

# Semirings of Evidence

Michael Baur and Thomas Studer

Institute of Computer Science  
University of Bern  
Switzerland  
`michael.baur@inf.unibe.ch`  
`thomas.studer@inf.unibe.ch`

**Abstract.** In traditional justification logic, evidence terms have the syntactic form of polynomials, but they are not equipped with the corresponding algebraic structure. 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. Last but not least the semiring approach seems promising for obtaining a realization procedure for modal fixed point logics.

**Keywords:** justification logic, semiring, completeness, realization

## 1 Introduction

Justification logic replaces the  $\Box$ -operator from modal logic with explicit evidence terms [5, 11, 32]. 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  $A$  [5, 31] 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 [6, 7, 14, 15, 39].

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 [8]. 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 [12–14].

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 [5].

The main contribution of the present paper is to 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 [5]. 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  $\omega$ -continuous semirings, i.e. semirings in which certain fixed points exist, may provide a solution to the problem of realizing modal fixed point logics like the logic of common knowledge. In these logics, some modal operators can be interpreted as fixed points of monotone operations. It seems likely that their realizations also should be fixed points of certain operations on semirings.

## Related Work

Our approach is heavily inspired by the semiring approach for provenance in database systems [26]. 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 [27].

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 [3, 4, 20–22, 24, 25].

There are only few systems available where justification terms are equipped with additional structure. Two prominent examples are based on  $\lambda$ -terms (in contrast to the combinatory terms of the Logic of Proofs). The reflective lambda calculus [2] includes reduction rules on proof terms. The intensional lambda calculus [10] 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 [28].

The present paper extends and corrects the results presented in [17]. We extend our previous work by two realization theorems that establish the precise relationship between semirings of evidence and traditional epistemic modal logic, see Section 4. Moreover we slightly changed the axiomatic system in order to fix a mistake in the completeness proof.

## 2 The Syntax of SE

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

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

$$c \in \mathbf{JConst}, x \in \mathbf{JVar}, s \cdot t, \text{ and } s + t,$$

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

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

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

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

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  $\sigma : \mathbf{JVar} \rightarrow \mathbf{Tm}$  by defining  $A\sigma := A[x_1/y_1] \dots [x_n/y_n][y_1/\sigma(x_1)] \dots [y_n/\sigma(x_n)]$ , where  $x_1, \dots, x_n$  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:

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

The rules of SE are:

$$\mathbf{MP} \quad \frac{A \quad A \rightarrow B}{B}$$

and

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

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 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  $C[x/s + t] \rightarrow C[x/t + s]$  is derived from an instance of the axiom scheme **c+** by **jv** and it is the same as  $A \rightarrow B$ .

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:*

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

A theory is just any set of formulas.

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

Often we drop the subscript  $\text{SE}$  in  $\vdash_{\text{SE}}$  when it is clear from the context. Moreover, we use  $\vdash_{\text{CL}}$  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  $c \in \text{JConst}$  with  $c : A \in T$*
2. *for all  $B \in T$  there exists  $c \in \text{JConst}$  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*

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

*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  $B \rightarrow A$  and  $B$ , then by I.H. exist  $t_1, t_2 \in \text{GTm}$  such that  $T \vdash_{\text{SE}} t_1 : (B \rightarrow A)$  and  $T \vdash_{\text{SE}} t_2 : B$ . Thus  $T \vdash_{\text{SE}} t : A$  holds for  $t = t_1 \cdot t_2$ .
3. If  $A[x/s]$  is obtained by **fv** from  $A$ , then by I.H. exists  $t \in \text{GTm}$  such that  $T \vdash_{\text{SE}} t : A$ . Finally, **fv** implies  $T \vdash_{\text{SE}} t : A[x/s]$ .  $\square$

*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 15. The implication

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

follows directly from rule **fv**.

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*

$$\vdash_{\text{SE}} A \quad \text{iff} \quad \vdash_{\text{CL}} A.$$

*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  $t \cdot$ . 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  $A \in \text{Fml}$ ,

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

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

Now consistency of SE follows immediately.

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

*Proof.* Assume towards contradiction that  $\vdash_{\text{SE}} \perp$ . By conservativity of SE over CL we get  $\vdash_{\text{CL}} \perp$ , which is a contradiction.  $\square$

*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  $\vdash x : P \rightarrow 0 : P$  is not valid because it can be shown that  $\not\vdash 1 : P \rightarrow 0 : P$ .

