Transitive Primal Infon Logic: the Propositional Case

Carlos Cotrini Yuri Gurevich

Technical Report
MSR-TR-2012-15, February 2012

Microsoft Research
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Transitive primal infon logic

Carlos Cotrini Yuri Gurevich

Abstract

Primal (propositional) logic **PL** is the $\{\wedge, \to\}$ fragment of intuitionistic logic, and primal (propositional) infon logic **PIL** is a conservative extension of **PL** with the quotation construct $p\,\texttt{said}$. Logic **PIL** was introduced by Gurevich and Neeman in 2009 in connection with the DKAL project. The derivation problem for **PIL** (and therefore for **PL**) is solvable in linear time, and yet **PIL** allows one to express many common access control scenarios. The most obvious limitations on the expressivity of logics **PL** and **PIL** are the failures of the transitivity rules

$$(\text{trans}_0)\ \frac{x \to y \qquad y \to z}{x \to z} \qquad (\text{trans})\ \frac{\texttt{pref}\ x \to y \qquad \texttt{pref}\ y \to z}{\texttt{pref}\ x \to z}$$

respectively where `pref` ranges over quotation prefixes p `said` q `said` $\ldots$. Here we investigate the extension **T** of **PL** with an axiom $x \to x$ and the inference rule (trans_0) as well as the extension **qT** of **PIL** with an axiom `pref` $x \to x$ and the inference rule (trans).

- [Subformula property] **T** has the subformula property: if $\Gamma \vdash y$ then there is a derivation of y from Γ comprising only subformulas of $\Gamma \cup \{y\}$. **qT** has a similar locality property.
- [Complexity] The derivation problems for **T** and **qT** are solvable in quadratic time.
- [Soundness and completeness] We define Kripke models for **qT** (resp. **T**) and show that the semantics is sound and complete.
- [Small models] **T** has the one-element-model property: if $\Gamma \nvdash y$ then there is a one-element counterexample. Similarly small (though not one-element) counterexamples exist for **qT**.

1 Introduction

With the advent of cloud computing, the need arises to manage policies automatically. In a brick-and-mortar setting, clerks learn unwritten policies from their peers; and if they don't know a particular policy, they know whom to ask. In the cloud, the are no clerks. The policies have to be handled automatically. The most challenging aspect is how to handle the interaction of the policies of different institutions, especially in federated scenarios where there is no central authority. Distributed Knowledge Authorization Language (DKAL) was created to deal with such problems [12, 5]. The DKAL project led to the introduction of *infon logic* [10]; here infons are pieces of information.

Propositional infon logic is a conservative extension of the $\{\wedge, \rightarrow\}$ fragment of propositional intuitionistic logic with the quotation construct p `said`. (Actually there were two quotation constructs, p `said` and p `implied` in [10] but the latter construct was later removed [11].) Unfortunately the derivability problem for infon logic is PSPACE-complete. Since an efficient algorithm for this problem is necessary for practical purposes, a fragment of this logic, called primal infon logic **PIL** was proposed. This fragment is decidable in linear time when a bound in the quotation depth is provided. This entailed a remarkable result: the reduct of **PIL** to propositional intuitionistic logic, named primal intuitionistic logic **PL**, is also decidable in linear time. **PL** is still quite expressive, although the cost for such an efficient fragment was high (The deduction theorem, among other properties of intuitionistic logic, were sacrificed). But this traced a new path for research: how to increase the expressive power of **PL** without considerably affecting its computational efficiency?

Yury Savateev [21] devised an extension $\mathbf{PL}^+$ of **PL** by adding the following rules:

$$\text{(trans)}\ \frac{x \to y \qquad y \to z}{x \to z} \qquad \text{(str)}\ \frac{(x \to y) \to z}{y \to z}$$

Savateev pointed out the existence of a polynomial-time algorithm for deciding $\mathbf{PL}^+$. The most obvious is a natural extension of the algorithm for **PL** [10]. This yields an algorithm of time $O(n^3)$. Somewhat surprisingly, if we strengthen **PL** by extending its Hilbert calculus with rules

$$\text{(trans*)}\ \frac{x_1 \to x_2 \qquad x_2 \to x_3 \quad \ldots \qquad x_{k-1} \to x_k}{x_1 \to x_k}$$

we obtain a logic which has the subformula property and is decidable in time $O(n^2)$. We called this new logic *transitive primal logic* **T**. Of course, we did not forget about primal infon logic and asked ourselves if these observations could be extended to **PIL**. This was easily done, giving rise to a logic we called *transitive primal infon logic* **qT**.

