Justification Logic, Semirings and Realizations

Inaugural dissertation
of the Faculty of Science,
University of Bern

presented by

Michael Baur

from Stocken-Höfen

Supervisor:

Prof. Dr. Thomas Studer

Institute of Computer Science

Justification Logic, Semirings and Realizations

Inaugural dissertation
of the Faculty of Science,
University of Bern

presented by

Michael Baur

from Stocken-Höfen
Supervisor:

Prof. Dr. Thomas Studer

Institute of Computer Science

Accepted by the Faculty of Science.

Bern, the 23rd of August 2023 — The Dean
Prof. Dr. Marco Herwegh

Acknowledgements

Most importantly I want to thank my supervisor Professor Thomas Studer for the great support of this work, including his introduction to justification logic, co-working with me, many good advices, the solid guidance and also his constant positive attitude.

I am grateful to all the members of the Logic and Theory Group of the institute of Computer Science of the University of Bern for creating a great atmosphere at the university, making me keep this time in best memory.

I also thank the anonymous reviewers of the research for this thesis for improving the content by many helpful comments and suggestions.

The research for this thesis was supported by the Swiss National Science Foundation.

Table of Contents

Chapter 1
Introduction

This thesis is based on [15–17].

1.1 An introductory example

Assume group A arrives at the mountain hut and is planing to climb the summit the following day. Therefore their goal is to find out if the conditions are good or bad. Everybody knows the theory including if the conditions are bad then they won't reach the summit. Group A sees from the hut that group B is on the summit. By using the theory they derive that the conditions are not bad. So they believe that the conditions are not bad. But then group C returns to the hut. They tried to reach the summit but turned around because they considered the conditions bad. Group C tells group A that they turned around because of bad conditions, which creates a contradiction for group A, leaving them in confusion.

Let us analyse this example by using logic. Therefore let X = bad conditions, Y = group B reaches the summit, $\neg$ the negation, $\wedge$ the and-connective, $\rightarrow$ the implication and the theory $T = \{X \rightarrow \neg Y\}$. Note that the theory is equivalent to $\{Y \rightarrow \neg X\}$. Here classical propositional logic models the reasoning of group A: Given X and Y, $\neg X$ is derived from $Y \rightarrow \neg X$ and Y. They get $X \wedge \neg X$, which is a contradiction. We see that classical propositional logic captures only a fraction of this example.

So we add a modal operator $\Box$, which can be interpreted as belief. We also add a subscript to $\Box$ defining the group, that has the belief. First of all everybody knows the theory: $\Box_A T$, $\Box_B T$ and $\Box_C T$. By seeing group B on the summit we have $\Box_A Y$. From group C we get $\Box_C X$ and $\Box_A X$. The $\Box$ operator passes the modus ponens, so $\Box_A(Y \rightarrow \neg X) \rightarrow (\Box_A Y \rightarrow \Box_A \neg X)$ is an axiom. Given $\Box_A T$ and $\Box_A Y$ we derive $\Box_A \neg X$. We therefore get $\Box_A(\neg X \wedge X)$. In the context of a belief modality this is not a contradiction, but it makes group A look pretty stupid.

Justification logic replaces the modal operator $\Box$ by an explicit justification term. Let b be the term justifying Y by seeing group B on the summit $(b : Y)$ and c for the information of group C $(c : X)$. Further we assume a justification term t for the theory $(t : (Y \rightarrow \neg X))$. When applying modus ponens with justifications it is standard to combine the terms by using multiplication, so $t : (Y \rightarrow \neg X) \rightarrow (b : Y \rightarrow t \cdot b : \neg X)$ is an axiom. We therefore derive $t \cdot b : \neg X$ and still have $c : X$. Instead of a belief modality we have now two different terms justifying these contradictory propositions. If we combine these through $\neg X \rightarrow (X \rightarrow \neg X \wedge X)$ and omit justifications for axioms we get $t \cdot b \cdot c : (\neg X \wedge X)$. The novel approach of the work in this thesis is to interpret such a term in a semiring, for example the Viterbi semiring $V = ([0, 1], max, \cdot, 0, 1)$, which models

trust. Because $\neg X \wedge X$ is a contradiction its confidence score must be 0, yielding $t \cdot b \cdot c = 0$ and then $t = 0$, $b = 0$ or $c = 0$. Therefore by interpreting justifications in a semiring, group A reaches the correct conclusion that group B reached the summit despite bad conditions, the shapes on the summit were not people or group C did not estimate the conditions properly.

1.2 Mathematical preliminaries

In this section we set up the mathematical background. This includes the definitions of a semiring, ω-continuity and Scott-continuity, some properties thereof and the Kleene fixed point theorem as an important result.

Definition 1. *Let S be a set and $+ : S \times S \to S$. $(S, +)$ is a* monoid *if:*

1. $(a + b) + c = a + (b + c)$ *for all* $a, b, c \in S$,
2. *there is* $e \in S$ *with* $e + a = a + e = a$ *for all* $a \in S$.

We also write $(S, +, e)$ for a monoid with neutral element e. A monoid is commutative if $a + b = b + a$ for all $a, b \in S$.

Definition 2 (Semiring). *$K = (S, +, \cdot, 0, 1)$, where S is the domain, is a semiring, if for all $a, b, c \in S$:*

1. $(S, +, 0)$ *is a commutative monoid*
2. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *and* $a \cdot 1 = 1 \cdot a = a$
3. $(a + b) \cdot c = a \cdot c + b \cdot c$ *and* $c \cdot (a + b) = c \cdot a + c \cdot b$
4. $a \cdot 0 = 0 \cdot a = 0$

Now we define some special cases of semirings, see also [21].

Definition 3. *Semirings can have the following properties:*

- *A semiring is* naturally ordered *if the relation $\leq$ given by $a \leq b \Leftrightarrow \exists s \in S : a + s = b$ is a partial order. That is the case iff $\leq$ is antisymmetric ($a \leq b$ and $b \leq a$ imply $a = b$).*
- *A semiring is* complete *if it has an infinitary sum operation satisfying:*
  $\sum_{i \in \emptyset} a_i = 0$,
  $\sum_{i \in \{j\}} a_i = a_j$,
  $\sum_{i \in \{j,k\}} a_i = a_j + a_k$ *for* $j \neq k$,
  $\sum_{j \in J} \sum_{i \in I_j} a_i = \sum_{i \in I} a_i$ *if* $\bigcup_{j \in J} I_j = I$ *and* $I_j \cap I_k = \emptyset$ *for* $j \neq k$,
  $\sum_{i \in I} (a \cdot a_i) = a \cdot (\sum_{i \in I} a_i)$,
  $\sum_{i \in I} (a_i \cdot a) = (\sum_{i \in I} a_i) \cdot a$.
- *A semiring is* ω-continuous *if it is naturally ordered, complete, and for all sequences $(a_i)_{i \in \mathbb{N}}$ with $a_i \in S$: $sup\{\sum_{i=0}^{n} a_i \mid n \in \mathbb{N}\}$ exists and is equal to $\sum_{i \in \mathbb{N}} a_i$, where sup is the smallest upper bound according to the natural order $\leq$.*

We are especially interested in ω-continuous semirings. By $\leq$ we denote the partial order given by the semiring being naturally ordered. $\leq$ is called a well-order on $X \subseteq S$ if it is a total order on X and defines a least element in X.

Definition 4. *Let $K = (R, +, \cdot, 0, 1)$ and $L = (S, +, \cdot, 0, 1)$ be ω-continuous semirings. A function $f : R \to S$ is Scott-continuous if for all countable subsets $X \subseteq R$ such that $\leq$ is a well-order on X: $sup(f(X)) = f(sup(X))$.*

An important property of Scott-continuous functions is the monotonicity, which is very easy to prove.

Lemma 1. *Scott-continuous functions are monotone ($a \leq b$ implies $f(a) \leq f(b)$).*

Proof. Let $f : R \to S$ be Scott-continuous and $a \leq b$. By definition of Scott-continuity we get $sup(\{f(a), f(b)\}) = sup(f(\{a, b\})) = f(sup(\{a, b\})) = f(b)$. This means $f(b)$ is an upper bound for $\{f(a), f(b)\}$, therefore $f(a) \leq f(b)$. □

Further we investigate in the preservation of Scott-continuity under operators, including those from the semiring. Scott-continuity is not only preserved under the addition but even under the infinitary sum operation of the ω-continuous semiring. It is also preserved under the multiplication. Both these properties come mainly from the definition of the infinitary sum operation and the ω-continuity. The multiplication case additionally needs a rearrangement of an infinite double sum. For function composition it is trivial. We summarize these preservation properties in the following lemma.

Lemma 2. *Let $K = (S, +, \cdot, 0, 1)$ be an ω-continuous semiring and $f_i : S \to S$ with $i \in \mathbb{N}$ Scott-continuous functions. Then*

1. *$\sum_{i\in\mathbb{N}} f_i$ is Scott-continuous, where $(\sum_{i\in\mathbb{N}} f_i)(x) := \sum_{i\in\mathbb{N}}(f_i(x))$,*
2. *$f_1 \cdot f_2$ is Scott-continuous, where $(f_1 \cdot f_2)(x) := f_1(x) \cdot f_2(x)$,*
3. *$f_1 \circ f_2$ is Scott-continuous.*

Proof. A countable set $X = \{x_0, x_1, ...\}$ with a well-order can be written as partial sums: There is a sequence $(a_i)_{i\in\mathbb{N}}$ such that $X = \{\sum_{i=0}^{n} a_i \mid n \in \mathbb{N}\}$ and $x_i \leq x_j$ for $i \leq j$. We therefore have $x_n = \sum_{i=0}^{n} a_n$. $sup(X) = \sum_{i\in\mathbb{N}} a_i$ follows by ω-continuity. $f_i(X)$ has also a well-order because of the monotonicity of Scott-continuous functions.

1. $(\sum_{i\in\mathbb{N}} f_i)(sup(X)) = \sum_{i\in\mathbb{N}} f_i(sup(X)) = \sum_{i\in\mathbb{N}} sup(f_i(X))$.
   By ω-continuity $sup(f_i(X))$ can be written as an infinite sum $\sum_{j\in\mathbb{N}} a_{ij}$. Then the derivation continues as
   $\sum_{i\in\mathbb{N}} \sum_{j\in\mathbb{N}} a_{ij} = \sum_{j\in\mathbb{N}} \sum_{i\in\mathbb{N}} a_{ij} = sup(\{\sum_{j=0}^{n}(\sum_{i\in\mathbb{N}} a_{ij}) \mid n \in \mathbb{N}\})$
   $= sup(\{(\sum_{i\in\mathbb{N}} f_i)(x_n) \mid n \in \mathbb{N}\}) = sup((\sum_{i\in\mathbb{N}} f_i)(X))$.
2. $(f_1 \cdot f_2)(sup(X)) = f_1(sup(X)) \cdot f_2(sup(X)) = sup(f_1(X)) \cdot sup(f_2(X))$.
   We write $sup(f_1(X))$ as $\sum_{i\in\mathbb{N}} b_i$ and $sup(f_2(X))$ as $\sum_{j\in\mathbb{N}} c_j$. Then the derivation continues as
   $(\sum_{i\in\mathbb{N}} b_i) \cdot (\sum_{j\in\mathbb{N}} c_j) = \sum_{j\in\mathbb{N}}((\sum_{i\in\mathbb{N}} b_i) \cdot c_j) = \sum_{j\in\mathbb{N}} \sum_{i\in\mathbb{N}} b_i \cdot c_j$

$= \sum_{(i,j)\in\mathbb{N}^2} b_i \cdot c_j = \sum_{n\in\mathbb{N}} \sum_{max(i,j)=n} b_i \cdot c_j$
$= sup(\{\sum_{max(i,j)\leq n} b_i \cdot c_j \mid n \in \mathbb{N}\}) = sup(\{\sum_{i=0}^{n} b_i \cdot \sum_{j=0}^{n} c_j \mid n \in \mathbb{N}\})$
$= sup(\{f_1(x_n) \cdot f_2(x_n) \mid n \in \mathbb{N}\}) = sup(\{(f_1 \cdot f_2)(x_n) \mid n \in \mathbb{N}\})$
$= sup((f_1 \cdot f_2)(X))$

3. $f_1(f_2(sup(X))) = f_1(sup(f_2(X))) = sup(f_1(f_2(X)))$. □

While the preservation properties of Scott-continuous functions will be important later, we use the monotonicity now to prove the fixed point theorem [30], which will be a crucial part in the realization of common knowledge.

Theorem 1 (Fixed point theorem). *Let $K = (S, +, \cdot, 0, 1)$ be a ω-continuous semiring and $f : S \to S$ a Scott-continuous function. Then f has a fixed point.*

The proof begins by building the ascending Kleene chain, a sequence starting at 0 then applying f repeatedly. It turns out that the supremum of this chain is a fixed point of f.

Proof. We show $f^n(0) \leq f^{n+1}(0)$ by induction on n. For $n = 0$ we have obviously $0 \leq f(0)$. If $f^{n-1}(0) \leq f^n(0)$ then by monotonicity of Scott-continuous functions we get $f(f^{n-1}(0)) \leq f(f^n(0))$ which is $f^n(0) \leq f^{n+1}(0)$. This allows us to define a sequence $(a_i)_{i\in\mathbb{N}}$ such that $\sum_{i=0}^{n} a_i = f^n(0)$. We define $X := \{f^n(0) \mid n \in \mathbb{N}\}$ and get $f(X) \cup \{0\} = X$. By the ω-continuity $sup(X)$ exists and is equal to $\sum_{i\in\mathbb{N}} a_i$. So we can apply it to obtain $sup(f(X)) = sup(f(X) \cup \{0\}) = sup(X)$. By using the definition of Scott-continuity we get $f(sup(X)) = sup(X)$, which shows that $sup(X)$ is a fixed point. □

Chapter 2
Modal logic

In this section we introduce the modal logics, that we will use later. They are all based on classical propositional logic (CL), which is the most used base of reasoning. We therefore start by introducing CL briefly.

2.1 Classical Propositional Logic

For the syntax let $\mathsf{Prop} = \{P_1, P_2, ...\}$ be an arbitrary set of atomic propositions. We define the formulas of CL inductively as follows:

- $\bot$,
- P_i, where $P_i \in \mathsf{Prop}$,
- $A \to B$, where A and B are formulas.

Further we define as usual:

- $\neg A := A \to \bot$,
- $\top := \neg \bot$,
- $A \vee B := \neg A \to B$,
- $A \wedge B := \neg(\neg A \vee \neg B)$,
- $A \leftrightarrow B := (A \to B) \wedge (B \to A)$.

We describe classical propositional logic by three axiom schemes and the modus ponens scheme. In an axiom scheme A, B and C can be arbitrary formulas. The axioms are all the formulas resulting from substituting A, B, C in an axiom scheme by formulas. The rules are built analogously from the modus ponens scheme.

CL1 $A \to (B \to A)$
CL2 $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
CL3 $\neg\neg A \to A$
MP $\dfrac{A \to B \quad A}{B}$

We write $\vdash_{\mathsf{CL}} A$ if A is derivable in CL.
For the semantics a model assigns a truth value to each formula. In classical propositional logic a model M consists solely of a truth assignment $* : \mathsf{Prop} \to \{\mathbb{F}, \mathbb{T}\}$ for atomic propositions. By $M \Vdash A$ we denote that A is true in M, which is defined as follows:

- $M \nVdash \bot$,
- $M \Vdash P_i \Leftrightarrow *(P_i) = \mathbb{T}$,
- $M \Vdash A \to B \Leftrightarrow M \nVdash A$ or $M \Vdash B$.

We say A is valid (in symbols: $\Vdash A$) if $M \Vdash A$ for all models M. The introduced axiomatic system is known to be sound and complete with respect to the introduced class of models (see [19]):

$$\vdash_{\mathsf{CL}} A \;\Leftrightarrow\; \Vdash A \quad \text{for all formulas } A.$$

2.2 Logics with a single modality

Modal logic extends propositional logic by modalities. We first discuss the case, where a single modality $\Box$ is added.

2.2.1 Syntax

For defining the language $\mathcal{L}_\Box$ inductively let Prop again be a set of atomic propositions. Then:

- $\bot \in \mathcal{L}_\Box$,
- $P_i \in \mathcal{L}_\Box$, where $P_i \in \mathsf{Prop}$,
- $A \to B \in \mathcal{L}_\Box$, where $A, B \in \mathcal{L}_\Box$,
- $\Box A \in \mathcal{L}_\Box$, where $A \in \mathcal{L}_\Box$.

A formula of the form $\Box A$ can be interpreted in different ways:

- A is believed to be true,
- A is known to be true,
- A is obligatory, and so on.

2.2.2 Axiomatic systems

With so many ways of interpreting modalities it is no surprise that there is not a single axiomatic system covering these cases. We introduce two of the most famous logics.
The logic K adds the axiom scheme **K** and the necessitation rule to CL:

CL1 $A \to (B \to A)$
CL2 $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
CL3 $\neg\neg A \to A$
K $\Box(A \to B) \to (\Box A \to \Box B)$
MP $\dfrac{A \to B \quad A}{B}$
Nec $\dfrac{A}{\Box A}$

In K we can have that $\Box A$ is true, but A is false. Therefore $\Box$ can be interpreted as belief instead of knowledge. The axiom **K** describes how belief passes the modus ponens rule: If $A \to B$ is believed and A is believed then B is also believed.
The logic $\mathsf{S4}$ adds the axiom schemes **t** and **4** to K:

t $\Box A \to A$
4 $\Box A \to \Box\Box A$

The axiom **t** is called the truth axiom. It suggests an interpretation of $\Box$ as knowledge rather than belief. If we interpret it as knowledge of an agent then it means if the agent knows A then A is true. Axiom **4** describes the ability of the agent to reason about his knowledge: If he knows A then he knows that he knows A.

2.2.3 Semantics

For modal logics it is standard to use Kripke semantics, also called possible world semantics. A formula of the form $\Box A$ is true in a world w, if and only if A is true in all worlds that are visible/accessible from w. The details differ depending on the logic. We introduce the Kripke semantics for the logic K and point out the differences to $\mathsf{S4}$.
Let W be a non-empty set of possible worlds, $R \subseteq W \times W$ an accessibility relation and $* : \mathsf{Prop} \to \mathcal{P}(W)$ a valuation function. Then $M = (W, R, *)$ is a Kripke model. For $\mathsf{S4}$ the accessibility relation has to be reflexive and transitive in order to deal with the axioms **t** and **4**. We define the truth value of a formula in a world w in M as follows:

- $M, w \nVdash \bot$,
- $M, w \Vdash P \Leftrightarrow w \in *(P)$,
- $M, w \Vdash A \to B \Leftrightarrow M, w \nVdash A$ or $M, w \Vdash B$,
- $M, w \Vdash \Box A \Leftrightarrow M, v \Vdash A$ for all v with $(w, v) \in R$.

Further we say that A is true in a model M if it is true in all worlds of M:

$$M \Vdash A \quad \Leftrightarrow \quad M, w \Vdash A \text{ for all } w \in W.$$

As before A is valid if it is true in all models. The logic K is known to be sound and complete with respect to Kripke models:

$$\vdash_{\mathsf{K}} A \;\Leftrightarrow\; \Vdash A \quad \text{for all formulas } A.$$

Analogously $\mathsf{S4}$ is sound and complete with respect to reflexive and transitive Kripke models. The proof in [35] for $\mathsf{S4}$ can easily be adapted to K.

2.3 The sequent calculus GK

In this section we introduce the sequent calculus GK, which is equivalent to the logic K, but built in a different way. It depends on multisets of formulas in $\mathcal{L}_\Box$. Such a multiset can be seen as a function $f : \mathcal{L}_\Box \to \mathbb{N}$ defining how many times each element is in the multiset. If Γ and Δ are multisets of formulas, then the expression $\Gamma \supset \Delta$ is a sequent. The sequent $\Gamma \supset \Delta$ can be interpreted informally as $\bigwedge \Gamma \to \bigvee \Delta$. The axioms of GK are

$$P \supset P \qquad \text{and} \qquad \bot \supset$$

where $P \in \mathsf{Prop}$. The rules of GK are the following:

$$(\to\supset)\ \frac{\Gamma \supset \Delta, A \qquad B, \Gamma \supset \Delta}{A \to B, \Gamma \supset \Delta} \qquad (\supset\to)\ \frac{A, \Gamma \supset \Delta, B}{\Gamma \supset \Delta, A \to B}$$

$$(\Box)\ \frac{\Gamma \supset A}{\Box\Gamma \supset \Box A}$$

$$(w\supset)\ \frac{\Gamma \supset \Delta}{A, \Gamma \supset \Delta} \qquad (\supset w)\ \frac{\Gamma \supset \Delta}{\Gamma \supset \Delta, A}$$

$$(c\supset)\ \frac{A, A, \Gamma \supset \Delta}{A, \Gamma \supset \Delta} \qquad (\supset c)\ \frac{\Gamma \supset \Delta, A, A}{\Gamma \supset \Delta, A}$$

The system GK is sound and complete for the modal logic K, see, e.g., [41, 43]:

$$\vdash_{\mathsf{GK}} \supset A \quad \Leftrightarrow \quad \vdash_{\mathsf{K}} A \quad \text{for all } A \in \mathcal{L}_{\Box}.$$

2.4 Common Knowledge

In this part we introduce common knowledge, which is a multi-modal logic. It represents a system with multiple agents and their knowledge or beliefs. For example agent 1 knows A is written as $\Box_1 A$. This principle can be applied to different modal logics, defining the role of the $\Box$ operator. In our case the underlying logic is K, so we do not have a truth axiom and the $\Box$ operators can be read as beliefs. Additionally there is the common knowledge operator C. CA means everybody knows A, everybody knows that everybody knows A and so on. By defining EA as everybody knows A we see that $CA = EA \wedge EEA \wedge ...$ is a fixed point of the function $f(X) = EA \wedge EX$.
Let $h \in \mathbb{N}_{\geq 1}$ be the number of agents and Prop a set of atomic propositions. We define the language $\mathcal{L}_{\mathcal{C}}$ of common knowledge inductively:

- $\bot \in \mathcal{L}_{\mathcal{C}}$,
- $P \in \mathcal{L}_{\mathcal{C}}$, where $P \in \mathsf{Prop}$,
- $A \to B \in \mathcal{L}_{\mathcal{C}}$, where $A, B \in \mathcal{L}_{\mathcal{C}}$,
- $\Box_i A \in \mathcal{L}_{\mathcal{C}}$, where $A \in \mathcal{L}_{\mathcal{C}}$ and $1 \leq i \leq h$,
- $CA \in \mathcal{L}_{\mathcal{C}}$, where $A \in \mathcal{L}_{\mathcal{C}}$.

We define $EA := \bigwedge_{i=1}^{h} \Box_i A$.
There are various axiomatic systems for common knowledge. They differ in three ways:

- The underlying logic shows by the axioms describing the reasoning of each agent. If it is for example $\mathsf{S4}$ then we have the truth axiom $\Box_i A \to A$ for $1 \leq i \leq h$.
- The common knowledge operator can be reflexive or not. This has an impact on the closure axioms and induction axioms. We choose the second option and therefore the closure axiom includes $CA \to EA$ instead of $CA \to A$.

– There are different ways to axiomatize the same logic. For common knowledge the induction rule is often used, which describes CA as a greatest fixed point by deriving $B \to CA$ from $B \to E(A \wedge B)$. We instead use the induction axiom. A proof for the equivalence can be found in [39].

The Hilbert-style system with induction axiom H_{Ax} consists of the following axiom schemes and rules:

CL	Every instance of a propositional tautology
Modal axioms	$\Box_i(A \to B) \to (\Box_i A \to \Box_i B)$
C-Modal axioms	$C(A \to B) \to (CA \to CB)$
Closure axioms	$CA \to EA \wedge ECA$
Induction axioms	$EA \wedge C(A \to EA) \to CA$
MP	$\dfrac{A \to B \quad A}{B}$
C-Nec	$\dfrac{A}{CA}$

For the semantics Kripke models are standard. We omit the introduction thereof, as it is not relevant to us and refer to [22, 39, 40].