### 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.

**Definition 5 (Semiring).**  $K = (S, +, \cdot, 0, 1)$ , where  $S$  is the domain, is a semiring, if for all  $a, b, c \in S$ :

1.  $(a + b) + c = a + (b + c)$ ,  $a + b = b + a$  and  $a + 0 = 0 + a = a$
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.  $a \cdot 0 = 0 \cdot a = 0$

Thus, unlike in a ring, there is no inverse to  $+$ . We also do not require  $\cdot$  to be commutative.

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  $I : \text{JConst} \rightarrow S$  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  $I : \text{Tm} \rightarrow S[\text{JVar}]$ , where  $S[\text{JVar}]$  is the polynomial semiring in  $\text{JVar}$  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  $\text{Fml}_S$  as the set of formulas where we use elements of  $S$  instead of justification terms.

1.  $\perp \in \text{Fml}_S$
2.  $P \in \text{Fml}_S$ , where  $P \in \text{Prop}$
3.  $A \rightarrow B \in \text{Fml}_S$ , where  $A \in \text{Fml}_S$  and  $B \in \text{Fml}_S$
4.  $s : A \in \text{Fml}_S$ , where  $A \in \text{Fml}_S$  and  $s \in S$

**Definition 6 (Evidence relation).** Let  $S$  be the domain of a semiring. We call  $J \subseteq S \times \text{Fml}_S$  an evidence relation if for all  $s, t \in S$  and all  $A, B \in \text{Fml}_S$ :

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

**Definition 7 (Valuation).** A valuation  $v$  is a function from  $\text{JVar}$  to  $S$ .

The polynomial  $I(t)$  can be viewed as a function  $t_I : S^n \rightarrow S$ , where  $n$  is the number of variables that occur in  $t$ . Hence, given an interpretation  $I : \text{JConst} \rightarrow S$  and a valuation  $v$ , every  $t \in \text{Tm}$  can be mapped to an element  $t_I(v(x_1), \dots, v(x_n))$  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.,

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

For  $A \in \text{Fml}$  we define  $A_I^v \in \text{Fml}_S$  inductively:

1.  $\perp_I^v := \perp$
2.  $P_I^v := P$ , where  $P \in \text{Prop}$
3.  $(A \rightarrow B)_I^v := A_I^v \rightarrow B_I^v$ , where  $A \in \text{Fml}$  and  $B \in \text{Fml}$
4.  $(s : A)_I^v := s_I^v : A_I^v$ , where  $A \in \text{Fml}$  and  $s \in \text{Tm}$

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

**Definition 8 (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.,  $* : \text{Prop} \rightarrow \{\mathbb{F}, \mathbb{T}\}$
3.  $I$  is an interpretation, i.e.,  $I : \text{JConst} \rightarrow S$
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 9 (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:

- $M, v \not\Vdash \perp$
- $M, v \Vdash P \quad \text{iff} \quad P^* = \mathbb{T}$
- $M, v \Vdash A \rightarrow B \quad \text{iff} \quad M, v \not\Vdash A \text{ or } M, v \Vdash B$
- $M, v \Vdash s : A \quad \text{iff} \quad J(s_I^v, A_I^v)$

Further we set  $M \Vdash A \quad \text{iff} \quad M, v \Vdash A$  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 10 (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

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

*Proof.* By induction on the structure of  $A$ .

- Case  $A = \perp$ . We have  $M, v \not\Vdash \perp$  and  $M, w \not\Vdash \perp$ .
- Case  $A = P$ . We have  $M, v \Vdash P \Leftrightarrow P^* = \mathbb{T} \Leftrightarrow M, w \Vdash P$ .
- Case  $A = B \rightarrow C$ . We have  $M, v \Vdash B \rightarrow C$   
 $\Leftrightarrow M, v \not\Vdash B \text{ or } M, v \Vdash C$   
 $\stackrel{\text{I.H.}}{\Leftrightarrow} M, w \not\Vdash B\sigma \text{ or } M, w \Vdash C\sigma$   
 $\Leftrightarrow M, w \Vdash B\sigma \rightarrow C\sigma \Leftrightarrow M, w \Vdash (B \rightarrow C)\sigma$ .
- Case  $A = s : B$ . We have  $M, v \Vdash s : B$   
 $\Leftrightarrow J(s_I^v, B_I^v)$   
 $\Leftrightarrow J(s_I(v(x_1), \dots, v(x_n)), B_I(v(x_1), \dots, v(x_n)))$   
 $\Leftrightarrow J(s_I((t_1)_I^w, \dots, (t_n)_I^w), B_I((t_1)_I^w, \dots, (t_n)_I^w))$   
 $\Leftrightarrow J((s\sigma)_I^w, (B\sigma)_I^w) \Leftrightarrow M, w \Vdash s\sigma : B\sigma$   
 $\Leftrightarrow M, w \Vdash (s : B)\sigma.$

