A Sequent Calculus for Signed Interval Logic

Thomas Marthedal Rasmussen

Informatics and Mathematical Modeling
Technical University of Denmark
DK-2800 Kgs. Lyngby, Denmark
tmr@imm.dtu.dk

June 2001

Technical Report
IMM-TR-2001-06

Abstract

We propose and discuss a complete sequent calculus formulation for Signed Interval Logic (SIL) with the chief purpose of improving proof support for SIL in practice.

The main theoretical result is a simple characterization of the limit between decidability and undecidability of quantifier-free SIL.

We present a mechanization of SIL in the generic proof assistant Isabelle and consider techniques for automated reasoning.

Many of the results and ideas of this report are also applicable to traditional (non-signed) interval logic and, hence, to Duration Calculus.

1 Introduction

Interval logics (e.g. [13, 24, 3, 23, 17]) are modal logics of temporal intervals: One can express properties such as "if property ϕ holds on this interval then property ψ must hold on all subintervals" or "property φ must hold on some interval eventually". Interval logics have proven very useful in the specification and verification of real-time and safety-critical systems. This has in particular been the case since the introduction of Duration Calculus (DC) [24] — an extension of interval logic with notions for reasoning of accumulated durations. A substantial amount of work on various interval logics and extensions, and, not least, many examples and case-studies have been carried out over the last decade.

Thus, interval logics have clearly demonstrated their raison d'être by now. Despite this, no thorough investigation of both theoretical and practical matters of relevance for (automated) proof support exists. Almost all case-studies have been carried out on a "pen and paper" basis. There have been some attempts with respect to proof support, e.g. [20, 9], but the emphasis there is (mainly) on getting a system "up and running" such as to be able to conduct case studies. This means that (parts of) the theoretical foundations are left ad hoc.

The present report is an initial attempt to try to remedy this disparity. We try to provide a good theoretical basis for automated proof support (viz. a sequent calculus). This turns out somewhat difficult from a strictly theoretical viewpoint. But because of the great need for automated proof support for interval logics we do not give up: We try to see how far we can push our framework such as to make it *useful for actually conducting proofs*.

The rest of this report is organized as follows: In Section 2 we introduce interval logic with emphasis on Signed Interval Logic (SIL). We motivate SIL and informally sketch syntax and semantics. In Section 3 we give a theoretical foundation for automated proof support for SIL, namely a complete sequent calculus. We consider pros and cons of this formulation. Then, in Section 4, we consider an interesting theoretical result: The limit between decidability and undecidability of quantifier-free SIL is the cut rule of the sequent calculus system. This result is utilized in Section 5 where we consider an implementation of the sequent calculus for SIL in Isabelle. A substantial amount of automation support has been developed. Finally, we give conclusions in Section 6.

2 Signed Interval Logic

Signed Interval Logic (SIL) was proposed in [17], with the introduction of the notion of a *direction* of an interval. The proof system of SIL turns out to be not more complicated than that of Interval Temporal Logic (ITL) [3] but SIL is (contrary to ITL) capable of specifying liveness properties. Other interval logics capable of this (such as Neighbourhood Logic (NL) [23]) have more complicated proof systems. We will in this section give an introduction to ITL and SIL (with emphasis on the latter). For space reasons and clarity we choose to give an informal description of the semantics at the expense of a formal treatment. (Full formal developments for ITL and SIL are given in [3] and [17], respectively.)

2.1 Interval Temporal Logic

The syntax of ITL is that of First Order Logic (FOL) with equality, with the addition of formulas built from the binary interval modality *chop*: $\frown$. We let $x, y, z, \ldots$ denote variables, $s, t, u, \ldots$ denote terms and $\phi, \psi, \varphi, \ldots$ denote formulas. Thus, we have formulas of the form $\phi \frown \psi$ beside the usual FOL formulas. A function/predicate symbol is either *rigid* or *flexible*. The meaning of a flexible symbol is dependent on the current interval whereas a rigid symbol is not. ITL includes the special function symbols $+, 0$ (which are rigid) and ℓ (which is flexible). Furthermore, $=$ and all variables are assumed rigid. A formula is *flexible* if it contains a flexible symbol; otherwise it is *rigid*. A formula is *chop-free* if it does not contain the symbol $\frown$.

Semantically, formulas of ITL are interpreted with respect to a given interval, which is represented by a pair $[b, e]$ (where $b \leq e$) of elements

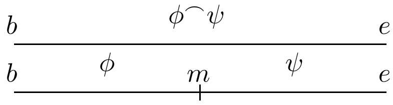

Figure 1: $\phi\frown\psi$ holds on $[b,e]$ iff there is $m \in [b,e]$ such that ϕ holds on $[b,m]$ and ψ on $[m,e]$

from an ordered temporal domain of time points. The meaning of the usual operators of FOL is independent of this interval whereas the meaning of $\frown$ is not; the semantics of $\frown$ is indicated in Fig. 1. We will refer to m of Fig. 1 as the chopping point of $\frown$. The chopping point will always lie inside the current interval on which we interpret a given formula. In general, modalities with this property are called contracting. With contracting modalities it is only possible to specify safety properties of a system. This is because once we have chosen the interval we want to observe we are restricted to specifying properties of this interval and its subintervals.

