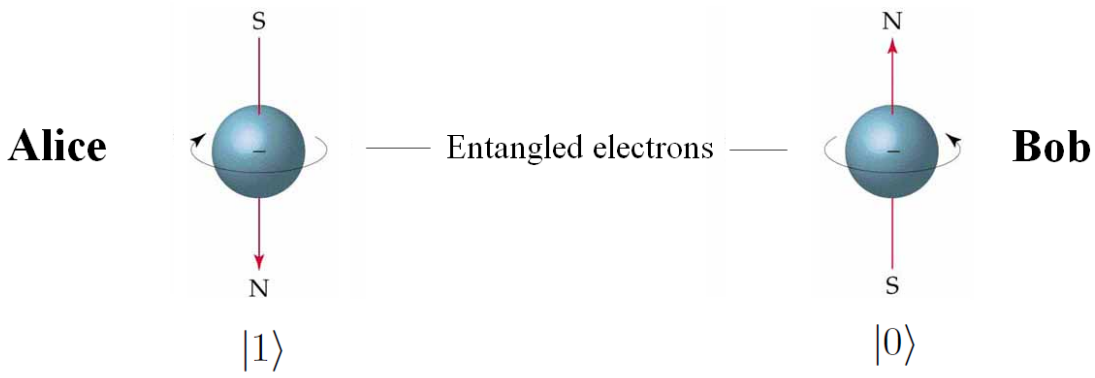


Figure 2.6: Possible outcome (2) of the measurement

If Alice measures 1, then Bob's measurement will return 0 with certainty. Thus, system B has been altered by Alice performing a local measurement on system A. This remains true even if the systems A and B are spatially separated.

Quantum entanglement is one of the central principles of quantum mechanics. It is used in the emerging technologies of quantum computing, communication, quantum cryptography and quantum teleportation.

Chapter 3

Logic and Quantum mechanics

J. von Neumann is known as the father of quantum logic. It is only a very short paragraph in chapter 3 of his book Grundlagen der Quantenmechanik [49] that forms the birth of quantum logic. In this passage, von Neumann introduced the idea of a logical calculus of physical properties. He argued that it is the relation between these properties on the one hand and the projection operators definable on a Hilbert space on the other hand that should make it possible to obtain some sort of logical calculus.

The developments of quantum logic went in two main directions [41]. The first is the original quantum logic project. In 1936 von Neumann co-authored a paper with G. Birkhoff [8]. Further developments were done by K. Husimi [24] and other authors. However some important impossibility results were obtained [2, 40]. D. Aerts, C. Randall and D. Foulis showed that orthomodular lattice approach rises problems when trying to describe compound systems consisting of subsystems that can exhibit quantum entanglement. Also they showed that tensor products of quantum logic do not exist.

The second direction is the Mackey-Piron way. This way was originated by G. Mackey in [26, 27]. G. Mackey searched for a list of transparant and physically plausible axioms or assumptions from which the Hilbert space model could ideally be deduced. The programme of Mackey was later further developed and extended by C. Piron in his PhD thesis in 1964 [35] and subsequent work [36].

Rather than taking the Hilbert space model of quantum physics for granted, Piron's aim was to "justify the use of Hilbert space". And that is exactly what Piron's celebrated representation theorem gives: an axiomatic system that can be represented as the logic of projection operators on a generalized Hilbert space. Piron's theorem was later improved by M. Solèr and R. Mayet [28, 42]. One of the lines of research in this direction is the development of modal quantum logics as quantum communication environments and logic of correlated knowledge, which we'll discuss later.

More about approaches on logic and quantum mechanics you can find in [1, 3, 7, 10, 13, 34, 38, 39, 43].

3.1 Quantum logic

Quantum logic can be formulated either as a modified version of propositional logic or as a noncommutative and non-associative many-valued logic [12, 16, 17].

Syntax of quantum logic is exactly the same as classical logic, except there is no implication operator defined.

Definition 2 (Syntax of quantum logic). *The language of quantum logic has the following syntax:*

$$F := a \mid \neg F \mid F \vee F \mid F \wedge F$$

where a is any atomic proposition.

The main difference between classical and quantum logic is the meaning. The interpretation of an elementary formula a is given by a closed linear subspace of Hilbert space H. Conjunction $\left[a \wedge b\right]$ is defined as instersection between subspaces $\left[a\right] \cap \left[b\right]$, negation $\left[\neg a\right]$ as $\left[a\right]^{\perp}$ and disjunction $\left[a \vee b\right]$ as $\left[a\right] \oplus \left[b\right]$.

Definition 3 (Semantics of quantum logic). *Semantics of quantum logic:*

- $\left[a\right]$ = *the subspace corresponding to proposion* a.
  P_a = *the projector onto* $\left[a\right]$.

- $\big[\neg a\big] = \big[a\big]^{\perp} = \Big\{|\psi\rangle \in H \;\big|\; \forall\, |\varphi\rangle \in \big[a\big]\;\; \langle\varphi|\psi\rangle = 0\Big\}$
  $P_{\neg a} = I - P_a$
- $\big[a \wedge b\big] = \big[a\big] \cap \big[b\big] = \Big\{|\psi\rangle \in H \;\big|\; |\psi\rangle \in \big[a\big],\; |\psi\rangle \in \big[b\big]\Big\}$
  $P_{a\wedge b} = \lim_{n\to\infty}(P_a P_b)^n$
- $\big[a \vee b\big] = \big[a\big] \oplus \big[b\big] = \Big\{|\psi\rangle \in H \big| \exists |\varphi\rangle \in \big[a\big], \exists |\eta\rangle \in \big[b\big]\; s.t. \, |\psi\rangle = \alpha|\varphi\rangle + \beta|\eta\rangle\Big\}$
  $P_{a\vee b} = I - \lim_{n\to\infty}((I - P_a)(I - P_b))^n$

Subspaces of Hilbert space form a lattice with partial order $\big[a\big] \leq \big[b\big]$ iff $P_a P_b = P_a$. To define the lattice, let us first explain a poset. A partially ordered set (or poset) is a set $PropS$ with partial order relation $\leq$ satisfying $\forall a, b, c \in PropS$:

- $a \leq a$.
- $a \leq b$ and $b \leq a$ iff $a = b$.
- if $a \leq b$ and $b \leq c$ then $a \leq c$.

Two elements $a, b \in PropS$ have a join or least upper bound if there is an element $a \vee b$ satisfying:

- $a \leq a \vee b$ and $b \leq a \vee b$.
- Any c satisfying $a \leq c$ and $b \leq c$ also satisfies $a \vee b \leq c$.

Two elements $a, b \in PropS$ have a meet or greater lower bound if there is an element $a \wedge b$ satisfying:

- $a \wedge b \leq a$ and $a \wedge b \leq b$.
- Any c satisfying $c \leq a$ and $c \leq b$ also satisfies $c \leq a \wedge b$.

Example 1. *Example of posets:*

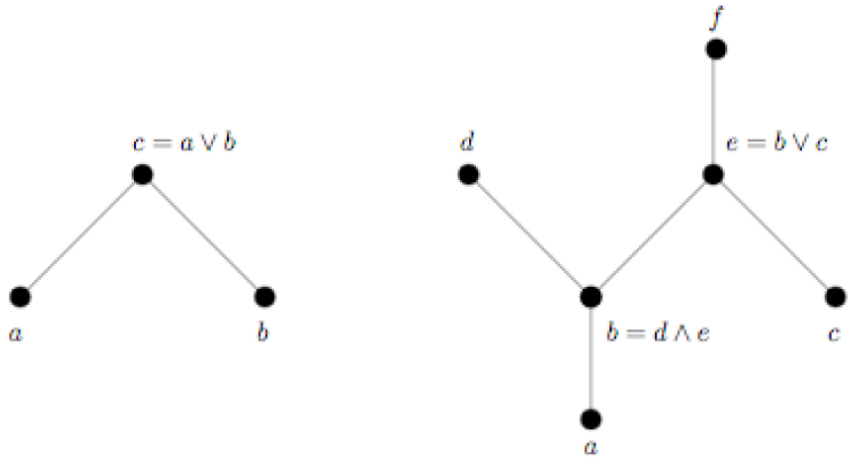


Figure 3.1: Posets

Definition 4 (Lattice). *A lattice is a poset where every pair of elements has a meet or a join.*

We will also require that there is a greatest element 1 and a least element 0. Atoms of a lattice are those elements for which 0 is the only smaller element.

Example 2. *Example of lattices:*

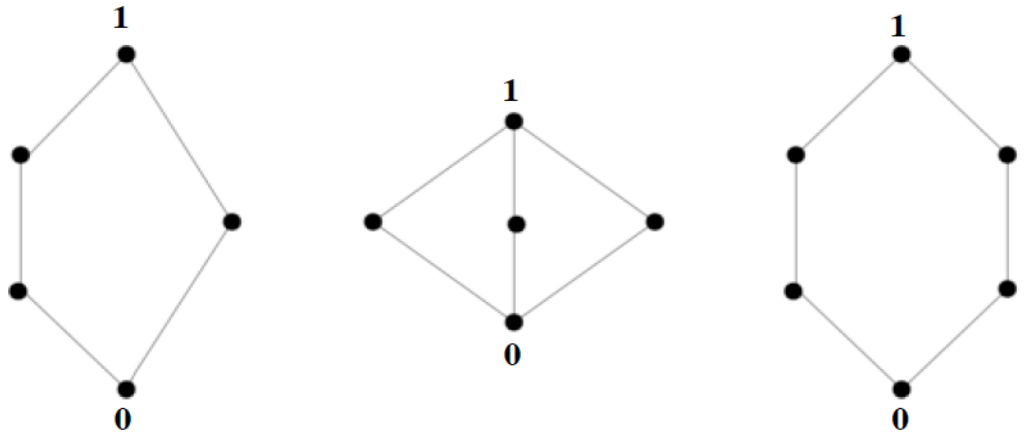


Figure 3.2: Lattices

Example 3. *Example of 2D Hilbert space:*

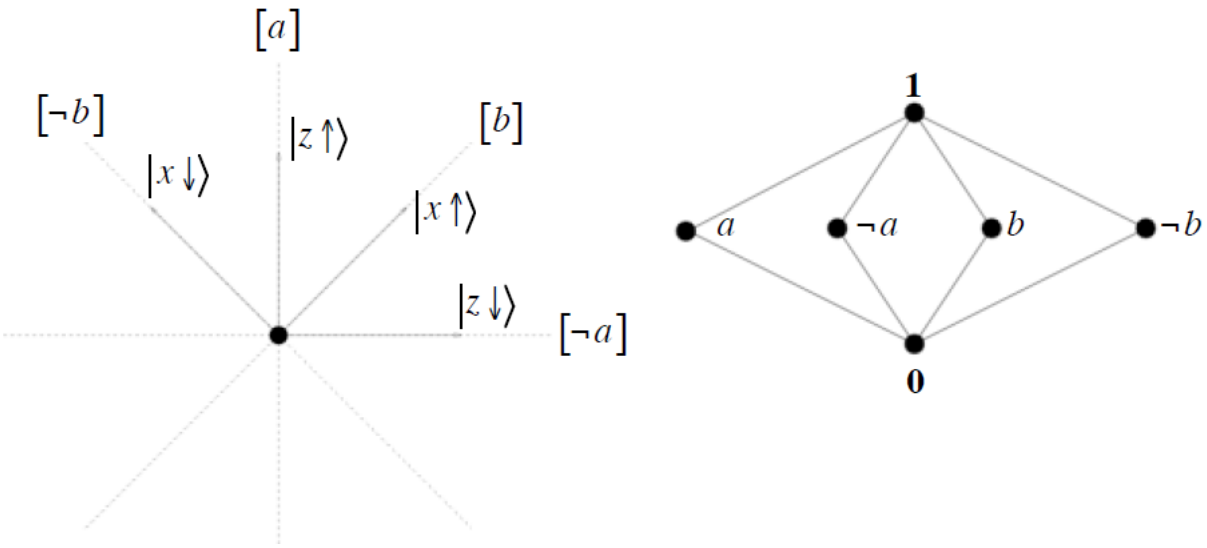


Figure 3.3: 2D Hilbert space

a = "The particle has spin up in the z-direction."
b = "The particle has spin up in the x-direction."

Orthomodular lattice approach is successful in describing single quantum systems, but it faces problems when trying to describe compound systems consisting of subsystems that can exhibit quantum entanglement. In quantum mechanics, such compound systems are represented via a tensor product of the underlying Hilbert spaces for each subsystem. Hence it would have been natural to find a general lattice-theoretic analogue of the tensor product as an operation on lattices that satisfies a given set of natural conditions. However, impossibility results in [2, 40] show that such an operation on orthomodular lattices (or posets) cannot exist.

Also quantum logic has no implication operator and so deductive system. The reason for it is the failure of the distributive law [8, 24]. Distributive law:

- $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

To illustrate why the distributive law fails, consider a particle moving on a line and let:

- a = "the particle has momentum in the interval [0, +1/6]"
- b = "the particle is in the interval [-1, 1]"
- c = "the particle is in the interval [1, 3]"

We might observe that:

- $a \wedge (b \vee c) = true$

In other words, that the particle's momentum is between 0 and $+1/6$, and its position is between -1 and $+3$. On the other hand, the propositions $a \wedge b$ and $a \wedge c$ are both false, since they assert tighter restrictions on simultaneous values of position and momentum than is allowed by the uncertainty principle in quantum mechanics. So:

- $(a \wedge b) \vee (a \wedge c) = false$

Thus the distributive law fails. Also it can be shown by lattice.