In the next two sections, we give some preliminaries and a formal definition of **qT**. Section 4 shows first that **PIL** with rules (trans*) has the subformula property, which is the cornerstone for the correctness of the algorithm that decides **qT**; next, the algorithm is presented. Section 5 explores two possibilities for the semantics of **qT**. Finally, section 6 presents **T**, which is the reduct of **qT** to its intuitionistic fragment and presents all the properties that it inherits from **qT**.

2 Preliminaries

Symbols $v_0, v_1, \ldots$ are *infon variables*. We presume an infinite list of *principal constants*. There is also an infon constant $\top$ which represents an infon (a piece of information) known to all principals. Infon formulas are built, as usual, from infon variables and an $\top$ by means of conjunction, implication and unary constructs q `said` φ where q ranges over principal constants.

For $q_1, q_2, \ldots, q_k$ principal constants, we call the string

$$q_1 \ \texttt{said}\ q_2 \ \texttt{said}\ \ldots q_k \ \texttt{said}$$

a *quotation prefix.* We regard the empty string ϵ as a quotation prefix as well.

The multiple derivability problem $MD(\mathsf{L})$ for a logic L, is the problem of deciding which formulas from a given set Δ are provable from another given set Γ.

3 Transitive primal infon logic

We present a Hilbert calculus for infon formulas. Here `pref` ranges over quotation prefixes, whereas $x, x_1, x_2, \ldots, x_n$ and y, over infon formulas.

Hilbert calculus $\mathcal{H}^{\mathsf{T}}$

Axioms

$$(\top) \quad \texttt{pref}\ \top \qquad\qquad (\text{x2x}) \quad \texttt{pref}\ (x \to x)$$

Inference rules

$$(\wedge\text{i}) \quad \frac{\texttt{pref}\ x \qquad \texttt{pref}\ y}{\texttt{pref}\ (x \wedge y)} \qquad (\wedge\text{e}) \quad \frac{\texttt{pref}\ (x \wedge y)}{\texttt{pref}\ x} \qquad \frac{\texttt{pref}\ (x \wedge y)}{\texttt{pref}\ y}$$

$$(\to\text{i}) \quad \frac{\texttt{pref}\ y}{\texttt{pref}\ (x \to y)} \qquad (\to\text{e}) \quad \frac{\texttt{pref}\ x \qquad \texttt{pref}\ (x \to y)}{\texttt{pref}\ y}$$

$$(\text{trans}) \ \frac{\texttt{pref}\ (x \to y) \qquad \texttt{pref}\ (y \to z)}{\texttt{pref}\ (x \to z)}$$

For any rule, the formulas over the line are *premises* and the formula under the line is the *conclusion.*

We call *transitive primal infon logic* the logic qT obtained from the set of infon formulas and the Hilbert calculus $\mathcal{H}^{\mathsf{T}}$.

For a set of formulas Γ, a *proof* of y from Γ in qT is a finite rooted tree such that each node u is labeled with a formula $F(u)$. The root node is labeled with y. Each leaf node is labeled with either an axiom of $\mathcal{H}^*$ or a formula in Γ. If node u has as children nodes $v_1, v_2, \ldots, v_n$, then $\dfrac{F(v_1) \qquad F(v_2) \quad \ldots \qquad F(v_n)}{F(u)}$ is an instance of an inference rule in $\mathcal{H}^{\mathsf{T}}$. The *size* of the proof is the size of this tree. Also, we will write $u : z$ in order to indicate that formula z is the label of node u. Finally, we say formula y is *provable* from Γ in **qT** if there is a proof of y from Γ in **qT**.