To specify liveness properties, we need to reach intervals outside the current interval. In general, modalities which can do this are called expanding. Neighbourhood Logic (NL) [23] is an example of an interval logic with expanding modalities. Both ITL and NL include a special symbol ℓ which represents the *length* of an interval. This property is not common for all interval logics.

2.2 Signed Interval Logic

The syntax of SIL is similar to that of ITL with the addition of the unary function symbol $-$. Semantically, SIL is an extension of ITL with the introduction of the notion of a *direction* (which can be either *forward* or *backward*) of an interval. The idea for SIL originates in [4]. where an interval logic with such a notion of a direction of an interval was informally developed.

An interval with a direction is in SIL represented by a *signed in-*

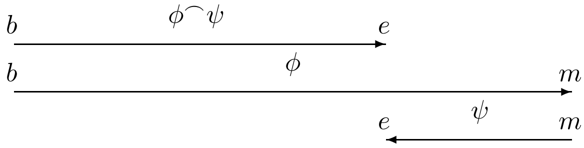

Figure 2: $\phi^\frown\psi$ holds on (b,e) iff there is m such that ϕ holds on (b,m) and ψ on (m,e)

terval (b,e). Both the pair (b,e) and the pair (e,b) represent the *same* interval but (e,b) has the opposite direction of (b,e). SIL inherits the special symbol ℓ from ITL. ℓ now gives the *signed length* of an interval. Intuitively, the absolute value of ℓ gives the length of the interval and the sign of ℓ determines the direction. Because of the directions of intervals, the meaning of $^\frown$ in SIL is altered: See Fig. 2. On the figure the direction of an interval is marked with a small arrowhead in either end of the interval. The chopping point can now lie anywhere and not just inside the current interval. This means that $^\frown$ of SIL has become an expanding modality, hence SIL can specify liveness properties.

SIL is a modal logic. Formally, the semantics sketched above is given in terms of a Kripke structure where the possible worlds are signed intervals. As $^\frown$ is a binary modality the accessibility relations is ternary and not binary as is the case for, e.g., the classical modal logic S4. What is non-orthodox about SIL is the inclusion of the flexible symbol ℓ, which is interpreted by a certain measure such that it is possible to perform simple arithmetic reasoning on signed lengths. For this to work we must require the domain of individuals (the *duration domain*) of the logic to have a certain structure, namely that of a group. SIL can be seen as extending S4 if we define the modalities $\Box$ and $\Diamond$ by $\Diamond\phi \mathrel{\widehat{=}} \mathrm{true}^\frown\phi^\frown\mathrm{true}$ and $\Box\phi \mathrel{\widehat{=}} \neg\Diamond\neg\phi$. In this setting, $\Diamond$ can be read as "for some signed interval" and $\Box$ as "for all signed intervals".

For a more formal treatment of the semantics of SIL we refer to [17]. In [17] a Hilbert-style proof system for SIL is also considered.

This system is an extension of that of FOL with equality. Any axiomatic basis for FOL can be chosen but one has to be careful when instantiating universally quantified formulas. To retain soundness we have to add extra side conditions requiring either the formula being instantiated to be chop-free or the term used in the instantiation to be rigid. (See [17] for details.) Furthermore, SIL contains axioms and inference rules defining the properties of $\frown$ and ℓ. (Again, see [17] for details.) Finally, SIL contains axioms expressing the properties of the domain, i.e. axioms defining a group. Provability in the Hilbert system is defined the standard way. We write $\vdash_{\mathrm{SIL}} \phi$ to denote theoremhood of ϕ in SIL. In [17] it is proved that the Hilbert proof system is sound and complete with respect to the semantics.

For the completeness result to go through, the duration domain (D) must at least have the structure of a group. But it is fairly easy to add further structure to D and still have completeness by reflecting this in the proof system. If we e.g. require D to be an Abelian group, the soundness and completeness result holds if we add a commutiativity axiom (for $+$) to the proof system. This commutiativity property is quite natural, hence we assume it from now on when referring to SIL. It will become crucial in Section 4 where we consider a decidability result.

To justify the name "interval logic" one could argue that it would be natural to require a total ordering on D. Again, by adding suitable (order) axioms to the proof system the completeness result will go through [18]. In this report we will not assume any ordering unless explicitly mentioned.

3 Sequent Calculus

In this section we discuss a sequent calculus proof system for SIL. After presenting the rules making up the system, we consider the structure of these rules from both a pragmatic and "aesthetic" viewpoint.

We assume the reader to be familiar with the basic notions of sequent calculi (cf., e.g., [21, 5]). For our presentation we use sequents

$\Gamma \vdash \Delta$ where Γ, Δ are multisets. A *basic sequent* is a sequent where $\Gamma \cap \Delta \neq \emptyset$.

Our presentation is inspired by [21]. Instead of multisets one can also consider sets [16, app. A] or sequences [6]. The latter will be relevant in Section 5.