Example 4. *The failure of the distributive law:*

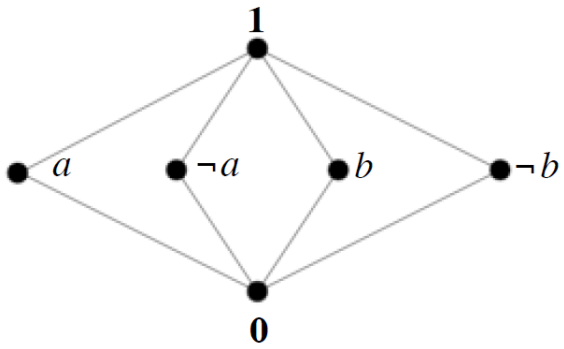


Figure 3.4: Failure of the distributive law

$a \wedge (b \vee \neg b) = a \wedge 1 = a$
$(a \wedge b) \vee (a \wedge \neg b) = 0 \vee 0 = 0$

Concluding the remarks on quantum logic, we may notice, that it is successful in describing single quantum systems, but it faces problems when trying to

describe compound systems consisting of subsystems that can exhibit quantum entanglement. Also it has no implication operator and deductive system, because of the failure of the distributive law.

3.2 Quantum communication environments

Anderson de Araújo and Marcelo Finger defined quantum communication environments in terms of the concepts of agents and informational states in [4]. The communication among agents is modeled, assuming that for each agent g in a group G there is a codification cod of the propositions of g as sequences of bits.

Definition 5 (Message). *Let $G = \{g_1, ..., g_n\}$ be a group of agents. The message assignment is the function $msg : \{1, 2, ..., n\} \to cod_i$, where $cod_i : g_i \to \{0, 1\}^m$ is a function which associates a code of length m to each proposition of agent g_i (this code is a sequence of bits with length m). Each $msg(i)$ will be called a message, and we will write M_G to denote the set of all messages of G.*

Messages of agent has a corresponding Hilbert space, that represents messages as physical entities [11, 32].

Definition 6 (Hilbert space of messages). *Let $G = \{g_1, ..., g_n\}$ be a group of agents. The set of possible messages H_G of G is the complex Hilbert space generated by M_G, i.e., H_G is a set of normalized vectors $| \ \rangle : M_G \to \mathbb{C}$, equipped with the inner product, such that $\Sigma_{m \in M_G} ||m\rangle|^2 < \infty$.*

In a quantum passing message system, each message is thought of as being in the possession of some agent, but this agent may change from time to time, as an agent can send some of its message to another. Following [46], a function is defined to denote the location of each message.

Definition 7 (Location). *Let H_G be the Hilbert space of the group of agents $G = \{g_1, ..., g_n\}$. The m-location assignment is the function $loc : H_G \to \{1, 2, ..., n\}$ such that $loc(msg(i))$ denotes that agent g_i has the message $msg(i)$ of H_G.*

Note that the letter m in the expression "m-location assignment" is to remember that the codes are sequences of qubits with length m. These sequences of qubits represent in quantum terms the previous codes of the messagens in M_G. The reliable synchronous communication of quantum messages among the agents can be modeled as the transmission of quantum messages from one agent to another agent in a group.

Definition 8 (Channel). *Let H_G be the Hilbert space of the group of agents $G = \{g_1, ..., g_n\}$. The channel assignment is the function $chan : \{1, 2, ..., n\}^2 \to H_G$ such that $chan(i, j) = |msg\rangle$ means that the quantum message $|msg\rangle$ has been transmitted from agent g_i to agent g_j.*

Suppose that $loc^{-1}(i) = \{i_l, ..., i_k\}$ is the set of indices of the quantum messages located at agent i. Then agent i is able to perform a general measurement on these k messages. We represent a quantum operation on k messages by a finite sequence of operators $M = (M_1, ..., M_l)$ with each M_j operating on H_G. Suppose the agents simultaneously perform the quantum measurements $(M_1, ..., M_l)$ where each M_i is a measurement on the $k_i = |loc^{-1}(i)|$ quantum message located at agent i. Each operation M_i products some outcome m_i, the index of some linear transformation M_j operating on H_G. A combined outcome of these measurements is represented by a new function from agents to outcomes.

Definition 9 (Measurement). *Let H_G be the set of possible messages of a group of agents $G = \{g_1, ..., g_n\}$ and $M = (M_1, ..., M_l)$ be a finite sequence of operators on H_G. The measurement assignment is the function $res : G \to M \times \mathbb{R}$ such that $res(i) = (M_i, m_i)$ records the measurement performed and the outcome obtained by the agent i.*

Each measurement M_i is a self-adjoint linear operator and the outcome of a measurement is a real number. So the measurement assignment res is well-defined. Having functions $msg, loc, chan, res$, quantum communication environments can be defined.

Definition 10 (Quantum communication environment). *A quantum communication environment is a tuple $E = (G, S)$, where G is a group of agents and $S = \{s_1, ..., s_m\}$ is the set of informational states for $s_j = (msg, loc, chan, res)$.*

3.2.1 Quantum communication language

A quantum communication language is specified by defining its alphabet, terms and formulas.

Definition 11 (Quantum communication language). *Let $E = (G, S)$ be a quantum communication environment. The language of E is the multimodal first-order language with equality L such that:*

1. *The alphabet of L has two sorts of variables, one sort for scalars and other for vectors, as well as an infinite set of basis variables $\{\vec{v}, \vec{w}, ...\}$ to represent the basis set considered for H_G;*
2. *For each of these basis variables $\vec{v}$, the alphabet of L also has a finite set of constant vectors $\vec{v_0}, ..., \vec{v_m}$ representing the vectors in the basis of H_G;*
3. *The alphabet of L has the scalar constants 0 and 1 and the vector constants $\vec{0}$ and $\vec{1}$;*
4. *The alphabet of L has the functions symbols $-, +$ and $\times$ for the usual operations on elements in a real-closed field, the function symbols $\neg_v, +_v, \times_s$ and $\times_v$ for the orthocomplement, matrix addition, multiplication by a scalar and matrix multiplication on vector spaces;*
5. *The alphabet of L has a unary probability operator P and a binary basis transformation M_{ij};*
6. *The alphabet of L has knowledge operators K_I, one for each subgroup of agents $I \subseteq G$;*
7. *Nothing more except the symbols specified above are in the alphabet of L.*

The definitions of all syntactic notions are as in [9], including the terms and formulas, except by the following differences.

Definition 12 (Set of terms). *The set of terms of L is such that:*

1. *The matrix terms of L are defined in the following way:*
   (a) *The constant vectors and variables for constant vectors are matrix terms;*
   (b) *If α and β are matrix terms and a is an scalar constant, then $\neg_v\alpha, a \times_s \alpha, \alpha +_v \beta$ and $\alpha \times_v \beta$ also are terms.*
2. *If α is a matrix term, then $P(\alpha)$ is a term of L. These terms are called probability terms.*
3. *If $\vec{v}$ and $\vec{w}$ are basis variables, then $M_{ij}(\vec{v}, \vec{w})$ is a term of L. These terms are called transformation terms.*
4. *The matrix, probability and transformation terms are just the terms of L defined by the conditions (1), (2) and (3) above.*

Moreover, the scalar terms are just the terms defined in L from 0 and 1 using $-, +$ or $\times$ as well as any pseudo-term defined using these scalar constants and funtions.

In quantum mechanics probability has a crucial role. Hence it is important to designate some special formulas that express facts about probabilities in quantum communication environments.

Definition 13 (Linear probability atom). *In the set of formulas of L a linear probability atom is an expression of the form $a_1 \times P^1(\alpha_1) + \cdots + a_k \times P^1(\alpha_k) = a$, where each a_i is a scalar term as well as a, and each α_i is a matrix term.*

As the language L has knowledge operators K_I for subgroups of agents, it can state facts about distributed knowledge in communication environments, such as in [5]. In particular, the description of the knowledge of an individual agent i is described by K_i. Besides, L has probability and transformation operators similar to [47], and so it can also state properties about quantum distributed knowledge. Concepts like entanglement of information, phase relations, uncertainty relation, etc, also can be expressed in L. This shows that the language L has enough expressiveness with respect to quantum communication environments. For instance, the statement that agent i knows the message α with probability $\frac{1}{\sqrt{2}}$ can be expressed by the sentence $K_iP(\alpha) = \frac{1}{\sqrt{2}}$ of the language L.

3.2.2 Quantum communication structures

Quantum communication environments are distributed systems, so the language L needs such semantics that it permits to consider the transmission of quantum messages among the agents. For such an aim, the notion of informational range is defined.

Definition 14 (Informational range). *Let $E = (G, S)$ be a communication environment. The informational range R_G of the group G is a family of binary relations $\approx_I$ on H_G, one for each $I \subseteq G$:*

$$R_G = \{\approx_I \subseteq H_G : I \subseteq G\}.$$

Intuitively, an informational range shows how the information is available among the subgroups of agents. From this concept, equivalence relations among the information associated to the messages of agents can be defined.

Definition 15 (E-quantum communication frame). *Let $E = (G, S)$ be a communication environment and R_G be the informational range of G. An E-quantum communication frame is a multi-modal frame (H_G, R_G) such that:*

1. *Equivalence: For each $I \subseteq G, \approx_I$ is an equivalence relation;*
2. *Observability: For all $s, r \in H_G$ and $I \subseteq G$, if $s = r$ then $s \approx_I r$;*
3. *Monotonicity: For all $I, J \subseteq G$, if $I \subseteq J$ then $\approx_J \subseteq \approx_I$;*
4. *Vacuousness: For all $s, r \in H_G, s \approx_\emptyset r$.*

A quantum communication structure can be defined in such a way:

Definition 16 (Quantum communication structure). *Let $E = (G, S)$ be a communication environment and (H_G, R_G) be an E-quantum communication frame. A quantum communication structure A for the language L is the tuple $A = (H_G, R_G, I_G)$ in which I_G is an interpretation function from L to H_G such that:*

1. *$I_G(0)$ is the number zero and $I_G(1)$ is the number one in the complex field $\mathbb{C}$ of H_G;*
2. *$I_G(\vec{0})$ is the null matrix and $I_G(\vec{1})$ is the identity matrix of H_G;*

3. *For each state constant $\vec{v_i}$ of L, $I_G(\vec{v_i})$ is the matrix $|v_i\rangle\langle v_i|$ where $|v_i\rangle$ is the i-th vector of the computational basis of H_G;*
4. *$I_G(-), I_G(+)$ and $I_G(\times)$ are the functions inverse, plus and times, respectively, on the complex field $\mathbb{C}$ of H_G;*
5. *$I_G(\neg_b)$ is the projection operator $\perp$ projecting onto the orthogonal complement of the image of H_G under the state considered, $I_G(+_v)$ is the matrix addition of H_G, $I_G(\times_s)$ is matrix multiplication by a scalar and $I_G(\times_v)$ is the matrix multiplication of H_G;*
6. *$I_G(P)$ is the unary operator on H_G such that $I_G(P)(|v_i\rangle)$ is the trace of the matrix $|v_i\rangle\langle v_i||v_i\rangle\langle v_i|$, i.e., $I_A(P)(|v_i\rangle) := Tr(|v_i\rangle\langle v_i||v_i\rangle\langle v_i|) := \sum_j(|v_i\rangle\langle v_i||v_i\rangle\langle v_i|)_{jj} = |\langle v_i|v_i\rangle|^2$;*
7. *$I_G(M_{i,j})$ is the binary operator on H_G such that $I_G(M_{i,j})(|v\rangle, |w\rangle)$ is the element v_{ij} such that $M = (v_{ij})$ is the $m \times m$ unitary complex matrix for which $M|v\rangle = |w\rangle$.*

From the notion of quantum communication structure, satisfatibility relation $\models_s$ is defined as in [9]. For modal formulas it is defined as:

$$A \models_s K_I\varphi \text{ if, and only if, for all } r \in H_G \text{ such that } r \approx_I s, A \models_r \varphi.$$

3.2.3 Quantum communication axiomatics

In this section a theory $\mathcal{T}$ for quantum communication environments will be defined. It is presupposed that a derivability relation $\vdash$ is defined according to some classical calculus for first-order logic, for instance the one in [9], and only additional axioms and rules of $\mathcal{T}$ will be specified.

The axiomatization of $\mathcal{T}$ consists of four parts, each dealing with one aspect of communication systems. The first part of $\mathcal{T}$ has axioms to express that the set of possible messages is an m-dimensional Hilbert space, where m is the maximum length of the messages in M_G, and that the Hilbert space is a orthocomplemented lattice.

A1. $(\vec{v_1} \vee \cdots \vee \vec{v_n}) \wedge (\neg i = j \rightarrow \neg(\vec{v_i} \wedge \vec{v_j}))$

A2. $(\alpha \times_v \neg_v \alpha = \vec{0}) \wedge (\alpha +_v \neg_v \alpha = \vec{1}) \wedge (\neg_v \neg_v \alpha = \alpha)$

A3. $(\alpha \leq \beta \rightarrow \neg_v \beta \leq \neg_v \alpha) \wedge (\alpha \times_v (\neg_v \alpha +_v (\alpha \times_v \beta)) \leq \beta)$

The second part of $\mathcal{T}$ has axioms to state the properties of the quantum probability operator for quantum communication environments.