□

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

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



*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  $M, v \Vdash x : (A \rightarrow B)$  and  $M, v \Vdash y : A$ . That is  $J(x_I^v, (A \rightarrow B)_I^v)$  and  $J(y_I^v, A_I^v)$  hold, which by Definition 6 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  $A$ :

- $A = \perp$  or  $A = P$ . Trivial.
- $A = B \rightarrow C$ .  $M, v \Vdash (B \rightarrow C)[x/s]$   
 $\Leftrightarrow M, v \Vdash B[x/s] \rightarrow C[x/s]$   
 $\Leftrightarrow M, v \not\Vdash B[x/s] \text{ or } M, v \Vdash C[x/s]$   
 $\stackrel{\text{I.H.}}{\Leftrightarrow} M, v \not\Vdash B[x/t] \text{ or } M, v \Vdash C[x/t]$   
 $\Leftrightarrow M, v \Vdash B[x/t] \rightarrow C[x/t]$   
 $\Leftrightarrow M, v \Vdash (B \rightarrow C)[x/t]$ .
- $A = u : B$ .  $M, v \Vdash (u : B)[x/s]$   
 $\Leftrightarrow M, v \Vdash u[x/s] : B[x/s]$   
 $\Leftrightarrow J(u[x/s]_I^v, B[x/s]_I^v)$   
 $\Leftrightarrow J(u[x/t]_I^v, B[x/t]_I^v)$   
 $\Leftrightarrow M, v \Vdash u[x/t] : B[x/t]$   
 $\Leftrightarrow M, v \Vdash (u : B)[x/t]$ .

By mentioning that all the semiring axioms have the form  $A[x/s] \rightarrow A[x/t]$  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

$$M, v \Vdash A \text{ for all valuations } v. \quad (2)$$

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

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

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

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

- $[t]$  is the equivalence class of  $t$  with respect to the semiring equalities, see Definition 5;
- $[s] + [t] := [s + t]$ ;
- $[s] \cdot [t] := [s \cdot t]$ ;
- $S_{\mathbf{Tm}} := \{[t] : t \in \mathbf{Tm}\}$ ;
- $K_{\mathbf{Tm}} := (S_{\mathbf{Tm}}, +, \cdot, [0], [1])$  is the free semiring over  $\mathbf{JConst} \cup \mathbf{JVar}$ .

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*

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

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  $I : \mathbf{JConst} \rightarrow S_{\mathbf{Tm}}$  with  $I(c) = [c]$ , a term  $s$ , and a valuation  $v : \mathbf{JVar} \rightarrow S_{\mathbf{Tm}}$  with  $v(x_i) = [t_i]$ . Then we have*

$$s_I^v = [s\sigma], \text{ where } \sigma(x_i) = t_i.$$

*Proof.* Induction on the structure of  $s$ :

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

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

$$\text{Thus } (s_1)_I^v + (s_2)_I^v = [s_1\sigma] + [s_2\sigma] = [(s_1 + s_2)\sigma].$$

- $(s_1 \cdot s_2)_I^v = (s_1)_I^v \cdot (s_2)_I^v$ . By I.H. we have

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

$$\text{Thus } (s_1)_I^v \cdot (s_2)_I^v = [s_1\sigma] \cdot [s_2\sigma] = [(s_1 \cdot s_2)\sigma] \quad \square$$

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

$$[\cdot] : \mathbf{Fml} \rightarrow \mathbf{Fml}_{S_{\mathbf{Tm}}}$$

as follows:

- $[\perp] := \perp$
- $[P] := P$
- $[A \rightarrow B] := [A] \rightarrow [B]$
- $[t : A] := [t] : [A]$

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  $[A] = A_I^v$ . Now we extend Lemma 5 to formulas.