For the sake of readability, we will use the terms *leaf* and *hypothesis* interchangeably. We will also say, in the context of a proof $\mathcal{P}$, that node u is the *conclusion* of an instance of L if $F(u)$ is the conclusion of an instance of L in $\mathcal{P}$.

Definition 1. We define $\mathbf{qT}_0$ as the fragment of **qT** obtained by removing all the formulas which have occurrences of $\top$ or $x \to x$ for any formula x and removing all the axioms in $\mathcal{H}^{\top}$. We will refer to the formulas of this fragment as $\mathbf{qT}_0$-formulas. △

Lemma 1. For any formula z there is an equivalent formula z' that is either $\top$ or a $\mathbf{qT}_0$-formula. Further, such z' can be computed in linear time.

Proof. By induction on the complexity of z.

- If z is a variable or constant $\top$, then $z' = z$.
- If $z = z_1 \wedge z_2$, we have to consider the following subcases:
  - If $z_1' = \top$ and $z_2' = \top$, then $z' = \top$.
  - If $z_1' = \top$ and $z_2' \neq \top$, then $z' = z_2'$.
  - If $z_1' \neq \top$ and $z_2' = \top$, then $z' = z_1'$.
  - If $z_1' \neq \top$ and $z_2' \neq \top$, then $z' = z_1' \wedge z_2'$.
- If $z = z_1 \to z_2$, again, there are several subcases:
  - If $z_1 = z_2$, then $z' = \top$.
  - If $z_2' = \top$, then $z' = \top$.
  - If $z_1' = \top$ and $z_2' \neq \top$, then $z' = z_2$.
  - If $z_1' \neq \top$ and $z_2' \neq \top$, then $z' = z_1' \to z_2'$.
- If $z = \texttt{pref}\ x$, and $x' = \top$, then $z' = \top$; otherwise, $z' = \texttt{pref}\ x'$.

By induction, it can be checked that z' and z are equivalent in **qT** and that z' is computable in linear time. □

Theorem 2. A formula x is provable from Γ in **qT** iff either $x' = \top$ or x' is provable from $\Gamma' \setminus \{\top\}$ in $\mathbf{qT}_0$.

Proof. (⇒) By induction on the proof of x from Γ in **qT**. If x is an axiom, then $x' = \top$ and we are done. If x is a hypothesis, then $x \in \Gamma$; which implies $x' \in \Gamma'$. Again, if $x' = \top$, we are done; otherwise, $x' \in \Gamma' \setminus \{\top\}$. Now, suppose that x is the conclusion of an instance of some inference rule L. All cases for L are similar. We present only two of them:

- Case $L = (\wedge\mathrm{i})$. In this case, $x = \texttt{pref}\ (x_1 \wedge x_2)$. By induction hypothesis, for $i = 1, 2$, either $(\texttt{pref}\ x_i)' = \top$ or $(\texttt{pref}\ x_i)'$ is provable from $\Gamma' \setminus \top$ for each i. If both x_i' are $\top$ then $x' = \top$. If $x_1' = \top$ but $x_2' \neq \top$, then $x' = \texttt{pref}\ x_2'$, which is provable from $\Gamma' \setminus \{\top\}$. When $x_2' = \top$ but $x_1' \neq \top$ the situation is similar. Finally, if both $(\texttt{pref}\ x_i)'$ are provable from $\Gamma' \setminus \{\top\}$, then $x' = \texttt{pref}\ (x_1' \wedge x_2')$ and by rule $(\wedge\mathrm{i})$, x' is provable from Γ'.