A4. $0 \leq P(\alpha) \wedge P(\alpha) \leq 1$

A5. $P(\alpha +_v \neg_v \beta) = 1$

A6. $P(\alpha \times_v \beta) + P(\alpha \times_v \neg_v \beta) = P(\alpha)$

A7. $\alpha = (a_1 \times_s \vec{v_1}) +_v \cdots +_v (a_n \times_s \vec{v_n}) \rightarrow (P(\beta) = |a_1|^2 + \cdots + |a_m|^2 \wedge \beta = (\sqrt{P(\beta)})^{-1} \times ((a_1 \times_s \vec{v_1}) +_v \cdots +_v (a_m \times_s \vec{v_m})))$ if the measurement was done on the vectors in $\{\vec{v_i}\}_{i \leq n}$.

The axioms explicitly formalize the main property of measurements in quantum mechanics. Besides, in this approach the distributivity of probability is the sentence $\alpha = \beta \rightarrow P(\alpha) = P(\beta)$, which is an immediate theorem due to the Leibniz's law for equality.

The third part of $\mathcal{T}$ has axioms for basis transformation, which corresponds to the identity matrix when the basis is not changed and consecutive basis transformations correspond to matrix multiplication.

A8. $M_{ij}(\vec{v}, \vec{w}) = M^*_{ij}(\vec{w}, \vec{v})$

A9. $(i = j \rightarrow M_{ij}(\vec{v}, \vec{v}) = 1) \wedge (\neg i = j \rightarrow M_{ij}(\vec{v}, \vec{v}) = 0)$

A10. $M_{ij}(\vec{v}, \vec{x}) = (M_{i1}(\vec{v}, \vec{w}) \times M_{i1}(\vec{w}, \vec{x})) + \cdots + (M_{im}(\vec{v}, \vec{w}) \times M_{im}(\vec{w}, \vec{x}))$

The computational basis for the transformations have been fixed, which is in accordance with the fact that quantum measurements in other basis can be carried out by combining unitary transformation and measurements on the computational basis [11]. In this way, the transition probability operator T (a quantum analogue of conditional probabilities) can be defined stating that $T(\vec{v_i}, \vec{w_j}) = |M_{i,j}(\vec{v}, \vec{w})|^2$. Moreover, from axioms A8 and A10, it is possible to derive unitarity of the transformations $((M_{i1}(\vec{v}, \vec{w}) \times M^*_{j1}(\vec{v}, \vec{w})) + \cdots + (M_{im}(\vec{v}, \vec{w}) \times M^*_{jm}(\vec{v}, \vec{w}))) = 1$.

The fourth, and last, part of $\mathcal{T}$ has axioms for knowledge operators. These axioms are the usual axioms of the epistemic logic [5], but in the context of the

general framework for distributed knowledge developed in quantum communication environments.

A11. If $\mathcal{T} \vdash \varphi$ then $\mathcal{T} \vdash K_G\varphi$.
A12. If $I \subseteq J$ then $\mathcal{T} \vdash K_I\varphi \to K_J\varphi$.
A13. $K_G(\varphi \to \psi) \to (K_G\varphi \to K_G\psi)$
A14. $K_G\varphi \to K_G K_G\varphi$
A15. $\neg K_G\varphi \to K_G \neg K_G\varphi$

Definition 17 (Theory of quantum communication environment). *Let $E = (G, S)$ be a quantum communication environment. The theory of E is the first-order theory $\mathcal{T}$ with the axioms and rules A1-A15 defined above plus a complete axiomatization for algebraically closed fields.*

Quantum communication environments is sound and complete system, but the language is very expressive and decidability has not been proved. Also it uses Hilbert spaces, which may rise many problems as in Quantum logic.

3.3 Logic of distributed knowledge

Logic of distributed knowledge S5$_n$(ED) is an epistemic logic, which allows to reason about distributed systems. Distributed knowledge of A within a group of agents G means that A follows from what the members of G individually know. For instance, A is distributed knowledge in group G (denoted $D_G A$) consisting of three agents of which the first one knows B, the second one knows $B \to C$, and the third one knows $B \wedge C \to A$.

The language of S5$_n$(ED) contains:

- Symbols of atomic propositions: $p_1, p_2, p_3, q_1, q_2, q_3, ...$;
- Symbols of formulas: $A_1, A_2, A_3, B_1, B_2, ...$;
- Logical connectives: $\wedge, \vee, \neg, \to$;
- Set of agents N: $a_1, a_2, a_3, ..., a_n$;
- Operators: $E, D, K_1, K_2, ..., K_n$;

Formula $K_a A$ means "agent a knows A", formula EA expresses "everybody knows that A".

Definition 18 (Syntax of logic of distributed knowledge). *The language of logic of distributed knowledge has the following syntax:*

$$A := p \mid \neg A \mid A \vee A \mid A \wedge A \mid A \to A \mid K_a A \mid D_G A \mid EA$$

where p is any atomic proposition, $a \in N, G \subseteq N$.

W. van der Hoek and J.J. -Ch. Meyer defined Hilbert style calculus for logic S5$_n$(ED) in [45]:

- Any axiomatization for propositional logic.
- Axioms for knowledge:

  K1. $(K_a A \wedge K_a(A \to B)) \to K_a B$

  K2. $K_a A \to A$

  K3. $K_a A \to K_a K_a A$

  K4. $\neg K_a A \to K_a \neg K_a A$
- Axioms for knowledge of everybody:

  E1. $(K_1 A \wedge ... \wedge K_n A) \to \mathrm{E}A$

  E2. $\mathrm{E}A \to (K_1 A \wedge ... \wedge K_n A)$
- Axioms for distributed knowledge:

  D1. $K_a A \to \mathrm{D}A$

  D2. $(\mathrm{D}A \wedge \mathrm{D}(A \to B)) \to \mathrm{D}B$

  D3. $\mathrm{D}A \to A$

  D4. $\mathrm{D}A \to \mathrm{DD}A$

  D5. $\neg \mathrm{D}A \to \mathrm{D}\neg \mathrm{D}A$
- Rules:

$$\frac{A, A \to B}{B}\ (\mathrm{R1}) \qquad \frac{A}{K_a A}\ (\mathrm{R2}) \qquad \frac{A}{\mathrm{D}A}\ (\mathrm{R3})$$

Gentzen style and Kanger style sequent calculi for logic $S5_n$(ED) are defined in [18]. Also you may find more about distributed knowledge in the works done by R. Fagin, J.Y. Halpern, S. Negri, R. Pliuškevičius in [14, 22, 23, 37].

3.3.1 Distributed knowledge and quantum systems

Distributed knowledge is the information obtainable by pooling together and closing under logical inference the "knowledge" of each of the "parts" (agents). According to this view, the implicit knowledge of a group is the same as its distributed knowledge. In other words, the information carried by a complex system is nothing but the "sum" of the information carried by its parts.

While this standard answer is adequate for classical physics, it fails for quantum systems. An entangled system carries more information than the sum of its parts. For instance, in a Bell state $|00\rangle + |11\rangle$ (entangled quantum state) when the information stored in two subsystems is correlated according to the identity rule, the agents associated to these subsystems will never recover fully the information possessed by the global system if they cannot correlate the results of their individual observations. In the Bell state the two subsystems 1 and 2 are in the mixed state.

Moreover, there are also examples of social situations in which this standard answer fails for real-life agents: whenever a group of agents can cooperate to make joint observations, the implicit knowledge of the group will typically go beyond distributed knowledge, which only takes into account the results of separate, uncorrelated observations by each of the members of the group.

Chapter 4

Logic of Correlated knowledge

Logic of correlated knowledge is an epistemic logic enriched by observational capabilities of agents. Traditionally, agents can make a logical inference, positive and negative introspection and their knowledge is truthful. Applications of the epistemic logic cover fields such as distributed systems, merging of knowledge bases, robotics or network security in computer science and artificial intelligence. By adding observational capabilities to agents, logic of correlated knowledge can be applied, in addition, to reason about multi-partite quantum systems and quantum correlations.

Quantum entanglement posed a problem to the lattice-theoretical approach of traditional Quantum Logic [2, 44]. Logic of correlated knowledge (LCK) abstracts away from Hilbert spaces and suggests to accomodate correlation models to quantum systems and quantum entanglement. Alexandru Baltag and Sonja Smets introduced logic of correlated knowledge and Hilbert style proof system in [5]. Our main focus is to present an automated proof search system for logic of correlated knowledge and to prove decidability of LCK, in this chapter. We are using the ideas of semantic internalization, suggested by Sara Negri in [30], to get algorithmic properties for sequent calculus.

We start from defining syntax, semantics, and the Hilbert style proof system for logic of correlated knowledge in Section 4.1. In Section 4.2, we present Gentzen style sequent calculus for LCK and properties of the proof system. Soundness and the properties of admissibility of weakening, contraction, cut,

and invertibility of rules are proved in Sections 4.3 and 4.4. In Section 4.5 we show completeness of the sequent calculus GS-LCK. And we finalize by proving decidability of logic of correlated knowledge in Section 4.6.

4.1 Logic of correlated knowledge

4.1.1 Syntax

Consider a set $N = \{a_1, a_2, ..., a_n\}$ of agents. Each agent can perform its local observations. Given sets $O_{a_1}, ..., O_{a_n}$ of possible observations for each agent, a joint observation is a tuple of observations $o = (o_a)_{a \in N} \in O_{a_1} \times ... \times O_{a_n}$ or $o = (o_a)_{a \in I} \in O_I$, where $O_I := \times_{a \in I} O_a$ and $I \subseteq N$. Joint observations together with results $r \in R$ make new atomic formulas o^r.

Each agent can know some information, and it is written as $K_{a_1}A$ or $K_{\{a_1\}}A$, which means that the agent a_1 knows A. A group of agents can also know some information and it is written as $K_{\{a_1,a_2,a_3\}}A$ or $K_I A$, where $I = \{a_1, a_2, a_3\}$. A more detailed description about the knowledge operator K is given in [14, 45].

Syntax of logic of correlated knowledge is defined as follows:

Definition 19 (Syntax of logic of correlated knowledge). *The language of logic of correlated knowledge has the following syntax:*

$$F := p \mid o^r \mid \neg F \mid F \vee F \mid F \wedge F \mid F \to F \mid K_I F$$

where p is any atomic proposition, $o = (o_a)_{a \in I} \in O_I, r \in R$, *and* $I \subseteq N$.

4.1.2 Semantics

Consider a system, composed of N components or locations. Agents can be associated to locations, where they will perform observations. States (configurations) of the system are functions $s : O_{a_1} \times ... \times O_{a_n} \to R$ or $s_I : O_I \to R$, where

$I \subseteq N$ and a set of results R is in the structure (R, Σ) together with an abstract operation $\Sigma : \mathcal{P}(R) \to R$ of composing results. $\mathcal{P}(R)$ is a power set of R. For every joint observation $e \in O_I$, the local state s_I is defined as:

$$s_I((e_a)_{a\in I}) := \Sigma\{s(o) : o \in O_{a_1} \times ... \times O_{a_n} \text{ such that } o_a = e_a \text{ for all } a \in I\}$$

If s and t are two possible states of the system and a group of agents I can make exactly the same observations in these two states, then these states are observationally equivalent to I, and it is written as $s \overset{I}{\sim} t$. Observational equivalence is defined as follows:

Definition 20 (Observational equivalence). *Two states s and t are observationally equivalent $s \overset{I}{\sim} t$ iff $s_I = t_I$.*

A model of logic of correlated knowledge is a multi-modal Kripke model [25], where the relations between states mean observational equivalence. It is defined as:

Definition 21 (Model of logic of correlated knowledge). *For a set of states S, a family of binary relations $\{\overset{I}{\sim}\}_{I\subseteq N} \subseteq S \times S$ and a function of interpretations $V : S \to (P \to \{true, false\})$, where P is a set of atomic propositions, the model of logic of correlated knowledge is a multi-modal Kripke model $(S, \{\overset{I}{\sim}\}_{I\subseteq N}, V)$ that satisfies the following conditions:*

1. *For each $I \subseteq N$, $\overset{I}{\sim}$ is labelled equivalence relation;*
2. *Information is monotonic: if $I \subseteq J$, then $\overset{J}{\sim} \subseteq \overset{I}{\sim}$;*
3. *Observability principle: if $s \overset{N}{\sim} s'$, then $s = s'$;*
4. *Vacuous information: $s \overset{\emptyset}{\sim} s'$ for all $s, s' \in S$.*

The satisfaction relation $\models$ for model M, state s and formulas o^r and $K_I A$ is defined as follows:

- $M, s \models K_I A$ iff $M, t \models A$ for all states $t \overset{I}{\sim} s$.
- $M, s \models o^r$ iff $s_I(o) = r$.

The formula $K_I A$ means that the group of agents I carries the information that A is the case, and o^r means that r is the result of the joint observation o.

If formula A is true in any state of any model, then it is named as a valid formula.