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

$$A_I^v = [A\sigma], \text{ where } \sigma(x_i) = t_i.$$

*Proof.* Induction on the structure of  $A$ :

- $\perp_I^v = \perp = [\perp]$
- $P_I^v = P = [P]$
- $(A \rightarrow B)_I^v = A_I^v \rightarrow B_I^v$   
 $\stackrel{\text{I.H.}}{=} [A\sigma] \rightarrow [B\sigma] = [(A \rightarrow B)\sigma]$
- $(s : A)_I^v = s_I^v : A_I^v$   
 $\stackrel{\text{I.H. and L. 5}}{=} [s\sigma] : [A\sigma] = [(s : A)\sigma]$  □

Let **Prop2** be an infinite set of atomic propositions with  $\mathbf{Prop} \cap \mathbf{Prop2} = \emptyset$ . Then there exists a bijective function  $f : S_{\mathbf{Tm}} \times \mathbf{Fml}_{S_{\mathbf{Tm}}} \rightarrow \mathbf{Prop2}$ . 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  $\mathbf{Prop} \cup \mathbf{Prop2}$ .

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

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

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

Suppose  $A' \in T'$ . Then there exist a formula  $B$  with  $B \in T$  or  $B$  is an axiom and  $\sigma : \mathbf{JVar} \rightarrow \mathbf{Tm}$  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  $T' \vdash_{\text{CL}} A'$  then  $T' \vdash_{\text{CL}} A[x/t]'$ .*

*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  $T' \vdash_{\text{CL}} A[x/t]'$ .

2. If  $A'$  is obtained by **MP** from  $B$  and  $B \rightarrow A'$  then  $B$  can be written as  $C'$  because  $f$  is surjective. The induction hypothesis ( $T' \vdash_{\text{CL}} C[x/t]'$  and  $T' \vdash_{\text{CL}} C[x/t]' \rightarrow A[x/t]'$ ) yields  $T' \vdash_{\text{CL}} A[x/t]'$ .  $\square$

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

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

*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  $T' \vdash_{\text{CL}} A'$ .
2. If  $A$  is obtained by **MP** from  $B$  and  $B \rightarrow A$  then the induction hypothesis ( $T' \vdash_{\text{CL}} B'$  and  $T' \vdash_{\text{CL}} B' \rightarrow A'$ ) immediately yields  $T' \vdash_{\text{CL}} A'$ .
3. If  $A[x/t]$  is obtained by **fv** from  $A$  then the induction hypothesis is  $T' \vdash_{\text{CL}} A'$ . By the previous lemma we conclude  $T' \vdash_{\text{CL}} A[x/t]'$ .

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  $\sigma : \text{JVar} \rightarrow \text{Tm}$  such that  $(B\sigma)' = A'$ . Trivially we have  $T \vdash_{\text{SE}} B$  and get by **fv** that  $T \vdash_{\text{SE}} B\sigma$ . 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  $T \vdash_{\text{SE}} A$  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  $T \vdash_{\text{SE}} A$  again by Lemma 4 and propositional reasoning.
3. If  $A'$  is obtained by **MP** from  $B \rightarrow A'$  and  $B$  then  $B$  can be written as  $C'$ . The induction hypothesis ( $T \vdash_{\text{SE}} C \rightarrow A$  and  $T \vdash_{\text{SE}} C$ ) implies  $T \vdash_{\text{SE}} A$ .  $\square$

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:*

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

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

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

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

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

By the truth definition in **CL** we find

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

From the definition of  $J$  in  $M$  we get

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

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

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

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  $A = \perp$ . We have  $M_* \not\Vdash \perp'$  and  $M, w \not\Vdash \perp$ .
- Case  $A = P$ . We have  $M_* \Vdash P' \Leftrightarrow M_* \Vdash P \Leftrightarrow P^* = \mathbb{T} \Leftrightarrow M, w \Vdash P$ .
- Case  $A = B \rightarrow C$ . We have  $M_* \Vdash ((B \rightarrow C)\sigma)'$ 
  - $\Leftrightarrow M_* \Vdash (B\sigma)' \rightarrow (C\sigma)'$
  - $\Leftrightarrow M_* \not\Vdash (B\sigma)' \text{ or } M_* \Vdash (C\sigma)'$
  - $\Leftrightarrow M, w \not\Vdash B \text{ or } M, w \Vdash C$  (by induction hypothesis)
  - $\Leftrightarrow M, w \Vdash B \rightarrow C$
  - $\Leftrightarrow M, w \Vdash B \rightarrow C$ .
- 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  $M_* \not\Vdash F'$ , we derive  $M, v \not\Vdash F$ , which finishes the proof.  $\square$