3.1 The Sequent Rules

We will consider sequent calculi made up of combinations of the following sets of sequent rules:[1] (**L**) Rules for propositional logic (viz. a left and a right rule for each of the operators $\wedge$, $\vee$, $\rightarrow$ and $\neg$). The rules are of a form such that if they are used in a backwards search they act as a decision procedure for propositional logic. (Cf., e.g., [5, p. 63].) (**P**) Rules for quantified formulas (viz. a left and right rule for each quantifier $\forall$ and $\exists$). (Cf., e.g., [5, p. 188].) If we add extra side conditions concerning rigidity and chop-freeness (as for the Hilbert proof system, cf. the discussion in the previous section) to the usual side conditions for the quantifier rules, we denote the rules **P'**. (**E**) Rules for equality. The form of these rules is inspired by [5, pp. 236–237]; they are slightly modified such as to make the proofs of Section 4 simpler (f and G are arbitrary function/predicate symbols of the logic):

$$\frac{\Gamma, t = t \vdash \Delta}{\Gamma \vdash \Delta} \text{(E1)} \qquad \frac{\Gamma \vdash s_i = t_i, \Delta \quad \Gamma, f(s_1, \ldots, s_n) = f(t_1, \ldots, t_n) \vdash \Delta}{\Gamma \vdash \Delta} \text{(E2)}$$

$$\frac{\Gamma \vdash s_i = t_i, \Delta \quad \Gamma \vdash G(s_1, \ldots, s_n), \Delta \quad \Gamma, G(t_1, \ldots, t_n) \vdash \Delta}{\Gamma \vdash \Delta} \text{(E3)}$$

If the only predicate symbol is $=$ and the only non-nullary function symbols are $+, -$ we denote the equality rules **E'**. (**4**) Rules for modal logic S4. We choose rules with weakening built-in (cf. [21, p. 229]):[2]

[1] All rules we consider in this report will be of the additive type.

[2] $\Box\Gamma \mathrel{\widehat{=}} \{\Box\phi \mid \phi \in \Gamma\}$.

$$\frac{\Gamma, \phi \ \vdash \ \Delta}{\Gamma, \Box\phi \ \vdash \ \Delta} \ (\mathrm{L}\Box) \qquad \frac{\Box\Gamma \ \vdash \ \phi, \Diamond\Delta}{\Gamma', \Box\Gamma \ \vdash \ \Box\phi, \Diamond\Delta, \Delta'} \ (\mathrm{R}\Box)$$

$$\frac{\Box\Gamma, \phi \ \vdash \ \Diamond\Delta}{\Gamma', \Box\Gamma, \Diamond\phi \ \vdash \ \Diamond\Delta, \Delta'} \ (\mathrm{L}\Diamond) \qquad \frac{\Gamma \ \vdash \ \phi, \Delta}{\Gamma \ \vdash \ \Diamond\phi, \Delta} \ (\mathrm{R}\Diamond)$$

If we include the rules below (where ϕ must be rigid) we denote the rules **4'**:

$$\frac{\Gamma, \phi \ \vdash \ \Delta}{\Gamma, \Diamond\phi \ \vdash \ \Delta} \ (\mathrm{LR}) \qquad \frac{\Gamma \ \vdash \ \phi, \Delta}{\Gamma \ \vdash \ \Box\phi, \Delta} \ (\mathrm{RR})$$

(**I**) Rules for chop. In (LL1), (RL1), (LL2) and (RL2), s (and t) must be rigid:

$$\frac{\Gamma, (\ell = s + t) \ \vdash \ \Delta}{\Gamma, (\ell = s)^\frown(\ell = t) \ \vdash \ \Delta} \ (\mathrm{LL2}) \qquad \frac{\Gamma \ \vdash \ (\ell = s + t), \Delta}{\Gamma \ \vdash \ (\ell = s)^\frown(\ell = t), \Delta} \ (\mathrm{RL2})$$

$$\frac{\Gamma, \phi \ \vdash \ \Delta}{\Gamma, \phi^\frown(\ell = 0) \ \vdash \ \Delta} \ (\mathrm{LL3}) \qquad \frac{\Gamma \ \vdash \ \phi, \Delta}{\Gamma \ \vdash \ \phi^\frown(\ell = 0), \Delta} \ (\mathrm{RL3})$$

$$\frac{\Gamma, \phi^\frown\varphi \ \vdash \ \Delta \quad \Gamma, \psi^\frown\varphi \ \vdash \ \Delta}{\Gamma, (\phi \vee \psi)^\frown\varphi \ \vdash \ \Delta} \ (\mathrm{LT1}) \qquad \frac{\Gamma \ \vdash \ \phi^\frown\varphi, \psi^\frown\varphi, \Delta}{\Gamma \ \vdash \ (\phi \vee \psi)^\frown\varphi, \Delta} \ (\mathrm{RT1})$$

$$\frac{\Gamma \ \vdash \ (\ell = s)^\frown\phi, \Delta}{\Gamma, (\ell = s)^\frown\neg\phi \ \vdash \ \Delta} \ (\mathrm{LL1}) \qquad \frac{\Gamma, (\ell = s)^\frown\phi \ \vdash \ \Delta}{\Gamma \ \vdash \ (\ell = s)^\frown\neg\phi, \Delta} \ (\mathrm{RL1})$$

$$\frac{\Box\Gamma, \phi \ \vdash \ \psi, \Diamond\Delta}{\Gamma', \Box\Gamma, \phi^\frown\varphi \ \vdash \ \psi^\frown\varphi, \Diamond\Delta, \Delta'} \ (\mathrm{LRM})$$

(**A**) Rules for associativity of chop:

$$\frac{\Gamma, \phi^\frown(\varphi^\frown\psi) \ \vdash \ \Delta}{\Gamma, (\phi^\frown\varphi)^\frown\psi \ \vdash \ \Delta} \ (\mathrm{LA2}) \qquad \frac{\Gamma \ \vdash \ \phi^\frown(\varphi^\frown\psi), \Delta}{\Gamma \ \vdash \ (\phi^\frown\varphi)^\frown\psi, \Delta} \ (\mathrm{RA2})$$