4.1.3 Hilbert style calculus HS-LCK

Alexandru Baltag and Sonja Smets defined the Hilbert style calculus for logic of correlated knowledge in [5]. Fixing a finite set $N = \{a_1, ..., a_n\}$ of agents, a finite result structure (R, Σ) and a tuple of finite sets $\vec{O} = (O_{a_1}, ..., O_{a_n})$ of observations, for every set $I, J \subseteq N$, every joint observation $o \in O_I$, $O_I = \times_{a \in I} O_a$, and results $r, p \in R$, the Hilbert style calculus for logic of correlated knowledge over $(R, \Sigma, \vec{O})$ is as follows:

- Axioms:

  H1. $A \to (B \to A)$

  H2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$

  H3. $(\neg A \to \neg B) \to (B \to A)$

  H4. $K_I(A \to B) \to (K_I A \to K_I B)$ *(Kripke's axiom)*

  H5. $K_I A \to A$ *(Truthfulness)*

  H6. $K_I A \to K_I K_I A$ *(Positive introspection)*

  H7. $\neg K_I A \to K_I \neg K_I A$ *(Negative introspection)*

  H8. $K_I A \to K_J A$, where $I \subseteq J$ *(Monotonicity of group knowledge)*

  H9. $A \to K_N A$ *(Observability)*

  H10. $\bigwedge_{o \in O_I} \bigvee_{r \in R} o^r$ *(Observations always yield results)*

  H11. $o^r \to \neg o^p$, where $r \neq p$ *(Observations have unique results)*

  H12. $o^r_I \to K_I o^r_I$ *(Groups know the results of their joint observations)*

H13. $(\bigwedge\limits_{o\in O_I} o^{r_o} \wedge K_I A) \rightarrow K_\emptyset(\bigwedge\limits_{o\in O_I} o^{r_o} \rightarrow A)$
(Group knowledge is correlated knowledge (i.e. is based on joint observations))

H14. $\bigwedge\limits_{o\in\bar{e}} o^{r_o} \rightarrow e^{\Sigma\{r_o : o\in\bar{e}\}}$, where $e \in O_I$, $\bar{e} := \{o = (o_i)_{i\in N} \in O_{i_1} \times ... \times O_{i_n} : o_i = e_i \text{ for all } i \in I\}$. *(Result composition axiom)*

- Rules:

$$\frac{A, A \rightarrow B}{B}\ (Modus\ ponens) \qquad \frac{A}{K_I A}\ (K_I - necessitation)$$

Sets I, J may be empty in axioms H4 - H8 and in rule $(K_I - necessitation)$.

The Hilbert style calculus HS-LCK for logic of correlated knowledge is sound and complete with respect to correlation models over $(R, \Sigma, \vec{O})$ [5].

4.2 Gentzen style sequent calculus GS-LCK

Gerhard Gentzen introduced sequent calculus in 1934 [15]. Sequents in the system GS-LCK are statements of the form $\Gamma \Rightarrow \Delta$, where Γ and Δ are finite, possibly empty multisets of relational atoms $s \overset{I}{\sim} t$ and labelled formulas $s : A$, where $s, t \in S$, $I \subseteq N$ and A is any formula in the language of logic of correlated knowledge. The formula $s : A$ means $s \models A$, and $s \overset{I}{\sim} t$ is an observational equivalence or relation between the states in the model of logic of correlated knowledge.

The sequent calculus consists of axioms and rules. Applying rules to the sequents, a proof-search tree for the root sequent is constructed. If axioms are in all the leaves of the proof-search tree, then the root sequent is called as a provable sequent and the conclusion Δ follows from the premise Γ of the root sequent.

Fixing a finite set $N = \{a_1, ..., a_n\}$ of agents, a finite result structure (R, Σ) and a tuple of finite sets $\vec{O} = (O_{a_1}, ..., O_{a_n})$ of observations, for every set $I, J \subseteq N$, every joint observation $o \in O_I,\ O_I = \times_{a \in I} O_a$, and results $r, p \in R$, the Gentzen style sequent calculus GS-LCK for logic of correlated knowledge over $(R, \Sigma, \vec{O})$ is as follows:

- Axioms:
  - $s : p, \Gamma \Rightarrow \Delta, s : p$.
  - $s : o^r, \Gamma \Rightarrow \Delta, s : o^r$.
  - $s : o^{r_1}, s : o^{r_2}, \Gamma \Rightarrow \Delta$, where $r_1 \neq r_2$.
- Propositional rules:

$$\frac{\Gamma \Rightarrow \Delta, s : A}{s : \neg A, \Gamma \Rightarrow \Delta}\ (\neg \Rightarrow) \qquad \frac{s : A, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, s : \neg A}\ (\Rightarrow \neg)$$

$$\frac{s : A, \Gamma \Rightarrow \Delta \qquad s : B, \Gamma \Rightarrow \Delta}{s : A \vee B, \Gamma \Rightarrow \Delta}\ (\vee \Rightarrow) \qquad \frac{\Gamma \Rightarrow \Delta, s : A, s : B}{\Gamma \Rightarrow \Delta, s : A \vee B}\ (\Rightarrow \vee)$$

$$\frac{s : A, s : B, \Gamma \Rightarrow \Delta}{s : A \wedge B, \Gamma \Rightarrow \Delta}\ (\wedge \Rightarrow) \qquad \frac{\Gamma \Rightarrow \Delta, s : A \qquad \Gamma \Rightarrow \Delta, s : B}{\Gamma \Rightarrow \Delta, s : A \wedge B}\ (\Rightarrow \wedge)$$

$$\frac{\Gamma \Rightarrow \Delta, s : A \qquad s : B, \Gamma \Rightarrow \Delta}{s : A \to B, \Gamma \Rightarrow \Delta}(\to\Rightarrow) \qquad \frac{s : A, \Gamma \Rightarrow \Delta, s : B}{\Gamma \Rightarrow \Delta, s : A \to B}(\Rightarrow\to)$$

- Knowledge rules:

$$\frac{t : A, s : K_I A, s \overset{I}{\sim} t, \Gamma \Rightarrow \Delta}{s : K_I A, s \overset{I}{\sim} t, \Gamma \Rightarrow \Delta}(K_I \Rightarrow) \qquad \frac{s \overset{I}{\sim} t, \Gamma \Rightarrow \Delta, t : A}{\Gamma \Rightarrow \Delta, s : K_I A}(\Rightarrow K_I)$$

The rule $(K_I \Rightarrow)$ requires that $I \neq N$ and $t : A$ be not in Γ. The rule $(\Rightarrow K_I)$ requires that $I \neq N$ and t be not in the conclusion. Set I maybe an empty set in both rules.

$$\frac{s : A, s : K_N A, s \overset{N}{\sim} s, \Gamma \Rightarrow \Delta}{s : K_N A, s \overset{N}{\sim} s, \Gamma \Rightarrow \Delta}(K_N \Rightarrow) \qquad \frac{s \overset{N}{\sim} s, \Gamma \Rightarrow \Delta, s : A}{\Gamma \Rightarrow \Delta, s : K_N A}(\Rightarrow K_N)$$

The rule $(K_N \Rightarrow)$ requires that $s : A$ be not in Γ. The rule $(\Rightarrow K_N)$ requires that $s : A$ be not in Δ.

- Observational rules:

$$\frac{s \overset{I}{\sim} t, \{s : o^{r_o}\}_{o \in O_I}, \{t : o^{r_o}\}_{o \in O_I}, \Gamma \Rightarrow \Delta}{\{s : o^{r_o}\}_{o \in O_I}, \{t : o^{r_o}\}_{o \in O_I}, \Gamma \Rightarrow \Delta}\ (OE)$$

The rule (OE) requires that $I \neq \emptyset$ and formulas $s \overset{I}{\sim} t$, $s : o^{r_o}$ and $t : o^{r_o}$ be not in Γ, where $o \in O_I$.

$$\frac{\{s : o_I^r, \Gamma \Rightarrow \Delta\}_{r \in R}}{\Gamma \Rightarrow \Delta}\ (OYR)$$

The rule (OYR) requires:

1. $s : o_I^r$ be not in Γ for all $r \in R$ and $s : o_I^{r_1}$ be in Δ for some $r_1 \in R$.
2. $I \neq \emptyset$.

$$\frac{s : e_I^{\Sigma\{r_{o_N} : o_N \in \bar{e}\}}, \{s : o_N^{r_{o_N}}\}_{o_N \in \bar{e}}, \Gamma \Rightarrow \Delta}{\{s : o_N^{r_{o_N}}\}_{o_N \in \bar{e}}, \Gamma \Rightarrow \Delta}\ (CR)$$

The rule (CR) requires that $s : e_I^{\Sigma\{r_{o_N} : o_N \in \bar{e}\}}$ be not in Γ.

- Substitution rules:

$$\frac{s:p, t:p, s \overset{N}{\sim} t, \Gamma \Rightarrow \Delta}{t:p, s \overset{N}{\sim} t, \Gamma \Rightarrow \Delta}(Sub(p) \Rightarrow) \qquad \frac{s:o^r, t:o^r, s \overset{I}{\sim} t, \Gamma \Rightarrow \Delta}{t:o^r, s \overset{I}{\sim} t, \Gamma \Rightarrow \Delta}(Sub(o^r) \Rightarrow)$$

  The rules $(Sub(p) \Rightarrow)$ and $(Sub(o^r) \Rightarrow)$ require that $s:p$ and $s:o^r$ be not in Γ, accordingly.

- Relational rules:

$$\frac{s \overset{I}{\sim} s, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta}\ (Ref) \qquad \frac{s \overset{I}{\sim} t, s \overset{I}{\sim} s', s' \overset{I}{\sim} t, \Gamma \Rightarrow \Delta}{s \overset{I}{\sim} s', s' \overset{I}{\sim} t, \Gamma \Rightarrow \Delta}\ (Trans)$$

  The rule (Ref) requires that s be in the conclusion and $s \overset{I}{\sim} s$ be not in Γ. The rule $(Trans)$ requires that $s \overset{I}{\sim} t$ be not in Γ.

$$\frac{s' \overset{I}{\sim} t, s \overset{I}{\sim} s', s \overset{I}{\sim} t, \Gamma \Rightarrow \Delta}{s \overset{I}{\sim} s', s \overset{I}{\sim} t, \Gamma \Rightarrow \Delta}\ (Eucl) \qquad \frac{s \overset{I}{\sim} t, s \overset{J}{\sim} t, \Gamma \Rightarrow \Delta}{s \overset{J}{\sim} t, \Gamma \Rightarrow \Delta}\ (Mon)$$

  The rule (Mon) stands for monotonicity and requires that $I \subseteq J$. Sets I, J may be empty. The rules $(Eucl)$ and (Mon) require that $s' \overset{I}{\sim} t$ and $s \overset{I}{\sim} t$ be not in Γ, accordingly.

The sequent calculus GS-LCK is sound and complete with respect to correlation models over $(R, \Sigma, \vec{O})$ [19, 20]. If a sequent is provable in GS-LCK, then the formula of a sequent is valid. Also, all valid formulas are provable in GS-LCK, which expresses the completeness of the system.

Theorem 1 (Soundness and completeness of GS-LCK). *The sequent calculus GS-LCK is sound and complete with respect to correlation models over* $(R, \Sigma, \vec{O})$.

It also has beautiful properties of invertibility and admissibility. If the sequent of the conclusion of the rule is provable, then sequents of the premises of the rule are provable, too. This property is named as invertibility of the rule. The rule can be applied inverted in the proof-search tree. The properties of weakening, contraction, and cut are admissible in GS-LCK, which are crucial in making an automated proof system.

Theorem 2 (Properties of GS-LCK). *The sequent calculus GS-LCK has the following properties:*

- *Invertibility of rules.*
- *Admissibility of weakening.*
- *Admissibility of contraction.*
- *Admissibility of cut.*
- *Termination.*

Proofs of soundness, completeness, and the properties of GS-LCK are given in the next sections.

4.3 Proof of soundness of GS-LCK

Definition 22 (Extended syntax). *Extended syntax of LCK is as follows:*

$$A := s : A_1 \mid s \overset{I}{\sim} t \mid s : A_1 \vee A \mid s : A_1 \wedge A \mid s : A_1 \to A$$

$$A_1 := p \mid o^r \mid \bot \mid \top \mid \neg A_1 \mid A_1 \vee A_2 \mid A_1 \wedge A_2 \mid A_1 \to A_2 \mid K_I A_1$$

where p is any atomic proposition, $o \in O_I, I \subseteq N, r \in R$ *and* $s, t \in S$.

Definition 23 (Extended semantics). *If* $s, t, v \in \mathbf{S}$ *and* $M \in \mathbf{M}$*, then the truthfulness of the formula in the state* v *of the model* M *is defined as follows:*

- $v \models s : A$ *iff* $s \models A$.
- $v \models s \overset{I}{\sim} t$ *iff* $s \overset{I}{\sim} t \in \mathbf{R}$.

Commas "," in Γ of the sequent $\Gamma \Rightarrow \Delta$ mean conjunction "$\wedge$", commas "," in Δ - disjunction "$\vee$". The arrow "$\Rightarrow$" stands for implication "$\to$".