## 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 formula 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  $\mathbf{Fml}$  to formulas of the modal logic  $\mathbf{K}$  that replaces all occurrences of  $s$  : in a formula of  $\mathbf{SE}$  with  $\Box$ .

**Definition 11.** *We say that a theory  $T$  is pure if for each formula  $A \in T$  we have that  $\vdash_{\mathbf{K}} A^\circ$ .*

We immediately get the following lemma.

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

$$T \vdash_{\mathbf{SE}} A \text{ implies } \vdash_{\mathbf{K}} A^\circ.$$

To investigate mappings from modal logic to  $\mathbf{SE}$ , we need the deductive system  $\mathbf{GK}$  for the logic  $\mathbf{K}$ .

**Definition 12.** *If  $\Gamma$  and  $\Delta$  are multisets of formulas, then the expression  $\Gamma \supset \Delta$  is a sequent.*

The axioms of  $\mathbf{GK}$  are

$$P \supset P \quad \text{and} \quad \perp \supset$$

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

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

$$\begin{array}{c}
(\Box) \frac{\Gamma \supset A}{\Box \Gamma \supset \Box A} \\
(w \supset) \frac{\Gamma \supset \Delta}{A, \Gamma \supset \Delta} \qquad (\supset w) \frac{\Gamma \supset \Delta}{\Gamma \supset \Delta, A} \\
(c \supset) \frac{A, A, \Gamma \supset \Delta}{A, \Gamma \supset \Delta} \qquad (\supset c) \frac{\Gamma \supset \Delta, A, A}{\Gamma \supset \Delta, A}
\end{array}$$

System GK is sound and complete for the modal logic K, see, e.g., [36, 40].

**Theorem 4.** *Let  $A$  be a formula of the language of modal logic. Then  $\vdash_{\text{GK}} \supset A$  if and only if  $A$  is valid in K.*

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 13.** *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  $T \vdash_{\text{SE}} \bigwedge \Gamma \rightarrow \bigvee \Delta$ .*

In the traditional approach to constructive realization [5, 32], one would say that  $\Gamma \supset \Delta$  is derivable in SE if  $\bigwedge \Gamma \vdash_{\text{SE}} \bigvee \Delta$ . 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 13.

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  $\mathbf{j+}$  is formulated with  $\wedge$  we can not use Artemov's original realization algorithm. But Kuznets [30] 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  $B \rightarrow C$  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 occurrence 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 14.** *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 15.** A theory  $T$  is schematic if it satisfies the following property: for each constant  $c \in \mathbf{JConst}$ , the set of axioms  $\{A \mid c : A \in T \text{ and } A \text{ is an axiom}\}$  consists of all instances of one or several (possibly zero) axiom schemes of SE.

**Lemma 10.** Let  $T$  be an axiomatically appropriate theory.

If  $T \vdash_{\text{SE}} s : (A \rightarrow B)$  and  $T \vdash_{\text{SE}} t : (B \rightarrow C)$  then  $T \vdash_{\text{SE}} d \cdot c \cdot t \cdot s : (A \rightarrow C)$ , where  $T \vdash_{\text{SE}} c : (B \rightarrow C \rightarrow (A \rightarrow (B \rightarrow C)))$  and  $T \vdash_{\text{SE}} d : (A \rightarrow (B \rightarrow C) \rightarrow (A \rightarrow B \rightarrow (A \rightarrow C)))$ .

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

**Definition 16.** Let  $T$  be an axiomatically appropriate theory and suppose

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

We define  $\text{syl}(s, t)$  such that

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

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

*Remark 3.* Lemma 10 guarantees the existence of  $\text{syl}(s, t)$ . Note that the term  $\text{syl}(s, t)$  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  $A_1, \dots, A_n$  and  $1 \leq i \leq n$

$$T \vdash_{\text{SE}} d_n : (A_i \rightarrow A_1 \vee \dots \vee A_n). \tag{6}$$

**Lemma 11.** Let  $T$  be an axiomatically appropriate theory and  $n \in \mathbb{N}_{>0}$ .

Assume there exists  $d_n$ .