(**Q**) Rules for quantifiers and chop. With side conditions similar to those of **P'**:

$$\frac{\Gamma, \phi^\frown\psi \ \vdash \ \Delta}{\Gamma, ((\exists x)\phi)^\frown\psi \ \vdash \ \Delta} \ (\mathrm{LBl}) \qquad \frac{\Gamma \ \vdash \ \phi[x/t]^\frown\psi, \Delta}{\Gamma \ \vdash \ ((\exists x)\phi)^\frown\psi\Delta} \ (\mathrm{RBl})$$

(**G**) Four axioms (i.e. rules with no premises) expressing the properties of an Abelian group.

$$\frac{}{\Gamma \ \vdash \ (s+t)+u = s+(t+u), \Delta} \ (\mathrm{SD1}) \qquad \frac{}{\Gamma \ \vdash \ s+0 = s, \Delta} \ (\mathrm{SD2})$$

$$\frac{}{\Gamma \ \vdash \ s+(-s) = 0, \Delta} \ (\mathrm{SD3}) \qquad \frac{}{\Gamma \ \vdash \ s+t = t+s, \Delta} \ (\mathrm{SD4})$$

We have actually left out some rules in I and Q, namely symmetric rules with respect to $\frown$. This is the case for all rules of I and Q except (LL2) and (RL2). In the case of, say, (LL3) we have the following rule as well:

$$\frac{\Gamma, \phi \ \vdash \ \Delta}{\Gamma, (\ell = 0)^\frown \phi \ \vdash \ \Delta} \ (\mathrm{LL3}')$$

Of structural rules, only the standard (additive) cut rule is included. The exchange rules are superfluous when we consider sequents of multisets. The weakening rules are built-in in the other rules (cf. (R$\Box$), (L$\Diamond$) and (LRM)). Finally, the contraction rules are derivable from cut, hence not included explicitly. It is *not* possible to eliminate cut from the system. This is a corollary of the undecidability/decidability result of Section 4 as we shall see.

The sequent calculus induced by the set of rules $R_1, R_2, \ldots, R_n$ will be denoted by $\mathfrak{G}[R_1 R_2 \cdots R_n]$. We can now be precise:

Definition 3.1 *The sequent calculus for SIL is* $\mathfrak{G}[\mathrm{LP}'\mathrm{E4}'\mathrm{IAQG}\{\mathrm{cut}\}]$.

A *proof of a sequent* $\Gamma \ \vdash \ \Delta$ *in a sequent calculus* $\mathfrak{G}[\mathcal{R}]$ is a finite tree of sequents with $\Gamma \ \vdash \ \Delta$ as root. The leaves are either basic sequents or instances of axioms of $\mathcal{R}$. The inner sequents of the tree are connected iff they match an instance of a (non-axiom) sequent rule of $\mathcal{R}$.

The proof that theoremhood in the Hilbert system is equivalent to theoremhood in the sequent calculus system is an extension of similar proofs for FOL (e.g. [21]).

Theorem 3.2

$$\vdash_{\mathrm{SIL}} \phi \quad \textit{iff} \quad \textit{there is a proof of } \{\} \vdash \phi \textit{ in } \mathfrak{G}[\mathrm{LP}'\mathrm{E4}'\mathrm{IAQG}\{\mathrm{cut}\}]$$

3.2 Structure of the Rules

The rules of LP4' are all well-known, thus the sequent calculus for SIL can be seen as an extension of a version of a sequent calculus for first-order modal logic S4 [21]. Notice that all these rules satisfy a subformula property which make them well-suited for backwards proof search.

The rules (LL2), (RL2), (LL3) and (RL4) express how interval lengths are additive and that an interval of length zero is a neutral element with respect to $\frown$. (LL3) and (RL4) satisfy the subformula property, and as the formulas in the premises of (LL2) and (RL2) are atomic they are all suited for backwards proof search. The rules (LT1), (RT1), (LL1), (RL1), (LBl) and (RBl) all have a particular form: They can be seen as introduction rules for $\vee$, $\neg$ and $\exists$ "under the chop". In other words, these rules resemble the corresponding rules for propositional logic but now the affected formulas are chopped formulas. It is possible to derive similar rules for $\wedge$, $\rightarrow$ and $\forall$. Note, that these rules do not satisfy the usual subformula property. But because of the above mentioned particular form it is possible to define a so-called chop-subformula property which gives rise to a decreasing measure in a backwards search. (An example: $\phi \frown \varphi$ is a chop-subformula of $(\phi \vee \psi) \frown \varphi$.) Finally, we have a monotonicity rule for $\frown$ (LRM) (satisfying the usual subformula property) and the associativity rules of A. The latter do not have the chop-subformula property but we can easily define a measure which makes the premise strictly less than the conclusion in these associativity rules as well.

We will not give more formal definitions of the above discussed properties but it should be clear that they imply that if starting with an arbitrary sequent, a backwards proof search using only the rules of L4'IA will always terminate in a finite number of steps.