Definition 24 (Formula of the sequent). *If Seq is a sequent* $\Gamma \Rightarrow \Delta$*, then* the formula of the sequent $F(Seq)$ *is obtained by:*

1) *putting* Γ *and* Δ *in parentheses;*
2) *replacing empty* Γ *by* $s : \top$*;*
3) *replacing empty* Δ *by* $s : \bot$*;*
4) *replacing commas "," by conjunction "*$\wedge$*" in* Γ*;*
5) *replacing commas "," by disjunction "*$\vee$*" in* Δ*;*
6) *replacing "*$\Rightarrow$*" by implication "*$\to$*".*

Example 5. $F(Seq) := (t : A_1 \wedge s : K_I A_1 \wedge s \overset{I}{\sim} t \wedge t : A_2) \to (s : B_1 \vee t : B_2)$ *is the formula of the sequent* $Seq := t : A_1, s : K_I A_1, s \overset{I}{\sim} t, t : A_2 \Rightarrow s : B_1, t : B_2$.

Definition 25 (Sequent without labels and relational atoms). *If Seq is a sequent, then a sequent without labels and relational atoms of Seq is obtained removing all labels near formulas and all relational atoms from Seq.*

Lemma 1 (Validity of the formula of the sequent). *If the formula of the sequent Seq is valid, then the formula of the sequent Seq without labels and relational atoms is valid, as well.*

Proof.
Suppose we have a set of states S of a model M. For each formula of the sequent we have a tuple of its labels $(s_1, ..., s_l) \in S \times ... \times S$. If the formula with labels $(s_1, ..., s_l)$ is valid, then it is valid with substituted labels $(s', ..., s')$, because $\{(s', ..., s') : s' \in S\} \subseteq \{(s_1, ..., s_l) : s_1, ..., s_l \in S\}$. Having $s \models s' : A$, iff $s' \models A$, we can remove the label s'.
All relational atoms become $s' \overset{I}{\sim} s', I \subseteq N$. They are valid because of reflexivity in models. Applying the rules of GS-LCK they appear only in the first argument of implication of the formula of the sequent. We can remove relational atoms, because having a valid formula $(A_1 \wedge ... \wedge A_l) \rightarrow (B_1 \vee ... \vee B_k)$ and removing valid formula A_i from the first argument of implication, the validity is maintained. $\square$

Theorem 3 (Soundness of GS-LCK). *If sequent S is provable in GS-LCK, then the formula of the sequent S without labels and relational atoms is valid with respect to correlation models over* $(R, \Sigma, \vec{O})$.

Proof.
We prove the validity of all axioms and soundness of all the rules of GS-LCK:

- Axioms:
  - Formula of the axiom $s : p, \Gamma \Rightarrow s : p, \Delta$ is valid, because it is true in any state of any model. The same is for the axiom $s : o^r, \Gamma \Rightarrow s : o^r, \Delta$.
  - Validity of the formula of the axiom $s : o^{r_1}, s : o^{r_2}, \Gamma \Rightarrow \Delta$, where $r_1 \neq r_2$, follows from the axiom "H11. $o^r \rightarrow \neg o^p$, where $r \neq p$".
- Propositional rules as in [31].
- Knowledge rules:

– Rule $(K_I \Rightarrow)$:

$$\frac{t : A, s : K_I A, s \overset{I}{\sim} t, \Gamma \Rightarrow \Delta}{s : K_I A, s \overset{I}{\sim} t, \Gamma \Rightarrow \Delta} (K_I \Rightarrow), \quad I \neq N.$$

We prove by contraposition that, if the formula of the premise $(t : A, s : K_I A, s \overset{I}{\sim} t, \Gamma \Rightarrow \Delta)$ of the rule $(K_I \Rightarrow)$ is valid, then the formula of the conclusion $(s : K_I A, s \overset{I}{\sim} t, \Gamma \Rightarrow \Delta)$ is valid, too.
The formula of the conclusion $(s : K_I A, s \overset{I}{\sim} t, \Gamma \Rightarrow \Delta)$ is false, when $s : K_I A$, $s \overset{I}{\sim} t$ and all formulas in Γ are true, and all formulas in Δ are false. By semantic definition of the knowledge operator K_I, formula A is true in all the states accessible from the state s by relation I. States t are accessible from the state s, because $s \overset{I}{\sim} t$ is true, therefore the formula $t : A$ is true. If $t : A$, $s : K_I A$, $s \overset{I}{\sim} t$ and all formulas in Γ are true and all formulas in Δ are false, then the formula of the premise $(t : A, s : K_I A, s \overset{I}{\sim} t, \Gamma \Rightarrow \Delta)$ is false.

– Rule $(\Rightarrow K_I)$:

$$\frac{s \overset{I}{\sim} t, \Gamma \Rightarrow \Delta, t : A}{\Gamma \Rightarrow \Delta, s : K_I A} (\Rightarrow K_I), \quad I \neq N \textit{ and } t \textit{ is not in the conclusion}.$$

The formula of conclusion $(\Gamma \Rightarrow \Delta, s : K_I A)$ is false, when all formulas in Γ are true and all formulas in Δ and $s : K_I A$ are false. If the formula $s : K_I A$ is false, then there exists a state t accessible from state s by relation I, where A is false. If $s \overset{I}{\sim} t$ and all formulas in Γ are true and all formulas in Δ and $t : A$ are false, then the formula of the premise $(s \overset{I}{\sim} t, \Gamma \Rightarrow \Delta, t : A)$ is false.
The label t cannot be in the conclusion, because we can get situations, where the formula of the premise $(s \overset{I}{\sim} t, \Gamma \Rightarrow \Delta, t : A)$ is valid and the formula of the conclusion $(\Gamma \Rightarrow \Delta, s : K_I A)$ is not. An example:

$$\frac{s \overset{I}{\sim} t, t : A \Rightarrow t : A}{t : A \Rightarrow s : K_I A} (\Rightarrow K_I)$$

– The validity of the rules $(K_N \Rightarrow)$ and $(\Rightarrow K_N)$ is proved in the same way.

- Observational rules:
  - Rule (OYR):

    $$\frac{\{s : o^r, \Gamma \Rightarrow \Delta\}_{r \in R}}{\Gamma \Rightarrow \Delta} \ (OYR)$$

    If R is a set of results, and o is a joint observation, then there exists a result $r \in R$ that o^r is true. If there exists r that o^r is true and all formulas in Γ are true and all formulas in Δ are false, then one formula of premises $(\{s : o^r, \Gamma \Rightarrow \Delta\}_{r \in R})$ is false.
  - Rule (CR):

    $$\frac{s : e^{\Sigma\{r_o : o \in \bar{e}\}}, \{s : o^{r_o}\}_{o \in \bar{e}}, \Gamma \Rightarrow \Delta}{\{s : o^{r_o}\}_{o \in \bar{e}}, \Gamma \Rightarrow \Delta} \ (CR)$$

    The contraposition is proved by the axiom "H14. $\bigwedge\limits_{o \in \bar{e}} o^{r_o} \rightarrow e^{\Sigma\{r_o : o \in \bar{e}\}}$".
  - The soundness of rules (OE), $(\ Sub(p) \Rightarrow)$ and $(\ Sub(o^r) \Rightarrow)$ is proved in the same way.
- Relational rules:
  - Rule (Mon):

    $$\frac{s \overset{I}{\sim} t, s \overset{J}{\sim} t, \Gamma \Rightarrow \Delta}{s \overset{J}{\sim} t, \Gamma \Rightarrow \Delta} \ (Mon)$$

    The contraposition follows from condition to models of LCK: 2. If $I \subseteq J$ then $\overset{J}{\sim} \subseteq \overset{I}{\sim}$.
  - The validity of rules (Ref), $(Trans)$ and $(Eucl)$ is proved in the same way.

We have proved the validity of all axioms and soundness of all the rules of GS-LCK. The statement of the theorem follows from lemma 1. $\square$

4.4 Proof of the properties of GS-LCK

Lemma 2 (Admissibility of contraction with atomic formulas).
If a sequent $(\Pi_{atomic}, \Pi_{atomic}, \Gamma \Rightarrow \Delta, \Lambda_{atomic}, \Lambda_{atomic})$ *is provable in GS-LCK, then the sequent* $(\Pi_{atomic}, \Gamma \Rightarrow \Delta, \Lambda_{atomic})$ *is also provable with the same bound of the height of the proof in GS-LCK.* Γ, Δ *are any multisets of formulas.* $\Pi_{atomic}, \Lambda_{atomic}$ *are any multisets of atomic formulas* $s : p, s : o^r, s \overset{I}{\sim} t$.

Proof.
Lemma 2 is proved by induction on the height $< h >$ of the proof of the sequent $(\Pi_{atomic}, \Pi_{atomic}, \Gamma \Rightarrow \Delta, \Lambda_{atomic}, \Lambda_{atomic})$.

$< h = 1 >$

If the sequent $(\Pi_{atomic}, \Pi_{atomic}, \Gamma \Rightarrow \Delta, \Lambda_{atomic}, \Lambda_{atomic})$ is an axiom, then the sequent $(\Pi_{atomic}, \Gamma \Rightarrow \Delta, \Lambda_{atomic})$ is an axiom too.

$< h > 1 >$

- The rule $(K_I \Rightarrow)$ was applied in the last step of the proof of the sequent.

  – One or two formulas of the principal pair is in Π_{atomic}.

  $$\frac{t : A, s : K_I A, s \overset{I}{\sim} t, s \overset{I}{\sim} t, \Pi'_{atomic}, \Pi'_{atomic}, \Gamma' \Rightarrow \Delta, \Lambda_{atomic}, \Lambda_{atomic}}{s : K_I A, s \overset{I}{\sim} t, s \overset{I}{\sim} t, \Pi'_{atomic}, \Pi'_{atomic}, \Gamma' \Rightarrow \Delta, \Lambda_{atomic}, \Lambda_{atomic}} (K_I \Rightarrow)$$

  The height of the proof of the premise of application of the rule $(K_I \Rightarrow)$ reduced to $< h - 1 >$. By the induction hypothesis the sequent $(t : A, s : K_I A, s \overset{I}{\sim} t, \Pi'_{atomic}, \Gamma' \Rightarrow \Delta, \Lambda_{atomic})$ is provable with the height h', where $h' \leq h - 1$. The sequent of the lemma is proved by applying the rule $(K_I \Rightarrow)$:

  $$\frac{t : A, s : K_I A, s \overset{I}{\sim} t, \Pi'_{atomic}, \Gamma' \Rightarrow \Delta, \Lambda_{atomic}}{s : K_I A, s \overset{I}{\sim} t, \Pi'_{atomic}, \Gamma' \Rightarrow \Delta, \Lambda_{atomic}} (K_I \Rightarrow)$$

  Other cases are prooved in a similar way.

– Any formula of the principal pair is not in Π_{atomic}.

$$\frac{t : A, s : K_I A, s \overset{I}{\sim} t, \Pi_{atomic}, \Pi_{atomic}, \Gamma' \Rightarrow \Delta, \Lambda_{atomic}, \Lambda_{atomic}}{s : K_I A, s \overset{I}{\sim} t, \Pi_{atomic}, \Pi_{atomic}, \Gamma' \Rightarrow \Delta, \Lambda_{atomic}, \Lambda_{atomic}} (K_I \Rightarrow)$$

By the induction hypothesis the sequent $(t : A, s : K_I A, s \overset{I}{\sim} t, \Pi_{atomic}, \Gamma' \Rightarrow \Delta, \Lambda_{atomic})$ is provable with the height h', where $h' \leq h - 1$. The sequent of the lemma is proved by applying the rule $(K_I \Rightarrow)$:

$$\frac{t : A, s : K_I A, s \overset{I}{\sim} t, \Pi_{atomic}, \Gamma' \Rightarrow \Delta, \Lambda_{atomic}}{s : K_I A, s \overset{I}{\sim} t, \Pi_{atomic}, \Gamma' \Rightarrow \Delta, \Lambda_{atomic}} (K_I \Rightarrow)$$

- The cases of the remaining rules are considered similarly.

□

Lemma 3 (Substitution). *If a sequent* $(\Gamma \Rightarrow \Delta)$ *is provable in GS-LCK, then sequent* $(\Gamma(t/s) \Rightarrow \Delta(t/s))$ *is also provable with the same bound of the height of the proof in GS-LCK.*

Proof.
Lemma 3 is proved by induction on the height $< h >$ of the proof of the sequent $(\Gamma \Rightarrow \Delta)$.

$< h = 1 >$

If the sequent $(\Gamma \Rightarrow \Delta)$ is an axiom, then the sequent $(\Gamma(t/s) \Rightarrow \Delta(t/s))$ is an axiom as well.

$< h > 1 >$

- The rule $(\Rightarrow K_I)$ was applied in the last step of the proof of the sequent.

$$\frac{s \overset{I}{\sim} t, \Gamma \Rightarrow \Delta, t : A}{\Gamma \Rightarrow \Delta, s : K_I A} (\Rightarrow K_I)$$

– Substitution (l/z).

By the induction hypothesis the sequent $(s \overset{I}{\sim} t, \Gamma(l/z) \Rightarrow \Delta(l/z), t : A)$ is provable with the height h', where $h' \leq h - 1$. The sequent of the lemma is proved by applying the rule $(\Rightarrow K_I)$:

$$\frac{s \overset{I}{\sim} t, \Gamma(l/z) \Rightarrow \Delta(l/z), t : A}{\Gamma(l/z) \Rightarrow \Delta(l/z), s : K_I A} \ (\Rightarrow K_I)$$

– Substitution (l/t).