2.5 The System S_{Ax}

The language of common knowledge is somehow incomplete: It represents the infinite formula $\bigwedge_{n=1}^{\infty} E^n A$ as CA but other infinite formulas like $\bigwedge_{n=1}^{\infty} E^{2n} A$ have no representation. We fill this gap by introducing the system S_{Ax}. We begin by defining the language $\mathcal{L}_{\mathcal{S}}$ based on a set of atomic propositions Prop inductively. h denotes the number of agents, $E := \{\Box_1, ..., \Box_h\}$, * is the Kleene star, ϵ the empty word and $C := E^* \setminus \{\epsilon\}$.

– $\bot \in \mathcal{L}_{\mathcal{S}}$,
– $P \in \mathcal{L}_{\mathcal{S}}$, where $P \in \mathsf{Prop}$,
– $A \to B \in \mathcal{L}_{\mathcal{S}}$, where $A, B \in \mathcal{L}_{\mathcal{S}}$,
– $SA \in \mathcal{L}_{\mathcal{S}}$, where $S \subseteq E^*$ and $A \in \mathcal{L}_{\mathcal{S}}$.

SA is informally read as $\bigwedge_{s \in S} sA$. Between common knowledge and S_{Ax} lies a difference in cardinality: Common knowledge represents only countably infinite different situations of agents knowing about A in a single formula. But all situations are described exactly by the powerset of E^*, which has the same cardinality as the set of real numbers. The language $\mathcal{L}_{\mathcal{S}}$ therefore features arbitrary subsets of E^*, covering the uncountably infinite number of possible situations.
The trivial translation $'$ from $\mathcal{L}_{\mathcal{C}}$ to $\mathcal{L}_{\mathcal{S}}$ replaces the modal operators by sets in the obvious way. For $R, S \subseteq E^*$ we define the concatenation as
$RS := \{rs \mid r \in R, s \in S\}$.
The system S_{Ax} consists of the following axiom schemes and rules:

CL	Every instance of a propositional tautology
Set axioms 1	$RA \wedge SA \leftrightarrow (R \cup S)A$
Set axioms 2	$R(SA) \leftrightarrow (RS)A$
Modal axioms	$S(A \to B) \to (SA \to SB)$
Induction axioms	$EA \wedge C(A \to EA) \to CA$
MP	$\dfrac{A \to B \quad A}{B}$
C-Nec	$\dfrac{A}{CA}$

We have to add two set axiom schemes but the C-Modal axioms fall together with the modal axioms and we can omit the closure axioms. Later we will also use the following equivalent axiomatization, which includes three explicit axiom schemes for CL and avoids the equivalence connective:

CL1	$A \to (B \to A)$
CL2	$(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
CL3	$((A \to \bot) \to \bot) \to A$
Set axioms 1.1	$RA \wedge SA \to (R \cup S)A$
Set axioms 1.2	$(R \cup S)A \to RA \wedge SA$
Set axioms 2.1	$R(SA) \to (RS)A$
Set axioms 2.2	$(RS)A \to R(SA)$
Modal axioms	$S(A \to B) \to (SA \to SB)$
Induction axioms	$EA \wedge C(A \to EA) \to CA$
MP	$\dfrac{A \to B \quad A}{B}$
C-Nec	$\dfrac{A}{CA}$

Obviously $\mathsf{S_{Ax}}$ is an extension of $\mathsf{H_{Ax}}$:

$$T \vdash_{\mathsf{H_{Ax}}} A \text{ implies } T' \vdash_{\mathsf{S_{Ax}}} A'.$$

The inverse translation * is more complicated. Because $\mathcal{L}_\mathcal{C}$ can't represent certain formulas of $\mathcal{L}_\mathcal{S}$, it is partial. But the domain can be chosen way bigger than ${\mathcal{L}_\mathcal{C}}'$. We define D as $\emptyset \in D$, $\{\epsilon\} \in D$, $\{\Box_i\} \in D$, $C \in D$, $R \in D$ and $S \in D$ implies $R \cup S \in D$ and $RS \in D$. We denote the language of $\mathcal{L}_\mathcal{S}$ restricted to sets in D as $\mathcal{L}_D$. For each $S \in D$ we fix a finite tree describing the composition of S in basic elements ($\emptyset$, $\{\epsilon\}$, $\{\Box_i\}$ and C). Such a tree has S on the root, basic elements on the leaves and each node (except leaves) has two successors, which are ordered. If a node is labelled by X, successor 1 by R and successor 2 by S, then we must have $X = R \cup S$ or $X = RS$. This tree is needed because $C = E \cup EC$. Then we can define $^\star : \mathcal{L}_D \to \mathcal{L}_\mathcal{C}$ according to the tree as follows:

- $\bot^\star = \bot$
- $P^\star = P$
- $(A \to B)^\star = A^\star \to B^\star$
- $(\emptyset A)^\star = \top$
- $(\{\epsilon\}A)^\star = A^\star$
- $(\{\Box_i\}A)^\star = \Box_i A^\star$

- $(CA)^\star = CA^\star$
- $((R \cup S)A)^\star = (RA)^\star \wedge (SA)^\star$
- $((RS)A)^\star = (R(SA))^\star$

For $T \subseteq \mathcal{L}_D$ and $A \in \mathcal{L}_D$ we get

$$T \vdash_{\mathsf{S_{Ax}}} A \text{ implies } T^\star \vdash_{\mathsf{H_{Ax}}} A^\star.$$

Therefore $\mathsf{S_{Ax}}$ is a conservative extension of $\mathsf{H_{Ax}}$.

Chapter 3
Semirings of Evidence

In traditional justification logic, evidence terms have the syntactic form of polynomials, but they are not equipped with the corresponding algebraic structure. In this chapter we present a novel semantic approach to justification logic that models evidence by a semiring. Hence justification terms can be interpreted as polynomial functions on that semiring. This provides an adequate semantics for evidence terms and clarifies the role of variables in justification logic. Moreover, the algebraic structure makes it possible to compute with evidence. Depending on the chosen semiring this can be used to model trust, probabilities, cost, etc.

Our approach is heavily inspired by the semiring approach for provenance in database systems [28]. There the idea is to label database tuples and to propagate expressions in order to annotate intermediate data and final outputs. One can then evaluate the provenance expressions in various semirings to obtain information about levels of trust, data prices, required clearance levels, confidence scores, probability distributions, update propagation, and many more [29].

This semiring framework has been adapted to many different query languages and data models. The core theoretical work of those approaches includes results on query containment, the construction of semirings, and fixed points [2, 3, 20, 23, 24, 26, 27].

There are only few systems available where justification terms are equipped with additional structure. Two prominent examples are based on λ-terms (in contrast to the combinatory terms of the Logic of Proofs). The reflective lambda calculus [1] includes reduction rules on proof terms. The intensional lambda calculus [9] has axioms for evidence equality and also features a reduction relation on the terms. Another example is Krupski's recent work on sharp justification logics [31].

This chapter is based on [16, 17].

3.1 Introduction to Justification Logic

Justification logic replaces the $\Box$-operator from modal logic with explicit evidence terms [4, 10, 35]. That is, instead of formulas $\Box A$, justification logic features formulas $t : A$, where t encodes evidence for A. Depending on the context, the term t may represent a formal proof of A [4, 34] or stand for an informal justification (like direct observation, public announcement, private communication, and so on) for an agent's knowledge or belief of A. With the introduction of possible world models, justification logic has become an important tool to discuss and analyze epistemic situations [5, 6, 13, 14, 42].

The terms of justification logic represent explicit evidence for an agent's belief or knowledge. Within justification logic, we can reason about this evidence.

For instance, we can track different pieces of evidence pertaining to the same fact, which is essential for distinguishing between factive and non-factive justifications. This is applied nicely in Artemov's analysis of Russel's Prime Minister example [7]. Evidence terms can also represent the reasoning process of an agent. Therefore, agents represented by justification logic systems are not logically omniscient according to certain complexity based logical omniscience tests [11–13].

In traditional justification logic, terms are built using the binary operations $+$ (called sum) and $\cdot$ (called application) and maybe other additional operations. Thus terms have the syntactic form of polynomials and are, in the context of the Logic of Proofs, indeed called proof polynomials.

This syntactic structure of polynomials is essentially used in the proof of realization, which provides a procedure that, given a theorem of a modal logic, constructs a theorem of the corresponding justification logic by replacing each occurrence of $\Box$ with an adequate justification term [4].

In this chapter we look at the syntactic structure of justification terms *algebraically*, that is, we interpret justifications by a semiring structure. The motivation for this is threefold:

1. It provides an appropriate semantics for variables in evidence terms. It was always the idea in justification logic that terms with variables justify derivations from assumptions. The variables represent the input values, i.e., (arbitrary) proofs of the assumptions [4]. But this was not properly reflected in the semantics where usually variables are treated like constants: to each term (no matter whether it contains variables or not) some set of formulas is assigned. In our semiring semantics, ground terms (i.e. terms not containing variables) are interpreted as elements of a semiring and terms with variables are interpreted as polynomial functions on the given semiring of justifications. Thus terms with variables are adequately represented and the role of variables is clarified.
2. The algebraic structure of terms makes it possible to compute with justifications. Depending on the choice of the semiring, we can use the term structure to model levels of trust (Viterbi semiring), costs of obtaining knowledge (tropical semiring), probabilistic evidence (powerset semiring), fuzzy justifications (Łukasiewicz semiring), and so on.
3. Considering ω-continuous semirings, i.e. semirings in which certain fixed points exist, provide a solution to the problem of realizing the logic of common knowledge (see Chapter 4).

3.2 The Syntax of SE

We begin by defining the justification language as usual. That is, we use a countable (infinite) set of constants $\mathsf{JConst} = \{0, 1, c_1, c_2, ...\}$ that includes two distinguished elements 0 and 1. Further we have a countable (infinite) set of variables $\mathsf{JVar} = \{x_1, x_2, ...\}$.

Definition 1 (Justification Term). *Justification terms are*

$$c \in \mathsf{JConst},\ x \in \mathsf{JVar},\ s \cdot t, \quad \textit{and} \quad s + t,$$

where s and t are justification terms. The set of all justification terms is called Tm*. A justification term that does not contain variables is called* ground term*.* GTm *denotes the set of all ground terms.*

Often we write only *term* for *justification term*. Further, we need a countable set of atomic propostions $\mathsf{Prop} = \{P_1, P_2, ...\}$.

Definition 2 (Formulas). *Formulas are $\bot$, P, $A \to B$ and $t : A$, where t is a justification term, $P \in \mathsf{Prop}$ and A, B are formulas. The set of all formulas is called* Fml*.*

The remaining logical connectives $\neg$, $\wedge$, $\vee$, and $\leftrightarrow$ are abbreviations as usual, e.g., $\neg A$ stands for $A \to \bot$.

We will make use of substitutions to present the axioms of the logic SE. Given a formula A we write $A[w/t]$ for the result of simultaneously replacing all occurrences of the variable w in A with the term t. For instance, if A is the formula $u : r \cdot w : B$, then $A[w/s + t]$ denotes the formula $u : r \cdot (s + t) : B$. For substituting all variables simultaneously we use a function $\sigma : \mathsf{JVar} \to \mathsf{Tm}$ by defining $A\sigma := A[x_1/y_1]...[x_n/y_n][y_1/\sigma(x_1)]...[y_n/\sigma(x_n)]$, where $x_1, ..., x_n$ are the variables occurring in A and the y_i are fresh variables. We will use the same notations for substitutions in terms.

Now we can define a deductive system for the logic SE about the semirings of evidence. It consists of the following axioms, where w, x, y, z are variables and A, B formulas.

The axioms of SE are:

CL	Every instance of a propositional tautology
j	$x : (A \to B) \to (y : A \to x \cdot y : B)$
j+	$x : A \wedge y : A \to (x + y) : A$
a+	$A[w/(x + y) + z] \to A[w/x + (y + z)]$
c+	$A[w/x + y] \to A[w/y + x]$
0+	$A[w/x + 0] \leftrightarrow A[w/x]$
am	$A[w/(x \cdot y) \cdot z] \leftrightarrow A[w/x \cdot (y \cdot z)]$
a0	$A[w/x \cdot 0] \leftrightarrow A[w/0]$ and $A[w/0 \cdot x] \leftrightarrow A[w/0]$
a1	$A[w/x \cdot 1] \leftrightarrow A[w/x]$ and $A[w/1 \cdot x] \leftrightarrow A[w/x]$
dl	$A[w/x \cdot (y + z)] \leftrightarrow A[w/x \cdot y + x \cdot z]$
dr	$A[w/(y + z) \cdot x] \leftrightarrow A[w/y \cdot x + z \cdot x]$

The rules of SE are:

$$\textbf{MP}\quad \frac{A \qquad A \to B}{B}$$

and

$$\textbf{jv}\quad \frac{A}{A[x/t]}$$

The axiom schemes **a+**, **c+**, **0+**, **am**, **a0**, **a1**, **dl** and **dr** are called semiring axioms. In the axiom scheme **j+**, we find an important difference to traditional justification logic where $\vee$ is used instead of $\wedge$, see also Section 3.4 later. The idea for **j+** is to read $s + t : A$ as *both s and t justify A.* This is useful, e.g., in the context of uncertain justifications where having two justifications is better than just having one. The rule **jv** shows the role of variables in SE, which differs from traditional justification logic. In our approach a formula $A(x)$ being valid means that $A(x)$ is valid *for all justifications x.*

Now we show by an example how the semiring axioms work. Assume a formula A contains an occurrence of $s+t$ (it may occur anywhere, even as a subterm of some other term). Starting from A, we want to derive the formula B, which is the same as A except that the occurrence of $s + t$ is replaced by $t + s$. So we let C be the formula A with this occurrence $s + t$ being replaced by a variable x that doesn't occur in A. Now $C[x/s+t] \to C[x/t+s]$ is derived from an instance of the axiom scheme **c+** by **jv** and it is the same as $A \to B$.

Let us mention two immediate consequences of our axioms. First a version of axiom **0+** with $x + 0$ is replaced by $0 + x$ is provable. Second, the direction from right to left in axiom **a+** is also provable.

Lemma 1. *The following formulas are derivable in* SE*:*

$$A[w/0 + x] \leftrightarrow A[w/x] \qquad \textit{and} \qquad A[w/x + (y + z)] \leftrightarrow A[w/(x + y) + z].$$

A theory is just any set of formulas.

Definition 3 (Theory). *A theory T is a subset of* Fml*. We use $T \vdash_{\mathsf{SE}} F$ to express that F is derivable from T in* SE*.*

Often we drop the subscript SE in $\vdash_{\mathsf{SE}}$ when it is clear from the context. Moreover, we use $\vdash_{\mathsf{CL}}$ for the derivability relation in classical propositional logic.

A theory can compensate for the absence of constant specifications. Usually, systems of justification logic are parametrized by a constant specification, i.e., a set containing pairs of constants and axioms. One then has a rule saying that a formula $c : A$ is derivable if (c, A) is an element of the constant specification. Here we do not adopt this approach but simply use a theory that includes $c : A$.

Definition 4. *A theory T is called axiomatically appropriate if*

1. *for all axioms A there exists $c \in \mathsf{JConst}$ with $c : A \in T$*
2. *for all $B \in T$ there exists $c \in \mathsf{JConst}$ with $c : B \in T$.*

Intuitively, in an axiomatically appropriate theory, all axioms have a justification and also all elements of the theory have a justification. Using axiomatically appropriate theories, we get an analogue of modal necessitation in SE.

Lemma 2 (Internalization). *Let T be an axiomatically appropriate theory. For any formula A, there exists a ground term t such that*

$$T \vdash A \quad \textit{implies} \quad T \vdash t : A.$$

Proof. Induction on a derivation of A.

1. $A \in T$ or A is an axiom: t exists by the definition of an axiomatically appropriate theory.
2. If A is obtained by **MP** from $B \to A$ and B, then by I.H. exist $t_1, t_2 \in \mathsf{GTm}$ such that $T \vdash_{\mathsf{SE}} t_1 : (B \to A)$ and $T \vdash_{\mathsf{SE}} t_2 : B$. Thus $T \vdash_{\mathsf{SE}} t : A$ holds for $t = t_1 \cdot t_2$.
3. If $A[x/s]$ is obtained by **jv** from A, then by I.H. exists $t \in \mathsf{GTm}$ such that $T \vdash_{\mathsf{SE}} t : A$. Finally, **jv** implies $T \vdash_{\mathsf{SE}} t : A[x/s]$. □

Remark 1 (Substitution). In order to replace variables with terms, we do not need any properties of the theory T. In particular, we do not require it to be schematic, see Definition 13. The implication

$$T \vdash_{\mathsf{SE}} A \quad \text{implies} \quad T \vdash_{\mathsf{SE}} A[x/t]$$

follows directly from rule **jv**.

Next we show that SE is a conservative extension of classical propositional logic, which implies consistency of SE.

Theorem 1 (Conservativity). *The logic SE is a conservative extension of classical propositional logic, CL, i.e., for all formulas A of the language of CL, we have*

$$\vdash_{\mathsf{SE}} A \quad \textit{iff} \quad \vdash_{\mathsf{CL}} A.$$

Proof. The claim from right to left is trivial as SE extends CL. For the direction from left to right, we consider a mapping $^\circ$ from Fml to formulas of CL that simply drops all occurrences of $t :$. In particular, for any CL-formula A, we have $A^\circ = A$. Now it is easy to prove by induction on the length of SE derivations that for all $A \in \mathsf{Fml}$,

$$\vdash_{\mathsf{SE}} A \quad \text{implies} \quad \vdash_{\mathsf{CL}} A^\circ.$$

Simply observe that for any axiom A of SE, A° is a propositional tautology, and that the rules of SE respect the $^\circ$-translation. □

Now consistency of SE follows immediately.

Corollary 1 (Consistency of SE). *The logic SE is consistent.*

Proof. Assume towards contradiction that $\vdash_{\mathsf{SE}} \bot$. By conservativity of SE over CL we get $\vdash_{\mathsf{CL}} \bot$, which is a contradiction. □

Remark 2. The deduction theorem does not hold in SE. This is due to possible occurrences of variables. For example $\{x : P\} \vdash 0 : P$ says that if every term justifies P then also 0 justifies P, which is trivial. However $\vdash x : P \to 0 : P$ is not valid because it can be shown that $\nvdash 1 : P \to 0 : P$.

3.3 The Semantics of SE

Our semantics of SE is similar to traditional semantics for justification logic in the sense that $t : A$ is given meaning by making use of an evidence relation. Usually, this evidence relation assigns to each term a set of formulas, i.e. the formulas that are justified by the term. The novelty of our approach is that the evidence relation maps elements of a semiring to sets of formulas and terms are interpreted by the elements of this semiring.

Note that we use $+$ and $\cdot$ both as symbols in our language of justification logic and as operations in the semiring. It will always be clear from the context which of the two is meant.

For the following, assume we are given a semiring $K = (S, +, \cdot, 0, 1)$. We use a function $I : \mathsf{JConst} \to S$ to map the constants of the language of SE to the domain S of the semiring. We call this function I an *interpretation* if $I(0) = 0$ and $I(1) = 1$. We now extend I to a homomorphism such that $I : \mathsf{Tm} \to S[\mathsf{JVar}]$, where $S[\mathsf{JVar}]$ is the polynomial semiring in JVar over S by setting:

1. $I(x) := x$ for variables x
2. $I(s + t) := I(s) + I(t)$ for terms s, t
3. $I(s \cdot t) := I(s) \cdot I(t)$ for terms s, t

Let $K = (S, +, \cdot, 0, 1)$ be a semiring with domain S. We define Fml_S as the set of formulas where we use elements of S instead of justification terms.

1. $\bot \in \mathsf{Fml}_S$
2. $P \in \mathsf{Fml}_S$, where $P \in \mathsf{Prop}$

3. $A \to B \in \mathsf{Fml_S}$, where $A \in \mathsf{Fml_S}$ and $B \in \mathsf{Fml_S}$
4. $s : A \in \mathsf{Fml_S}$, where $A \in \mathsf{Fml_S}$ and $s \in S$

Definition 5 (Evidence relation). *Let S be the domain of a semiring. We call $J \subseteq S \times \mathsf{Fml_S}$ an* evidence relation *if for all $s, t \in S$ and all $A, B \in \mathsf{Fml_S}$:*

1. *$J(s, A \to B)$ and $J(t, A)$ imply $J(s \cdot t, B)$*
2. *$J(s, A)$ and $J(t, A)$ imply $J(s + t, A)$*

Definition 6 (Valuation). *A valuation v is a function from JVar to S.*

The polynomial $I(t)$ can be viewed as a function $t_I : S^n \to S$, where n is the number of variables that occur in t. Hence, given an interpretation $I : \mathsf{JConst} \to S$ and a valuation v, every $t \in \mathsf{Tm}$ can be mapped to an element $t_I(v(x_1), ..., v(x_n))$ in S, which we denote by t_I^v. By abuse of notation, we only mention the variables that occur in the term t. For a variable x we have

$$v(x) = x_I(v(x)) = x_I^v.$$

Given the definition of the polynomial function t_I, we find, e.g.,

$$x_I^v \cdot y_I^v = x_I(v(x)) \cdot y_I(v(y)) = (x \cdot y)_I(v(x), v(y)) = (x \cdot y)_I^v. \tag{1}$$

For $A \in \mathsf{Fml}$ we define $A_I^v \in \mathsf{Fml_S}$ inductively:

1. $\bot_I^v := \bot$
2. $P_I^v := P$, where $P \in \mathsf{Prop}$
3. $(A \to B)_I^v := A_I^v \to B_I^v$, where $A \in \mathsf{Fml}$ and $B \in \mathsf{Fml}$
4. $(s : A)_I^v := s_I^v : A_I^v$, where $A \in \mathsf{Fml}$ and $s \in \mathsf{Tm}$

Let $A \in \mathsf{Fml}$ and let $x_1, \ldots, x_n$ be the variables that occur in A. Then A_I denotes the function $A_I : S^n \to \mathsf{Fml_S}$ defined by $A_I(y_1, ..., y_n) := A_I^v$ where v is such that $v(x_i) = y_i$.

Definition 7 (Semiring model). *A* semiring model *is a tuple $M = (K, *, I, J)$ where*

1. *$K = (S, +, \cdot, 0, 1)$ is a semiring*
2. *$*$ is a truth assignment for atomic propositions, i.e., $* : \mathsf{Prop} \to \{\mathbb{F}, \mathbb{T}\}$*
3. *I is an interpretation, i.e., $I : \mathsf{JConst} \to S$*
4. *J is an evidence relation.*

First we define truth in a semiring model for a given valuation. Because variables represent arbitrary justifications, we require a formula to be true for all valuations in order to be true in a semiring model. This means a formula with variables is interpreted as universally quantified.

Definition 8 (Truth in a semiring model). *Let $M = (K, *, I, J)$ be a semiring model, v a valuation and A a formula. $M, v \Vdash A$ is defined as follows:*

- $M, v \nVdash \bot$
- $M, v \Vdash P \quad$ *iff* $\quad P^* = \mathbb{T}$
- $M, v \Vdash A \to B \quad$ *iff* $\quad M, v \nVdash A$ *or* $M, v \Vdash B$
- $M, v \Vdash s : A \quad$ *iff* $\quad J(s_I^v, A_I^v)$

Further we set $M \Vdash A \quad$ *iff* $\quad M, v \Vdash A$ *for all valuations* v.

For a semiring model M and a theory T, $M \Vdash T$ means $M \Vdash A$ for all $A \in T$.

Definition 9 (Semantic consequence). *A theory* T entails *a formula* F*, in symbols* $T \Vdash F$*, if for each semiring model* M *we have that*

$$M \Vdash T \text{ implies } M \Vdash F.$$

By unfolding the definitions, we immediately get the following lemma, which is useful to establish soundness of SE.

Lemma 3. *Let* $M = (K, *, I, J)$ *be a semiring model and let* v *and* w *be valuations with* $v(x_i) = (t_i)_I^w$ *for variables* x_i *and terms* t_i*. Then*

$$M, v \Vdash A \quad \textit{iff} \quad M, w \Vdash A\sigma, \textit{ where } \sigma(x_i) = t_i.$$

Proof. By induction on the structure of A.