If  $T \vdash_{\text{SE}} s_i : (A_i \rightarrow B)$  for all  $i$ , then for an arbitrary  $t \in \mathbf{Tm}$

$$T \vdash_{\text{SE}} t : A_i \rightarrow \text{syl}(d_n, e_n \cdot s_1 \cdot \dots \cdot s_n) \cdot t : B,$$

where  $T \vdash_{\text{SE}} e_n : ((A_1 \rightarrow B) \rightarrow (\dots \rightarrow ((A_n \rightarrow B) \rightarrow (A_1 \vee \dots \vee A_n \rightarrow B)) \dots))$ .

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

$$\text{syl}(d_n, e_n \cdot s_1 \cdot \dots \cdot s_n) : (A_i \rightarrow B) \rightarrow (t : A_i \rightarrow \text{syl}(d_n, e_n \cdot s_1 \cdot \dots \cdot s_n) \cdot t : B)$$

we infer  $T \vdash_{\text{SE}} t : A_i \rightarrow \text{syl}(d_n, e_n \cdot s_1 \cdot \dots \cdot s_n) \cdot t : B$  for all  $i$ .  $\square$



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  $A_1 \rightarrow (\dots \rightarrow (A_n \rightarrow A_1 \wedge \dots \wedge A_n) \dots)$  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*

$$T \vdash_{\text{SE}} t_1 : A_1 \wedge \dots \wedge t_n : A_n \rightarrow c_n \cdot t_1 \cdot \dots \cdot t_n : (A_1 \wedge \dots \wedge A_n),$$

where  $T \vdash_{\text{SE}} c_n : (A_1 \rightarrow (\dots \rightarrow (A_n \rightarrow A_1 \wedge \dots \wedge A_n) \dots))$ .

For a multiset  $\Gamma$  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  $\Gamma_i \subseteq \text{Fml}$  with  $|\Gamma_i| = m$  such that  $T \vdash_{\text{SE}} \bigwedge \Gamma_i \rightarrow A$ . Then there exists  $q \in \text{Tm}$  such that for each  $\Gamma_i$  we have  $T \vdash_{\text{SE}} \bigwedge x : \Gamma_i \rightarrow q : A$  where  $x$  is a variable.*

*Proof.* By internalization we find ground terms  $s_i$  such that

$$T \vdash_{\text{SE}} s_i : (\bigwedge \Gamma_i \rightarrow A).$$

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

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

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

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

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

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

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

Note that supporting weakening is rather natural. For instance, it corresponds to accepting the  $R\vee$  rule in Gentzen system  $\mathbf{G3}$ , see, e.g. [40]. 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 18.**  *$A \in \mathbf{Fml}$  is a balanced disjunction of depth 0. If  $A$  and  $B$  are balanced disjunctions 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  $\Gamma_i \subseteq \mathbf{Fml}$  with  $|\Gamma_i| = m$  such that  $T \vdash_{\mathbf{SE}} \bigwedge \Gamma_i \rightarrow A$ . Then there exists  $q \in \mathbf{Tm}$  such that for each  $\Gamma_i$  we have  $T \vdash_{\mathbf{SE}} \bigwedge x : \Gamma_i \rightarrow q : A$ , 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  $A_1, \dots, A_{2^l}$

$$T \vdash_{\mathbf{SE}} d_{2^l} : (A_i \rightarrow A_1 \vee \dots \vee A_{2^l}),$$

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

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

and

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

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

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

and

$$d_l : (A_{l+1} \vee \dots \vee A_{2l} \rightarrow (A_1 \vee \dots \vee A_l) \vee (A_{l+1} \vee \dots \vee A_{2l})).$$

The term  $\mathit{syl}(d_l, d_2)$  does not depend on the formulas  $A_1, \dots, A_{2l}$  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  $q \in \mathbb{Tm}$  such that  $T \vdash_{\text{SE}} \bigwedge x : \Gamma_i \rightarrow q : A$  for all  $i \leq 2^k$ , including all  $i \leq n$ .  $\square$

In order to prove a realization theorem, we need a notion to relate different occurrences of  $\square$  in a GK-derivation. The main definition will be that of an essential family of  $\square$ -occurrences, which goes back to [5] (for some examples see [32]).