There is no label t in the sequent $\Gamma \Rightarrow \Delta, s : K_I A$ because of the requirement of the application of the rule $(\Rightarrow K_I)$ that t is a new label.

– Substitution (l/s) and $l \neq t$.

By the induction hypothesis the sequent $(l \overset{I}{\sim} t, \Gamma(l/s) \Rightarrow \Delta(l/s), t : A)$ is provable with the height h', where $h' \leq h - 1$. The sequent of the lemma is proved by applying the rule $(\Rightarrow K_I)$:

$$\frac{l \overset{I}{\sim} t, \Gamma(l/s) \Rightarrow \Delta(l/s), t : A}{\Gamma(l/s) \Rightarrow \Delta(l/s), l : K_I A} \ (\Rightarrow K_I)$$

– Substitution (l/s) and $l = t$.

By the induction hypothesis with substitution (w/t), the sequent $(s \overset{I}{\sim} w, \Gamma \Rightarrow \Delta, w : A)$ is provable with the height h', where $h' \leq h - 1$. The label w is a new label absent in the sequent. By the inducion hypothesis with substitution (l/s), the sequent $(l \overset{I}{\sim} w, \Gamma(l/s) \Rightarrow \Delta(l/s), w : A)$ is provable with the height h'', where $h'' \leq h - 1$. The sequent of the lemma is proved by applying the rule $(\Rightarrow K_I)$:

$$\frac{l \overset{I}{\sim} w, \Gamma(l/s) \Rightarrow \Delta(l/s), w : A}{\Gamma(l/s) \Rightarrow \Delta(l/s), l : K_I A} \ (\Rightarrow K_I)$$

- The rule (Ref) was applied in the last step of the proof of the sequent.

$$\frac{s \overset{I}{\sim} s, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta} \ (Ref)$$

– Substitution (s/t), and relational atom $s \overset{I}{\sim} t$ is in Γ.

By the induction hypothesis, the sequent $(s \overset{I}{\sim} s, s \overset{I}{\sim} s, \Gamma(s/t) \Rightarrow \Delta(s/t))$ is provable with the height h', where $h' \leq h - 1$. The sequent of the lemma is proved by applying Lemma 2.

– Other substitutions are considered in a similar way.

- The cases of the remaining rules are considered similarly.

□

Theorem 4 (Admissibility of weakening). *If a sequent* $(\Gamma \Rightarrow \Delta)$ *is provable in GS-LCK, then a sequent* $(\Pi, \Gamma \Rightarrow \Delta, \Lambda)$ *is provable with the same bound of the height of the proof in GS-LCK, too.* $\Pi, \Gamma, \Delta, \Lambda$ *are any multisets of formulas.*

Proof.
Theorem 4 is proved by induction on the height $< h >$ of the proof of the sequent $(\Gamma \Rightarrow \Delta)$.

$< h = 1 >$

If the sequent $(\Gamma \Rightarrow \Delta)$ is an axiom, then the sequent $(\Pi, \Gamma \Rightarrow \Delta, \Lambda)$ is an axiom, as well.

$< h > 1 >$

- The rule $(\Rightarrow K_I)$ was applied in the last step of the proof of the sequent.

$$\frac{s \overset{I}{\sim} t, \Gamma \Rightarrow \Delta, t : A}{\Gamma \Rightarrow \Delta, s : K_I A} \ (\Rightarrow K_I)$$

– A new label t for the application of the rule $(\Rightarrow K_I)$ is in Π or Λ.
By Lemma 3, the sequent $(s \overset{I}{\sim} t, \Gamma \Rightarrow \Delta, t : A)$ with substitution (l/t) is provable. By the induction hypothesis, the sequent $(s \overset{I}{\sim} l, \Pi, \Gamma \Rightarrow \Delta, \Lambda, l : A)$ is provable with the height h', where $h' \leq h - 1$. Here l is a new label, absent in Π, Γ, Δ and Λ. The sequent of the theorem is

proved by applying the rule $(\Rightarrow K_I)$:

$$\frac{s \overset{I}{\sim} l, \Pi, \Gamma \Rightarrow \Delta, \Lambda, l : A}{\Pi, \Gamma \Rightarrow \Delta, \Lambda, s : K_I A} \ (\Rightarrow K_I)$$

– The new label t for application of the rule $(\Rightarrow K_I)$ is absent in Π or Λ. By the induction hypothesis, the sequent $(s \overset{I}{\sim} t, \Pi, \Gamma \Rightarrow \Delta, \Lambda, t : A)$ is provable with the height h', where $h' \leq h - 1$. The sequent of the theorem is proved by applying the rule $(\Rightarrow K_I)$:

$$\frac{s \overset{I}{\sim} t, \Pi, \Gamma \Rightarrow \Delta, \Lambda, t : A}{\Pi, \Gamma \Rightarrow \Delta, \Lambda, s : K_I A} \ (\Rightarrow K_I)$$

- The cases of the remaining rules are considered similarly.

□

Theorem 5 (Invertibility of rules). *All the rules of GS-LCK are invertible with the same bound of the height of the proof.*

Proof.
Theorem 5 is proved for each rule separately.
The rule $(K_I \Rightarrow)$

$$\frac{t : A, s : K_I A, s \overset{I}{\sim} t, \Gamma \Rightarrow \Delta}{s : K_I A, s \overset{I}{\sim} t, \Gamma \Rightarrow \Delta} \ (K_I \Rightarrow)$$

Invertibility is proved by induction on the height $< h >$ of the proof of the sequent of the conclusion of the rule $(K_I \Rightarrow)$.

$< h = 1 >$

If the sequent $(s : K_I A, s \overset{I}{\sim} t, \Gamma \Rightarrow \Delta)$ is an axiom, then the sequent $(t : A, s : K_I A, s \overset{I}{\sim} t, \Gamma \Rightarrow \Delta)$ is an axiom, too.

$< h > 1 >$

- The formula $s \overset{I}{\sim} t$ is the principal formula.

  - The rule ($Sub(o^r) \Rightarrow$) was applied in the last step of the proof of the sequent.

    $$\frac{s : o^r, s : K_I A, s \overset{I}{\sim} t, t : o^r, \Gamma' \Rightarrow \Delta}{s : K_I A, s \overset{I}{\sim} t, t : o^r, \Gamma' \Rightarrow \Delta} \; (\, Sub(o^r) \Rightarrow)$$

    By the induction hypothesis, the sequent $(t : A, s : o^r, s : K_I A, s \overset{I}{\sim} t, t : o^r, \Gamma' \Rightarrow \Delta)$ is provable with the height h', where $h' \leq h - 1$. The sequent of the premise of the rule $(K_I \Rightarrow)$ is proved by applying the rule ($Sub(o^r) \Rightarrow$):

    $$\frac{t : A, s : o^r, s : K_I A, s \overset{I}{\sim} t, t : o^r, \Gamma' \Rightarrow \Delta}{t : A, s : K_I A, s \overset{I}{\sim} t, t : o^r, \Gamma' \Rightarrow \Delta} \; (Sub(o^r) \Rightarrow)$$

  - For rules $(K_I \Rightarrow)$, $(Trans)$, $(Eucl)$, (Mon) in a similar way.

- The case where the formula $s : K_I A$ is the principal formula and the case where formulas $s \overset{I}{\sim} t$ and $s : K_I A$ both are not principal formulas are considered similarly.

Invertibility of the remaining rules is proved in a similar way.

□

Theorem 6 (Admissibility of contraction). *If a sequent* $(\Pi, \Pi, \Gamma \Rightarrow \Delta, \Lambda, \Lambda)$ *is provable in GS-LCK, then sequent* $(\Pi, \Gamma \Rightarrow \Delta, \Lambda)$ *is provable with the same bound of the height of the proof in GS-LCK, too.* $\Pi, \Gamma, \Delta, \Lambda$ *are any multisets of formulas.*

Proof.

Theorem 6 is proved by induction on the ordered tuple pair $< c, h >$, where c is the sum of complexity of all the formulas in Π and Λ, and h is the height of the proof of the sequent $(\Pi, \Pi, \Gamma \Rightarrow \Delta, \Lambda, \Lambda)$.

$< c \geq 1, h = 1 >$

If the sequent $(\Pi, \Pi, \Gamma \Rightarrow \Delta, \Lambda, \Lambda)$ is an axiom, then the sequent $(\Pi, \Gamma \Rightarrow \Delta, \Lambda)$ is an axiom, too.

$< c \geq 1, h > 1 >$

- The rule $(\neg \Rightarrow)$ was applied in the last step of the proof of the sequent.

  - The principal formula is in Π.

    $$\frac{s : \neg A, \Pi', \Pi', \Gamma \Rightarrow \Delta, \Lambda, \Lambda, s : A}{s : \neg A, s : \neg A, \Pi', \Pi', \Gamma \Rightarrow \Delta, \Lambda, \Lambda} (\neg \Rightarrow)$$

    By invertibility of the rule $(\neg \Rightarrow)$, the sequent $(\Pi', \Pi', \Gamma \Rightarrow \Delta, \Lambda, \Lambda, s : A, s : A)$ is provable. The value of the ordered tuple pair has reduced to $< c - 1, h >$. By the induction hypothesis, the sequent $(\Pi', \Gamma \Rightarrow \Delta, \Lambda, s : A)$ is provable with the height h', where $h' \leq h - 1$. The sequent of the theorem is proved by applying the rule $(\neg \Rightarrow)$:

    $$\frac{\Pi', \Gamma \Rightarrow \Delta, \Lambda, s : A}{s : \neg A, \Pi', \Gamma \Rightarrow \Delta, \Lambda} (\neg \Rightarrow)$$

  - The principal formula is absent in Π.

    $$\frac{\Pi, \Pi, \Gamma \Rightarrow \Delta, \Lambda, \Lambda, s : A}{s : \neg A, \Pi, \Pi, \Gamma \Rightarrow \Delta, \Lambda, \Lambda} (\neg \Rightarrow)$$

    By the induction hypothesis, the sequent $(\Pi, \Gamma \Rightarrow \Delta, \Lambda, s : A)$ is provable with the height h', where $h' \leq h - 1$. The sequent of the theorem is proved by applying the rule $(\neg \Rightarrow)$:

    $$\frac{\Pi, \Gamma \Rightarrow \Delta, \Lambda, s : A}{s : \neg A, \Pi, \Gamma \Rightarrow \Delta, \Lambda} (\neg \Rightarrow)$$

- The cases of the remaining rules are considered similarly.

□

Theorem 7 (Admissibility of cut). *If sequents* $(\Gamma \Rightarrow \Delta, F)$ *and* $(F, \Pi \Rightarrow \Lambda)$ *are provable in GS-LCK, then sequent* $(\Pi, \Gamma \Rightarrow \Delta, \Lambda)$ *is provable in GS-LCK too.* F *is any formula and* $\Pi, \Gamma, \Delta, \Lambda$ *are any multisets of formulas.*

Proof.
Theorem 7 is proved by induction on the ordered tuple pair $< c, h >$, where c is the complexity of formula F, and h is the sum of heights of the proof of the sequents $(\Gamma \Rightarrow \Delta, F)$ and $(F, \Pi \Rightarrow \Lambda)$.

$< c \geq 1, h = 2 >$

The sequents $(\Gamma \Rightarrow \Delta, F)$ and $(F, \Pi \Rightarrow \Lambda)$ are the axioms. If formula F is not principal in one at least of the sequents, then $(\Pi, \Gamma \Rightarrow \Delta, \Lambda)$ is an axiom. If formula F is principal in both sequents, then F should be in Γ and Δ or only in Γ (the case where the axiom is of type $s : o^{r_1}, s : o^{r_2}, \Gamma \Rightarrow \Delta$). Therefore the sequent $(\Pi, \Gamma \Rightarrow \Delta, \Lambda)$ is also an axiom.

$< c \geq 1, h > 2 >$

- Formula F is not principal in the sequent $(\Gamma \Rightarrow \Delta, F)$.

  – The rule $(Sub(o^r) \Rightarrow)$ was applied in the last step of the proof of the sequent $(\Gamma \Rightarrow \Delta, F)$.

  $$\frac{s : o^r, t : o^r, s \overset{N}{\sim} t, \Gamma \Rightarrow \Delta, F}{t : o^r, s \overset{N}{\sim} t, \Gamma \Rightarrow \Delta, F} \, (Sub(o^r) \Rightarrow)$$

  By the induction hypothesis, the sequent $(s : o^r, t : o^r, s \overset{N}{\sim} t, \Pi, \Gamma \Rightarrow \Delta, \Lambda)$ is provable. The sequent of the theorem is proved by applying the rule $(Sub(o^r) \Rightarrow)$:

  $$\frac{s : o^r, t : o^r, s \overset{N}{\sim} t, \Pi, \Gamma \Rightarrow \Delta, \Lambda}{t : o^r, s \overset{N}{\sim} t, \Pi, \Gamma \Rightarrow \Delta, \Lambda} \, (Sub(o^r) \Rightarrow)$$

  – For applications of other rules in a similar way.