- Case $A = \bot$. We have $M, v \nVdash \bot$ and $M, w \nVdash \bot$.
- Case $A = P$. We have $M, v \Vdash P \Leftrightarrow P^* = \mathbb{T} \Leftrightarrow M, w \Vdash P$.
- Case $A = B \to C$. We have $M, v \Vdash B \to C$
  $\Leftrightarrow M, v \nVdash B$ or $M, v \Vdash C$
  $\overset{\text{I.H.}}{\Leftrightarrow} M, w \nVdash B\sigma$ or $M, w \Vdash C\sigma$
  $\Leftrightarrow M, w \Vdash B\sigma \to C\sigma \Leftrightarrow M, w \Vdash (B \to C)\sigma$.
- Case $A = s : B$. We have $M, v \Vdash s : B$
  $\Leftrightarrow J(s_I^v, B_I^v)$
  $\Leftrightarrow J(s_I(v(x_1), ..., v(x_n)), B_I(v(x_1), ..., v(x_n)))$
  $\Leftrightarrow J(s_I((t_1)_I^w, ..., (t_n)_I^w), B_I((t_1)_I^w, ..., (t_n)_I^w))$
  $\Leftrightarrow J((s\sigma)_I^w, (B\sigma)_I^w) \Leftrightarrow M, w \Vdash s\sigma : B\sigma$
  $\Leftrightarrow M, w \Vdash (s : B)\sigma$. □

Theorem 2 (Soundness). *Let* T *be an arbitrary theory. Then:*

$$T \vdash F \quad \textit{implies} \quad T \Vdash F.$$

Proof. As usual by induction on the length of the derivation of F. Let $M = (K, *, I, J)$ be a semiring model such that $M \Vdash T$. To establish our claim when F is an axiom or an element of T, we let v be an arbitrary valuation and show $M, v \Vdash F$ for the following cases:

1. $F \in T$. Trivial.
2. **CL**. Trivial.

3. **j**. Assume $M, v \Vdash x : (A \to B)$ and $M, v \Vdash y : A$. That is $J(x_I^v, (A \to B)_I^v)$ and $J(y_I^v, A_I^v)$ hold, which by Definition 5 implies $J(x_I^v \cdot y_I^v, B_I^v)$. Hence by (1) we get $J((x \cdot y)_I^v, B_I^v)$, which yields $M, v \Vdash x \cdot y : B$.
4. **j+**. Similar to the previous case.
5. For the semiring axioms we prove

$$M, v \Vdash A[x/s] \Leftrightarrow M, v \Vdash A[x/t] \text{ for all formulas } A,$$

where $s_I^v = t_I^v$ by induction on the structure of A:
   - $A = \bot$ or $A = P$. Trivial.
   - $A = B \to C$. $M, v \Vdash (B \to C)[x/s]$
     $\Leftrightarrow M, v \Vdash B[x/s] \to C[x/s]$
     $\Leftrightarrow M, v \nVdash B[x/s]$ or $M, v \Vdash C[x/s]$
     $\overset{\text{I.H.}}{\Leftrightarrow} M, v \nVdash B[x/t]$ or $M, v \Vdash C[x/t]$
     $\Leftrightarrow M, v \Vdash B[x/t] \to C[x/t]$
     $\Leftrightarrow M, v \Vdash (B \to C)[x/t]$.
   - $A = u : B$. $M, v \Vdash (u : B)[x/s]$
     $\Leftrightarrow M, v \Vdash u[x/s] : B[x/s]$
     $\Leftrightarrow J(u[x/s]_I^v, B[x/s]_I^v)$
     $\Leftrightarrow J(u[x/t]_I^v, B[x/t]_I^v)$
     $\Leftrightarrow M, v \Vdash u[x/t] : B[x/t]$
     $\Leftrightarrow M, v \Vdash (u : B)[x/t]$.

   By mentioning that all the semiring axioms have the form $A[x/s] \to A[x/t]$ or $A[x/s] \leftrightarrow A[x/t]$ with $s_I^v = t_I^v$, we finish this case.

The case when F has been derived by **MP** follows by I.H. as usual. For the case when $F = A[x/t]$ has been derived from A by **jv**, we find by I.H. that $M \Vdash A$, which is

$$M, v \Vdash A \text{ for all valuations } v. \tag{2}$$

Given the term t and an arbitrary valuation w, we find that there exists a valuation v such that $v(x) = t_I^w$ and $v(y) = w(y)$ for all $y \neq x$. By Lemma 3 we get

$$M, v \Vdash A \quad \text{iff} \quad M, w \Vdash A[x/t].$$

Thus using (2), we obtain $M, w \Vdash A[x/t]$. Since w was arbitrary, we conclude $M \Vdash A[x/t]$. □

Next we establish completeness of SE with respect to semiring models. For the completeness proof, we consider the free semiring over $\mathsf{JConst} \cup \mathsf{JVar}$. We have for $s, t \in \mathsf{Tm}$:

- $[t]$ is the equivalence class of t with respect to the semiring equalities, see Definition 2;
- $[s] + [t] := [s + t]$;
- $[s] \cdot [t] := [s \cdot t]$;
- $S_{\mathsf{Tm}} := \{[t] : t \in \mathsf{Tm}\}$;
- $K_{\mathsf{Tm}} := (S_{\mathsf{Tm}}, +, \cdot, [0], [1])$ is the free semiring over $\mathsf{JConst} \cup \mathsf{JVar}$.

The following lemma states that SE respects the semiring equalities.

Lemma 4. *Let T be a theory and s, t be terms with $[s] = [t]$. For each formula A we have*

$$T \vdash_{\mathsf{SE}} A[w/s] \quad \textit{iff} \quad T \vdash_{\mathsf{SE}} A[w/t].$$

Assume we are given an interpretation I that maps constants to their equivalence class and a valuation v that maps each variable x_i to the equivalence class $[t_i]$ of some term t_i. The following lemma states that the interpretation of a term s under I and v is the equivalence class of s with each x_i being replaced by t_i.

Lemma 5. *Assume that we are given an interpretation $I : \mathsf{JConst} \to S_{\mathsf{Tm}}$ with $I(c) = [c]$, a term s, and a valuation $v : \mathsf{JVar} \to S_{\mathsf{Tm}}$ with $v(x_i) = [t_i]$. Then we have*

$$s^v_I = [s\sigma], \textit{ where } \sigma(x_i) = t_i.$$

Proof. Induction on the structure of s:

- $c^v_I = [c]$ by definition of I.
- $(x_i)^v_I = [t_i]$ by definition of v.
- $(s_1 + s_2)^v_I = (s_1)^v_I + (s_2)^v_I$. By I.H. we have

$$(s_1)^v_I = [s_1\sigma] \quad \text{and} \quad (s_2)^v_I = [s_2\sigma].$$

  Thus $(s_1)^v_I + (s_2)^v_I = [s_1\sigma] + [s_2\sigma] = [(s_1 + s_2)\sigma]$.
- $(s_1 \cdot s_2)^v_I = (s_1)^v_I \cdot (s_2)^v_I$. By I.H. we have

$$(s_1)^v_I = [s_1\sigma] \quad \text{and} \quad (s_2)^v_I = [s_2\sigma].$$

  Thus $(s_1)^v_I \cdot (s_2)^v_I = [s_1\sigma] \cdot [s_2\sigma] = [(s_1 \cdot s_2)\sigma]$ □

We extend the notion of equivalence to formulas by defining the function

$$[\cdot] : \mathsf{Fml} \to \mathsf{Fml}_{S_{\mathsf{Tm}}}$$

as follows:

- $[\bot] := \bot$
- $[P] := P$
- $[A \to B] := [A] \to [B]$
- $[t : A] := [t] : [A]$

Intuitively $[A]$ is the formula where each justification term is replaced by its equivalence class in the free semiring. Observe that if $I(c) = [c]$ and $v(x) = [x]$, then $[A] = A^v_I$. Now we extend Lemma 5 to formulas.

Lemma 6. *Assume that we are given the interpretation $I : \mathsf{JConst} \to S_{\mathsf{Tm}}$ with $I(c) = [c]$, a formula A, and a valuation $v : \mathsf{JVar} \to S_{\mathsf{Tm}}$ with $v(x_i) = [t_i]$. Then we have*

$$A^v_I = [A\sigma], \textit{ where } \sigma(x_i) = t_i.$$

Proof. Induction on the structure of A:

- $\bot_I^v = \bot = [\bot]$
- $P_I^v = P = [P]$
- $(A \to B)_I^v = A_I^v \to B_I^v$
  $\overset{\text{I.H.}}{=} [A\sigma] \to [B\sigma] = [(A \to B)\sigma]$
- $(s : A)_I^v = s_I^v : A_I^v$
  $\overset{\text{I.H. and L. 5}}{=} [s\sigma] : [A\sigma] = [(s : A)\sigma]$ □

Let $\mathsf{Prop2}$ be an infinite set of atomic propositions with $\mathsf{Prop} \cap \mathsf{Prop2} = \emptyset$. Then there exists an bijective function $f : S_{\mathsf{Tm}} \times \mathsf{Fml}_{S_{\mathsf{Tm}}} \to \mathsf{Prop2}$. We assume f to be fixed for the rest of this section. Based on this function we define a translation $'$ that maps formulas of Fml to pure propositional formulas containing atomic propositions from $\mathsf{Prop} \cup \mathsf{Prop2}$.

1. $\bot' := \bot$
2. $P' := P$
3. $(A \to B)' := A' \to B'$
4. $(t : A)' := f([t], [A])$

Let T be a theory. We define the corresponding theory:

$$T' := \{(A\sigma)' \mid A \in T \text{ or } A \text{ is an axiom of } \mathsf{SE}, \sigma : \mathsf{JVar} \to \mathsf{Tm}\}.$$

Suppose $A' \in T'$. Then there exist a formula B with $B \in T$ or B is an axiom and $\sigma : \mathsf{JVar} \to \mathsf{Tm}$ such that $(B\sigma)' = A'$. This implies $B\sigma[x/t]' = A[x/t]'$. Now we have $A[x/t]' \in T'$. Therefore the following implication is proved:

$$A' \in T' \Rightarrow A[x/t]' \in T' \tag{3}$$

In fact this does not only hold for formulas in T' but also for all formulas derived from T' by classical propositional logic.

Lemma 7. *If* $T' \vdash_{\mathsf{CL}} A'$ *then* $T' \vdash_{\mathsf{CL}} A[x/t]'$.

Proof. Induction on the derivation of A'. Note that T' contains all the axioms of CL. So we can omit this case.

1. If $A' \in T'$ then $A[x/t]' \in T'$ by the above observation and thus $T' \vdash_{\mathsf{CL}} A[x/t]'$.
2. If A' is obtained by **MP** from B and $B \to A'$ then B can be written as C' because f is surjective. The induction hypothesis ($T' \vdash_{\mathsf{CL}} C[x/t]'$ and $T' \vdash_{\mathsf{CL}} C[x/t]' \to A[x/t]'$) yields $T' \vdash_{\mathsf{CL}} A[x/t]'$. □

The translation $'$ respects the derivability relation of SE. Hence we have the following lemma.

Lemma 8. $T \vdash_{\mathsf{SE}} A \Leftrightarrow T' \vdash_{\mathsf{CL}} A'$

Proof. Left to right by induction on a derivation of A:

1. If $A \in T$ or A is an axiom then $A' \in T'$ and therefore $T' \vdash_{\mathsf{CL}} A'$.
2. If A is obtained by **MP** from B and $B \to A$ then the induction hypothesis ($T' \vdash_{\mathsf{CL}} B'$ and $T' \vdash_{\mathsf{CL}} B' \to A'$) immediately yields $T' \vdash_{\mathsf{CL}} A'$.
3. If $A[x/t]$ is obtained by **jv** from A then the induction hypothesis is $T' \vdash_{\mathsf{CL}} A'$. By the previous lemma we conclude $T' \vdash_{\mathsf{CL}} A[x/t]'$.

Right to left by induction on a derivation of A':

1. If $A' \in T'$ then there exist a formula B with $B \in T$ or B is an axiom and $\sigma : \mathsf{JVar} \to \mathsf{Tm}$ such that $(B\sigma)' = A'$. Trivially we have $T \vdash_{\mathsf{SE}} B$ and get by **jv** that $T \vdash_{\mathsf{SE}} B\sigma$. Since f is injective, the only difference between A and $B\sigma$ is that some terms may be replaced by equivalent ones (modulo the semiring). Therefore, we get $T \vdash_{\mathsf{SE}} A$ by using Lemma 4.
2. If A' is a propositional tautology then so is A because f is injective, but some terms in A may be replaced by equivalent ones. We get $T \vdash_{\mathsf{SE}} A$ again by Lemma 4 and propositional reasoning.
3. If A' is obtained by **MP** from $B \to A'$ and B then B can be written as C'. The induction hypothesis ($T \vdash_{\mathsf{SE}} C \to A$ and $T \vdash_{\mathsf{SE}} C$) implies $T \vdash_{\mathsf{SE}} A$.

□

Lemma 8 gives us the ability to switch from SE to CL and vice versa. Therefore, we can use completeness of CL to obtain completeness for SE.

Theorem 3 (Completeness). *Let T be an arbitrary theory. Then:*

$$T \Vdash F \quad \textit{implies} \quad T \vdash F.$$

Proof. We will prove the contraposition, which means for $T \nvdash F$ we will construct a semiring model M and find a valuation v, such that $M \Vdash T$ and $M, v \nVdash F$. Assume $T \nvdash F$. By Lemma 8 we get $T' \nvdash_{\mathsf{CL}} F'$. The completeness of CL delivers $* : \mathsf{Prop} \cup \mathsf{Prop2} \to \{\mathbb{F}, \mathbb{T}\}$, such that for the CL-model M_* consisting of $*$ we have $M_* \Vdash T'$ and $M_* \nVdash F'$. Now we can define the semiring model M:

- $M := (K_{\mathsf{Tm}}, *|_{\mathsf{Prop}}, I, J)$
- $*|_{\mathsf{Prop}}$ is the restriction of $*$ to Prop
- $I : \mathsf{JConst} \to S_{\mathsf{Tm}}$, $I(c) := [c]$
- $J := \{([t], [A]) \mid M_* \Vdash f([t], [A])\}$

In order to prove that M is a semiring model, we need to show that J is an evidence relation.

1. From $M_* \Vdash T'$ we derive $M_* \Vdash (s : (A \to B) \to (t : A \to s \cdot t : B))'$ $\forall s, t \in \mathsf{Tm}$ and $\forall A, B \in \mathsf{Fml}$ by using the definition of T' and (3). It follows

   $$M_* \Vdash f([s], [A \to B]) \to (f([t], [A]) \to f([s \cdot t], [B])).$$

   By the truth definition in CL we find

   $$\text{if } f([s], [A \to B])^* = \mathbb{T} \text{ and } f([t], [A])^* = \mathbb{T} \text{ then } f([s \cdot t], [B])^* = \mathbb{T}.$$

   From the definition of J in M we get

   $$\text{if } J([s], [A] \to [B]) \text{ and } J([t], [A]) \text{ then } J([s] \cdot [t], [B]).$$

2. From $M_* \Vdash T'$ we derive $M_* \Vdash (s : A \wedge t : A \to s + t : A)'$ $\forall s, t \in \mathsf{Tm}$ and $\forall A \in \mathsf{Fml}$ by using the definition of T' and (3). It follows

$$M_* \Vdash f([s],[A]) \wedge f([t],[A]) \to f([s+t],[A]) \ \forall s, t \in \mathsf{Tm} \text{ and } \forall A \in \mathsf{Fml}.$$

By the truth definition in CL we find

$$\text{if } f([s],[A])^* = \mathbb{T} \text{ and } f([t],[A])^* = \mathbb{T} \text{ then } f([s+t],[A])^* = \mathbb{T}.$$

From the definition of J in M we get

$$\text{if } J([s],[A]) \text{ and } J([t],[A]) \text{ then } J([s]+[t],[A]).$$

Knowing that M is a semiring model we prove

$$M_* \Vdash (A\sigma)' \Leftrightarrow M, w \Vdash A \tag{4}$$

by induction on the structure of A, where $w(x_i) = [t_i]$ and $\sigma(x_i) = t_i$.

- Case $A = \bot$. We have $M_* \nVdash \bot'$ and $M, w \nVdash \bot$.
- Case $A = P$. We have $M_* \Vdash P' \Leftrightarrow M_* \Vdash P \Leftrightarrow P^* = \mathbb{T} \Leftrightarrow M, w \Vdash P$.
- Case $A = B \to C$. We have $M_* \Vdash ((B \to C)\sigma)'$
  $\Leftrightarrow M_* \Vdash (B\sigma)' \to (C\sigma)'$
  $\Leftrightarrow M_* \nVdash (B\sigma)'$ or $M_* \Vdash (C\sigma)'$
  $\Leftrightarrow M, w \nVdash B$ or $M, w \Vdash C$ (by induction hypothesis)
  $\Leftrightarrow M, w \Vdash B \to C$
  $\Leftrightarrow M, w \Vdash B \to C$.
- Case $A = s : B$. We have $M_* \Vdash ((s : B)\sigma)'$
  $\Leftrightarrow M_* \Vdash (s\sigma : B\sigma)'$
  $\Leftrightarrow M_* \Vdash f([s\sigma],[B\sigma])$ (by definition of $'$)
  $\Leftrightarrow J([s\sigma],[B\sigma])$ (by definition of J)
  $\Leftrightarrow J(s_I^w,[B\sigma])$ (by Lemma 5)
  $\Leftrightarrow J(s_I^w, B_I^w)$ (by Lemma 6)
  $\Leftrightarrow M, w \Vdash s : B$

Now we show $M \Vdash T$, i.e. $M, w \Vdash T$ for all valuations w. Hence let w be an arbitrary valuation (assume $w(x_i) = [t_i]$ and $\sigma(x_i) = t_i$) and $A \in T$. It follows $A' \in T'$ and by (3) also $(A\sigma)' \in T'$. From $M_* \Vdash T'$ we get $M_* \Vdash (A\sigma)'$. (4) implies $M, w \Vdash A$. Since w was arbitrary we conclude $M \Vdash T$.

Now we consider the special case of (4) where $w = v$ with $v(x) = [x]$. We have

$$M_* \Vdash A' \Leftrightarrow M, v \Vdash A$$

Remembering $M_* \nVdash F'$, we derive $M, v \nVdash F$, which finishes the proof. □

3.4 Realization

Realization is concerned with the relationship between justification logic and modal logic. Replacing all terms in a formula of justification logic by $\Box$-operators

yields a formulas of modal logic. This is called *forgetful projection* since by this translation, one 'forgets' the explicit evidence for one's beliefs. It is fairly obvious that the forgetful projection of a theorem of justification logic yields a theorem of modal logic. This is so since the translation of any axiom of justification logic yields a theorem of modal logic and the translation of the rules also yields (derivable) rules of modal logic.

The converse direction, called *realization*, is more interesting and also more difficult to establish. We show that, under certain natural conditions, there is a construction that replaces all modalities in a theorem of modal logic by justification terms such that the resulting formula is a theorem of justification logic.

In this section, we let $\circ$ be the mapping from Fml to formulas of the modal logic K that replaces all occurrences of $s:$ in a formula of SE with $\Box$.

Definition 10. *We say that a theory T is* pure *if for each formula $A \in T$ we have that $\vdash_{\mathsf{K}} A^{\circ}$.*

We immediately get the following lemma.

Lemma 9 (Forgetful projection). *Let T be a pure theory. For any formula A we have*

$$T \vdash_{\mathsf{SE}} A \quad \textit{implies} \quad \vdash_{\mathsf{K}} A^{\circ}.$$

To investigate mappings from modal logic to SE, we need the deductive system GK for the logic K as defined in Section 2.3. So instead of directly realising modal formulas, we realise sequents of GK. Therefore we define what it means for a sequent to be derivable in SE.

Definition 11. *Let $\Gamma \supset \Delta$ be a sequent where each $\Box$ is replaced by some term. $\Gamma \supset \Delta$ is called derivable in SE from a theory T if $T \vdash_{\mathsf{SE}} \bigwedge \Gamma \to \bigvee \Delta$.*

In the traditional approach to constructive realization [4, 35], one would say that $\Gamma \supset \Delta$ is derivable in SE if $\bigwedge \Gamma \vdash_{\mathsf{SE}} \bigvee \Delta$. This does not work in the framework of SE since the deduction theorem does not hold for SE (see Remark 2). Therefore, we use an approach according to Definition 11.

In the realization procedure, most of the effort goes into constructing terms for the Box-modalities introduced in the rule ($\Box$), which is the next thing we are going to do. Because $\mathsf{j+}$ is formulated with $\wedge$ we can not use Artemov's original realization algorithm. But Kuznets [33] found a realization procedure with the same ideas as Artemov except that justification terms are constructed without $+$. It can be applied in the context of SE.

For the following definition we need the notion of positive and negative occurrences of $\Box$ within a given modal formula A. First we assign a polarity to each subformula occurrence within A as follows.

1. The only occurrence of A within A is given positive polarity.
2. If a polarity is already assigned to an occurrence $B \to C$ within A, then the same polarity is assigned to C and the opposite polarity is assigned to B.
3. If a polarity is already assigned to an occurrence $\Box B$ within A, then the same polarity is assigned to B.

Now we assign a polarity to each occurence of $\Box$ as follows: the leading $\Box$ in an occurrence of $\Box B$ within A has the same polarity as the occurrence of $\Box B$ within A.

Definition 12. *A* realization *r is a mapping from modal formulas to* Fml *such that for each modal formula F we have $(r(F))^\circ = F$. A realization is* normal *if all negative occurrences of $\Box$ are mapped to distinct justification variables.*

As usual, we need a notion of schematicness to obtain a realization result.

Definition 13. *A theory T is schematic if it satisfies the following property: for each constant $c \in \mathsf{JConst}$, the set of axioms $\{A \mid c : A \in T$ and A is an axiom$\}$ consists of all instances of one or several (possibly zero) axiom schemes of* SE.

Lemma 10. *Let T be an axiomatically appropriate theory.*
If $T \vdash_{\mathsf{SE}} s : (A \to B)$ and $T \vdash_{\mathsf{SE}} t : (B \to C)$ then $T \vdash_{\mathsf{SE}} d \cdot c \cdot t \cdot s : (A \to C)$, where $T \vdash_{\mathsf{SE}} c : (B \to C \to (A \to (B \to C)))$ and
$T \vdash_{\mathsf{SE}} d : (A \to (B \to C) \to (A \to B \to (A \to C)))$.

Proof. The proof is encoded as $(d \cdot (c \cdot t)) \cdot s$. The constants c and d exist because T is axiomatically appropriate. □

Definition 14. *Let T be an axiomatically appropriate theory and suppose*

$$T \vdash_{\mathsf{SE}} s : (A \to B) \text{ and } T \vdash_{\mathsf{SE}} t : (B \to C).$$

We define $syl(s,t)$ such that

$$T \vdash_{\mathsf{SE}} syl(s,t) : (A \to C) \tag{5}$$

and $syl(s,t)$ is the least term (according to some given fixed ordering on terms) that satisfies (5).

Remark 3. Lemma 10 guarantees the existence of $syl(s,t)$. Note that the term $syl(s,t)$ depends on the formulas A, B and C. This dependency disappears if the theory T is schematic.

For the rest of this section we denote by d_n a term such that for all formulas $A_1, ..., A_n$ and $1 \leq i \leq n$

$$T \vdash_{\mathsf{SE}} d_n : (A_i \to A_1 \vee ... \vee A_n). \tag{6}$$

Lemma 11. *Let T be an axiomatically appropriate theory and $n \in \mathbb{N}_{>0}$.*
Assume there exists d_n.
If $T \vdash_{\mathsf{SE}} s_i : (A_i \to B)$ for all i, then for an arbitrary $t \in \mathsf{Tm}$

$$T \vdash_{\mathsf{SE}} t : A_i \to syl(d_n, e_n \cdot s_1 \cdot ... \cdot s_n) \cdot t : B,$$

where $T \vdash_{\mathsf{SE}} e_n : ((A_1 \to B) \to (... \to ((A_n \to B) \to (A_1 \vee ... \vee A_n \to B))...))$.