3.3 Sequent Calculi for Modal Logics

From a more "aesthetic" viewpoint, one can ask what a sequent calculus looks like in general. In [22] some general principles for each connective/modality $\circ$ of a logic is suggested:

- *Separation.* The sequent rules for $\circ$ should not exhibit any connective other than $\circ$.

- *Weakly symmetric.* The rules for $\circ$ should either be left or right introduction rules.

- *Symmetric.* Both left and right introduction rules for $\circ$.

- *Weakly explicit.* The rules for $\circ$ exhibit $\circ$ only in the conclusion sequents.

- *Explicit.* Only one occurrence of $\circ$ in the conclusion.

If we are to relate these principles to SIL, we see that the problem is the chop modality. Both separation and explicitness fail whereas we almost achieve symmetry; only the monotonicity rule breaks the symmetry.

The problem of not satisfying these principles is not that of SIL alone but stems from more fundamental difficulties with giving sequent calculus formulations to modal logics. Indeed, in [2] it is argued that only some very simple modal logics can be given “nice and natural” sequent calculus formulations.

The standard formulation for S4 is that used in e.g. [21]. This is also the formulation we have used in our sequent calculus for SIL, cf. the rules of 4. Other proposals for sequent calculus systems for some of the simple modal logics (K,T,S4,S5) are surveyed in the introduction of [22]. It is interesting to note that none of these systems satisfy all of the above principles and properties.

In [7] cut-free systems for S4.3, S4.3.1, and S4.14 are given. It is still within the standard sequent calculus framework but now the rules themselves get more complicated, such that, e.g., the subformula property does not hold any more. The rules are still *analytic* in the sense that if the conclusion is known then the premise(s) are completely determined.

There have been various proposals for generalized systems based on extended formalisms of the standard sequent calculus formulation. One example of this is [22] which also contains a survey of other proposals in this direction.

4 Decidability Modulo Cut

SIL is an extension of FOL; SIL is thus undecidable because FOL is. In this section we consider Quantifier Free SIL ($\mathrm{SIL}_{\mathrm{QF}}$) with $=$ being the only predicate symbol and $+, -$ being the only non-nullary function symbols. We show that the limit between decidability and undecidability of $\mathrm{SIL}_{\mathrm{QF}}$ is the cut rule.

4.1 Undecidability

First we show that $\mathrm{SIL}_{\mathrm{QF}}$ is undecidable in general, i.e. we show that it is undecidable whether $\vdash_{\mathrm{SIL}} \phi$ for arbitrary ϕ of $\mathrm{SIL}_{\mathrm{QF}}$. For this we need some results concerning logics $\mathcal{L}$ with a binary modality [10].

The syntax of $\mathcal{L}$ is that of propositional logic with the addition of formulas of the form $\alpha \frown \beta$. Furthermore, for $\mathcal{L}$ to be a logic with a binary modality it must contain the following axioms and inference rules: 1) All propositional tautologies, the substitution rule and modus ponens. 2) Axiom saying that $\frown$ distributes over $\vee$. 3) A monotonicity rule for $\frown$. The *minimal* logic with a binary modality is the logic with a binary modality consisting only of these axioms and rules. If $\mathcal{L}$ contains an associativity axiom for $\frown$ it is called *associative.* If it contains a necessitation rule it is called *normal.* We can thus speak of the minimal [associative] [normal] logic with a binary modality.

We give a standard Kripke-style semantics for $\mathcal{L}$ with models based on frames (W, R) where W is a set of possible worlds and R is a ternary accessibility relation on W. Satisfiability and validity is defined the standard way.

Consider the minimal normal logic ($\mathcal{L}_{\mathrm{AF}}$) with a binary modality. It is easy to check that all axioms of $\mathcal{L}_{\mathrm{AF}}$ are valid and that all inference rules of $\mathcal{L}_{\mathrm{AF}}$ preserve validity in the class of all frames. In fact, we have a much stronger result: $\mathcal{L}_{\mathrm{AF}}$ is characterized exactly by the class of all frames.

Given a set U we define a *square frame* (W, R) as follows: $W = U \times U$ and $R = \{((a,c),(c,b),(a,b)) \mid a,b,c \in U\}$. We are interested in validity of a formula α in the class of all square frames, written $\Vdash_{SQ} \alpha$. A logic is called a *square extension* of the minimal logic with a binary modality if it is valid in the class of all square frames. It is easy to check that the associativity axiom is valid in the class of all square frames. We can thus speak of a square extension of the minimal associative logic with a binary modality.

We now consider the logic $\mathcal{L}_{\mathrm{SQ}}$ with a binary modality characterized by the class of all square frames. By this we mean the logic whose theorems are exactly those valid in all square frames. This logic is a square extension of the minimal associative logic by the above definitions.[3]

We now cite a central result of [10].

Theorem 4.1 *Any square extension of the minimal associative logic with a binary modality is undecidable.*

Hence, it is undecidable whether $\Vdash_{SQ} \alpha$

A formula of $\mathcal{L}$ will also be a formula of $\mathrm{SIL}_{\mathrm{QF}}$. This means that we have shown undecidability of $\mathrm{SIL}_{\mathrm{QF}}$ if we can show that it is undecidable whether $\vdash_{\mathrm{SIL}} \alpha$ for arbitrary α of $\mathcal{L}$. But by the completeness theorem for SIL this is equivalent to the decidability question of $\models_{\mathrm{SIL}} \alpha$. We are thus done by the following proposition which is proved by simple structural induction on the definitions of $\models$ and $\Vdash$.