- Formula F is not principal in the sequent $(F, \Pi \Rightarrow \Lambda)$.
  The case is considered in a similar way.

- Formula F is principal in both sequents $(\Gamma \Rightarrow \Delta, F)$ and $(F, \Pi \Rightarrow \Lambda)$.

– The sequent $(\Gamma \Rightarrow \Delta, F)$ is an axiom and the rule (OE) was applied in the last step of the proof of the sequent $(F, \Pi \Rightarrow \Lambda)$.

$$s : o_1^{r_{o_1}}, \Gamma \Rightarrow \Delta, s : o_1^{r_{o_1}}$$

$$\frac{s \overset{I}{\sim} t, s : o_1^{r_{o_1}}, \{s : o^{r_o}\}_{o \in \{O_I \setminus o_1\}}, \{t : o^{r_o}\}_{o \in O_I}, \Pi \Rightarrow \Lambda}{s : o_1^{r_{o_1}}, \{s : o^{r_o}\}_{o \in \{O_I \setminus o_1\}}, \{t : o^{r_o}\}_{o \in O_I}, \Pi \Rightarrow \Lambda}(OE)$$

By the induction hypothesis, the sequent $(s : o_1^{r_{o_1}}, s \overset{I}{\sim} t, \{s : o^{r_o}\}_{o \in \{O_I \setminus o_1\}}, \{t : o^{r_o}\}_{o \in O_I}, \Pi, \Gamma \Rightarrow \Delta, \Lambda)$ is provable. The sequent of the theorem is proved by applying the rule (OE):

$$\frac{s : o_1^{r_{o_1}}, s \overset{I}{\sim} t, \{s : o^{r_o}\}_{o \in \{O_I \setminus o_1\}}, \{t : o^{r_o}\}_{o \in O_I}, \Pi, \Gamma \Rightarrow \Delta, \Lambda}{s : o_1^{r_{o_1}}, \{s : o^{r_o}\}_{o \in \{O_I \setminus o_1\}}, \{t : o^{r_o}\}_{o \in O_I}, \Pi, \Gamma \Rightarrow \Delta, \Lambda}(OE)$$

– The cases of the remaining rules are considered similarly.

□

4.5 Proof of completeness of GS-LCK

Theorem 8 (Completeness of GS-LCK). *If formula A is valid with respect to correlation models over $(R, \Sigma, \vec{O})$, then sequent $(\Rightarrow s : A)$ is provable in GS-LCK.*

Proof.
The Hilbert style proof system HS-LCK for logic of correlated knowledge is complete. Showing the provability of all valid formulas of HS-LCK in GS-LCK, the completeness of GS-LCK is proved. Theorem 11 is proved by induction on the number of steps $< NSteps >$, used to prove formula A in HS-LCK.

$< NSteps = 1 >$

Formula A is an axiom of calculus HS-LCK.

- The axiom "H4. $K_I(A \to B) \to (K_I A \to K_I B)$", was used.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{t : A, ... \Rightarrow t : B, t : A \qquad t : B, t : A, ... \Rightarrow t : B}{t : A \to B, t : A, s \overset{I}{\sim} t, s : K_I(A \to B), s : K_I A \Rightarrow t : B}(\to\Rightarrow)}{t : A, s \overset{I}{\sim} t, s : K_I(A \to B), s : K_I A \Rightarrow t : B}(K_I \Rightarrow)}{s \overset{I}{\sim} t, s : K_I(A \to B), s : K_I A \Rightarrow t : B}(K_I \Rightarrow)}{s : K_I(A \to B), s : K_I A \Rightarrow s : K_I B}(\Rightarrow K_I)}{s : K_I(A \to B) \Rightarrow s : K_I A \to K_I B}(\Rightarrow\to)}{\Rightarrow s : K_I(A \to B) \to (K_I A \to K_I B)}(\Rightarrow\to)$$

- The axiom "H8. $K_I A \to K_J A, \;$ when $\; I \subseteq J$", was used.

$$\dfrac{\dfrac{\dfrac{\dfrac{t : A, s \overset{I}{\sim} t, s \overset{J}{\sim} t, s : K_I A \Rightarrow t : A}{s \overset{I}{\sim} t, s \overset{J}{\sim} t, s : K_I A \Rightarrow t : A}(K_I \Rightarrow)}{s \overset{J}{\sim} t, s : K_I A \Rightarrow t : A}(Mon)}{s : K_I A \Rightarrow s : K_J A}(\Rightarrow K_J)}{\Rightarrow s : K_I A \to K_J A}(\Rightarrow\to)$$

- The axiom "H12. $o^r_I \to K_I o^r_I$", was used.

$$\dfrac{\dfrac{\dfrac{t : o^r_I, s \overset{I}{\sim} t, s : o^r_I \Rightarrow t : o^r_I}{s \overset{I}{\sim} t, s : o^r_I \Rightarrow t : o^r_I}(\ Sub(o^r) \Rightarrow)}{s : o^r_I \Rightarrow s : K_I o^r_I}(\Rightarrow K_I)}{\Rightarrow s : o^r_I \to K_I o^r_I}(\Rightarrow\to)$$

- The axiom "H13. $(\underset{o\in O_I}{\wedge} o^{r_o} \wedge K_I A) \to K_\emptyset(\underset{o\in O_I}{\wedge} o^{r_o} \to A)$, when $I \subset N$", was used.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{t : A, s \overset{I}{\sim} t, t : \underset{o\in O_I}{\wedge} o^{r_o}, s \overset{\emptyset}{\sim} t, s : \underset{o\in O_I}{\wedge} o^{r_o}, s : K_I A \Rightarrow t : A}{s \overset{I}{\sim} t, t : \underset{o\in O_I}{\wedge} o^{r_o}, s \overset{\emptyset}{\sim} t, s : \underset{o\in O_I}{\wedge} o^{r_o}, s : K_I A \Rightarrow t : A}(K_I \Rightarrow)}{t : \underset{o\in O_I}{\wedge} o^{r_o}, s \overset{\emptyset}{\sim} t, s : \underset{o\in O_I}{\wedge} o^{r_o}, s : K_I A \Rightarrow t : A}(OE)}{s \overset{\emptyset}{\sim} t, s : \underset{o\in O_I}{\wedge} o^{r_o}, s : K_I A \Rightarrow t : \underset{o\in O_I}{\wedge} o^{r_o} \to A}(\Rightarrow\to)}{s \overset{\emptyset}{\sim} t, s : \underset{o\in O_I}{\wedge} o^{r_o} \wedge K_I A \Rightarrow t : \underset{o\in O_I}{\wedge} o^{r_o} \to A}(\wedge \Rightarrow)}{s : \underset{o\in O_I}{\wedge} o^{r_o} \wedge K_I A \Rightarrow s : K_\emptyset(\underset{o\in O_I}{\wedge} o^{r_o} \to A)}(\Rightarrow K_\emptyset)}{\Rightarrow s : (\underset{o\in O_I}{\wedge} o^{r_o} \wedge K_I A) \to K_\emptyset(\underset{o\in O_I}{\wedge} o^{r_o} \to A)}(\Rightarrow\to)$$

- The remaining axioms are considered in a similar way.

$< NSteps > 1 >$

One of the rules $(Modus\ ponens)$ or $(K_I - necessitation)$ of calculus HS-LCK was applied in the last step of the proof of the formula.

- The rule $(Modus\ ponens)$ was applied.

$$\dfrac{A, A \to B}{B}\ (Modus\ ponens)$$

  By the induction hypothesis, sequents $(\Rightarrow s : A)$ and $(\Rightarrow s : A \to B)$ are provable in GS-LCK. By invertibility of the rule $(\Rightarrow\to)$, the sequent $(s : A \Rightarrow s : B)$ is provable. The sequent $(\Rightarrow s : B)$ of the theorem is proved by applying Theorem 7 "Admissibility of cut".

- The rule $(K_I - necessitation)$ was applied.

$$\dfrac{A}{K_I A}\ (K_I - necessitation)$$

  By the induction hypothesis, the sequent $(\Rightarrow s : A)$ is provable in GS-LCK. By Lemma 3 "Substition", the sequent $(\Rightarrow t : A)$ is provable. By Theorem 4

"Admissibility of weakening", the sequent $(s \overset{I}{\sim} t \Rightarrow t : A)$ is provable. The sequent of the theorem is proved by applying the rule $(\Rightarrow K_I)$:

$$\frac{s \overset{I}{\sim} t \Rightarrow t : A}{\Rightarrow s : K_I A} \ (\Rightarrow K_I)$$

□

4.6 Decidability of logic of correlated knowledge

Decidability of logic of correlated knowledge is showed by first defining the terminating proof search procedure for LCK. Procedure uses tables $TableLK$ and $TableRK$ to save principal formulas of the applications of the rules $(K_I \Rightarrow)$, $(K_N \Rightarrow)$ and $(\Rightarrow K_I)$. Also chains of new appeared relational atoms of applications of the rule $(\Rightarrow K_I)$ are saved in table $TableRK$.

Definition 26 (Table TableLK). *Table TableLK of the principal pairs of the applications of the rules $(K_I \Rightarrow)$ and $(K_N \Rightarrow)$:*

TableLK	
Main formula	*Relational atom*

Example 6. *Example of TableLK:*

TableLK	
Main formula	*Relational atom*
$s : K_I A$	$s \overset{I}{\sim} t$
$l : K_I B$	$l \overset{I}{\sim} z$

Definition 27 (Negative and positive parts of a sequent). *Negative and positive parts of a sequent $\Gamma \Rightarrow \Delta$ are called negative and positive parts of the formula of the sequent $\wedge\Gamma \rightarrow \vee\Delta$, accordingly.*

For any given sequent, $n(K_I)$ denotes the number of knowledge operators K_I in the negative part of the sequent. We use this notation in defining $TableRK$.

Definition 28 (Table TableRK). *Table TableRK of the principal formulas and chains of new appeared relational atoms of the applications of the rule $(\Rightarrow K_I)$:*

TableRK			
Main formula	*Chain of the relational atoms*	*Length of chain*	*Max*

where Max is the maximum length of the chain, defined by $n(K_I) + 1$.

Example 7. *Example of TableRK:*

TableRK			
Main formula	*Chain of the relational atoms*	*Length of chain*	*Max*
$s, s_1, s_2, w_1 : K_I A$	$s \overset{I}{\sim} s_1, s_1 \overset{I}{\sim} s_2, s_2 \overset{I}{\sim} s_3$	*3*	*5*
	$s \overset{I}{\sim} t_1$	*1*	*5*
	$s \overset{I}{\sim} w_1, w_1 \overset{I}{\sim} w_2$	*2*	*5*
$z, z_1 : K_J B$	$z \overset{J}{\sim} z_1, z_1 \overset{J}{\sim} z_2$	*2*	*7*

Definition 29 (Procedure of the proof search). *Procedure GS-LCK-PROC of the proof search in the sequent calculus GS-LCK:*

Initialisation:

- *Define set N of agents, tuple of sets $\vec{O} = (O_{a_1}, ..., O_{a_n})$ of possible observations and result structure (R, Σ).*
- *Initialise the tables $TableLK$ and $TableRK$ by setting Max values to $(n(K_I)+1)$, the length of the chain to 0 and the other cells leaving empty.*
- *Set Output = False.*

PROCEDURE GS-LCK-PROC(Sequent, TableLK, TableRK, Output)

BEGIN

1. *Check if the sequent is the axiom. If the sequent is the axiom, set* $Output = True$ *and go to step Finish.*
2. *If possible, apply any of the rules* $(\neg \Rightarrow), (\Rightarrow \neg), (\Rightarrow \vee), (\wedge \Rightarrow), (\Rightarrow \rightarrow)$ *and go to step 1.*
3. *If possible, apply any of the rules* $(\vee \Rightarrow), (\Rightarrow \wedge)$ *or* $(\rightarrow \Rightarrow)$ *and call procedure GS-LCK-PROC() for the premises of the application:*

   Output1 = False;
   Output2 = False;

   GS-LCK-PROC(Premise1, TableLK, TableRK, Output1);
   GS-LCK-PROC(Premise2, TableLK, TableRK, Output2);

   IF (Output1 == True) AND (Output2 == True)
   THEN Set Output = True and go to Finish;
   ELSE Set Output = False and go to Finish;

4. *If possible to apply any of the rules* $(K_I \Rightarrow)$ *or* $(K_N \Rightarrow)$*, check if the principal pair is absent in the table TableLK. If it is absent, apply rule* $(K_I \Rightarrow)$ *or* $(K_N \Rightarrow)$*, add principal pair to TableLK and go to step 1.*
5. *If possible to apply rule* $(\Rightarrow K_I)$*, check if the principal formula is absent in the table TableRK and the length of the chain is lower than Max. If the principal formula is absent and the length of the chain is lower than Max, apply rule* $(\Rightarrow K_I)$*, add principal formula and new relational atom to TableRK, increment the length of the chain by 1, and go to step 1.*
6. *If possible, apply rule* (OYR) *and call procedure GS-LCK-PROC() for the premises of the application:*

   For each k set Output(k) = False and call GS-LCK-PROC(Premise(k), TableLK, TableRK, Output(k)), where k is the index of the premise;

   IF (for each k Output(k) == True)

THEN Set Output = True and go to Finish;
ELSE Set Output = False and go to Finish;

7. *If possible, apply any of the rules* $(\Rightarrow K_N), (OE), (CR), (Sub(p) \Rightarrow), (Sub(o^r) \Rightarrow), (Ref), (Trans), (Eucl)$ *or* (Mon) *and go to step 1.*
8. *Finish.*

END

Procedure GS-LCK-PROC gets the sequent, $TableLK$, $TableRK$, starting $Output$ and returns "True", if the sequent is provable. Otherwise - "False", if it is not provable. Procedure is constructed in such a way, that it produces proofs, where number of applications of the knowledge rules of sequent calculus GS-LCK is finite. Also number of applications of other rules are bounded by requirements to rules and finite initial sets of agents, observations and results, which allows procedure to perform terminating proof search [21].