Proof. The existence of e_n follows from the internalization property. By using **j** and **MP** n times we get $T \vdash_{\mathsf{SE}} e_n \cdot s_1 \cdot ... \cdot s_n : (A_1 \vee ... \vee A_n \to B)$. Applying the *syl*-function constructed in Lemma 10 gives $T \vdash_{\mathsf{SE}} syl(d_n, e_n \cdot s_1 \cdot ... \cdot s_n) : (A_i \to B)$ for all i. From **j** as

$$syl(d_n, e_n \cdot s_1 \cdot ... \cdot s_n) : (A_i \to B) \to (t : A_i \to syl(d_n, e_n \cdot s_1 \cdot ... \cdot s_n) \cdot t : B)$$

we infer $T \vdash_{\mathsf{SE}} t : A_i \to syl(d_n, e_n \cdot s_1 \cdot ... \cdot s_n) \cdot t : B$ for all i. □

In the definition of d_n the brackets of the disjunction are missing, because they don't matter: If d_n exists for one specific placement of the brackets then so does e_n and we can apply the previous lemma.

The next lemma is an easy consequence of axiom **j**. Note that the existence of the constant c_n follows from $A_1 \to (... \to (A_n \to A_1 \wedge ... \wedge A_n)...))$ being an instance of **CL** and T being axiomatically appropriate.

Lemma 12. *Let T be an axiomatically appropriate theory and $n \in \mathbb{N}_{>0}$. Then*

$$T \vdash_{\mathsf{SE}} t_1 : A_1 \wedge ... \wedge t_n : A_n \to c_n \cdot t_1 \cdot ... \cdot t_n : (A_1 \wedge ... \wedge A_n),$$

where $T \vdash_{\mathsf{SE}} c_n : (A_1 \to (... \to (A_n \to A_1 \wedge ... \wedge A_n)...))$.

For a multiset Γ and a variable x define $x : \Gamma := \{x : A \mid A \in \Gamma\}$. Further we define terms x^k recursively by $x^0 := 1$ and $x^{k+1} := x^k \cdot x$. Remember that by axiom **am**, we have associativity of the application operation. Therefore, and by axiom **a1**, we may use, e.g., the term $c \cdot ((1 \cdot x) \cdot x)$ where one would expect $(c \cdot x) \cdot x$.

Lemma 13. *Let T be an axiomatically appropriate theory, $n \in \mathbb{N}_{>0}$, and assume that d_n exists as in* (6)*. Further assume that for all i such that $1 \leq i \leq n$, we are given multisets $\Gamma_i \subseteq \mathsf{Fml}$ with $|\Gamma_i| = m$ such that $T \vdash_{\mathsf{SE}} \bigwedge \Gamma_i \to A$.*
Then there exists $q \in \mathsf{Tm}$ such that for each Γ_i we have $T \vdash_{\mathsf{SE}} \bigwedge x : \Gamma_i \to q : A$ where x is a variable.

Proof. By internalization we find ground terms s_i such that

$$T \vdash_{\mathsf{SE}} s_i : (\bigwedge \Gamma_i \to A).$$

Because T is axiomatically appropriate and we assume that d_n exists, we can use Lemma 11 and get for an arbitrary variable x that

$$T \vdash_{\mathsf{SE}} c_m \cdot x^m : \bigwedge \Gamma_i \to syl(d_n, e_n \cdot s_1 \cdot ... \cdot s_n) \cdot c_m \cdot x^m : A.$$

By Lemma 12 we have $T \vdash_{\mathsf{SE}} \bigwedge x : \Gamma_i \to c_m \cdot x^m : \bigwedge \Gamma_i$ for all i. This leads to

$$T \vdash_{\mathsf{SE}} \bigwedge x : \Gamma_i \to syl(d_n, e_n \cdot s_1 \cdot ... \cdot s_n) \cdot c_m \cdot x^m : A.$$

Therefore $q = syl(d_n, e_n \cdot s_1 \cdot ... \cdot s_n) \cdot c_m \cdot x^m$. □

In the next definition, it is essential that both implications are justified by the same term. An axiomatically appropriate and schematic theory does not guarantee this.

Definition 15. *A theory T* supports weakening *if there exists a ground term t such that for all formulas A, B*

$$t : (A \to A \vee B) \in T \quad \textit{and} \quad t : (B \to A \vee B) \in T.$$

Note that supporting weakening is rather natural. For instance, it corresponds to accepting the $R\vee$ rule in Gentzen system $\mathsf{G3}$, see, e.g. [43]. By this rule, we can infer from the (multi-)set $\{A, B\}$ both $A \vee B$ and $B \vee A$. Thus from A we get by weakening admissibility $\{A, B\}$ and thus both $A \vee B$ and $B \vee A$ by exactly the same reasoning. Therefore, the justification term representing this should also be the same.

Definition 16. *$A \in \mathsf{Fml}$ is a balanced disjunction of depth 0. If A and B are balanced disjuctions of depth m, then $A \vee B$ is a balanced disjunction of depth $m + 1$.*

For Lemma 11 and Lemma 13 we assumed that a term d_n exists. Next we show that such terms do exist (for n being a power of 2) if we work with a schematic theory and balanced disjunctions. This leads to the formulation of Lemma 14, which is the same as Lemma 13 without the extra assumption about the term d_n, but with a schematic theory that supports weakening. This provides the crucial step in the proof of the realization theorem.

Lemma 14. *Let T be an axiomatically appropriate and schematic theory that supports weakening and let $n \in \mathbb{N}_{>0}$. We assume that for all i with $1 \leq i \leq n$, we are given multisets $\Gamma_i \subseteq \mathsf{Fml}$ with $|\Gamma_i| = m$ such that $T \vdash_{\mathsf{SE}} \bigwedge \Gamma_i \to A$.*
Then there exists $q \in \mathsf{Tm}$ such that for each Γ_i we have $T \vdash_{\mathsf{SE}} \bigwedge x : \Gamma_i \to q : A$, where x is a variable.

Proof. We first show by induction that for all $l \in \mathbb{N}$ terms d_{2^l} exists such that for all formulas $A_1, \ldots, A_{2^l}$

$$T \vdash_{\mathsf{SE}} d_{2^l} : (A_i \to A_1 \vee \cdots \vee A_{2^l}),$$

i.e. the terms from (6) exist for $n = 2^l$.

For the base case we note that term d_1 exists by the internalization property (this requires T to be axiomatically appropriate).

For the induction step, first observe that the term d_2 exists since T supports weakening. Now suppose

$$d_l : (A_i \to A_1 \vee \ldots \vee A_l) \text{ where } 1 \leq i \leq l$$

and

$$d_l : (A_i \to A_{l+1} \vee \ldots \vee A_{2l}) \text{ where } l + 1 \leq i \leq 2l.$$

Then $syl(d_l, d_2)$ serves as d_{2l} because of

$$d_2 : (A_1 \vee ... \vee A_l \to (A_1 \vee ... \vee A_l) \vee (A_{l+1} \vee ... \vee A_{2l}))$$

and

$$d_2 : (A_{l+1} \vee ... \vee A_{2l} \to (A_1 \vee ... \vee A_l) \vee (A_{l+1} \vee ... \vee A_{2l})).$$

The term $syl(d_l, d_2)$ does not depend on the formulas $A_1, ..., A_{2l}$ because T is schematic. Therefore schematicness and the property of supporting weakening of T imply the existence of d_{2^l} for all $l \in \mathbb{N}$, where the disjunction is balanced of depth l.

To finish the proof, we define $k \in \mathbb{N}$ such that $2^{k-1} < n \leq 2^k$ and then $\Gamma_i := \Gamma_1$ for $n + 1 \leq i \leq 2^k$. Now we can apply Lemma 13 and get $q \in \mathsf{Tm}$ such that $T \vdash_{\mathsf{SE}} \bigwedge x : \Gamma_i \to q : A$ for all $i \leq 2^k$, including all $i \leq n$. □

In order to prove a realization theorem, we need a notion to relate different occurences of $\Box$ in a GK-derivation. The main definition will be that of an essential family of $\Box$-occurences, which goes back to [4] (for some examples see [35]).

An instance of a GK-rule relates to formulas F and G if either

1. the rule instance does not transform F and $F = G$ or
2. G results from F in the application of the rule instance

For example in

$$(\supset\to)\frac{A, \Gamma \supset \Delta, B}{\Gamma \supset \Delta, A \to B}$$

the formula A in the premise is related to the formula $A \to B$ in the conclusion.

Let $\mathcal{D}$ be a derivation in GK. We say that two occurrences of $\Box$ in $\mathcal{D}$ are *related* if they occur at the same position in related formulas of premises and conclusions of a rule instance in $\mathcal{D}$;[1] we close this relationship of related occurrences under transitivity.

All occurrences of $\Box$ in $\mathcal{D}$ naturally split into disjoint *families* of related occurrences. Note that the rules of GK preserve the polarity of related occurrences. Thus, all occurrences in a given family have the same polarity and we speak of *positive* and *negative families*, respectively.

We call a family *essential* if at least one of its members is introduced on the right-hand side of a $(\Box)$ rule.

Theorem 4 (Realization). *Let T be a theory that is axiomatically appropriate, schematic and that supports weakening.*
Then there exists a realization r such that for all formulas A of the language of modal logic, we have $\vdash_K A \Rightarrow T \vdash_{\mathsf{SE}} r(A)$.

Proof. Let $\mathcal{D}$ be the GK derivation that proves $\supset A$. The realization r is constructed in three steps:

[1] that is, e.g., an occurrence of $\Box$ in the premise A in the above instance of $(\supset\to)$ is related the the occurrence of $\Box$ at the same position in the subformula A of $A \to B$ in the conclusion

1. Modify the derivation. For each essential family f do the following: If n ($\Box$) rules introduce a $\Box$-operator to f, their premises are $\Gamma_i \supset A$, $1 \leq i \leq n$, and none of the Γ_i is empty then use first ($w \supset$) to duplicate formulas of Γ_i such that all Γ_i have the same cardinality. After applying the ($\Box$) rule remove the duplicates by ($c \supset$).
2. For each negative family and each non-essential positive family, replace all $\Box$ occurrences by the variable x.
3. For each essential family f do the following: Enumerate the ($\Box$) rules from 1 to n. The premises are $\Gamma_i \supset A$, where $1 \leq i \leq n$. Step 1 guarantees either $|\Gamma_1| = ... = |\Gamma_n| =: m$ or $\Gamma_k = \emptyset$ for some k. In the first case construct a term q according to Lemma 14. In the second case a term q can be found by the internalization property. Replace each $\Box$ of f by q.

We call the resulting derivation after these three steps $\mathcal{D}'$. Now we prove by induction on the GK-derivation that all sequents in $\mathcal{D}'$ are derivable in SE from the theory T.

1. $P \supset P$: $r(P \to P) = P \to P$ which is derivable is SE.
2. $\bot\supset$: $r(\bot\to\bot) =\bot\to\bot$ which is derivable is SE.
3. ($\Box$): The case without empty Γ_i's is covered in Lemma 14. In the other case the premise is $\Gamma_j \supset A$. The I.H. for $\Gamma_k = \emptyset$ is $T \vdash_{\mathsf{SE}} r(A)$. Because the term for the introduced $\Box$ was constructed according to the internalization property this implies $T \vdash_{\mathsf{SE}} r(\Box A)$. By propositional reasoning we infer $T \vdash_{\mathsf{SE}} r(\bigwedge \Box\Gamma_i) \to r(\Box A)$ for all i, therefore $T \vdash_{\mathsf{SE}} r(\bigwedge \Box\Gamma_i \to \Box A)$ for all i.
4. For the remaining rules the desired result is obtained by propositional reasoning. $\Box$

However, the realization obtained by the previous theorem will not be normal. In traditional justification logic normal realizations can be achieved using the sum-operation, which there (unlike in SE) is axiomatized by

$$s : A \vee t : A \to s + t : A.$$

Since we work with general theories (instead of simple constant specifications) and with variables that are interpreted universally, we can mimick the traditional sum-operation and perform the usual realization procedure given in [4, 35].

Theorem 5 (Normal realization). *Let T be an axiomatically appropriate and schematic theory such that for some constant c*

$$x : A \to c \cdot x \cdot y : (A \vee B) \in T \quad \textit{and} \quad y : B \to c \cdot x \cdot y : (A \vee B) \in T.$$

Then there exists a normal realization r such that for all modal formulas F,

$$\vdash_{\mathsf{K}} F \quad \textit{implies} \quad T \vdash_{\mathsf{SE}} r(F).$$

Proof. From the assumptions we get

$$T \vdash_{\mathsf{SE}} s : A \to c \cdot s \cdot t : (A \vee A) \text{ and } T \vdash_{\mathsf{SE}} t : A \to c \cdot s \cdot t : (A \vee A).$$

The internalization property delivers a term u, such that $T \vdash_{\mathsf{SE}} u : (A \vee A \to A)$. Applying **j** yields $T \vdash_{\mathsf{SE}} c \cdot s \cdot t : (A \vee A) \to u \cdot c \cdot s \cdot t : A$. Therefore we have

$$T \vdash_{\mathsf{SE}} s : A \to u \cdot c \cdot s \cdot t : A \text{ and } T \vdash_{\mathsf{SE}} t : A \to u \cdot c \cdot s \cdot t : A$$

and finally

$$T \vdash_{\mathsf{SE}} s : A \vee t : A \to u \cdot c \cdot s \cdot t : A.$$

We can define the plus from traditional justification logic as $s * t := u \cdot c \cdot s \cdot t$. Because T is schematic, there is one u justifying all instances of $A \vee A \to A$, which ensures that $s * t$ doesn't depend on A. Therefore Artemov's realization procedure [4] can be used. We only need a small adjustment in the case of the $(\Box)$ rule, which we show next.

Let an occurrence of a $(\Box)$ rule have number i in the enumeration of all n_f $(\Box)$ rules in a given family f. The corresponding node in the GK derivation $\mathcal{D}'$ is labelled by

$$\frac{B_1, ..., B_n \supset A}{x_1 : B_1, ..., x_n : B_n \supset s_1 * ... * s_{n_f} : A}$$

where the x's are variables, the s's are terms and s_i is a provisional variable. By the induction hypothesis we have

$$T \vdash_{\mathsf{SE}} B_1 \wedge ... \wedge B_n \to A.$$

It can be shown by induction on the derivation of A that there exists a term t such that

$$T \vdash_{\mathsf{SE}} x_1 : B_1 \wedge ... \wedge x_n : B_n \to t : A.$$

Thus

$$T \vdash_{\mathsf{SE}} x_1 : B_1 \wedge ... \wedge x_n : B_n \to s_1 * ... * s_{i-1} * t * s_{i+1} * ... * s_{n_f} : A.$$

Substitute t for s_i everywhere in $\mathcal{D}'$. The built-in substitution property **jv** ensures that this doesn't affect the already established derivability results. □

3.5 Applications

The semiring interpretation of evidence has a wide range of applications. Many of them require a particular choice of the semiring. The following are of particular interest to us (see also [29]):

- $V = ([0, 1], \max, \cdot, 0, 1)$ is called the Viterbi semiring. We can think of the elements of V as *confidence scores* and use them to model trust.
- $T = (\mathbb{R}^{\infty}_{+}, \min, +, \infty, 0)$ is called the tropical semiring. This is connected to *shortest path problems*. In the context of epistemic logic, we can employ this semiring to model the costs of obtaining knowledge. Among other things, this might provide a fresh perspective on the logical omniscience problem, related to the approaches in [11–13].

- $P = (\mathcal{P}(S), \cup, \cap, \emptyset, S)$ is called the powerset lattice (semiring). This is closely related to the recently introduced subset models for justification logic [36–38]. This semiring can be used to model probabilistic evidence and aggregation thereof, see, e.g., [8].
- $F = ([0,1], \max, \max(0, a + b - 1), 0, 1)$ is called the Łukasiewicz semiring. We can use it to model fuzzy evidences. Ghari [25] provides a first study of fuzzy justification logic that is based on this kind of operations for combining evidence.

Another stream of possible applications emerges from the fact that terms with variables represent actual functions. If the underlying semiring is ω-continuous, then the induced polynomial functions are ω-continuous and, therefore, monotone [32]. Hence, they have least and greatest fixed points. Thus it looks very promising to consider this kind of semirings to realize modal fixed point logics like common knowledge (see Chapter 4).

Common knowledge of a proposition A is a fixed point of $\lambda X.(\mathsf{E}A \wedge \mathsf{E}X)$. There are justification logics with common knowledge available [5, 18] but their exact relationship to modal common knowledge is still open.

Chapter 4
Realization of Common Knowledge

In this chapter, which is based on [15], we introduce the justification logic SE_K, which uses polynomials over a semiring as justification terms. Then we relate our justification logic to the modal logic of common knowledge. Instead of just one $\Box$ operator it has $\Box_1, ..., \Box_n$ representing knowledge of multiple agents. Further it is extended by the common knowledge operator C, where CA is informally defined as everybody knows A, everybody knows that everybody knows A and so on. Everybody knows A is usually written as EA and this leads to $CA = EA \wedge ECA$. So CA is a fixed point of the function $f(x) = EA \wedge Ex$. If a formula is derivable in common knowledge then our realization procedure generates terms to replace the modal operators with while maintaining derivability.

On the mathematical side we use ω-continuous semirings and the Kleene fixed point theorem from lattice theory. In contrast to rings there is no need for additive inverses in semirings. This can lead to a partial order: a is less than b if the sum of a and some other element equals b. For a semiring to be ω-continuous this has to be the case and further there is an infinitary sum operation satisfying some natural properties, which include matching the supremum of partial sums. Then it is interesting to consider Scott-continuous functions (they commute with the supremum) on such semirings. The Kleene fixed point theorem states that a Scott-continuous function f on a ω-continuous semiring has a fixed point, which can be written as $sup\{0, f(0), f(f(0)), ...\}$.

With terms constructed from schematic letters the algorithm would yield an infinite term as the fixed point. Therefore we use in this chapter the elements of a semiring as justification terms. This allows us to apply the Kleene fixed point theorem. If $f(x) = x$ then $f(x) : A \to x : A$ is trivial. This is needed for two different things:

- In Common Knowledge the common knowledge operator C is a fixed point, which can be defined as $CA = EA \wedge ECA$. The Kleene fixed point theorem ensures the existence of a suitable term for realizing C.
- Further it delivers a realization procedure for the modus ponens rule. The applications of the modus ponens rule in a proof build together a system of equations, which in the context of normal realizations turns out to be of the form $x = f(x)$.

By using the elements of the semiring directly as justification terms, we create a logic that lies between a justification logic in the traditional sense and its semantics. We are convinced that it is also possible to form the justification terms from constants, variables and operators, similar to [16]. This would be a lot more work, because one additionally has to deal with properties of semirings like infinite sums. In our setting properties of the semiring automatically transfer to the logic.

4.1 The Syntax of $\mathsf{SE_K}$

Having the mathematical background we continue by defining the justification language for the logic $\mathsf{SE_K}$. Let K be a semiring and $\mathsf{JVar} = \{x_1, x_2, ...\}$ a countably infinite set of variables. Justification terms are polynomials over K in variables JVar and inductively defined as

$$s \in S,\ x \in \mathsf{JVar},\ t_1 + t_2, \quad \text{and} \quad t_1 \cdot t_2,$$

where t_1 and t_2 are justification terms and $+, \cdot$ are the operations from the semiring. The set of all justification terms is called Tm. A justification term that does not contain variables is called *ground term*. GTm $(= S)$ denotes the set of all ground terms. Often we write only *term* for *justification term*. Since terms *are* polynomials over K, for example x and $x \cdot 1$ are the same term. We can consider terms as functions over S, $t : S^n \to S$, where n is the number of different variables occurring in t. The range of t is $range(t) := t(S^n)$ as expected. Further, we need a countable set of atomic propositions $\mathsf{Prop} = \{P_1, P_2, ...\}$. Now we define the set of formulas Fml as follows:

- $\bot \in \mathsf{Fml}$,
- $P \in \mathsf{Fml}$, where $P \in \mathsf{Prop}$,
- $A \to B \in \mathsf{Fml}$, where $A, B \in \mathsf{Fml}$,
- $t : A \in \mathsf{Fml}$, where $t \in \mathsf{Tm}$ and $A \in \mathsf{Fml}$.

The remaining logical connectives $\neg$, $\wedge$, $\vee$, and $\leftrightarrow$ are abbreviations as usual. The set of ground formulas GFml consists of all formulas without variables. Now we can define a deductive system for the logic $\mathsf{SE_K}$ about the semirings of evidence. It consists of the following axioms:

CL	Every instance of a propositional tautology
j	$x : (A \to B) \to (y : A \to x \cdot y : B)$
j+	$x : A \wedge y : A \leftrightarrow (x + y) : A$

The rules of $\mathsf{SE_K}$ are:

$$\textbf{MP}\quad \frac{A \qquad A \to B}{B},$$

$$\textbf{jv}\quad \frac{A}{A[x/t]}$$

and

$$\textbf{jx}\quad \frac{A[x/s] \text{ for all } s \in range(t)}{A[x/t]}$$

where x is a variable, $s \in S$, t is a term, and $A[x/t]$ denotes the result of substituting t for x in A.

A theory T is a subset of Fml. Having a rule with possibly infinitely many premises forces a definition of a proof different than a sequence of formulas constructed according to the rules. Therefore a proof for a formula A from a theory T is a tree with A on the root and axioms or elements of T on the leafs

constructed according to the rules of $\mathsf{SE_K}$, such that every branch has a finite length. This allows us to prove properties by induction on the proof. If there exists a proof for A then A is derivable from T, which we denote by $T \vdash_{\mathsf{SE_K}} A$.

Example 1. We define $K = (\mathbb{N}, +, \cdot, 0, 1)$ and $T = \{1 : A\}$. By **j+** we get $T \vdash_{\mathsf{SE_K}} n : A$ for all $n \in \mathbb{N}$. This is exactly the meaning of $x : A$, which we derive by using **jx**.

Example 2. We define $K = (\mathcal{P}(\mathbb{N}), \cup, \cap, \emptyset, \mathbb{N})$, $X = \{n \in \mathbb{N} \mid n \text{ is even}\}$ and $T = \{X : A\}$. By **j+** we get $T \vdash_{\mathsf{SE_K}} N : A$ for all $N \subseteq X$. This is exactly the meaning of $(x \cap X) : A$, which we derive by using **jx**.

4.2 The Semantics of $\mathsf{SE_K}$

In this section we denote the semiring always by $K = (S, +, \cdot, 0, 1)$. We define a valuation as a function from JVar to S. This extends to terms by commuting with the semiring operations. It further extends to formulas in the obvious way. We denote the result of applying the valuation v to the formula A by A_v.

Definition 1 (Evidence relation). *$J \subseteq S \times \mathsf{GFml}$ is an* evidence relation *if for all $s, t \in S$ and all ground formulas A, B:*

1. *$J(s, A \to B)$ and $J(t, A)$ imply $J(s \cdot t, B)$*
2. *$J(s, A)$ and $J(t, A)$ is equivalent to $J(s + t, A)$*

Definition 2 (Semiring model). *A* semiring model *is a tuple $M = (*, J)$ where*

1. *$*$ is a truth assignment for atomic propositions, i.e., $* : \mathsf{Prop} \to \{\mathbb{F}, \mathbb{T}\}$*
2. *J is an evidence relation.*

Definition 3 (Truth in a semiring model). *Let $M = (*, J)$ be a semiring model and $A \in \mathsf{GFml}$. $M \Vdash A$ is defined as follows:*

- *$M \nVdash \bot$*
- *$M \Vdash P$ iff $P^* = \mathbb{T}$*
- *$M \Vdash A \to B$ iff $M \nVdash A$ or $M \Vdash B$*
- *$M \Vdash s : A$ iff $J(s, A)$*

For an arbitrary $A \in \mathsf{Fml}$ we set $M \Vdash A$ iff $M \Vdash A_v$ for all valuations v.

Truth in a theory means it is true in all models satisfying the theory: $T \Vdash A$ if $M \Vdash A$ for all M with $M \Vdash T$.
The following lemma states that substituting a variable by a term has the same effect as using a different valuation. This proves soundness in the case **jv**.