- Case $L = (\to\mathrm{e})$. In this case, suppose that $x = \texttt{pref}\ x_2$ and that the premises for L are $\texttt{pref}\ x_1$ and $\texttt{pref}\ (x_1 \to x_2)$. If $x_1 = x_2$, then $\texttt{pref}\ x_1 = \texttt{pref}\ x_2$; but since $\texttt{pref}\ x_1$ is a premise, the induction hypothesis yields the result for $\texttt{pref}\ x_2$. Suppose, then, that $x_1 \neq x_2$. If $x_2' = \top$, then $(\texttt{pref}\ x_2)' = \top$, and we are done. Otherwise, if $x_2' \neq \top$ but $x_1 = \top$, then, by induction hypothesis, $(\texttt{pref}\ (x_1 \to x_2))' = \texttt{pref}\ x_2'$ is provable from $\Gamma' \setminus \{\top\}$; but $\texttt{pref}\ x_2' = x'$, so x' is provable from $\Gamma' \setminus \{\top\}$. Finally, if both x_1' and x_2' are different from $\top$, then, by induction hypothesis, both $(\texttt{pref}\ x_1)'$ and $(\texttt{pref}\ (x_1 \to x_2))'$ are provable from $\Gamma' \setminus \{\top\}$; but $(\texttt{pref}\ (x_1 \to x_2))'$ in this case is equal to $\texttt{pref}\ (x_1' \to x_2')$. It is clear from here, by an application of rule $(\to\mathrm{e})$, that $\texttt{pref}\ x_2'$ is provable from Γ'.

$(\Leftarrow)$ First, Γ and x are equivalent to Γ' and x' respectively; second, the proof of x' from Γ' in $\mathbf{qT}_0$ is also a proof in $\mathbf{qT}$. From these two observations we conclude that x is provable from Γ in $\mathbf{qT}$. □

Corollary 3. There is a linear time reduction from $MD\,(\mathbf{T})$ to $MD\,(\mathbf{T}_0)$.

Proof. Consider the problem of deciding which formulas in Δ follow from Γ in $\mathbf{qT}$. Compute the $\mathbf{qT}_0$ equivalents Γ' and Δ' of Γ and Δ respectively. By theorem 2, for each $\delta \in \Delta$, either $\delta' = \top$, or δ' is provable from $\Gamma' \setminus \{\top\}$ iff δ is provable from Γ. Therefore, mark as provable those $\delta \in \Delta$ such that $\delta' = \top$. The problem is now to decide which $\mathbf{qT}_0$-formulas in $\Delta' \setminus \{\top\}$ follow from $\Gamma' \setminus \{\top\}$ in $\mathbf{qT}_0$. □

4 A quadratic-time algorithm for transitive primal infon logic

4.1 An auxiliary Hilbert calculus for qT

Definition 2. (Local formulas) Let z be a $\mathbf{qT}_0$-formula. The $\mathbf{qT}_0$-formulas *local* to z are defined by induction:

- z is a $\mathbf{qT}_0$-formula local to z.

- If $\texttt{pref}\ (x \wedge y)$ is local to z, then $\texttt{pref}\ x$ and $\texttt{pref}\ y$ are local to z.

- If $\texttt{pref}\ (x \to y)$ is local to z, then $\texttt{pref}\ x$ and $\texttt{pref}\ y$ are local to z.

Formula x is local to a set of $\textbf{\textsf{qT}}_0$-formulas Γ if it is local to a formula in Γ. $\triangle$

If we remove rule (trans) from $\mathcal{H}^{\mathsf{T}}$, we obtain the Hilbert calculus of primal infon logic. This calculus has the locality property: Any formula in Δ that is provable from Γ can be derived using only formulas local to $\Gamma \cup \Delta$. Building on this property, Gurevich and Neeman presented an algorithm for $MD(\textbf{\textsf{PIL}})$ (i.e. the multi-derivability problem for primal infon logic) which works in linear time [10]. We will extend their algorihtm so it decides $MD(\textbf{\textsf{qT}})$ in quadratic time. The first obstacle we face is that $\mathcal{H}^{\mathsf{T}}$ does not have the locality property. For example, any proof of $x \to w$ from $\{x \to y, y \to z, z \to w\}$ requires either $x \to z$ or $y \to w$. This difficulty is removed by using the following alternative but equivalent Hilbert calculus.