Proposition 4.2 $\models_{\mathrm{SIL}} \alpha$ *iff* $\Vdash_{SQ} \alpha$.

4.2 A Decidable Fragment

We now show that $\mathrm{SIL}_{\mathrm{QF}}$ without cut is decidable. To be more precise, we show that it is decidable whether a sequent is provable in $\mathfrak{G}[\mathrm{LP'E'4'IAQG}]$.

[3] It would be nice if $\mathcal{L}_{\mathrm{SQ}}$ was simply the minimal associative [normal] logic with a binary modality. Unfortunately, $\mathcal{L}_{\mathrm{SQ}}$ is not even finitely axiomatizable [12].

We say that a formula is *atomic* iff it is of the form $s = t$. Clearly, an atomic formula is quantifier-free. An *atomic basic sequent* $\Gamma \vdash \Delta$ is a basic sequent where all formulas of $\Gamma \cap \Delta$ are atomic. A proof in an *atomic sequent calculus* $\overline{\mathfrak{G}}[\mathcal{R}]$ is a proof in $\mathfrak{G}[\mathcal{R}]$ where basic sequents are atomic. Let $\overline{\Gamma} \mathrel{\widehat{=}} \{\phi \in \Gamma \mid \phi \text{ is atomic}\}$. As formulas are quantifier-free, variables can never be instantiated and can thus be regarded as constants. Such formulas with no (instantiable) variables are called *ground*. If a sequent $\Gamma \vdash \Delta$ is an instance of the conclusion of a sequent rule R, we say that R is *applicable* to $\Gamma \vdash \Delta$.

The following lemma states that after using the terminating proof search described in the previous section, what is left, is to use equality reasoning on Abelian groups.

Lemma 4.3 *Given a non-basic sequent of* $\mathrm{SIL}_{\mathrm{QF}}$*, if none of the sequent rules of* L4′IA *are applicable then the following propositions are equivalent*

1. *There is a proof of* $\Gamma \vdash \Delta$ *in* $\mathfrak{G}[\mathrm{LP'E'4'IAQG}]$.
2. *There is a proof of* $\overline{\Gamma} \vdash \overline{\Delta}$ *in* $\overline{\mathfrak{G}}[\mathrm{E'G}]$

Proof Trivially, *2.* implies *1.* For the other direction, notice that as we only consider quantifier-free formulas the sequent rules of P′ and Q will never be applicable. We can therefore restrict attention to provability in $\mathfrak{G}[\mathrm{LE4'IAG}]$. By assumption, none of the sequent rules of L4′IA are applicable. Of the remaining rules, only those of E′ can generate new sequents; but the additional formulas of those will always be atomic, hence the rules of L4′IA will continue being non-applicable. Thus, we only have to consider provability in $\mathfrak{G}[\mathrm{E'G}]$.

Assume $\Gamma \vdash \Delta$ is provable in $\mathfrak{G}[\mathrm{E'G}]$ because $\Gamma \vdash \Delta$ is an instance of an axiom of G. Then clearly $\overline{\Gamma} \vdash \overline{\Delta}$ will be an instance of the same axiom of G and we have a proof in $\overline{\mathfrak{G}}[\mathrm{E'G}]$. The only possibility left is that $\Gamma \vdash \Delta$ is provable in $\mathfrak{G}[\mathrm{E'G}]$ because one of the rules of E′ is applied to $\Gamma \vdash \Delta$. In this case there are three possibilities for each of the new sequents $\Gamma' \vdash \Delta'$: 1) $\Gamma' \vdash \Delta'$ is an instance of an axiom of G. Then we are done as above. 2) $\Gamma' \vdash \Delta'$ is a basic sequent. As

$\Gamma \ \vdash \ \Delta$ was not a basic sequent $\Gamma' \ \vdash \ \Delta'$ must be an atomic basic sequent (because of the structure of the rules of E$'$). Thus, we have a proof of $\overline{\Gamma'} \ \vdash \ \overline{\Delta'}$ in $\overline{\mathfrak{G}}$[E$'$G]. 3) $\Gamma' \ \vdash \ \Delta'$ is provable in $\mathfrak{G}$[E$'$G] because one of the rules of E$'$ is applied to $\Gamma \ \vdash \ \Delta$. Then we are done by induction. □

An *equational system* E is a set of *equations* $s = t$ where s, t are terms build from function symbols and variables. A *structure* M consists of a domain D and a function assigning a meaning (in D) to each function symbol and variable. The meaning of terms is defined the usual way. We say that M *satisfies* the equation $s = t$ iff s and t are given the same meaning by M. We write $E \ \models_{\text{equ}} \ s = t$ if all structures that satisfy all equations in E also satisfy $s = t$. Now, the relation $E \ \vdash_{\text{equ}} \ s = t$ is defined as the least relation satisfying $E \ \vdash_{\text{equ}} \ s = t$ if $(s = t) \in E$ and $E \ \vdash_{\text{equ}} \ t = t$, and closed under symmetry, transitivity, substitution and congruence. The following classic result relate $\models_{\text{equ}}$ and $\vdash_{\text{equ}}$.

Theorem 4.4 (Birkhoff) $E \ \models_{\text{equ}} \ s = t$ *iff* $E \ \vdash_{\text{equ}} \ s = t$.