Lemma 1. *Let v and w be valuations with $x_v = t_w$ for a variable x and a term t and $y_v = y_w$ for every other variable. Then for all $A \in \mathsf{Fml}$*

$$A_v = A[x/t]_w.$$

The proof is straightforward by induction on the structure of A. Next we prove a similar lemma for the case **jx**.

Lemma 2. *Let $M = (*, J)$ be a semiring model, t a term and A a formula. Then*

$$M \Vdash A[x/s] \text{ for all } s \in range(t) \quad \textit{iff} \quad M \Vdash A[x/t].$$

Proof. $M \Vdash A[x/s]$ for all $s \in range(t)$
$\Leftrightarrow M \Vdash A[x/s]_v$ for all $s \in range(t)$ and all v (truth in a semiring model)
$\Leftrightarrow M \Vdash A[x/t_v]_v$ for all v (t_v quantified over all v gives $range(t)$)
$\Leftrightarrow M \Vdash A[x/t]_v$ for all v (t is evaluated anyway)
$\Leftrightarrow M \Vdash A[x/t]$ (truth in a semiring model)
□

With these two lemmas we can easily prove soundness.

Theorem 1 (Soundness). *Let T be an arbitrary theory. Then:*

$$T \vdash F \quad \textit{implies} \quad T \Vdash F.$$

Proof. By induction on the depth of the derivation tree of F. Let $M = (*, J)$ be a semiring model such that $M \Vdash T$. If we are able to show $M \Vdash F_v$ for an arbitrary valuation v, we have shown $M \Vdash F$.

1. $F \in T$. Trivial.
2. **CL**. Trivial.
3. **j**. Assume $M \Vdash (x : (A \to B))_v$ and $M \Vdash (y : A)_v$. That is $J(x_v, (A \to B)_v)$ and $J(y_v, A_v)$ hold, which by Definition 1 implies $J(x_v \cdot y_v, B_v)$. Because of $x_v \cdot y_v = (x \cdot y)_v$ we get $J((x \cdot y)_v, B_v)$, which yields $M \Vdash (x \cdot y : B)_v$.
4. **j+**. $M \Vdash (x : A)_v$ and $M \Vdash (y : A)_v$ is equivalent to $J(x_v, A_v)$ and $J(y_v, A_v)$, which by Definition 1 is equivalent to $J(x_v + y_v, A_v)$ and $M \Vdash (x + y : A)_v$.
5. **MP**. Trivial.
6. **jv**. $M \Vdash A_w$ for all valuations w by induction hypothesis. Given the term t we find that there exists a valuation w such that $t_v = x_w$. By Lemma 1 we get $M \Vdash A[x/t]_v$.
7. **jx**. $M \Vdash A[x/s]$ for all $s \in range(t)$ by induction hypothesis. $M \Vdash A[x/t]$ follows by Lemma 2. □

For the completeness proof we fix a set of atomic propositions $\mathsf{Prop2}$ with $\mathsf{Prop} \cap \mathsf{Prop2} = \emptyset$ and a bijection $f : S \times \mathsf{GFml} \to \mathsf{Prop2}$. $\mathsf{Prop2}$ needs to have the same cardinality as $S \times \mathsf{GFml}$. Then we define the translation $'$ for ground formulas as follows:

- $\bot' = \bot$
- $P' = P$ for $P \in \mathsf{Prop}$
- $(A \to B)' = A' \to B'$
- $(s : A)' = f(s, A)$

For a theory T we define $T' := \{(A_v)' \mid A \in T \text{ or } A \text{ is an axiom of } \mathsf{SE_K}, v \text{ is a valuation}\}$. We get the following lemma.

Lemma 3. *$T \vdash_{\mathsf{SE_K}} A \Leftrightarrow T' \vdash_{\mathsf{CL}} (A_v)'$ for all valuations v*

Proof. Left to right by induction on a derivation of A:

- If $A \in T$ or A is an axiom then $(A_v)' \in T'$ for all valuations v.
- If A is derived from $B \to A$ and B by **MP** then the induction hypothesis is $T' \vdash_{\mathsf{CL}} ((B \to A)_v)'$ and $T' \vdash_{\mathsf{CL}} (B_v)'$. From the first part we get $T' \vdash_{\mathsf{CL}} (B_v)' \to (A_v)'$, then we use **MP** to obtain $T' \vdash_{\mathsf{CL}} (A_v)'$.
- If $A[x/t]$ is derived from A by **jv** then the I.H. is $T' \vdash_{\mathsf{CL}} (A_w)'$. Since for every v there is a w such that $A[x/t]_v = A_w$, we get $T' \vdash_{\mathsf{CL}} (A[x/t]_v)'$.
- If $A[x/t]$ is derived from $A[x/s]$ for all $s \in \mathit{range}(t)$ by **jx** then the I.H. is $T' \vdash_{\mathsf{CL}} (A[x/s]_w)'$ for all $s \in \mathit{range}(t)$. For an arbitrary valuation v there is $s \in \mathit{range}(t)$ with $s = t_v$. It follows $A[x/t]_v = A[x/s]_v$ and therefore $T' \vdash_{\mathsf{CL}} (A[x/t]_v)'$.

For the direction from right to left we prove first $T \vdash_{\mathsf{SE_K}} A$ for $A \in \mathsf{GFml}$ from the assumption $T' \vdash_{\mathsf{CL}} A'$ by induction on a derivation of A'. Note that there is an unique $A \in \mathsf{GFml}$ given A'.

- If $A' \in T'$ then A is derived using **jv** on an $\mathsf{SE_K}$-axiom or on an element of T.
- If A' is an instance of **CL** then so is A, because f is injective.
- If A' is obtained by **MP** from $B \to A'$ and B then we use the formula C with $C' = B$. We have $T \vdash_{\mathsf{SE_K}} C \to A$ and $T \vdash_{\mathsf{SE_K}} C$ by I.H. which leads to $T \vdash_{\mathsf{SE_K}} A$.

Let $A \in \mathsf{Fml}$ such that $T' \vdash_{\mathsf{CL}} (A_v)'$ for all valuations v. From above we get $T \vdash_{\mathsf{SE_K}} A_v$ for all valuations v. We obtain $T \vdash_{\mathsf{SE_K}} A$ by applying **jx** for every variable that occurs in A. □

Now that we can switch between $\mathsf{SE_K}$ and CL we can use the completeness of CL to obtain completeness for $\mathsf{SE_K}$.

Theorem 2 (Completeness). *Let T be an arbitrary theory. Then:*

$$T \Vdash F \quad \textit{implies} \quad T \vdash F.$$

Proof. Assume $T \nvdash F$. By Lemma 3 there exists a valuation w such that

$$T' \nvdash_{\mathsf{CL}} (F_w)'.$$

The completeness of CL delivers $* : \mathsf{Prop} \cup \mathsf{Prop2} \to \{\mathbb{F}, \mathbb{T}\}$, such that for the CL-model M_* consisting of $*$ we have $M_* \Vdash T'$ and $M_* \nVdash (F_w)'$. Now we can define the semiring model M:

- $M := (*|_{\mathsf{Prop}}, J)$
- $*|_{\mathsf{Prop}}$ is the restriction of $*$ to Prop
- $J := \{(s, A) \mid M_* \Vdash f(s, A)\}$

In order to prove that M is a semiring model, we need to show that J is an evidence relation.

1. Assume $J(s, A \to B)$ and $J(t, A)$, so $A \in \mathsf{GFml}$ and $A \to B \in \mathsf{GFml}$
   $\Rightarrow M_* \Vdash f(s, A \to B)$ and $M_* \Vdash f(t, A)$ (by definition of J)
   $M_* \Vdash (x : (A \to B) \to (y : A \to x \cdot y : B))'_v$ for all v ($M_* \Vdash T'$)
   $\Rightarrow M_* \Vdash (s : (A \to B) \to (t : A \to s \cdot t : B))'$ (for v with $x_v = s$ and $y_v = t$)
   $\Leftrightarrow M_* \Vdash f(s, A \to B) \to (f(t, A) \to f(s \cdot t, B))$ (by definition of f and $'$)
   $\Rightarrow M_* \Vdash f(s \cdot t, B)$ (truth in a CL-model)
   $\Rightarrow J(s \cdot t, B)$ (by definition of J)
2. $M_* \Vdash ((x : A \wedge y : A \leftrightarrow x + y : A)_v)'$ for all v ($M_* \Vdash T'$)
   $\Rightarrow M_* \Vdash (s : A \wedge t : A \leftrightarrow s + t : A)'$ (for v with $x_v = s$ and $y_v = t$)
   $\Leftrightarrow M_* \Vdash f(s, A) \wedge f(t, A) \leftrightarrow f(s + t, A)$ (by definition of f and $'$)
   $\Rightarrow J(s, A)$ and $J(t, A)$ is equivalent to $J(s + t, A)$ (by definition of J)

Knowing that M is a semiring model we prove

$$M_* \Vdash A' \Leftrightarrow M \Vdash A \text{ for all } A \in \mathsf{GFml}$$

by induction on the structure of A.

- Case $A = \bot$. $M_* \nVdash \bot'$ and $M \nVdash \bot$.
- Case $A = P$, where $P \in \mathsf{Prop}$. $M_* \Vdash P' \Leftrightarrow M_* \Vdash P \Leftrightarrow P^* = \mathbb{T} \Leftrightarrow M \Vdash P$.
- Case $A = B \to C$. $M_* \Vdash (B \to C)'$
  $\Leftrightarrow M_* \Vdash B' \to C'$
  $\Leftrightarrow M_* \nVdash B'$ or $M_* \Vdash C'$
  $\Leftrightarrow M \nVdash B$ or $M \Vdash C$ (by induction hypothesis)
  $\Leftrightarrow M \Vdash B \to C$.
- Case $A = s : B$. $M_* \Vdash (s : B)'$
  $\Leftrightarrow M_* \Vdash f(s, B)$ (by definition of $'$)
  $\Leftrightarrow J(s, B)$ (by definition of J)
  $\Leftrightarrow M \Vdash s : B$.

Now we show $M \Vdash T$. Let $A \in T$. We get $(A_v)' \in T'$ for all valuations v by definition of T'. We know $M_* \Vdash T'$, which means $M_* \Vdash (A_v)'$ for all valuations v. By using the previously proved equivalence we obtain $M \Vdash A_v$ for all valuations, which is $M \Vdash A$. From $M_* \nVdash (F_w)'$ we get $M \nVdash F_w$ and therefore $M \nVdash F$. □

4.3 Realization of Common Knowledge

This section investigates in the relationship between $\mathsf{S_{Ax}}$ and $\mathsf{SE_K}$. We show that if a theory has certain properties, we can replace each set in a $\mathsf{S_{Ax}}$ theorem by a term and get a formula that is derivable in $\mathsf{SE_K}$ from the theory. We begin by defining one such property: axiomatic appropriateness.

Definition 4. *A theory T is called axiomatically appropriate if for each A that is in T or is an axiom there is a variable x not occurring in A such that $x : A \in T$.*

Axiomatic appropriateness is used to deal with the rule **C-Nec** of $\mathsf{S_{Ax}}$. Having a universally quantified variable as a justification matches the idea that all agents are aware of the theory and the axioms. The existence of a variable x with $x : A \in T$ for $A \in T$ and axioms A extends to all derivable formulas.

Lemma 4 (Internalization). *Let T be an axiomatically appropriate theory. For any formula A, there exists a variable x not occurring in A such that*

$$T \vdash_{\mathsf{SE_K}} A \quad \textit{implies} \quad T \vdash_{\mathsf{SE_K}} x : A.$$

Proof. By induction on the derivation of A.

- If $A \in T$ or A is an axiom then such a variable exists by the definition of axiomatic appropriateness.
- If B is derived from A and $A \to B$ by **MP** then by induction hypothesis we have $x : A$ and $y : (A \to B)$. Because x doesn't occur in A we get $1 : A$ by **jv**. From $y : (A \to B) \to (1 : A \to y : B)$, which is derived from an instance of **j** by **jv**, we derive $y : B$.
- If $A[x/t]$ is derived from A by **jv** then by induction hypothesis we have $y : A$. We use **jv** to replace y with a variable z not occurring in A or $A[x/t]$ and $z \neq x$. We obtain $z : A[x/t]$ by using **jv** again.
- If $A[x/t]$ is derived by **jx** then by induction hypothesis for every $A[x/s]$ with $s \in \mathit{range}(t)$ there is such a variable. Because all the $A[x/s]$ contain the same variables we can find a variable y not occurring in $A[x/t]$ or any of the $A[x/s]$ and $y \neq x$. We use **jv** to obtain $y : A[x/s]$ for all $s \in \mathit{range}(t)$ and then **jx** delivers $y : A[x/t]$. □

Corollary 1. *Let T be an axiomatically appropriate theory. For any formula A and term t*

$$T \vdash_{\mathsf{SE_K}} A \quad \textit{implies} \quad T \vdash_{\mathsf{SE_K}} t : A.$$

4.3.1 Supporting concatenation

In this subsection we deal with **Set axioms 2**. In $\mathsf{S_{Ax}}$ $R(SA)$ is equivalent to $(RS)A$, meaning that two sets can always be concatenated and a set can be split up. The built in semiring K lacks such an operation. Therefore we add a whole semiring L, which implements concatenation as the multiplication operation while the additive monoid is shared with K.

Definition 5. *Let $L = (S, +, *, 0, 1_L)$ be a semiring. A theory T* supports concatenation *if $a : b : A \leftrightarrow a * b : A \in T$ for all $a, b \in S$ and $A \in \mathsf{Fml}$.*

4.3.2 The induction principle

In common knowledge we have the induction axiom $EA \wedge C(A \to EA) \to CA$. From $C(A \to EA)$ we derive $E(A \to EA)$ and $EC(A \to EA)$ by the closure axiom. From the first one we get $EA \to EEA$ and from the second one we continue by $EE(A \to EA)$ which gives $EEA \to EEEA$ and so on. Now that we have EA we can put these together and derive $EA \wedge EEA \wedge EEEA \wedge ...$ which is CA. The only reason why the induction axiom is not derivable is that it would need infinitely many derivation steps.

This derivation process works in $\mathsf{SE_K}$ analogously. We define the sequence corresponding to E^n, then use the axiom $\mathsf{j+}$ to put the evidence into a single justification term. Because the derivation also fails when stepping up to the infinite sum, we make use of the theory.
Let $K = (S, +, \cdot, 0, 1_K)$ and $L = (S, +, *, 0, 1_L)$ be ω-continuous semirings and $a, b, c \in S$. We define $ind : S^3 \to S$ as $ind_0(a, b, c) := a$, $ind_{n+1}(a, b, c) := (b \cdot ind_n(a, b, c)) * c$ and finally $ind(a, b, c) := \sum_{n\in\mathbb{N}} ind_n(a, b, c)$.

Definition 6. *A theory T supports induction if*

$$a : A \wedge b : (A \to c : A) \to ind(a, b, c) : A \in T \text{ for all } A \in \mathsf{Fml} \text{ and } a, b, c \in S.$$

Note that $T \vdash_{\mathsf{SE_K}} a : A \wedge b : (A \to c : A) \to \sum_{k=0}^{n} ind_k(a, b, c) : A$ for all $n \in \mathbb{N}$ if T supports concatenation.

4.3.3 Forgetful projection

When realizing $\mathsf{S4}$ by using the Logic of Proofs LP there is only one forgetful projection, which simply replaces each term with a box. But with $\mathsf{S_{Ax}}$ on the side of modal logic there are multiple modal operators and therefore multiple forgetful projections to consider.
A forgetful projection decides for which agents a term is a justification. Having two terms justifying the same formula is equivalent to saying the sum of these terms justifies the formula. Therefore the sum is a justification for the agents who already had a justification in at least one of the terms. The multiplication is used for the modus ponens. Because $A \to B$ *and* A are needed, the multiplication of the terms is only a justification for those agents which had justifications for both formulas. In conclusion the operations of K and L have to correspond to $\cup$, $\cap$ and $*$.
We additionally restrict forgetful projections by basing them on $f : S \to \mathcal{P}(E^*)$, so $s \in S$ will be assigned $f(s) \in \mathcal{P}(E^*)$ independent to the formula it is justifying.

Definition 7 (Forgetful projection). *Let $K = (S, +, \cdot, 0, 1_K)$ and $L = (S, +, *, 0, 1_L)$ be semirings. A* forgetful projection on K, L *is a function $f : S \to \mathcal{P}(E^*)$ such that for all $a, b \in S$:*

- $f(a + b) = f(a) \cup f(b)$,
- $f(a \cdot b) = f(a) \cap f(b)$,
- $f(a * b) = f(a)f(b)$.

A forgetful projection *is a function $^\circ : \mathsf{GFml} \to \mathcal{L}_\mathcal{S}$ defined as follows:*

- $\bot^\circ := \bot$
- $P^\circ := P$
- $(A \to B)^\circ := A^\circ \to B^\circ$
- $(s : A)^\circ := f(s)A^\circ$.

Note that forgetful projections are only defined for ground formulas. For example $x : P \to x : Q$ cannot be represented by a single formula of common knowledge, because there is no quantification over whole formulas. For example the $\mathcal{L}_\mathcal{S}$ formula $SP \to SQ$ is read as $(sP\ \forall s \in S)$ implies $(sQ\ \forall s \in S)$. Therefore it is not possible to define the forgetful projection for formulas containing variables. However we can define T° for arbitrary theories by including $(A_v)^\circ$ in T° for all valuations v and $A \in T$.

Lemma 5. *Let T be a theory and $^\circ$ a forgetful projection. Then for all $A \in \mathsf{GFml}$*

$$T \vdash_{\mathsf{SE_K}} A \text{ implies } T^\circ \vdash_{\mathsf{S_{Ax}}} A^\circ.$$

Proof. We prove $T^\circ \vdash_{\mathsf{S_{Ax}}} (A_v)^\circ$ for all valuations v and $A \in \mathsf{Fml}$ by induction on a derivation of A. When we write A°_v, the valuation v is applied before $^\circ$.

- $A \in T$ implies $(A_v)^\circ \in T^\circ$ by definition of T°.
- If A is an instance of **CL** then so are all $(A_v)^\circ$.
- **j**. $(x : (A \to B) \to (y : A \to x \cdot y : B))^\circ_v$
  $= (x_v : (A_v \to B_v) \to (y_v : A_v \to x_v \cdot y_v : B_v))^\circ$
  $= f(x_v)(A^\circ_v \to B^\circ_v) \to (f(y_v)A^\circ_v \to (f(x_v) \cap f(y_v))B^\circ_v)$.
  This is derivable from the modal axiom
  $(f(x_v) \cap f(y_v))(A^\circ_v \to B^\circ_v) \to ((f(x_v) \cap f(y_v))A^\circ_v \to (f(x_v) \cap f(y_v))B^\circ_v)$
  by using **Set axioms 1** and propositional reasoning.
- **j+**. $(x : A \wedge y : A \leftrightarrow x + y : A)^\circ_v = (x_v : A_v \wedge y_v : A_v \leftrightarrow x_v + y_v : A_v)^\circ$
  $= (f(x_v)A^\circ_v \wedge f(y_v)A^\circ_v \leftrightarrow f(x_v + y_v)A^\circ_v)$
  $= (f(x_v)A^\circ_v \wedge f(y_v)A^\circ_v \leftrightarrow (f(x_v) \cup f(y_v))A^\circ_v)$, which is an instance of **Set axioms 1**.
- **MP**. If B is derived from $A \to B$ and A then by induction hypothesis $(A \to B)^\circ_v = A^\circ_v \to B^\circ_v$ and A°_v are derivable. B°_v follows by **MP**.
- **jv**. If $A[x/t]$ is derived from A then by induction hypothesis A°_w is derivable for all valuations w. Let v be an arbitrary valuation. For the valuation w defined as $w(x) = t_v$ and $w(y) = v(y)$ if $y \neq x$ we get $A_w = A[x/t]_v$ by Lemma 1 and therefore $A[x/t]^\circ_v$ is derivable.
- **jx**. If $A[x/t]$ is derived from $A[x/s]$ for all $s \in \mathit{range}(t)$ then by induction hypothesis $T^\circ \vdash_{\mathsf{S_{Ax}}} A[x/s]^\circ_w$ for all $s \in \mathit{range}(t)$ and w. Let v be an arbitrary valuation. For the valuation w defined as $w(x) = t_v$ and $w(y) = v(y)$ if $y \neq x$ we get $A_w = A[x/t]_v$ by Lemma 1. Further there exists a $s \in \mathit{range}(t)$ with $s = t_v$, so $A_w = A[x/s]_w$. From $A[x/s]_w = A[x/t]_v$ we finally conclude $T^\circ \vdash_{\mathsf{S_{Ax}}} A[x/t]^\circ_v$. □

4.3.4 The realization mapping

Given a forgetful projection we can map ground formulas to $\mathcal{L}_\mathcal{S}$-formulas. Now we define the realization mapping as an inverse to the given forgetful projection. Instead of forgetting information we now want to generate it, which will lead to many different possibilities on how to do this.

Definition 8 (Realization). *Let $^\circ$ be a forgetful projection. A* realization *r is a mapping from $\mathcal{L}_\mathcal{S}$ to* GFml *such that $r(A)^\circ = A$ for all $A \in \mathcal{L}_\mathcal{S}$.*

We also want to define what a normal realization is in this context. Usually a normal realization is a realization that replaces distinct negative occurrences of $\Box$ by distinct variables. The problem is the following: Our variables range over all elements of the semiring, which means that they represent all $X \in \mathcal{P}(E^*)$ and there is no term ranging exactly over $f^{-1}(X)$. We solve this problem by using abstract variables and functions. The idea is that we can always write for example $0 : P$ and $1 : P$ as $z : P$ for $z \in \{0, 1\}$.

Definition 9. *Let $K = (S, +, \cdot, 0, 1)$ be a semiring. We define* abstract formulas *as follows:*

1. *$Z = \{z_1, z_2, ...\}$ is a countably infinite set of* abstract variables*.*
2. *Each abstract variable $z_i \in Z$ has a domain $A_i \subseteq S$.*
3. *Every $g : A_{i_1} \times ... \times A_{i_n} \to S$ is an* abstract term *(n is the number of abstract variables). The set of all abstract terms is denoted by* ATm*.*
4. *The set of all* abstract formulas *is denoted by* AFml *and inductively defined as $\bot$, $P \in \mathsf{Prop}$, $A \to B$ and $g : A$, where $A, B \in \mathsf{AFml}$ and $g \in \mathsf{ATm}$.*

By using a valuation z for abstract variables we can map $g \in \mathsf{ATm}$ to $g_z \in S$ and $A \in \mathsf{AFml}$ to $A_z \in \mathsf{GFml}$. For $A \in \mathsf{AFml}$ we define $T \vdash_{\mathsf{SE_K}} A$ as $T \vdash_{\mathsf{SE_K}} A_z$ for all z. We avoid abstract formulas in theories in order to not mix variables with abstract variables. Given a forgetful projection on K, L f and $^\circ$ it makes sense to extend $^\circ$ for $A \in \mathsf{AFml}$ if for every $g \in \mathsf{ATm}$ occurring in A we have $|\{f(g_z) \mid z \text{ is a valuation}\}| = 1$. Then we pick an arbitrary valuation z and set

- $\bot^\circ = \bot$
- $P^\circ = P$
- $(A \to B)^\circ = A^\circ \to B^\circ$
- $(g : A)^\circ = f(g_z)A^\circ$.

Definition 10. *Let f be a forgetful projection on K, L and $^\circ$ the corresponding forgetful projection. $A \in \mathsf{AFml}$ realizes $B \in \mathcal{L}_\mathcal{S}$ normally if each negative set occurrence R in B is realized by a distinct abstract variable with domain $f^{-1}(R)$, A° is defined and equal to B.*

Definition 11. *Let f be a forgetful projection on K, L and $^\circ$ the corresponding forgetful projection. A* normal realization *r is a mapping from $\mathcal{L}_\mathcal{S}$ to* AFml *such that $r(A)$ realizes A normally for all $A \in \mathcal{L}_\mathcal{S}$.*

It is obvious that for all valuations z for abstract variables and normal realizations r the mapping $A \mapsto r(A)_z$, where $A \in \mathcal{L}_\mathcal{S}$, is a realization.