Lemma 4 (Permutation of the rule $(K_I \Rightarrow)$). *Rule* $(K_I \Rightarrow)$ *permutes down with respect to all rules of GS-LCK, except rules* $(\Rightarrow K_I)$ *and* (OE)*. Rule* $(K_I \Rightarrow)$ *permutes down with rules* $(\Rightarrow K_I)$ *and* (OE) *in case the principal atom of* $(K_I \Rightarrow)$ *is not active in it.*

Proof.
The Lemma 4 is proved in the same way as the Lemma 6.3. in [30]. □

Lemma 5 (Number of applications of the rule $(K_I \Rightarrow)$). *If a sequent* S *is provable in GS-LCK, then there exists the proof of* S *such that rule* $(K_I \Rightarrow)$ *is applied no more than once on the same pair of principal formulas on any branch.*

Proof.
The Lemma 5 is proved by induction on the number N of pairs of applications of rule $(K_I \Rightarrow)$ on the same branch with the same principal pair.

$< N = 0 >$ The proof of the lemma is obtained.

$< N > 0 >$

We diminish the inductive paramater in the same way as in the proof of Corollary 6.5. in [30], using Lemma 4. QED $\square$

Lemma 6 (Number of applications of the rule $(\Rightarrow K_I)$). *If a sequent S is provable in GS-LCK, then there exists the proof of S such that for each formula $s : K_I A$ in its positive part there are at most $n(K_I)$ applications of $(\Rightarrow K_I)$ iterated on a chain of accessible worlds $s \overset{I}{\sim} s_1, s_1 \overset{I}{\sim} s_2$, ..., with principal formula $s_i : K_I A$. The latter proof is called regular.*

Proof.
The Lemma 6 is proved by induction on the number N of series of applications of rule $(\Rightarrow K_I)$, which make the initial proof non-regular.

$< N = 0 >$ The proof of the lemma is obtained.

$< N > 0 >$

We diminish the inductive paramater in the same way as in the proof of Proposition 6.9. in [30]. QED $\square$

Theorem 9 (Termination of GS-LCK-PROC). *The procedure GS-LCK-PROC performs terminating proof search for each formula over $(R, \Sigma, \vec{O})$.*

Proof.
From construction of the procedure GS-LCK-PROC follows that the number of applications of the rules $(K_I \Rightarrow)$ and $(\Rightarrow K_I)$ is finite.

All the propositional rules reduce the complexity of the root sequent. Since the sets $N, (R, \Sigma), \vec{O}$ and the number of applications of the rules $(K_I \Rightarrow)$, $(\Rightarrow K_I)$ are finite, and the requirements are imposed on the rules, the number of applications of the rules $(K_N \Rightarrow), (\Rightarrow K_N), (OE), (OYR), (CR), (Sub(p) \Rightarrow), (Sub(o^r) \Rightarrow$

$), (Ref), (Trans), (Eucl)$ and (Mon) is also finite.

According to finite number of applications of all rules, the procedure GS-LCK-PROC performs the terminating proof search for any sequent. QED □

Theorem 10 (Soundness and completeness of GS-LCK-PROC). *The procedure GS-LCK-PROC is sound and complete over* $(R, \Sigma, \vec{O})$.

Proof.
From construction of the procedure GS-LCK-PROC follows that if procedure returns "True" for a sequent S, then S is provable in GS-LCK. If procedure returns "False", then sequent S is not provable in GS-LCK, according to Lemma 5 and Lemma 6. QED □

Theorem 11 (Decidibility of LCK). *Logic LCK is decidable.*

Proof.
From Theorem 10 and Theorem 9 follows that GS-LCK-PROC is a decision procedure for logic LCK. QED □

Chapter 5

Conclusions

Logical approaches deal with problems of expressiveness, quantum entanglement, impossibility of implication operator and deductive system, undecidability, failure of the distributive law, when try to handle knowledge about quantum systems. One of the latest results in this field is logic of correlated knowledge. LCK abstracts away from algebraic structure of quantum mechanics and accomodates correlation models to quantum systems. Alexandru Baltag and Sonja Smets defined Hilbert style proof system for LCK in [5]. However, automated proof system had not been proposed for logic of correlated knowledge, yet.

Automated proof system for LCK has been created in the dissertation research. The system consists of the sequent calculus GS-LCK and the proof search procedure GS-LCK-PROC. Sequent calculus is sound, complete and satisfy the properties of invertibility of rules, admissibility of weakening, contraction and cut. The procedure GS-LCK-PROC is terminating and allows to check if the sequent is provable. Also it has been proved, that logic of correlated knowledge is decidable. Using the terminating procedure GS-LCK-PROC the validity of all formulas of LCK can be checked.

Logic of correlated knowledge is applicable in analysing and handling knowledge about measurements performed on elementary particles of quantum systems. Automated proof system for logic of correlated knowledge can be applied to reason about quantum systems in automated way, using computers.

Bibliography

[1] S. Abramsky and R. Duncan. A categorical quantum logic. *Mathematical Structures in Computer Science*, 16:469–489, 2006.

[2] D. Aerts. Description of compound physical systems and logical interaction of physical systems. *Current Issues on Quantum Logic*, 8:381–405, 1981.

[3] A. Araujo and M. Finger. A formal system for quantum communication environments. *VIII - Brazilian National Meeting for Artificial Intelligence*, pages 1–11, 2011.

[4] A. de Araújo and M. Finger. A formal system for quantum communication environments. *Encontro Nacional de Inteligencia Artificial (ENIA2011)*, pages 1–10, 2011.

[5] A. Baltag and S. Smets. Correlated knowledge: an epistemic-logic view on quantum entanglement. *International Journal of Theoretical Physics*, 49(12): 3005–3021, 2010.

[6] S. Barnett. *Quantum Information*. Oxford University Press, Oxford, 2009.

[7] G. Battilotti. Characterization of quantum states in predicative logic. *Int. J. Theor. Phys.*, 50:3669–3681, 2011.

[8] G. Birkhoff and J. von Neumann. The logic of quantum mechanics. *Annals of Mathematics*, 37:823–843, 1936.

[9] W. Carnielli and C. Pizzi. Modalities and multimodalities. *Logic, Epistemology, and the Unity of Science*, 2008.

[10] B. Coecke, C. Heunen, and A. Kissinger. Compositional quantum logic. *Computation, Logic, Games, and Quantum Foundations*, pages 21–36, 2013.

[11] C. Cohen-Tannoudji, B. Diu, and F. Laloë. Quantum mechanics. *Wiley, New York*, 1977.

[12] M. L. Dalla Chiara and R. Giuntini. Unsharp quantum logics. *Foundations of Physics*, 24:1161–1177, 1994.

[13] R. Duncan. Believe it or not, bell states are a model of multiplicative linear

logic. *Technical Report PRG-RR-04-18*, 2004.

[14] R. Fagin, J. Y. Halpern, and M. Y. Vardi. What can machines know? on the properties of knowledge in distributed systems. *Journal of the ACM*, 39(2): 328–376, 1992.

[15] G. Gentzen. Untersuchungen uber das logische schliesen. i. *Mathematische Zeitschrift*, 39(2):176–210, 1934.

[16] G. Georgescu. N-valued logics and lukasiewicz-moisil algebras. *Axiomathes*, 16(1-2):123, 2006.

[17] G. Georgescu and C. Vraciu. On the characterization of centered lukasiewicz algebras. *J. Algebra*, 16:486–495, 1970.

[18] H. Giedra. Cut free sequent calculus for logic s5n(ed). *Lithuanian Mathematical Journal*, 51 (spec. issue):336–341, 2010.

[19] H. Giedra and J. Sakalauskaitė. Sequent calculus for logic of correlated knowledge. *Lithuanian Mathematical Journal*, 52 (spec. issue):243–248. 2011.

[20] H. Giedra, J. Sakalauskaitė, and R. Alonderis. Proof system for logic of correlated knowledge. *Submitted to Logic Journal of the IGPL*, 2014.

[21] H. Giedra, J. Sakalauskaitė, and R. Alonderis. Decidability of logic of correlated knowledge. *Informatica*, 2014. In print.

[22] R. Hakli and S. Negri. Proof theory for distributed knowledge. In *Computational Logic in Multi-Agent Systems: 8th International Workshop, CLIMA VIII, Porto, Portugal, September 10-11, 2007. Revised Selected and Invited Papers*, pages 100–116. Springer-Verlag, 2008.

[23] J. Y. Halpern and Y. Moses. A guide to completeness and complexity for modal logics of knowledge and belief. *Artificial Intelligence*, 54:319–379, 1992.

[24] K. Husimi. Studies on the foundations of quantum mechanics i. *Physico-Mathematical Soc. Japan 9*, pages 766–78, 1937.

[25] S. Kripke. Semantical analysis of modal logic i. normal propositional calculi. *Zeitschrift fur mathematische Logik und Grundlagen der Mathematik*, 9:67–96, 1963.

[26] G. Mackey. Quantum mechanics and hilbert space. *American Mathematical Monthly*, 64(2):45–57, 1957.

[27] G. Mackey. The mathematical foundations of quantum mechanics. *W.A. Benjamin, NY*, 1963.

[28] R. Mayet. Some characterizations of the underlying division ring of a

hilbert lattice by automorphisms. *International Journal of Theoretical Physics*, 37(1):109–114, 1998.

[29] J. Mehra and H. Rechenberg. The historical development of quantum theory. *Springer-Verlag*, 1982.

[30] S. Negri. Proof analysis in modal logic. *Journal of Philosophical Logic*, 34(5): 507–544, 2005.

[31] S. Negri and J. von Plato. *Structural Proof Theory*. Cambridge University Press, 2001.

[32] M. Nielsen and I. Chuang. Quantum computation and quantum information. *Cambridge University Press*, pages 112–113, 2000.

[33] A. Peres. *Quantum Theory: Concepts and Methods*. Springer, 1993.

[34] A. Pietarinen. Propositional logic of imperfect information: Foundations and applications. *Notre Dame Journal of Formal Logic*, 42(4):193–210, 2001.

[35] C. Piron. *Axiomatique quantique (PhD-Thesis)*. PhD thesis, GPO Engineering Department (London), 1964.

[36] C. Piron. Foundations of quantum physics. *W.A. Benjamin Inc., Massachusetts*, 1976.

[37] R. Pliuškevičius and A. Pliuškevičienė. Termination of derivations in a fragment of transitive distributed knowledge logic. *Informatica*, 19(4):597–616, 2008.

[38] F. Prost and C. Zerrari. A logical analysis of entanglement and separability in quantum higher-order functions. *Technical report, LIG*, 2008.

[39] F. Prost and C. Zerrari. Reasoning about entanglement and separability in quantum higher-order functions. *In Proceedings of Unconventional Computation 2009 (UC'09), Lecture Notes in Computer Science. Springer*, 2009.

[40] C. Randall and D. Foulis. Tensor products of quantum logics do not exist. *Notices Amer. Math. Soc.*, 26(6), 1979.

[41] S. Smets. Logic and quantum physics. *Journal of the Indian Council of Philosophical Research Special Issue*, XXVII(2), 2010.

[42] M.P. Solèr. Characterization of hilbert spaces by orthomodular spaces. *Communications in Algebra*, 23(1):219–243, 1995.

[43] R. Srinivasan. Quantum superposition principle justified in a new non-aristotelian finitary logic. *International Journal of Quantum Information*, 3(1): 263–267, 2005.

[44] F. Valckenborgh. *Compound Systems in Quantum Axiomatics*. PhD thesis,

Vrije Universiteit Brussel, 2001.

[45] W. van der Hoek and J.-J. Ch. Meyer. A complete epistemic logic for multiple agents–combining distributed and common knowledge. *Epistemic Logic and the Theory of Games and Decisions*, pages 35–68, 1997.

[46] R. van der Meyden and M. Patra. Knowledge in quantum systems. *Theoretical Aspects of Rationality and Knowledge*, 6433:104–117, 2003.

[47] R. van der Meyden and M. Patra. A logic for probability in quantum systems. *Baaz, M. and Makowsky, J., editors, Computer Science Logic*, volume 2803 of Lecture Notes in Computer Science:427–440, 2003.

[48] L. van Hove. Von neumann's contributions to quantum mechanics. *Bulletin of the American Mathematical Society 64*, pages 95–99, 1958.

[49] J. von Neumann. Grundlagen der quantenmechanik, berlin. *Springer Verlag*, 1932.

[50] A. Whitaker. *The New Quantum Age*. Oxford University Press, Oxford, 2012.