Hilbert calculus $\mathcal{H}^*$

Axioms

$$(\top) \qquad \texttt{pref}\ \top$$

Inference rules

$$(\wedge\text{i}) \quad \frac{\texttt{pref}\ x \qquad \texttt{pref}\ y}{\texttt{pref}\ (x \wedge y)} \qquad (\wedge\text{e}) \quad \frac{\texttt{pref}\ (x \wedge y)}{\texttt{pref}\ x} \qquad \frac{\texttt{pref}\ (x \wedge y)}{\texttt{pref}\ y}$$

$$(\to\text{i}) \quad \frac{\texttt{pref}\ y}{\texttt{pref}\ (x \to y)} \qquad (\to\text{e}) \quad \frac{\texttt{pref}\ x \qquad \texttt{pref}\ (x \to y)}{\texttt{pref}\ y}$$

$$(\text{trans*}) \quad \frac{\texttt{pref}\,(x_1 \to x_2) \qquad \texttt{pref}\,(x_2 \to x_3) \quad \dots \qquad \texttt{pref}\,(x_{k-1} \to x_k)}{\texttt{pref}\,(x_1 \to x_k)}$$

Of course, $\mathcal{H}^*$ and $\mathcal{H}^{\mathsf{T}}$ are equivalent. On one hand, axiom (x2x) and rule (trans) are obtained from (trans*) when $k = 1$ and $k = 3$ respectively. On the other hand, (trans*) is obtained by repeated application of rule (trans).

The objective of this subsection is to prove that $\mathcal{H}^*$ does have the desired locality property: if a formula y is provable from Γ, then y can be derived from Γ using only formulas local to $\Gamma \cup \{y\}$. We start with some auxiliary definitions and lemmas:

Definition 3. (Normal and minimal normal proof) A proof $\mathcal{P}$ in $\textbf{\textsf{qT}}_0$ is *normal* if none of the following subtrees appear in $\mathcal{P}$:

$$(\to\mathrm{e})\ \dfrac{\dfrac{\vdots}{\texttt{pref}\ x_1} \qquad (\text{trans*})\ \dfrac{\dfrac{\vdots}{\texttt{pref}\ (x_1 \to x_2)} \quad \dfrac{\vdots}{\texttt{pref}\ (x_2 \to x_3)\ \ \dots} \quad \dfrac{\vdots}{\texttt{pref}\ (x_{k-1} \to x_k)}}{\texttt{pref}\ (x_1 \to x_k)}}{\texttt{pref}\ x_k}$$

$$(\text{trans*})\ \dfrac{\dfrac{\vdots}{\texttt{pref}\ (x_1 \to x_2)\ \ \dots} \qquad (\to\mathrm{i})\ \dfrac{\dfrac{\vdots}{\texttt{pref}\ x_i}}{\texttt{pref}\ (x_{i-1} \to x_i)} \qquad \dfrac{\vdots}{\dots\ \ \texttt{pref}\ (x_{k-1} \to x_k)}}{\texttt{pref}\ (x_1 \to x_k)}$$

△

$\mathcal{P}$ is *minimal normal* if, in addition, there is no normal proof with smaller size than the size of $\mathcal{P}$.

Lemma 4. Any proof in $\mathbf{qT}_0$ can be converted to a normal proof.

Proof. It suffices to realize that the subtrees above can be rewritten in the following way:

$$(\to\mathrm{e})\ \dfrac{(\to\mathrm{e})\ \dfrac{\dfrac{\vdots}{\texttt{pref}\ x_1} \quad \dfrac{\vdots}{\texttt{pref}\ (x_1 \to x_2)}}{\texttt{pref}\ x_2} \qquad \dfrac{\vdots}{\texttt{pref}\ (x_2 \to x_3)}}{\dfrac{\texttt{pref}\ x_3}{}}$$

$$(\to\mathrm{e})\ \dfrac{(\to\mathrm{e})\ \dfrac{\vdots \qquad\qquad \vdots}{\texttt{pref}\ x_{k-1}} \qquad \dfrac{\vdots}{\texttt{pref}\ (x_{k-1} \to x_k)}}{\texttt{pref}\ x_k}$$