4.3.5 Minimal Realization

In this subsection we define the smallest semiring K, such that there is a realization in $\mathsf{SE_K}$. The semiring contains for each $R \subseteq E^*$ exactly one element, which we choose to be equal to R in order to keep things simple.
For $h \in \mathbb{N}_{>0}$ we recall $E = \{\Box_1, ..., \Box_h\}$. We obtain the semiring K by setting $K = (\mathcal{P}(E^*), \cup, \cap, \emptyset, E^*)$ and L by $L = (\mathcal{P}(E^*), \cup, *, \emptyset, \{\epsilon\})$. Later we will refer to these semirings as K_{min} and L_{min}. Obviously the identity function is a forgetful projection, which we denote by $^{\circ_{min}}$.

Theorem 3 (Minimal Realization). *There exists a realization r such that*

$$T^{\circ_{min}} \vdash_{\mathsf{S_{Ax}}} A \quad \Leftrightarrow \quad T \vdash_{\mathsf{SE_K}} r(A)$$

for all $A \in \mathcal{L}_\mathcal{S}$ and every axiomatically appropriate theory T that supports concatenation and induction.

We omit the proof because it is a special case of the main theorem. The realization r can be defined as follows: $r(\bot) = \bot$, $r(P) = P$, $r(A \to B) = r(A) \to r(B)$ and $r(SA) = S : r(A)$. It is the only inverse to this forgetful projection. Even though the minimal realization theorem is trivial, it shows how some of the pieces connect.

4.3.6 General Realization

We construct a more general realization in two steps. First we find (initial) terms such that all the axioms are derivable. Second we restrict them in order to make the application of the modus ponens rule possible. For the second step it is important that the initial terms are general enough. In ω-continuous semirings this corresponds exactly to normal realizations.

Definition 12 (Semiring-homomorphism). *Let K_1 and K_2 be two semirings with domains S_1 and S_2. A semiring-homomorphism from K_1 to K_2 is a function $f : S_1 \to S_2$ such that for all $a, b \in S_1$:*

1. $f(a + b) = f(a) + f(b)$
2. $f(a \cdot b) = f(a) \cdot f(b)$

Note that the operations in K_1 and K_2 are not necessarily the same, but it is always clear from the context, which one is meant. Let $K = (S, +, \cdot, 0, 1)$ be a semiring and f a semiring-homomorphism from K to the semiring K_{min} from the previous subsection. Suppose $f(a) = f(b)$ for some $a, b \in S$. We find $f(a + b) = f(a) + f(b) = f(a) \cup f(b) = f(a) = f(b)$ and the same for the multiplication. This shows that the sets $f^{-1}(a)$ defined as $\{c \in S \mid f(c) = a\}$ are closed under addition and multiplication.

Given $A \in \mathcal{L}_\mathcal{S}$ we assign a 0-1-sequence to each occurrence of a subformula in A and each occurrence of a set:

- A itself has the empty sequence (length 0),

- given the sequence of $B \to C$ as $\alpha_1...\alpha_n$ then the sequence $\alpha_1...\alpha_n 0$ is assigned to C and the sequence $\alpha_1...\alpha_n 1$ is assigned to B,
- given the sequence of SB as $\alpha_1...\alpha_n$ then the same sequence is assigned to S and $\alpha_1...\alpha_n 0$ is assigned to B.

This transfers to $A \in \mathsf{Fml}$ and $A \in \mathsf{AFml}$ in the obvious way. Now we define a set occurrence within $A \in \mathcal{L}_\mathcal{S}$ formally as the tuple (α, A) and a set occurrence within an $\mathsf{S_{Ax}}$-proof as (α, p), where p is a node in the proof tree. The set of all sequences assigned to set occurrences in A is denoted by $\alpha(A)$. We can easily assign a polarity to a set occurrence (α, A) by defining the sum of a sequence $\alpha = \alpha_1...\alpha_n$ as $\sum \alpha := \sum_{i=1}^{n} \alpha_i$ and the polarity as $P(\alpha, A) := (-1)^{\sum \alpha}$.
If α is the sequence assigned to the subformula SB of $A \in \mathcal{L}_\mathcal{S}$, we extract the set from the occurrence by setting $\langle \alpha, A \rangle := S$. We use the same notation for $A \in \mathsf{Fml}$ and $A \in \mathsf{AFml}$ to extract the (abstract) term.
For a node p we denote the formula it is labelled with by $\langle p \rangle$. In an $\mathsf{S_{Ax}}$-proof we call two set occurrences *related* if one of the following conditions holds:

1. (α, p) is related to itself.
2. If $\langle p \rangle = A$, $\langle q \rangle = CA$ and q is the successor of p then (α, p) and $(0\alpha, q)$ are related.
3. If $\langle p_1 \rangle = A \to B$, $\langle p_2 \rangle = A$ and they have a common successor q with $\langle q \rangle = B$ then $(0\alpha, p_1)$ and (α, q) are related.

We close this symmetric relation under transitivity. Then all set occurrences are split into disjoint families. We see that all set occurrences in a family contain the same set and have the same polarity, because $(-1)^{\sum 0\alpha} = (-1)^{\sum \alpha}$. Let f be a family. If $(\alpha, A) \in f$ we assign the polarity $P(f) := P(\alpha, A)$ to the family and we set $\langle f \rangle := \langle \alpha, A \rangle$.
Two set occurrences in the same formula always belong to different families and all the members of a family are on the same branch of the derivation tree, which implies an order.
The ability to address one specific term or set occurrence within a formula allows us to define a different type of substitution: We define $A[\alpha/t]$ to be the formula resulting from A by substituting the occurrence (α, A) with the term $t \in \mathsf{ATm}$. This is needed in the formulation of the following lemma, which states that positive occurrences can be decreased and negative occurrences increased, while maintaining derivability.

Lemma 6. *Let T be an axiomatically appropriate theory, s an element of the semiring, $A \in \mathsf{GFml}$ and α a 0-1-sequence assigned to a term in A. If ($s \leq \langle \alpha, A \rangle$ and $P(\alpha, A) = 1$) or ($s \geq \langle \alpha, A \rangle$ and $P(\alpha, A) = -1$) then $T \vdash_{\mathsf{SE_K}} A \to A[\alpha/s]$.*

Proof. Proof by induction on the structure of A:

- $A = \bot$. $A[\alpha/s] = A$ makes it trivial.
- $A = P$. $A[\alpha/s] = A$ makes it trivial.
- $A = B \to C$. It follows that $\alpha \neq \epsilon$.

- $(\alpha = 0\beta)$: The induction hypothesis is
  $(s \leq \langle \beta, C\rangle$ and $P(\beta, C) = 1)$ or $(s \geq \langle \beta, C\rangle$ and $P(\beta, C) = -1)$ implies $T \vdash_{\mathsf{SE_K}} C \to C[\beta/s]$.
  This is equivalent to
  $(s \leq \langle \alpha, A\rangle$ and $P(\alpha, A) = 1)$ or $(s \geq \langle \alpha, A\rangle$ and $P(\alpha, A) = -1)$ implies $T \vdash_{\mathsf{SE_K}} C \to C[\beta/s]$.
  We derive $(B \to C) \to (B \to C[\beta/s])$ by propositional reasoning, which can be written as $(B \to C) \to (B \to C)[\alpha/s]$.
- $(\alpha = 1\beta)$: By applying the inverse substitution (from $A[\alpha/s]$ to A) we see that the lemma is equivalent to
  $(s \geq \langle \alpha, A\rangle$ and $P(\alpha, A) = 1)$ or $(s \leq \langle \alpha, A\rangle$ and $P(\alpha, A) = -1)$ implies $T \vdash_{\mathsf{SE_K}} A[\alpha/s] \to A$.
  So we write the induction hypothesis as
  $(s \geq \langle \beta, B\rangle$ and $P(\beta, B) = 1)$ or $(s \leq \langle \beta, B\rangle$ and $P(\beta, B) = -1)$ implies $T \vdash_{\mathsf{SE_K}} B[\beta/s] \to B$.
  This is equivalent to
  $(s \geq \langle \alpha, A\rangle$ and $P(\alpha, A) = -1)$ or $(s \leq \langle \alpha, A\rangle$ and $P(\alpha, A) = 1)$ implies $T \vdash_{\mathsf{SE_K}} B[\beta/s] \to B$.
  We derive $(B \to C) \to (B[\beta/s] \to C)$ by propositional reasoning, which can be written as $(B \to C) \to (B \to C)[\alpha/s]$.

– $A = t : B$.

- $(\alpha = \epsilon)$: We have $P(\alpha, A) = 1$. If $s \leq t = \langle \alpha, A\rangle$ then there is r such that $s + r = t$. We derive $t : B \to s : B$ from $\mathbf{j+}$ (and $\mathbf{jv}$) as
  $s : B \wedge r : B \leftrightarrow t : B$.
- $(\alpha = 0\beta)$: The induction hypothesis is
  $(s \leq \langle \beta, B\rangle$ and $P(\beta, B) = 1)$ or $(s \geq \langle \beta, B\rangle$ and $P(\beta, B) = -1)$ implies $T \vdash_{\mathsf{SE_K}} B \to B[\beta/s]$.
  This is equivalent to
  $(s \leq \langle \alpha, A\rangle$ and $P(\alpha, A) = 1)$ or $(s \geq \langle \alpha, A\rangle$ and $P(\alpha, A) = -1)$ implies $T \vdash_{\mathsf{SE_K}} B \to B[\beta/s]$.
  Because T is axiomatically appropriate we can apply the internalization corollary and get $1 : (B \to B[\beta/s])$. From $\mathbf{j}$ we infer $t : B \to t : B[\beta/s]$, which can be written as $t : B \to (t : B)[\alpha/s]$. □

Before we can define the initial terms we need to be able to address the set occurrences in schematic part of the axioms precisely. If we want to realize for example $RA \wedge SA \to (R \cup S)A$ by something of the form $s : A \wedge t : A \to s + t : A$ we need to find the right terms for the occurrences hiding in A. The normal realization forces that the different A's are realized differently. However we will use the previous lemma to derive it from the corresponding axiom.
We define the schematic set of an axiom scheme of $\mathsf{S_{Ax}}$ as a set of sets. Each element corresponds to a schematic letter in an axiom scheme.

Definition 13 (Schematic set).

– $F = A \to (B \to A)$. $ss(F) := \{\{1, 00\}, \{01\}\}$

- $F = (A \to (B \to C)) \to ((A \to B) \to (A \to C))$.
  $ss(F) := \{\{001, 11, 011\}, \{010, 101\}, \{100, 000\}\}$
- $F = ((A \to \bot) \to \bot) \to A$. $ss(F) := \{\{111, 0\}\}$
- $F = RA \wedge SA \to (R \cup S)A = ((RA \to (SA \to \bot)) \to \bot) \to (R \cup S)A$.
  $ss(F) := \{\{1110, 11010, 00\}\}$
- $F = (R \cup S)A \to RA \wedge SA = (R \cup S)A \to ((RA \to (SA \to \bot)) \to \bot)$.
  $ss(F) := \{\{10, 0110, 01010\}\}$
- $F = R(SA) \to (RS)A$. $ss(F) := \{\{100, 00\}\}$
- $F = (RS)A \to R(SA)$. $ss(F) := \{\{10, 000\}\}$
- $F = S(A \to B) \to (SA \to SB)$. $ss(F) := \{\{010, 101\}, \{100, 000\}\}$
- $F = EA \wedge C(A \to EA) \to CA = \neg(EA \to \neg C(A \to EA)) \to CA$
  $= ((EA \to (C(A \to EA) \to \bot)) \to \bot) \to CA$.
  $ss(F) := \{\{1110, 1101000, 00, 110101\}\}$

We see that in a schematic set no sequence is an extension of another. Therefore each set occurrence (α, F) in the schematic part of an axiom can be uniquely written as $(\beta\gamma, F)$, where $\beta \in A \in ss(F)$. We call this the unique composition. The first part defines the occurrence of the schematic letter, the second part the position therein.
For $A \in ss(F)$ we define $A^p := \{\alpha \in A \mid (-1)^{\sum \alpha} = p\}$, where $p \in \{-1, 1\}$. Now we relate two set occurrences in an axiom if they appear in the same position of two different occurrences of the same schematic letter and have opposite polarities.

Definition 14 (Schematic relation). *The* schematic relation R *of an axiom* F *of* $\mathsf{S_{Ax}}$ *is defined for* $\alpha_1 = \beta_1\gamma_1$ *and* $\alpha_2 = \beta_2\gamma_2$ *(unique compositions) as* $\alpha_1 R \alpha_2 \Leftrightarrow \exists A \in ss(F)$, $\beta_1 \in A^x$, $\beta_2 \in A^{-x}$ *and* $\gamma_1 = \gamma_2$.

Note that the schematic relation is symmetric and $\alpha R \beta$ implies $\langle \alpha, F\rangle = \langle \beta, F\rangle$.

Example. Let $F = (XA \to YA) \to (ZA \to (XA \to YA))$ be an instance of the axiom scheme **CL1**. The schematic set is $ss(F) = \{\{1, 00\}, \{01\}\}$ and the set occurrences (from left to right) are listed by $\{11, 10, 01, 001, 000\}$. They are all schematic and the unique compositions are given by $\{1|1, 1|0, 01|, 00|1, 00|0\}$. For $a = \{1, 00\} \in ss(F)$ we have $a^{+1} = \{00\}$ and $a^{-1} = \{1\}$. Therefore the schematic relation R is defined by $11R001$ and $10R000$. As expected it relates both X and both Y as they appear at the same position within the schematic letter.

It is easy to prove that two set occurrences share either all related occurrences or none.

Lemma 7. *Let* F *be an axiom of* $\mathsf{S_{Ax}}$, R *the schematic relation,* (α, F) *an occurrence in the schematic part,* $\alpha R \alpha_1$ *and* $\alpha R \alpha_2$.
Then $\{\gamma \mid \alpha_1 R \gamma\} = \{\gamma \mid \alpha_2 R \gamma\}$.

Proof. Let $\alpha = \beta\gamma$, $\alpha_1 = \beta_1\gamma_1$ and $\alpha_2 = \beta_2\gamma_2$ be the unique compositions. Then there is $A \in ss(F)$ such that $\beta_1, \beta_2 \in A^x$, $\beta \in A^{-x}$ and $\gamma = \gamma_1 = \gamma_2$. $\alpha_1 R \delta \Leftrightarrow$ there exists $\delta' \in A^{-x}$ such that $\delta = \delta'\gamma \Leftrightarrow \alpha_2 R \delta$. □

In the definition of the initial terms we will use three types of functions, which we assume to be given and fixed.

Definition 15. *Let $K = (S, +, \cdot, 0, 1_K)$ and $L = (S, +, *, 0, 1_L)$ be ω-continuous semirings, $f : S \to \mathcal{P}(E^*)$ a forgetful projection on K, L and $X, Y \in \mathcal{P}(E^*)$.*

- *A function $lb : f^{-1}(X)^2 \to f^{-1}(X)$ is a lower bound function if $lb(x, y) \leq x$ and $lb(x, y) \leq y$.*
- *A function $sp_{X,Y} : f^{-1}(X \cup Y) \to f^{-1}(X)$ splits the plus if $sp_{X,Y}(x) \leq x$.*
- *A function $sd_{X,Y} : f^{-1}(XY) \to f^{-1}(X) \times f^{-1}(Y)$ splits the dot if $\pi_1 sd_{X,Y}(x) * \pi_2 sd_{X,Y}(x) \leq x$.*

A lower bound function $lb : S^2 \to S$ has an extension to $lb : S^n \to S$ for all $n \in \mathbb{N}$, meaning it is defined for finite subsets of S. It can be done inductively by setting $lb(\{a\}) := a$ and $lb(\{a_1, ..., a_n\}) := lb(lb(\{a_1, ..., a_{n-1}\}), a_n)$. By definition lb is an abstract term.
Given an S_{Ax}-proof we assign an abstract term to each family, which we call the initial term of a family, because it only depends on the formula containing the first member of the family.

Definition 16 (Initial terms). *Given an S_{Ax}-proof and a forgetful projection on K, L f we assign the following* initial terms *to the families. We denote the initial term of the family g by $I(g)$ or $I(\alpha, A)$, where $(\alpha, A) \in g$. If $P(g) = -1$ then we choose $i \in \mathbb{N}_{\geq 1}$ and set $I(g) = z_i$ (with domain $f^{-1}(\langle g \rangle)$), such that $P(g_1) = P(g_2) = -1$ and $g_1 \neq g_2$ implies $I(g_1) \neq I(g_2)$. For the positive families we distinguish how they are introduced:*

- *Set axioms 1.1:* $F = RA \wedge SA \to (R \cup S)A$
  $= ((RA \to (SA \to \bot)) \to \bot) \to (R \cup S)A$.
  $I(0, F) := I(111, F) + I(1101, F)$.
- *Set axioms 1.2:* $F = (R \cup S)A \to RA \wedge SA$
  $= (R \cup S)A \to ((RA \to (SA \to \bot)) \to \bot)$.
  $I(011, F) := sp_{R,S}(I(1, F))$,
  $I(0101, F) := sp_{S,R}(I(1, F))$.
- *Set axioms 2.1:* $F = (R(SA) \to (RS)A)$.
  $I(0, F) := I(1, F) * I(10, F)$.
- *Set axioms 2.2:* $F = (RS)A \to R(SA)$.
  $I(0, F) := \pi_1 sd_{R,S}(I(1, F))$,
  $I(00, F) := \pi_2 sd_{R,S}(I(1, F))$.
- *Modal axioms:* $F = S(A \to B) \to (SA \to SB)$.
  $I(00, F) := I(1, F) \cdot I(01, F)$.
- *Induction axioms:* $F = EA \wedge C(A \to EA) \to CA$
  $= \neg(EA \to \neg C(A \to EA)) \to CA$
  $= ((EA \to (C(A \to EA) \to \bot)) \to \bot) \to CA$.
  $I(0, F) := ind(I(111, F), I(1101, F), I(110100, F))$.
- *C-Nec: If CA is derived from A by C-Nec then we set $I(\epsilon, CA) := z_i$, where z_i is a fresh abstract variable with domain $f^{-1}(C)$.*

– *The remaining families are introduced in the schematic part of the axioms. Let g be a family with $P(g) = 1$ and (α, F) the first member. Then we set $I(\alpha, F) := lb(\{I(\beta, F) \mid \alpha R \beta\})$, where R is the schematic relation and $lb(\emptyset) := z_i$.*

First we need to prove that the forgetful projection maps each initial term back to the set of its family.

Lemma 8. *Let $K = (S, +, \cdot, 0, 1_K)$ and $L = (S, +, *, 0, 1_L)$ be ω-continuous semirings, $^\circ$ a forgetful projection and $\mathcal{D}$ an S_{Ax}-proof.*
Then $f(I(g)) = \langle g \rangle$ for all families g.

Proof. Let f be the forgetful projection on K, L. For each set occurrence (α, F) in $\mathcal{D}$ that is the first member of a family we have to prove $f(I(\alpha, F)) = \langle \alpha, F \rangle$. If $P(\alpha, F) = -1$ then this holds by definition.

– Set axioms 1.1: $f(I(0, F)) = f(I(111, F) + I(1101, F))$
$= f(I(111, F)) \cup f(I(1101, F)) = \langle 111, F \rangle \cup \langle 1101, F \rangle = \langle 0, F \rangle$.
– Set axioms 1.2: $f(I(011, F)) = f(sp_{R,S}(I(1, F))) = R = \langle 011, F \rangle$, because the range of $sp_{R,S}$ is $f^{-1}(R)$.
$f(I(0101, F)) = f(sp_{S,R}(I(1, F))) = S = \langle 0101, F \rangle$, because the range of $sp_{S,R}$ is $f^{-1}(S)$.
– Set axioms 2.1: $f(I(0, F)) = f(I(1, F) * I(10, F)) = f(I(1, F)) f(I(10, F))$
$= \langle 1, F \rangle \langle 10, F \rangle = \langle 0, F \rangle$.
– Set axioms 2.2: $f(I(0, F)) = f(\pi_1 sd_{R,S}(I(1, F))) = R = \langle 0, F \rangle$, because the range of $\pi_1 sd_{R,S}$ is $f^{-1}(R)$.
$f(I(00, F)) = f(\pi_2 sd_{R,S}(I(1, F))) = S = \langle 00, F \rangle$, because the range of $\pi_2 sd_{R,S}$ is $f^{-1}(S)$.
– Modal axioms: $f(I(00, F)) = f(I(1, F) \cdot I(01, F))$
$= f(I(1, F)) \cap f(I(01, F)) = \langle 1, F \rangle \cap \langle 01, F \rangle = \langle 00, F \rangle$.
– Induction axioms: Let $a = I(111, F)$, $b = I(1101, F)$ and $c = I(110100, F)$. By using the properties of the forgetful projection f and complete semirings we calculate $f(ind(a, b, c))$ as follows: $f(ind(a, b, c)) = f(\sum_{n \in \mathbb{N}} ind_n)$
$= f((\sum_{n \in \mathbb{N}} ind_{n+1}) + ind_0) = f(\sum_{n \in \mathbb{N}} ind_{n+1}) \cup f(ind_0)$
$= f(\sum_{n \in \mathbb{N}} (b \cdot ind_n) * c) \cup f(a) = f((\sum_{n \in \mathbb{N}} b \cdot ind_n) * c) \cup E$
$= f(\sum_{n \in \mathbb{N}} b \cdot ind_n) f(c) \cup E = f(b \cdot \sum_{n \in \mathbb{N}} ind_n) E \cup E$
$= (f(b) \cap f(\sum_{n \in \mathbb{N}} ind_n)) E \cup E = (C \cap f(ind(a, b, c))) E \cup E$.
We see that it is a fixed point of the function $g : \mathcal{P}(E^*) \to \mathcal{P}(E^*)$ with $g(X) := (C \cap X)E \cup E$. Let $X \in \mathcal{P}(E^*)$ with $g(X) = X$. We prove $E^n \subseteq X$ for $n \geq 1$ by induction on n. For $n = 1$: $E \subseteq (C \cap X)E \cup E = g(X) = X$. If $E^n \subseteq X$ then $E^n \subseteq C \cap X$, $E^{n+1} \subseteq (C \cap X)E$ and $E^{n+1} \subseteq (C \cap X)E \cup E = g(X) = X$. This implies $C \subseteq X$. Because $C = E^* \backslash \{\epsilon\}$ it remains to show that $\epsilon \notin X$. It is easy to see that all elements in $g(X)$ have length at least 1 and therefore $\epsilon \notin g(X) = X$. Finally $f(I(0, F)) = f(ind(a, b, c)) = C = \langle 0, F \rangle$.
– C-Nec: $f(I(\epsilon, CA)) = f(z_i) = C$ by definition.
– Let a positive family be introduced by the set occurrence (α, F) in the schematic part of an axiom. Then $f(I(\alpha, F)) = f(lb(\{I(\beta, F) \mid \alpha R \beta\})) =$

$\langle \alpha, F\rangle$, because $\alpha R\beta$ implies $\langle \alpha, F\rangle = \langle \beta, F\rangle$ and
$lb : f^{-1}(\langle \alpha, F\rangle)^{|\{I(\beta,F)|\alpha R\beta\}|} \to f^{-1}(\langle \alpha, F\rangle)$. □

For proving the derivability of these initial formulas we use the following idea: Assume $(RP \vee SP \to TP)[\alpha_1/x][\alpha_2/y][\alpha_3/I(\alpha_3, F)] = x : P \vee y : P \to lb(x, y) : P$. Substituting the negative occurrences with the positive one gives the axiom $lb(x, y) : P \vee lb(x, y) : P \to lb(x, y) : P$. Because $x, y \geq lb(x, y)$ and the polarity is negative, we can apply Lemma 6 and derive $x : P \vee y : P \to lb(x, y) : P$.
First we strengthen the notation for substitutions. Let $\mathcal{A} = \{\alpha_1, ..., \alpha_n\}$ be a finite set of sequences and $f : \mathcal{A} \to \mathsf{ATm}$ a function. Then we define the substitution $A[\mathcal{A}/f(x)] := A[\alpha_1/f(\alpha_1)]...[\alpha_n/f(\alpha_n)]$. Further we shorten the notation for replacing all occurrences by setting $A[f(x)] := A[\alpha(A)/f(x)]$.
Now let F be an axiom of $\mathsf{S_{Ax}}$, R the schematic relation, (α, F) an occurrence in the schematic part with $P(\alpha, F) = -1$ and $\alpha R\beta$. Then by the previous definition $I(\beta, F) = lb(\{I(\gamma, F) \mid \beta R\gamma\})$. By Lemma 7 this is the same for all β with $\alpha R\beta$. Therefore we can define $I^+(\alpha, F) := I(\beta, F)$. If there is no β with $\alpha R\beta$ we set $I^+(\alpha, F) = I(\alpha, F)$. $\alpha R\beta$ implies $I^+(\alpha, F) \leq I(\alpha, F)$.
The following lemma states that substituting the negative occurrences with the positive one(s) results in all occurrences of a schematic letter being equal.