Proposition 4.5 *Let $\overline{\Gamma}$ and $\overline{\Delta}$ be multisets of atomic ground formulas. Then the following two propositions are equivalent:*

1. $\overline{\Gamma} \ \vdash \ \overline{\Delta}$ *is provable in* $\overline{\mathfrak{G}}$[E$'$G]

2. $\overline{\Gamma} \cup \mathsf{Grp} \ \models_{\text{equ}} \ s = t$ *for some* $s = t \in \overline{\Delta}$

where $\mathsf{Grp} \mathrel{\widehat{=}} \{(x+y)+z = x+(y+z),\ x+0 = x,\ x+(-x) = 0,\ x+y = y+x\}$.

Proof Theorem 4.4 is used implicitly several times in the proof. Let $E \mathrel{\widehat{=}} \overline{\Gamma} \cup \mathsf{Grp}$. To show that *2.* implies *1.* we assume that $E \ \models_{\text{equ}} \ s = t$ for some $s = t \in \overline{\Delta}$ and proceed by structural induction over the proof of $E \ \vdash_{\text{equ}} \ s = t$. For the other direction we proceed by induction over the proof of $\overline{\Gamma} \ \vdash \ \overline{\Delta}$ in $\overline{\mathfrak{G}}$[E$'$G]. □

In the case of $\overline{\Delta}$ being singleton, *2.* above is a formulation of the decision problem known as *the word problem for finitely presented Abelian groups.* But this problem is known to be decidable [8].

Theorem 4.6 *Let* $\Gamma \ \vdash \ \Delta$ *be a sequent of* $\mathrm{SIL}_{\mathrm{QF}}$*. It is decidable whether there is a proof of* $\Gamma \ \vdash \ \Delta$ *in* $\mathfrak{G}[\mathrm{LP'E'4'IAQG}]$.

Proof Perform a non-deterministic backwards proof search using only the rules of L4'IA. By the results of Section 3 this search will terminate in a finite number of steps. Now apply Lemma 4.3 and Proposition 4.5 and the theorem follows. □

As provability is undecidable in $\mathfrak{G}[\mathrm{LP'E'4'IAQG}\{\mathrm{cut}\}]$ we thus have:

Corollary 4.7 *It is not possible to eliminate cut from the sequent calculus for SIL,* $\mathfrak{G}[\mathrm{LP'E'4'IAQG}\{\mathrm{cut}\}]$.

The results of this section tell us that any (quantifier-free) theorem can be proved by splitting it in a number of lemmas (using cut) and then solve these lemmas automatically by the decision procedure sketched in the proofs above.

5 Mechanization

In this section we give an overview of our mechanization in Isabelle of our sequent calculus for SIL. We will not go into details but instead sketch some of the overall decisions we have made.

Isabelle is a generic proof assistant [14]. Various object logics have been (and can be) formalized by extending Isabelle's meta-logic, which is intuitionistic higher order logic. One of these object logics is first order sequent calculus LK. We can almost build on LK as it is, but we have to make some adjustments to accommodate the rigidity and chop-freeness side conditions (cf. the discussion in Section 2). Formally, we have to embed these side conditions within the logic itself by defining a set of appropriate rules. How this can be done is discussed in [19].

Because of the simple structure of these rules, the side conditions can be handled (almost) fully automatic.

5.1 Encoding SIL

The encoding of the SIL extension as such is fairly straightforward. We base the modal logic part of SIL on the principles of the (undocumented) modal object logics distributed with Isabelle. In particular, this means that we handle the special side conditions of the rules (R$\Box$), (L$\Diamond$) and (LRM) by means of a certain set of Horn clauses as for the object logic S4.

5.2 Simplification on Abelian Groups

The basic structure of terms is that of an Abelian group. We would like the simplifier to automate most of the reasoning with these terms. The simplifier of Isabelle is based on the theory of Ordered Rewriting [11]. A complete set of reductions for Abelian groups exists within this theory [11]; we hence prove and add these to the simplifier. The standard lexicographic ordering on terms used in Isabelle does not work in this case though, and we thus have to redefine the term ordering. We keep Isabelle's strict ordering for nullary terms $a_1 < a_2 < \dots$ and extend it to $+ < - < a_1 < a_2 < \dots$. We define the order on terms as the lexicographic path ordering [1] induced by this order and the simplifier can now reduce any term to its unique normal form.

5.3 The SIL Reasoner

Isabelle provides a classical reasoner for LK consisting of tactics performing e.g. depth-first search using the rules of LK. We rewrite this reasoner for SIL as it has to accommodate the side conditions concerning rigidity, chop-freeness and those of the modal logic part in a transparent way. The use of the SIL reasoner is in the spirit of [15]: When new notions (say, $\Box$) are introduced, corresponding rules are added to the reasoner. Reasoning is thus done on a higher level as definitions are *not* expanded. When other (suitable) rules are later derived they are added to the reasoner as soon as possible to keep the search space small. This in particular means that all (derived) rules satisfying the chop-subformula property (this ensures termination) are added to the reasoner, e.g. the derived rules for $\wedge$ mentioned in Section 3.

5.4 Experience

We have proved several lemmas and theorems, and derived many useful rules of SIL, utilizing the automated proof support developed in Isabelle. The result of the previous section is reflected fairly well: The proofs are essentially all split in smaller or bigger parts all of which can then be solved automatically by the simplifier and/or the (rewritten) classical reasoner. These parts are often non-trivial with respect to doing the proof by hand.