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

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

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

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

All occurrences of  $\square$  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  $(\square)$  rule.

**Theorem 5 (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  $\vdash_K A \Rightarrow T \vdash_{\text{SE}} r(A)$ .*

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

1. Modify the derivation. For each essential family  $f$  do the following: If  $n$   $(\square)$  rules introduce a  $\square$ -operator to  $f$ , their premises are  $\Gamma_i \supset A$ ,  $1 \leq i \leq n$ , and none of the  $\Gamma_i$  is empty then use first  $(w \supset)$  to duplicate formulas of  $\Gamma_i$  such that all  $\Gamma_i$  have the same cardinality. After applying the  $(\square)$  rule remove the duplicates by  $(c \supset)$ .
2. For each negative family and each non-essential positive family, replace all  $\square$  occurrences by the variable  $x$ .

<sup>1</sup> that is, e.g., an occurrence of  $\square$  in the premise  $A$  in the above instance of  $(\supset \rightarrow)$  is related to the occurrence of  $\square$  at the same position in the subformula  $A$  of  $A \rightarrow B$  in the conclusion

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  $|\Gamma_1| = \dots = |\Gamma_n| =: m$  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.  $P \supset P: r(P \rightarrow P) = P \rightarrow P$  which is derivable in SE.
2.  $\perp \supset: r(\perp \rightarrow \perp) = \perp \rightarrow \perp$  which is derivable in SE.
3.  $(\Box)$ : The case without empty  $\Gamma_i$ '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  $T \vdash_{\text{SE}} r(A)$ . Because the term for the introduced  $\Box$  was constructed according to the internalization property this implies  $T \vdash_{\text{SE}} r(\Box A)$ . By propositional reasoning we infer  $T \vdash_{\text{SE}} r(\bigwedge \Box \Gamma_i \rightarrow r(\Box A))$  for all  $i$ , therefore  $T \vdash_{\text{SE}} r(\bigwedge \Box \Gamma_i \rightarrow \Box A)$  for all  $i$ .
4. For the remaining rules the desired result is obtained by propositional reasoning.  $\square$

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

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

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 [5, 32].

**Theorem 6 (Normal realization).** *Let  $T$  be an axiomatically appropriate and schematic theory such that for some constant  $c$*

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

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

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

*Proof.* From the assumptions we get

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

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

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

and finally

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

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  $A \vee A \rightarrow A$ , which ensures that  $s * t$  doesn't depend on  $A$ . Therefore Artemov's realization procedure [5] can be used. We only need a small adjustment in the case of the  $(\square)$  rule, which we show next.

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

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

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

$$T \vdash_{\text{SE}} B_1 \wedge \dots \wedge B_n \rightarrow A.$$

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

$$T \vdash_{\text{SE}} x_1 : B_1 \wedge \dots \wedge x_n : B_n \rightarrow t : A.$$

Thus

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

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

## 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 [27]):

- $V = ([0, 1], \max, \cdot, 0, 1)$  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 [12–14].
- $P = (\mathcal{P}(S), \cup, \cap, \emptyset, S)$  is called the powerset lattice (semiring). This is closely related to the recently introduced subset models for justification logic [33–35]. This semiring can be used to model probabilistic evidence and aggregation thereof, see, e.g., [9].
- $F = ([0, 1], \max, \max(0, a + b - 1), 0, 1)$  is called the Łukasiewicz semiring. We can use it to model fuzzy evidences. Ghari [23] 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  $\omega$ -continuous, then the induced polynomial functions are  $\omega$ -continuous and, therefore, monotone [29]. 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.

Common knowledge of a proposition  $A$  is a fixed point of  $\lambda X.(EA \wedge EX)$ . There are justification logics with common knowledge available [6, 19] but their exact relationship to modal common knowledge is still open.

We believe that non-wellfounded and cyclic proof systems [1, 16, 18, 38] are the right proof-theoretic approach to settle this question. In those systems, proofs can be regarded as fixed points and hence justifications realizing those cyclic proofs will be fixed points in a semiring. For this purpose, making use of formal power series, which might be thought of as infinite polynomials, look very promising. First results in this direction have been obtained by Shamkanov [37] who presents a realization procedure for Gödel-Löb logic based on cyclic proofs.