Lemma 9. *Let F be an axiom of $\mathsf{S_{Ax}}$, $\mathcal{A}$ the non-schematic set occurrences, $\mathcal{B}$ the schematic set occurrences, $F' = F[\mathcal{A}/I(x, F)][\mathcal{B}^{+1}/I(x, F)][\mathcal{B}^{-1}/I^+(x, F)]$, $a \in ss(F)$ and $\alpha, \beta \in a$. Then the subformula equality $(\alpha, F') = (\beta, F')$ holds.*

Proof. We have to prove $\langle \alpha\gamma, F'\rangle = \langle \beta\gamma, F'\rangle$ for an arbitrary $\gamma \in \alpha((\alpha, F'))$.

- $P(\alpha\gamma, F') = -1, P(\beta\gamma, F') = 1$:
  $\langle \alpha\gamma, F'\rangle = I^+(\alpha\gamma, F)$ and $\langle \beta\gamma, F'\rangle = I(\beta\gamma, F)$ by definition of F'.
  $\alpha, \beta \in a$ with opposite polarity delivers $\alpha\gamma R\beta\gamma$ from which we infer $I^+(\alpha\gamma, F) = I(\beta\gamma, F)$.
- $P(\alpha\gamma, F') = 1, P(\beta\gamma, F') = -1$: Symmetrical to the previous case.
- $P(\alpha\gamma, F') = 1, P(\beta\gamma, F') = 1$:
  $\langle \alpha\gamma, F'\rangle = I(\alpha\gamma, F)$ and $\langle \beta\gamma, F'\rangle = I(\beta\gamma, F)$ by definition of F'. We get $I(\alpha\gamma, F) = lb(\{I(\delta\gamma, F) \mid \delta \in a^{-P(\alpha,F)}\}) = I(\beta\gamma, F)$ from the definition of I and the schematic relation.
- $P(\alpha\gamma, F') = -1, P(\beta\gamma, F') = -1$:
  $\langle \alpha\gamma, F'\rangle = I^+(\alpha\gamma, F)$ and $\langle \beta\gamma, F'\rangle = I^+(\beta\gamma, F)$ by definition of F'.
  If there exists $\delta \in a^{-P(\alpha,F)}$ we get $I^+(\alpha\gamma, F) = I(\delta\gamma, F) = I^+(\beta\gamma, F)$.
  If $a^{-P(\alpha,F)} = \emptyset$ then F is an instance of CL1 and $|a^{P(\alpha,F)}| = |a| = 1$, which implies $\alpha = \beta$ and obviously $\langle \alpha\gamma, F'\rangle = \langle \beta\gamma, F'\rangle$. □

The subformula equality is used to show that F' is easily derivable.

Lemma 10. *Let $K = (S, +, \cdot, 0, 1_K)$ and $L = (S, +, *, 0, 1_L)$ be ω-continuous semirings, T an axiomatically appropriate theory that supports concatenation and induction, $F \in \mathcal{L}_\mathcal{S}$ an axiom of $\mathsf{S_{Ax}}$. Then $T \vdash_{\mathsf{SE_K}} F[I(x, F)]$.*

Proof. We denote the non-schematic set occurrences by $\mathcal{A}$, the schematic set occurrences by $\mathcal{B}$ and $F' = F[\mathcal{A}/I(x,F)][\mathcal{B}^{+1}/I(x,F)][\mathcal{B}^{-1}/I^+(x,F)]$ as before. Now we first prove $T \vdash_{\mathsf{SE_K}} F'$.

- $F = A \to (B \to A)$. By Lemma 9 there exist A', B' such that $F' = A' \to (B' \to A')$, which is a propositional tautology.
- $F = (A \to (B \to C)) \to ((A \to B) \to (A \to C))$. By Lemma 9 there exist A', B', C' such that $F' = (A' \to (B' \to C')) \to ((A' \to B') \to (A' \to C'))$, which is a propositional tautology.
- $F = ((A \to \bot) \to \bot) \to A$. By Lemma 9 there exists A' such that $F' = ((A' \to \bot) \to \bot) \to A'$, which is a propositional tautology.
- $F = RA \wedge SA \to (R \cup S)A$. By Lemma 9 there exists A' such that $F' = z_1 : A' \wedge z_2 : A' \to z_1 + z_2 : A'$, which is an instance of $\mathbf{j}+$.
- $F = (R \cup S)A \to RA \wedge SA$. By Lemma 9 there exists A' such that $F' = z_1 : A' \to sp_{R,S}(z_1) : A' \wedge sp_{S,R}(z_1) : A'$. $sp_{R,S}(z_1) \leq z_1$ and $sp_{S,R}(z_1) \leq z_1$ because sp splits the plus. $T \vdash_{\mathsf{SE_K}} F'$ follows from $\mathbf{j}+$ and propositional reasoning.
- $F = R(SA) \to (RS)A$. By Lemma 9 there exists A' such that $F' = z_1 : z_2 : A' \to z_1 * z_2 : A'$. T supporting concatenation yields $T \vdash_{\mathsf{SE_K}} F'$.
- $F = (RS)A \to R(SA)$. By Lemma 9 there exists A' such that $F' = z_1 : A' \to \pi_1 sd_{R,S}(z_1) : \pi_2 sd_{R,S}(z_1) : A'$. Because sd splits the dot $\pi_1 sd_{R,S}(z_1) * \pi_2 sd_{R,S}(z_1) \leq z_1$ and from $\mathbf{j}+$ and propositional reasoning we infer $T \vdash_{\mathsf{SE_K}} z_1 : A' \to \pi_1 sd_{R,S}(z_1) * \pi_2 sd_{R,S}(z_1) : A'$. T supporting concatenation yields $T \vdash_{\mathsf{SE_K}} F'$.
- $F = S(A \to B) \to (SA \to SB)$. By Lemma 9 there exist A', B' such that $F' = z_1 : (A' \to B') \to (z_2 : A' \to z_1 \cdot z_2 : B')$, which is an instance of $\mathbf{j}$.
- $F = EA \wedge C(A \to EA) \to CA$. By Lemma 9 there exists A' such that $F' = z_1 : A' \wedge z_2 : (A' \to z_3 : A') \to ind(z_1, z_2, z_3) : A'$. T supporting induction yields $T \vdash_{\mathsf{SE_K}} F'$.

Knowing $T \vdash_{\mathsf{SE_K}} F'$, $I^+(x,F) \leq I(x,F)$ and $P(\alpha, F) = -1$ for $\alpha \in \mathcal{C}^{-1}$ we apply Lemma 6 and get $T \vdash_{\mathsf{SE_K}} F[I(x,F)]$. □

With this lemma we completed the first step of the realization procedure. For the second step we restrict certain initial terms by replacing them by a fixed point of a function given through another initial term. The existence of such a fixed point will follow from the Scott-continuity of the initial terms, which we have to prove first. It only works if the given functions lb, sp and sd are Scott-continuous.

Lemma 11. *Let $K = (S, +, \cdot, 0, 1_K)$ and $L = (S, +, *, 0, 1_L)$ be ω-continuous semirings, lb, sp and sd Scott-continuous functions. Then all initial terms are Scott-continuous functions.*

Proof. The initial term of a negative family, a positive family introduced by C-Nec or of the form $lb(\emptyset)$ is just an identity function, which is obviously Scott-continuous. The initial terms of the positive families introduced in the schematic part of an axiom have the form $lb(\{z_1, ..., z_n\})$, which is by assumption Scott-continuous. By Lemma 2 the initial terms of Set axioms 1.1, Set axioms 2.1,

Modal axioms and Induction axioms are Scott-continuous. Scott-continuity of initial terms for Set axioms 1.2 and Set axioms 2.2 is again given by assumption. □

Next we define MP-connections. The intuition behind this concept is that in the application of modus ponens the formulas $(1, A \to B)$ and A need to be realized the same way, so we connect the families of two set occurrences if they appear in the same position within the different A's.

Definition 17. *If the node p_1 is labelled with $A \to B$, p_2 with A and they have a common successor q labelled with B then we call the families of $(1\alpha, p_1)$ and (α, p_2)* MP-connected. *Notation: f_1 MP f_2.*

The following lemma states some important observations about MP-connections.

Lemma 12. *If f_1 MP f_2 then:*

1. *$P(f_1) \neq P(f_2)$.*
2. *Not f_1 MP f if $f \neq f_2$ and not f_2 MP f if $f \neq f_1$.*
3. *f_1 and f_2 do not occur in the derived formula.*

Proof. 1: $P(1\alpha, p_1) = (-1)^{\sum 1\alpha} = (-1)^{1+\sum \alpha} = -(-1)^{\sum \alpha} = -P(\alpha, p_2)$.
2: Since **MP** eliminates both A's it is the last member of each family that creates the MP-connection. Because there is only one last member each family can have at most one MP-connection.
3: The connection is created by MP, which eliminates f_1 and f_2. □

For our main theorem we prove a specific version of the fixed point theorem. Additionally the fixed point needs to be mapped to the correct element in $\mathcal{P}(E^*)$ by the forgetful projection. Therefore we have to assume that there is a zero element in each $f^{-1}(X)$, so we can start applying the functions repeatedly from there.

Theorem 4 (Specific fixed point theorem). *Let K be a semiring, the function $f : K \to X$ a partition into ω-continuous monoids $f^{-1}(x)$, $v \in X^n$ and $h : f^{-1}(v) \to f^{-1}(v)$ a Scott-continuous function.*
Then there exists $x = (x_1, ..., x_n) \in f^{-1}(v)$ with $h(x) = x$.

Proof. For every $x \in X$ the set $f^{-1}(x)$ has a neutral element 0_x, because $f^{-1}(x)$ is a monoid. We write v in its components as $(v_1, ..., v_n)$. Then we define the sequence $a_0 = (0_{v_1}, ..., 0_{v_n})$ and $a_{k+1} = h(a_k)$. Because Scott-continuous functions are monotone, we have $a_k \leq a_{k+1}$ for all $k \in \mathbb{N}$. Now we define $(x_1, ..., x_n)$ as $sup(\bigcup_{k=0}^{\infty}\{a_k\})$. It follows $h(x_1, ..., x_n) = h(sup(\bigcup_{k=0}^{\infty}\{a_k\}))$, which by Scott-continuity is equal to $sup(h(\bigcup_{k=0}^{\infty}\{a_k\}))$. By definition of the sequence a we get $sup(\bigcup_{k=1}^{\infty}\{a_k\}))$. $sup(\bigcup_{k=0}^{\infty}\{a_k\}))$ results from the monotonicity of a and it is exactly how $(x_1, ..., x_n)$ was defined, so $h(x) = x$ is proved. For an arbitrary $i \leq n$ let b_k be $\pi_i(a_k)$. The monotonicity thereof allows us to write it as partial sums of a sequence c in $f^{-1}(v_i)$: $b_k = \sum_{j=0}^{k} c_j$. It follows $x_i = sup(\bigcup_{k=0}^{\infty}\{b_k\}))$

$= sup\{\sum_{j=0}^{k} c_j \mid k \in \mathbb{N}\} = \sum_{j\in\mathbb{N}} c_j$ by the ω-continuity of $f^{-1}(v_i)$. The completeness of the monoid $f^{-1}(v_i)$ delivers $x_i \in f^{-1}(v_i)$. Since i was arbitrary we have $(f(x_1), ..., f(x_n)) = (v_1, ..., v_n)$. □

While most of the work on the second step is still left to do, we state now our main theorem.

Theorem 5 (Realization of Common Knowledge). *Let $K = (S, +, \cdot, 0, 1_K)$ and $L = (S, +, *, 0, 1_L)$ be ω-continuous semirings. If there exists a function f that is a semiring-homomorphism from K to K_{min} and from L to L_{min} such that for all $a \in \mathcal{P}(E^*)$ $(f^{-1}(a), +, 0_{f^{-1}(a)})$ is a ω-continuous monoid and there exist the Scott-continuous functions lb, sp and sd then there exists a normal realization r such that*

$$\vdash_{\mathsf{S_{Ax}}} A \Rightarrow T \vdash_{\mathsf{SE_K}} r(A)$$

for all $A \in \mathcal{L}_{\mathcal{S}}$ and every axiomatically appropriate theory T that supports concatenation and induction.

Proof. Assume there exists a function f that is a semiring-homomorphism from K to K_{min} and from L to L_{min} such that all $(f^{-1}(a), +, 0_{f^{-1}(a)})$ are ω-continuous monoids and there exist the Scott-continuous functions *lb*, *sp* and *sd*. We construct a normal realization r based on the forgetful projection $^\circ$ generated by using f as the forgetful projection on K, L. That f is a forgetful projection on K, L follows from the fact that f is a semiring-homomorphism from K to K_{min} and from L to L_{min}. Let $\mathcal{D}$ be an $\mathsf{S_{Ax}}$-proof tree for A. We say that a node of $\mathcal{D}$ is derivable if the formula it is labelled with is derivable. We denote the negative families with a MP-connection by $f_1, ..., f_n$ with f_i MP g_i for $1 \leq i \leq n$ and $z_i = I(f_i)$. Further we denote the domain of z_i by A_i and set $D := A_1 \times ... \times A_n$. The remaining variables occurring in the initial terms are $z_{n+1}, ..., z_m$. We define $H(z_{n+1}, ..., z_m)$ as the function $h : D \to D$ defined by $h(z_1, ..., z_n) := (I(g_1)(z_1, ..., z_m), ..., I(g_n)(z_1, ..., z_m))$. If $z_{n+1}, ..., z_m$ are fixed then $I(g_i)$ becomes a function that depends only on $z_1, ..., z_n$. A countable set $X \subseteq D$ with a well-order can be written as $\{(x_{i1}, ..., x_{in}) \mid x_{ij} \in A_j, i \in \mathbb{N}\}$, where $x_{ij} \leq x_{i+1,j}$.
Therefore $sup(h(X)) = sup(h(\{(x_{i1}, ..., x_{in}) \mid x_{ij} \in A_j, i \in \mathbb{N}\}))$
$= sup(\{(I(g_1)(x_{i1}, ..., x_{in}), ..., I(g_n)(x_{i1}, ..., x_{in})) \mid x_{ij} \in A_j, i \in \mathbb{N}\})$
$= (sup_{i\in\mathbb{N}}(I(g_1)(x_{i1}, ..., x_{in})), ..., sup_{i\in\mathbb{N}}(I(g_n)(x_{i1}, ..., x_{in})))$
$= (I(g_1)(sup_{i\in\mathbb{N}}(x_{i1}, ..., x_{in})), ..., I(g_n)(sup_{i\in\mathbb{N}}(x_{i1}, ..., x_{in})))$
$= h(sup_{i\in\mathbb{N}}(x_{i1}, ..., x_{in})) = h(sup(X))$. So h is Scott-continuous and we can apply the specific fixed point theorem, which delivers $x = (x_1, ..., x_n) \in D$ with $h(x) = x$. We set $F(z_{n+1}, ..., z_m) := (x_1, ..., x_n)$. We define the realization r for different things in $\mathcal{D}$:

- a family g: $r(g) = \pi_i F$ if $g = f_i$ or $g = g_i$, $r(g) = I(g)[z_1/\pi_1 F]...[z_n/\pi_n F]$ otherwise.
- a set occurrence (α, p): $r(\alpha, p) = r(g)$, where (α, p) is a member of g.
- the derived formula A: $r(A) = \langle root\rangle[r(x, root)]$, where *root* is the node of the derived formula.

For $A \in \mathcal{L}_{\mathcal{S}}$ with $\vdash_{\mathsf{S_{Ax}}} A$ we show that $T \vdash_{\mathsf{SE_K}} r(A)$ by induction on $\mathcal{D}$. Precisely we show for each node p that $T \vdash_{\mathsf{SE_K}} \langle p\rangle[r(x,p)]$.

- Let $\langle p\rangle = A$ be an axiom of $\mathsf{S_{Ax}}$ and z an arbitrary valuation for abstract formulas. We define y as $y(z_i) = (\pi_i F)_z$ for $1 \leq i \leq n$ and $y(z_j) = z(z_j)$ otherwise. Further let f be a family. We prove $I(f)_y = r(f)_z$ by distinguishing three cases:
  - If f has no MP-connection then $I(f)_y = I(f)[z_1/(\pi_1 F)_z]...[z_n/(\pi_n F)_z]_y$ $= I(f)[z_1/(\pi_1 F)_y]...[z_n/(\pi_n F)_y]_y = I(f)[z_1/\pi_1 F]...[z_n/\pi_n F]_y = r(f)_y$ $= r(f)_z$, because $z_1, ..., z_n$ do not occur in $r(f)$.
  - If f has a MP-connection and $P(f) = -1$ then $f = f_i$ for some i and $I(f)_y = (z_i)_y = (\pi_i F)_z = r(f)_z$.
  - If f has a MP-connection and $P(f) = 1$ then $f = g_i$ and we use the fixed point property. For $h(x_1, ..., x_n) = H((z_{n+1})_z, ..., (z_m)_z)(x_1, ..., x_n)$ we have $h((\pi_1 F)_z, ..., (\pi_n F)_z) = ((\pi_1 F)_z, ..., (\pi_n F)_z)$ and by projecting on the i-th component we get $I(g_i)((\pi_1 F)_z, ..., (\pi_n F)_z, (z_{n+1})_z, ..., (z_m)_z)$ $= (\pi_i F)_z$. We use this equation in the following derivation.
    $I(f)_y = I(g_i)_y$
    $= I(g_i)[z_1/(\pi_1 F)_z]...[z_n/(\pi_n F)_z][z_{n+1}/(z_{n+1})_z]...[z_m/(z_m)_z]$
    $= (\pi_i F)_z = r(f)_z$.

  In all cases we got $I(f)_y = r(f)_z$. By Lemma 10 we know $T \vdash_{\mathsf{SE_K}} \langle p\rangle[I(x, \langle p\rangle)]$ including $\langle p\rangle[I(x, \langle p\rangle)]_y$, which now implies $\langle p\rangle[r(x,p)]_z$. Since z was arbitrary, we conclude $T \vdash_{\mathsf{SE_K}} \langle p\rangle[r(x,p)]$.
- If $\langle q\rangle = B$ is derived from $\langle p_1\rangle = A \to B$ and $\langle p_2\rangle = A$ by **MP** then by induction hypothesis $T \vdash_{\mathsf{SE_K}} \langle p_1\rangle[r(x,p_1)]$ and $T \vdash_{\mathsf{SE_K}} \langle p_2\rangle[r(x,p_2)]$. By the definition of a MP-connection all families of the form $(1\alpha, p_1)$ and (α, p_2) are MP-connected. Let $(1\alpha, p_1)$ be a set occurrence. If $(1\alpha, p_1)$ is negative then it is a member of f_i for some i and (α, p_2) is a member of g_i. We get $r(1\alpha, p_1) = r(\alpha, p_2)$ because $r(f_i) = r(g_i) = \pi_i F$. If $(1\alpha, p_1)$ is positive then it is a member of g_i for some i and (α, p_2) is a member of f_i and we also get $r(1\alpha, p_1) = r(\alpha, p_2)$. Since α was arbitrary we have $(1, \langle p_1\rangle)[r(1x, p_1)] = \langle p_2\rangle[r(x, p_2)]$. So $\langle p_1\rangle[r(x, p_1)]$ can be written as $\langle p_2\rangle[r(x, p_2)] \to (0, \langle p_1\rangle)[r(0x, p_1)]$, which means $(0, \langle p_1\rangle)[r(0x, p_1)]$ is derivable by **MP**. We assumed $(0, \langle p_1\rangle) = \langle q\rangle$ and since $(0x, p_1)$ is related to (x, q) we also have $r(0x, p_1) = r(x, q)$, therefore $(0, \langle p_1\rangle)[r(0x, p_1)] = \langle q\rangle[r(x, q)]$.
- If $\langle q\rangle = CA$ is derived from $\langle p\rangle = A$ by **C-Nec** then by induction hypothesis $T \vdash_{\mathsf{SE_K}} \langle p\rangle[r(x,p)]$. Note that $(0, \langle q\rangle) = \langle p\rangle$ and $r(0x, q) = r(x, p)$. Let z be a valuation for abstract formulas. From the internalization corollary we derive $T \vdash_{\mathsf{SE_K}} r(\epsilon, q)_z : \langle p\rangle[r(x,p)]_z$. We finish the case by stating $r(\epsilon, q)_z : (\langle p\rangle[r(x,p)]_z) = r(\epsilon, q)_z : ((0, \langle q\rangle)[r(0x, q)]_z) = \langle q\rangle[r(x, q)]_z$.

It remains to show that r is a normal realization. So let $(\alpha, root)$ and $(\beta, root)$ be negative occurrences with $\alpha \neq \beta$. By the definition of I we have $I(\alpha, root) = z_i$ and $I(\beta, root) = z_j$ with $i \neq j$. By Lemma 12 the families of $(\alpha, root)$ and $(\beta, root)$ do not have a MP-connection and therefore $i, j > n$. The definition of r implies $r(\alpha, root) = I(\alpha, root) = z_j \neq z_i = I(\beta, root) = r(\beta, root)$.
We calculate the domains of the realization terms as follows: $f(h(z_1, ..., z_n)) =$

$f(I(g_1),...,I(g_n)) = (\langle g_1\rangle,...,\langle g_n\rangle)$ by Lemma 8. Because the specific fixed point theorem delivers a fixed point in the same monoid we also have $f(F) = (\langle g_1\rangle,...,\langle g_n\rangle)$. Since the derived formula contains only families without MP-connection we are in the case $r(g) = I(g)[z_1/\pi_1 F]...[z_n/\pi_n F]$. We know $f(I(g)) = \langle g\rangle$ again by Lemma 8, actually $\{f(I(g)(z_1,..,z_m)) \mid z_i \in A_i\} = \{\langle g\rangle\}$. From $f(\pi_i F) = \langle g_i\rangle = \langle f_i\rangle$ and $A_i = f^{-1}(\langle f_i\rangle)$ we infer $\{\pi_i F \mid z_i \in A_i\} \subseteq A_i$ and further $\{f(I(g)) \mid i \leq n \Rightarrow z_i \in \{\pi_i F \mid z_i \in A_i\}, i > n \Rightarrow z_i \in A_i\} = \{\langle g\rangle\}$, which yields $\{f(I(g)[z_1/\pi_1 F]...[z_n/\pi_n F]) \mid z_i \in A_i\} = \{\langle g\rangle\}$. Therefore $f(r(g)) = \langle g\rangle$. Finally we conclude that $r(A)^\circ$ is defined and equal to A. □

Remark. The theorem also has a trivial proof. One can easily show, that the realization which maps all positive families g to $0_{f^{-1}(\langle g\rangle)}$, satisfies the conditions because of Lemma 6, but it is useless. We assume that the realization constructed in the proof has some interesting maximality properties.

We extend our theorem to arbitrary theories of common knowledge. Here we make sure not to mix variables with abstract variables.