6 Conclusion

Our main goal of this work was to improve proof support for interval logics. We developed a sequent calculus which, despite not being completely satisfactory, turned out to be useful for actual conducting proofs, not least because of the decidability result of Section 4.

The emphasis of this report has been on SIL. Due to the similarity (in many respects) of ITL and SIL, most of the results are (in slightly modified form) applicable to ITL and, hence, DC as well.

Acknowledgments

A large part of the work with Isabelle was carried out while I was visiting Larry Paulson at the Computer Laboratory, University of Cambridge. I would like to thank Larry Paulson for always finding the time to discuss Isabelle and related issues. Also thanks to Michael R. Hansen for valuable comments and suggestions to my work on SIL in general and for proofreading a draft of this report.

References

[1] Franz Baader and Tobias Nipkow. *Term Rewriting and All That.* Cambridge University Press, 1998.

[2] R.A. Bull and K. Segerberg. Basic Modal Logic. In D.M. Gabbay and F. Guenthner, editors, *Handbook of Philosophical Logic*, volume II, pages 1–88. Reidel, 1984.

[3] Bruno Dutertre. Complete Proof Systems for First Order Interval Temporal Logic. In *Logic in Computer Science, LICS'95*, pages 36–43. IEEE Computer Society Press, 1995.

[4] Marcin Engel and Hans Rischel. Dagstuhl-Seminar Specification Problem - a Duration Calculus Solution. Unpublished Manuscript, Dept. of Computer Science, Technical University of Denmark, September 1994.

[5] Jean H. Gallier. *Logic for Computer Science: Foundations of Automatic Theorem Proving.* Harper & Row, 1986.

[6] G. Gentzen. Untersuchungen über das logische Schliessen. *Mathematische Zeitschrift*, 39:176–210,405–431, 1935.

[7] Rajeev P. Goré. *Cut-free Sequent and Tableau Systems for Propositional Normal Modal Logics.* PhD thesis, Computer Laboratory, University of Cambridge, May 1992. Technical Report 257.

[8] A.G. Hamilton. *Logic for Mathematicians.* Cambridge University Press, Revised edition, 1988.

[9] Søren T. Heilmann. *Proof Support for Duration Calculus.* PhD thesis, Dept. of Information Technology, Technical University of Denmark, January 1999.

[10] Á. Kurucz, I. Németi, I. Sain, and A. Simon. Decidable and Undecidable Logics with a Binary Modality. *Journal of Logic, Language and Information*, 4:191–206, 1995.

[11] U. Martin and T. Nipkow. Ordered Rewriting and Confluence. In *Automated Deduction, CADE-10*, volume 449 of *Lecture Notes in Artificial Intelligence*, pages 366–380. Springer-Verlag, 1990.

[12] Maarten Marx and Yde Venema. *Multi-Dimensional Modal Logic*, volume 4 of *Applied Logic Series.* Kluwer Academic Publishers, 1997.

[13] B. Moszkowski. A Temporal Logic for Multilevel Reasoning about Hardware. *IEEE Computer*, 18(2):10–19, 1985.

[14] Lawrence C. Paulson. *Isabelle, A Generic Theorem Prover*, volume 828 of *Lecture Notes in Computer Science.* Springer-Verlag, 1994.

[15] Lawrence C. Paulson. Generic Automatic Proof Tools. In Robert Veroff, editor, *Automated Reasoning and Its Applications: Essays in Honour of Larry Wos*, pages 23–47. MIT Press, 1997.

[16] Dag Prawitz. *Natural Deduction. A Proof-Theoretical Study.* Almquist & Wiksell, 1965.

[17] Thomas M. Rasmussen. Signed Interval Logic. In J. Flum and M. Rodriguez-Artalejo, editors, *Computer Science Logic, CSL'99*, volume 1683 of *Lecture Notes in Computer Science*, pages 157–171. Springer-Verlag, 1999.

[18] Thomas M. Rasmussen. Signed Interval Logic on Totally Ordered Domains. Unpublished note, Dept. of Information Technology, Technical University of Denmark, June 1999.

[19] Thomas M. Rasmussen. Labelled Natural Deduction for Interval Logics. In *Computer Science Logic, CSL'01*, Lecture Notes in Computer Science. Springer-Verlag, 2001. To appear.

[20] Jens Ulrik Skakkebæk. *A Verification Assistant for a Real-Time Logic.* PhD thesis, Dept. of Computer Science, Technical University of Denmark, November 1994.

[21] A.S. Troelstra and H. Schwichtenberg. *Basic Proof Theory.* Cambridge Tracts in Theoretical Computer Science 43. Cambridge University Press, 1996.

[22] Heinrich Wansing. Sequent Calculi for Normal Modal Propositional Logics. *Journal of Logic and Computation*, 4(2):125–142, 1994.

[23] Zhou Chaochen and Michael R. Hansen. An Adequate First Order Interval Logic. In *COMPOS'97*, volume 1536 of *Lecture Notes in Computer Science*, pages 584–608. Springer-Verlag, 1998.

[24] Zhou Chaochen, C.A.R. Hoare, and Anders P. Ravn. A Calculus of Durations. *Information Processing Letters*, 40(5):269–276, 1991.