### Acknowledgements

We thank the anonymous reviewers of the present journal version as well as the reviewers of the CLAR conference version of this paper for many helpful comments and suggestions for improvement. We also thank Vladimir Krupski for noticing a bug in an earlier version of this paper. We are grateful to Daniyar Shamkanov for the discussion about cyclic proofs and realization. This research is supported by the Swiss National Science Foundation grant 200020\_184625.

### References

1. Afshari, B., Leigh, G.E.: Cut-free completeness for modal mu-calculus. In: 2017 32nd Annual ACM/IEEE Symposium on Logic in Computer Science (LICS). pp. 1–12 (2017). <https://doi.org/10.1109/LICS.2017.8005088>
2. Alt, J., Artemov, S.: Reflective  $\lambda$ -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](https://doi.org/10.1007/3-540-45504-3_2)
3. 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>
4. 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>
5. Artemov, S.: Explicit provability and constructive semantics. Bulletin of Symbolic Logic **7**(1), 1–36 (Mar 2001)
6. 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>

7. Artemov, S.: The logic of justification. *The Review of Symbolic Logic* **1**(4), 477–513 (Dec 2008). <https://doi.org/10.1017/S1755020308090060>
8. 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](https://doi.org/10.1007/978-3-642-15025-8_3)
9. Artemov, S.: On aggregating probabilistic evidence. In: Artemov, S., Nerode, A. (eds.) *LFCS 2016, LNCS*, vol. 9537, pp. 27–42. Springer (2016)
10. 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](https://doi.org/10.1007/978-3-540-72734-7_2)
11. Artemov, S., Fitting, M.: *Justification Logic: Reasoning with Reasons*. Cambridge University Press (2019)
12. 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](https://doi.org/10.1007/11874683_9)
13. 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>
14. 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>
15. 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>
16. Baston, C., Capretta, V.: The coinductive formulation of common knowledge. In: Avigad, J., Mahboubi, A. (eds.) *Interactive Theorem Proving - 9th International Conference, ITP 2018, Proceedings, LNCS*, vol. 10895, pp. 126–141. Springer (2018). [https://doi.org/10.1007/978-3-319-94821-8\\_8](https://doi.org/10.1007/978-3-319-94821-8_8)
17. 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)
18. Bucheli, S., Kuznets, R., Studer, T.: Two ways to common knowledge. In: Bolander, T., Braüner, T. (eds.) *Proc. M4M–6*, pp. 83–98. No. 262 in *ENTCS*, Elsevier (2010). <https://doi.org/10.1016/j.entcs.2010.04.007>
19. 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>
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. 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>
22. 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>

23. Ghari, M.: Pavelka-style fuzzy justification logics. *Logic Journal of the IGPL* **24**(5), 743–773 (2016)
24. 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>
25. 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>
26. 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>
27. 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>
28. Krupski, V.N.: On sharp justification logics. *Moscow University Mathematics Bulletin* **1**, 71–75 (2020), originally published in Russian
29. 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)
30. Kuznets, R.: A note on the use of sum in the Logic of Proofs. In: Drossos, C., Pappas, P., Tsinakis, C. (eds.) *Proceedings of the 7th Panhellenic Logic Symposium*. pp. 99–103. Patras University Press, Patras University, Greece (Jul 15–19, 2009)
31. Kuznets, R., Studer, T.: Weak arithmetical interpretations for the logic of proofs. *Logic Journal of IGPL* **24**(3), 424–440 (2016)
32. Kuznets, R., Studer, T.: *Logics of Proofs and Justifications*. College Publications (2019)
33. 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)
34. 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)
35. Lehmann, E., Studer, T.: Exploring subset models for justification logic (submitted)
36. 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)
37. Shamkanov, D.: A realization theorem for the Gödel–Löb provability logic. *Sbornik: Mathematics* **207**(9), 1344–1360 (2016). <https://doi.org/10.4213/sm8667>
38. Studer, T.: On the proof theory of the modal  $\mu$ -calculus. *Studia Logica* **89**(3), 343–363 (2008). <https://doi.org/10.1007/s11225-008-9133-6>
39. 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>
40. Troelstra, A.S., Schwichtenberg, H.: *Basic Proof Theory*. Cambridge University Press, second edn. (2000)