Definition 18. *Let $T' \subseteq \mathcal{L}_\mathcal{S}$ be a theory of common knowledge. $T \subseteq \mathsf{Fml}$ realizes T' normally if for all $A' \in T'$ there is $A \in \mathsf{AFml}$ realizing A' normally and $A_z \in T$ for all abstract valuations z.*

Theorem 6. *Let $K = (S, +, \cdot, 0, 1_K)$ and $L = (S, +, *, 0, 1_L)$ be ω-continuous semirings. If there exists a function f that is a semiring-homomorphism from K to K_{min} and from L to L_{min} such that all $(f^{-1}(a), +, 0_{f^{-1}(a)})$ are ω-continuous monoids and there exist the Scott-continuous functions lb, sp and sd then for every axiomatically appropriate theory T that realizes T' normally (with Scott-continuous terms) and supports concatenation and induction there exists a normal realization r such that*

$$T' \vdash_{\mathsf{S_{Ax}}} A \Rightarrow T \vdash_{\mathsf{SE_K}} r(A) \quad \textit{for all } A \in \mathcal{L}_\mathcal{S}.$$

This adds another case to the proof: If a family is introduced by the theory we treat the corresponding abstract term as the initial term.
The proof of the main theorem is very different from the proof of the realization theorem between S4 and the logic of proofs (LP) shown in [35]. There a sequent calculus equivalent to S4 is used and put into relation with S4. Here we work directly with the modal logic, which includes the modus ponens rule. We therefore get an algorithm, that realizes the modus ponens directly by using a fixed point. Such an idea can be useful in all cases, where there is a modus ponens rule and no equivalent sequent calculus (e.g. Common Knowledge).

4.4 Examples

Let $M = (R, +, \cdot, 0_M, 1_M)$ be an ω-continuous semiring. Examples include real numbers $(\mathbb{R}^\infty_{\geq 0}, +, \cdot, 0, 1)$, the Viterbi semiring $([0,1], max, \cdot, 0, 1)$, the tropical semiring $(\mathbb{R}^\infty_{\geq 0}, min, +, \infty, 0)$ and the powerset semiring $(\mathcal{P}(X), \cup, \cap, \emptyset, X)$.

We construct a semiring K for h agents by using one element of M per $\Box$-operator. We define the alphabet E_M as $\{\Box_i^r \mid 1 \leq i \leq h, r \in R\}$ and $f(\Box_i^r) = \Box_i$, which extends to words by commuting with concatenation. We apply the $+$ of M only on the first character of two words, which have to be identical in the rest, while the $\cdot$ is component-wise.

- $\Box_i^{r_1} c_2 ... c_n + \Box_i^{s_1} c_2 ... c_n = \Box_i^{r_1 + s_1} c_2 ... c_n$
- $\Box_{i_1}^{r_1} ... \Box_{i_n}^{r_n} \cdot \Box_{i_1}^{s_1} ... \Box_{i_n}^{s_n} = \Box_{i_1}^{r_1 \cdot s_1} ... \Box_{i_n}^{r_n \cdot s_n}$

A set X of words is stable if there are no $w_1, w_2 \in X$ with $w_1 \neq w_2$ such that $w_1 + w_2$ is defined. $X'Y := \{w_1 \in X \mid \neg \exists w_2 \in Y : w_1 + w_2 \text{ is defined}\}$. Now we can define $K = (S, +, \cdot, 0, 1)$ as follows:

- $S = \{X \subseteq E_M^* \mid X \text{ is stable}\}$,
- $x + y = x'y \cup y'x \cup \{w_1 + w_2 \mid w_1 \in x, w_2 \in y, w_1 + w_2 \text{ is defined}\}$,
- $x \cdot y = \{w_1 \cdot w_2 \mid w_1 \in x, w_2 \in y, w_1^\circ = w_2^\circ\}$,
- $0 = \emptyset$,
- $1 = \{\Box_i^{1_M} \mid 1 \leq i \leq h\}^*$.

One can prove that K is a ω-continuous semiring. The structure L resulting by replacing the multiplication by concatenation is also a ω-continuous semiring. Further f is a semiring-homomorphism from K to K_{min} and from L to L_{min} and $(f^{-1}(X), +, 0_{f^{-1}(X)})$ is a ω-continuous monoid for all $X \in \mathcal{P}(E^*)$.

Example 1

Now we consider a shortest path example using this construction with the tropical semiring. For better readability we omit the curly brackets on singleton sets. Let $T' = \{\Box_1(A \to B), \Box_1(B \to C)\}$ and $T = \{\Box_1^x : (A \to B), \Box_1^y : (B \to C), ...\}$ axiomatically appropriate. For $T' \vdash_{\mathsf{S_{Ax}}} \Box_1(A \to C)$ we have the following derivation:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Box_1((A \to B) \to ((B \to C) \to (A \to C)))} \quad \dfrac{}{(\Box_1(A \to B) \to \Box_1((B \to C) \to (A \to C)))}}{\Box_1((A \to B) \to ((B \to C) \to (A \to C)))} \quad \dfrac{}{(A \to B) \to ((B \to C) \to (A \to C))}}{\Box_1(A \to B) \to \Box_1((B \to C) \to (A \to C))} \quad \dfrac{}{\Box_1(A \to B)}}{\dfrac{\dfrac{}{\Box_1((B \to C) \to (A \to C))} \quad \dfrac{}{(\Box_1(B \to C) \to \Box_1(A \to C))}}{\Box_1((B \to C) \to (A \to C))}}$$
$$\dfrac{\Box_1(B \to C) \to \Box_1(A \to C) \qquad \Box_1(B \to C)}{\Box_1(A \to C)}$$

By inserting the initial terms we get

$$\dfrac{\dfrac{\dfrac{\dfrac{}{z_2 : ((A \to B) \to ((B \to C) \to (A \to C)))} \quad \dfrac{}{(z_3 : (A \to B) \to z_2 \cdot z_3 : ((B \to C) \to (A \to C)))}}{z_3 : (A \to B) \to z_2 \cdot z_3 : ((B \to C) \to (A \to C))} \quad \dfrac{}{z_6 : (A \to B)}}{\dfrac{\dfrac{}{z_4 : ((B \to C) \to (A \to C))} \quad \dfrac{}{(z_5 : (B \to C) \to z_4 \cdot z_5 : (A \to C))}}{z_2 \cdot z_3 : ((B \to C) \to (A \to C))}}$$
$$\dfrac{z_5 : (B \to C) \to z_4 \cdot z_5 : (A \to C) \qquad z_7 : (B \to C)}{z_4 \cdot z_5 : (A \to C)}$$

With $A = \{s \in S \mid s^\circ = \{\Box_1\}\} = \{\{\Box_1^z\} \mid z \in R\}$ the domains of these abstract variables are as follows:

Variable	z_1	z_2	z_3	z_4	z_5	z_6	z_7
Domain	A	A	A	A	A	$\{\{\Box_1^x\}\}$	$\{\{\Box_1^y\}\}$

In order to apply the modus ponens of $\mathsf{SE_K}$ we need the following equalities, which come from the MP-connections:
$z_2 = z_1$, $z_3 = z_6$, $z_4 = z_2 \cdot z_3$ and $z_5 = z_7$. This is equivalent to a fixed point of $h(z_2, z_3, z_4, z_5) := (z_1, z_6, z_2 \cdot z_3, z_7)$. We find such a point by applying h repeatedly to the 0 in the monoid A^4, which is $(\{\Box_1^\infty\}, \{\Box_1^\infty\}, \{\Box_1^\infty\}, \{\Box_1^\infty\})$.

- $h(\{\Box_1^\infty\}, \{\Box_1^\infty\}, \{\Box_1^\infty\}, \{\Box_1^\infty\}) = (z_1, z_6, \{\Box_1^\infty\}, z_7)$
- $h(z_1, z_6, \{\Box_1^\infty\}, z_7) = (z_1, z_6, z_1 \cdot z_6, z_7)$
- $h(z_1, z_6, z_1 \cdot z_6, z_7) = (z_1, z_6, z_1 \cdot z_6, z_7)$

This yields the following (abstract) proof in $\mathsf{SE_K}$:

$$\dfrac{\dfrac{\dfrac{z_1 : ((A \to B) \to ((B \to C) \to (A \to C))) \to (z_6 : (A \to B) \to z_1 \cdot z_6 : ((B \to C) \to (A \to C)))}{z_6 : (A \to B) \to z_1 \cdot z_6 : ((B \to C) \to (A \to C))} \dfrac{(A \to B) \to ((B \to C) \to (A \to C))}{z_1 : ((A \to B) \to ((B \to C) \to (A \to C)))}}{z_1 \cdot z_6 : ((B \to C) \to (A \to C))} z_6 : (A \to B)}{z_1 \cdot z_6 : (z_7 : (B \to C) \to z_1 \cdot z_6 \cdot z_7 : (A \to C))} \dfrac{}{z_1 \cdot z_6 : ((B \to C) \to (A \to C))}}{z_7 : (B \to C) \to z_1 \cdot z_6 \cdot z_7 : (A \to C)} \quad z_7 : (B \to C)}{z_1 \cdot z_6 \cdot z_7 : (A \to C)}$$

Applying a valuation on $z_1 \cdot z_6 \cdot z_7$ gives $\{\Box_1^z\} \cdot \{\Box_1^x\} \cdot \{\Box_1^y\} = \{\Box_1^{z+x+y}\}$. If we assume that justifications for axioms come for free we get $\{\Box_1^{x+y}\} : (A \to C)$, which is exactly the shortest path. This means that the realization procedure is maximal in a way ($\{\Box_1^\infty\} : (A \to C)$ is also derivable).

Example 2

For this example we use the positive real numbers and infinity with standard addition and multiplication. Let $T' = \{(\Box_1 P \to \Box_1 P) \to Q\}$ be a theory of common knowledge and $T = \{(z_2^2 + \{\Box_1^{\frac{1}{4}}\} : P \to z_2 : P) \to Q, ...\}$. We consider the following proof of Q in $\mathsf{S_{Ax}}$:

$$\dfrac{(\Box_1 P \to \Box_1 P) \to Q \qquad \Box_1 P \to \Box_1 P}{Q}$$

By inserting the initial terms we get

$$\dfrac{(z_2^2 + \{\Box_1^{\frac{1}{4}}\} : P \to z_2 : P) \to Q \qquad z_1 : P \to z_1 : P}{Q}$$

The MP-connections give the equalities $z_1 = z_2^2 + \{\Box_1^{\frac{1}{4}}\}$ and $z_2 = z_1$. For $h(z_1, z_2) = (z_2^2 + \{\Box_1^{\frac{1}{4}}\}, z_1)$ we have $h^n(\{\Box_1^0\}, \{\Box_1^0\}) = (\{\Box_1^x\}, \{\Box_1^y\})$ with the following values for x and y:

n	0	1	2	3	4	5	∞
x	0	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{5}{16}$	$\frac{5}{16}$	$\frac{89}{256}$	$\frac{1}{2}$
y	0	0	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{5}{16}$	$\frac{5}{16}$	$\frac{1}{2}$

This yields the following proof in $\mathsf{SE_K}$:

$$\dfrac{(\{\Box_1^{\frac{1}{2}}\} : P \to \{\Box_1^{\frac{1}{2}}\} : P) \to Q \qquad \{\Box_1^{\frac{1}{2}}\} : P \to \{\Box_1^{\frac{1}{2}}\} : P}{Q}$$

Example 3

Let $F = EXA \wedge C(XA \to EXA) \to CXA$ be an induction axiom. The realization r is obtained by inserting the initial terms:

$$z_1 : z_4 : A \wedge z_2 : (lb(z_4, z_5) : A \to z_3 : z_5 : A) \to ind(z_1, z_2, z_3) : lb(z_4, z_5) : A.$$

Let T be an axiomatically appropriate theory that supports induction. Then for $B = lb(z_4, z_5) : A$ the theory T proves

$$z_1 : B \wedge z_2 : (B \to z_3 : B) \to ind(z_1, z_2, z_3) : B.$$

By Lemma 6, T also proves $r(F)$, because $z_4, z_5 \geq lb(z_4, z_5)$.

Conclusion

The evidence terms in traditional justification logic have the form of polynomials, but semantically this structure is ignored by assigning a set of formulas to each term. We introduced the logic SE and the corresponding semantics, where terms are mapped to actual polynomials over a semiring. This gives a clear distinction between constants and variables, because constants in a term are mapped to elements in the semiring, yielding a function in the variables of the term. Further it is possible to compute with justifications. This can be used to model trust (Viterbi semiring), probabilities (powerset semiring), cost (tropical semiring), etc., depending on the chosen semiring.

For the logic SE and its semantics we prove soundness and completeness. The completeness proof does not follow the standard line with maximal consistent sets. Instead we used a mapping to classical propositional logic, which basically replaces formulas of the form $t : A$ by a fresh atomic proposition. Then we clarified the relationship between SE and the modal logic K by two realization theorems. The proof of the first one is closely related to a realization procedure without $+$, found by Kuznets.

Then we considered ω-continuous semirings with the motivation that every Scott-continuous function on such a semiring has a fixed point, which can be used to establish a connection between common knowledge and justification logic. We therefore introduced the logic SE_K with its semantics and proved soundness and completeness in a similar way as before. The main difference between SE and SE_K is that the latter uses the polynomials over a semiring directly as justification terms. Apart from simplifying a lot this change was necessary for using the fixed points, because a fixed point is given by the (infinite) ascending Kleene chain, which would result in an infinite term.

The infinite sum operation on the justification terms turned out to be too complex for common knowledge itself. For example terms for E^0, E^2, E^4 and so on can be added to create a term for $\sum_{n\in\mathbb{N}} E^{2n}$, which has no finite representation in common knowledge. We therefore introduced the system S_Ax (as an extension of common knowledge), which allows arbitrary sets of words of modal operators. Working towards a realization theorem we found a way of addressing occurrences of subformulas by a 0-1-sequence. This made the proof significantly more rigorous. When we dealt with the modus ponens rule we saw that all the applications of MP in a proof created a system of equations of the form $x = f(x)$. We therefore used the fixed point theorem and got a realization algorithm that realizes the modus ponens rule directly and yields a normal realization.

In the future it could be interesting to try to generalize this approach. By using fixed points one could find a realization procedure for more general modal fixed point logics including the modal μ-calculus.

References

1. Alt, J., Artemov, S.: Reflective λ-calculus. In: Kahle, R., Schroeder-Heister, P., Stärk, R. (eds.) Proof Theory in Computer Science, International Seminar, PTCS 2001, Dagstuhl Castle, Germany, October 7–12, 2001, Proceedings, LNCS, vol. 2183, pp. 22–37. Springer (2001). https://doi.org/10.1007/3-540-45504-3_2
2. Amsterdamer, Y., Davidson, S.B., Deutch, D., Milo, T., Stoyanovich, J., Tannen, V.: Putting lipstick on pig: Enabling database-style workflow provenance. Proc. VLDB Endow. **5**(4), 346–357 (2011). https://doi.org/10.14778/2095686.2095693
3. Amsterdamer, Y., Deutch, D., Tannen, V.: Provenance for aggregate queries. In: Proceedings of the Thirtieth ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems. pp. 153–164. PODS '11, ACM (2011). https://doi.org/10.1145/1989284.1989302
4. Artemov, S.: Explicit provability and constructive semantics. Bulletin of Symbolic Logic **7**(1), 1–36 (Mar 2001)
5. Artemov, S.: Justified common knowledge. Theoretical Computer Science **357**(1–3), 4–22 (Jul 2006). https://doi.org/10.1016/j.tcs.2006.03.009
6. Artemov, S.: The logic of justification. The Review of Symbolic Logic **1**(4), 477–513 (Dec 2008). https://doi.org/10.1017/S1755020308090060
7. Artemov, S.: Tracking evidence. In: Blass, A., Dershowitz, N., Reisig, W. (eds.) Fields of Logic and Computation, LNCS, vol. 6300, pp. 61–74. Springer (2010). https://doi.org/10.1007/978-3-642-15025-8_3
8. Artemov, S.: On aggregating probabilistic evidence. In: Artemov, S., Nerode, A. (eds.) LFCS 2016. LNCS, vol. 9537, pp. 27–42. Springer (2016)
9. Artemov, S., Bonelli, E.: The intensional lambda calculus. In: Artemov, S., Nerode, A. (eds.) Logical Foundations of Computer Science, International Symposium, LFCS 2007, New York, NY, USA, June 4–7, 2007, Proceedings, LNCS, vol. 4514, pp. 12–25. Springer (2007). https://doi.org/10.1007/978-3-540-72734-7_2
10. Artemov, S., Fitting, M.: Justification Logic: Reasoning with Reasons. Cambridge University Press (2019)
11. Artemov, S., Kuznets, R.: Logical omniscience via proof complexity. In: Ésik, Z. (ed.) Computer Science Logic, 20th International Workshop, CSL 2006, 15th Annual Conference of the EACSL, Szeged, Hungary, September 25–29, 2006, Proceedings, LNCS, vol. 4207, pp. 135–149. Springer (2006). https://doi.org/10.1007/11874683_9
12. Artemov, S., Kuznets, R.: Logical omniscience as a computational complexity problem. In: Heifetz, A. (ed.) Theoretical Aspects of Rationality and Knowledge, Proceedings of the Twelfth Conference (TARK 2009). pp. 14–23. ACM, Stanford University, California (Jul 6–8, 2009). https://doi.org/10.1145/1562814.1562821
13. Artemov, S., Kuznets, R.: Logical omniscience as infeasibility. APAL **165**(1), 6–25 (Jan 2014). https://doi.org/10.1016/j.apal.2013.07.003
14. Baltag, A., Renne, B., Smets, S.: The logic of justified belief, explicit knowledge, and conclusive evidence. APAL **165**(1), 49–81 (2014). https://doi.org/http://dx.doi.org/10.1016/j.apal.2013.07.005
15. Baur, M.: Realization of common knowledge (submitted)
16. Baur, M., Studer, T.: Semirings of evidence. In: Dastani, M., Dong, H., van der Torre, L. (eds.) Proceedings of Logic and Argumentation CLAR 2020, pp. 42–57. Springer (2020)
17. Baur, M., Studer, T.: Semirings of Evidence. Journal of Logic and Computation **31**(8), 2084–2106 (02 2021)

18. Bucheli, S., Kuznets, R., Studer, T.: Justifications for common knowledge. Journal of Applied Non-classical Logic **21**(1), 35–60 (Jan–Mar 2011). https://doi.org/10.3166/JANCL.21.35-60
19. Church, A.: Introduction to Mathematical Logic. Princeton Mathematical Series, Princeton University Press (1996), https://books.google.ch/books?id=JDLQOMKbdScC
20. Deutch, D., Moskovitch, Y., Tannen, V.: Provenance-based analysis of data-centric processes. The VLDB Journal **24**(4), 583–607 (2015). https://doi.org/10.1007/s00778-015-0390-5
21. Esparza, J., Kiefer, S., Luttenberger, M.: On fixed point equations over commutative semirings. In: Thomas, W., Weil, P. (eds.) STACS 2007. pp. 296–307. Springer Berlin Heidelberg, Berlin, Heidelberg (2007)
22. Fagin, R., Halpern, J.Y., Moses, Y., Vardi, M.Y.: Reasoning About Knowledge. MIT Press (1995)
23. Foster, J.N., Green, T.J., Tannen, V.: Annotated XML: Queries and provenance. In: Proceedings of the Twenty-seventh ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems. pp. 271–280. PODS '08, ACM (2008). https://doi.org/10.1145/1376916.1376954
24. Geerts, F., Unger, T., Karvounarakis, G., Fundulaki, I., Christophides, V.: Algebraic structures for capturing the provenance of SPARQL queries. J. ACM **63**(1) (2016). https://doi.org/10.1145/2810037
25. Ghari, M.: Pavelka-style fuzzy justification logics. Logic Journal of the IGPL **24**(5), 743–773 (2016)
26. Green, T.J.: Containment of conjunctive queries on annotated relations. In: Proceedings of the 12th International Conference on Database Theory. pp. 296–309. ICDT '09, ACM (2009). https://doi.org/10.1145/1514894.1514930
27. Green, T.J., Ives, Z.G., Tannen, V.: Reconcilable differences. Theory of Computing Systems **49**(2), 460–488 (2011). https://doi.org/10.1007/s00224-011-9323-x
28. Green, T.J., Karvounarakis, G., Tannen, V.: Provenance semirings. In: Proceedings of the Twenty-sixth ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems. pp. 31–40. ACM (2007). https://doi.org/10.1145/1265530.1265535
29. Green, T.J., Tannen, V.: The semiring framework for database provenance. In: Proceedings of the 36th ACM SIGMOD-SIGACT-SIGAI Symposium on Principles of Database Systems. pp. 93–99. ACM (2017). https://doi.org/10.1145/3034786.3056125
30. Kleene, S.C.: Introduction to Metamathematics. Groningen: P. Noordhoff N.V. (1952)
31. Krupski, V.N.: On sharp justification logics. Moscow University Mathematics Bulletin **1**, 71–75 (2020), originally published in Russian
32. Kuich, W.: Semirings and formal power series: Their relevance to formal languages and automata. In: Rozenberg, G., Salomaa, A. (eds.) Handbook of Formal Languages, Vol. 1, pp. 609–677. Springer-Verlag (1997)
33. Kuznets, R.: A note on the use of sum in the Logic of Proofs. In: Drossos, C., Peppas, P., Tsinakis, C. (eds.) Proceedings of the 7th Panhellenic Logic Symposium. pp. 99–103. Patras University Press, Patras University, Greece (Jul 15–19, 2009)
34. Kuznets, R., Studer, T.: Weak arithmetical interpretations for the logic of proofs. Logic Journal of IGPL **24**(3), 424–440 (2016)
35. Kuznets, R., Studer, T.: Logics of Proofs and Justifications. College Publications (2019)

36. Lehmann, E., Studer, T.: Subset models for justification logic. In: Iemhoff, R., Moortgat, M., de Queiroz, R. (eds.) Logic, Language, Information, and Computation - WoLLIC 2019, pp. 433–449. Springer (2019)
37. Lehmann, E., Studer, T.: Belief expansion in subset models. In: Artemov, S., Nerode, A. (eds.) Proceedings of Logical Foundations of Computer Science LFCS'20, pp. 85–97. Springer (2020)
38. Lehmann, E., Studer, T.: Exploring subset models for justification logic. In: Fitting, M. (ed.) Selected Topics from Contemporary Logics, pp. 605–634. College Publications (2021)
39. Marti, M., Studer, T.: The proof theory of common knowledge. In: van Ditmarsch, H., Sandu, G. (eds.) Jaakko Hintikka on knowledge and game theoretical semantics. Outstanding Contributions to Logic, Springer (2018)
40. Meyer, J.J.C., Hoek, W.V.D.: Epistemic Logic for AI and Computer Science. Cambridge University Press (1995)
41. Mints, G.: Lewis' systems and system T (1965–1973). In: Mints, G. (ed.) Selected Papers in Proof Theory, Studies in Proof Theorie, vol. 3, pp. 221—294. Bibliopolis (1992)
42. Studer, T.: Decidability for some justification logics with negative introspection. Journal of Symbolic Logic **78**(2), 388–402 (Jun 2013). https://doi.org/10.2178/jsl.7802030
43. Troelstra, A.S., Schwichtenberg, H.: Basic Proof Theory. Cambridge University Press, second edn. (2000)

Erklärung

gemäss Art. 18 PromR Phil.-nat. 2019

Name/Vorname: Baur Michael

Matrikelnummer: 15-114-671

Studiengang: Informatik

Bachelor ☐ Master ☐ Dissertation ☑

Titel der Arbeit: Justification Logic, Semirings and Realizations

LeiterIn der Arbeit: Prof. Thomas Studer

Ich erkläre hiermit, dass ich diese Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen benutzt habe. Alle Stellen, die wörtlich oder sinngemäss aus Quellen entnommen wurden, habe ich als solche gekennzeichnet. Mir ist bekannt, dass andernfalls der Senat gemäss Artikel 36 Absatz 1 Buchstabe r des Gesetzes über die Universität vom 5. September 1996 und Artikel 69 des Universitätsstatuts vom 7. Juni 2011 zum Entzug des Doktortitels berechtigt ist. Für die Zwecke der Begutachtung und der Überprüfung der Einhaltung der Selbständigkeitserklärung bzw. der Reglemente betreffend Plagiate erteile ich der Universität Bern das Recht, die dazu erforderlichen Personendaten zu bearbeiten und Nutzungshandlungen vorzunehmen, insbesondere die Doktorarbeit zu vervielfältigen und dauerhaft in einer Datenbank zu speichern sowie diese zur Überprüfung von Arbeiten Dritter zu verwenden oder hierzu zur Verfügung zu stellen.

Biel, 05.06.2023

Ort/Datum

M. Baur

Unterschrift