$$(\to\mathrm{e})\ \dfrac{\dfrac{\vdots}{\texttt{pref}\ x_i} \quad \dfrac{\vdots}{\texttt{pref}\ (x_i \to x_{i+1})}}{\dfrac{\texttt{pref}\ x_{i+1}}{}}$$

$$(\to\mathrm{i})\ \dfrac{(\to\mathrm{e})\ \dfrac{(\to\mathrm{e})\ \dfrac{\vdots \qquad\qquad \vdots}{\texttt{pref}\ x_{k-1}} \qquad \dfrac{\vdots}{\texttt{pref}\ (x_{k-1} \to x_k)}}{\texttt{pref}\ x_k}}{\texttt{pref}\ (x_1 \to x_k)}$$

□

Definition 4. (Relevant components) Let z be a $\mathbf{qT}_0$-formula. The *relevant components* of z are defined by induction:

- z is a relevant component of z.
- If $\texttt{pref}\ (x \wedge y)$ is a relevant component of z, then $\texttt{pref}\ x$ and $\texttt{pref}\ y$ are relevant components of z.

- If pref $(x \to y)$ is a relevant component of z, then pref y is a relevant components of z.

$\triangle$

Lemma 5. Let $\mathcal{P}$ be a minimal normal proof in $\mathbf{qT}_0$, whose hypothesis are in Γ. If a node u is the conclusion of an instance of L, and $F(u)$ is a relevant component of some premise there, then $F(u)$ is local to Γ.

Proof. We prove this equivalent version of the lemma. For any node u in $\mathcal{P}$, either

- $F(u)$ is local to Γ or
- u is the conclusion of an instance of an inference rule L, in which $F(u)$ is not a relevant component of any premise of that instance.

Let $j_0, j_1, \ldots, j_n$ be a maximal sequence of nodes satisfying the following conditions:

1. $j_0 = u$.
2. For $i < n$, j_{i+1} is a child of j_i.
3. For $i \leq n$, x is a relevant component of $F(j_i)$.

If j_n is a hypothesis, then, by requirement (3), $F(u)$ is local to $F(j_n)$ and we are done. Now, let us suppose that j_n is the conclusion of an inference rule L. By the maximality of the sequence, L cannot be ($\wedge$e) nor ($\to$e). If $L = (\wedge\text{i})$, then the part of $\mathcal{P}$ where L occurs must have the following form:

$$L\,\dfrac{\dfrac{\vdots}{\texttt{pref}\ y} \qquad \dfrac{\vdots}{\texttt{pref}\ z}}{\dfrac{j_n : \texttt{pref}\ (y \wedge z)}{\vdots}}$$

Note that $F(u)$ must be pref $(y \wedge z)$; otherwise, by requirement (3), $F(u)$ must be a relevant component of pref y or pref z and that would allow to extend the sequence to one of the premises, which would contradict the maximality of the sequence. Note also that, since $\mathcal{P}$ is a minimal normal proof, n must be 0; otherwise, we could shorten $\mathcal{P}$ as follows:

$$L\,\dfrac{\dfrac{\vdots}{\texttt{pref}\ y} \qquad \dfrac{\vdots}{\texttt{pref}\ z}}{\dfrac{j_n : \texttt{pref}\ (y \wedge z)}{\dfrac{\vdots}{\dfrac{j_0 : \texttt{pref}\ (y \wedge z)}{\vdots}}}} \quad \Rightarrow \quad L\,\dfrac{\dfrac{\vdots}{\texttt{pref}\ y} \qquad \dfrac{\vdots}{\texttt{pref}\ z}}{\dfrac{j_0 : \texttt{pref}\ (y \wedge z)}{\vdots}}$$

Thus, either $F(u)$ is local to $\Gamma \cup \{y\}$, or $F(u)$ is the conclusion of $(\wedge\mathrm{i})$ and $F(u)$ is not local to any premise of that instance. The other cases for L are similar. □

Theorem 6. Let $\mathcal{P}$ be a minimal normal proof of y from Γ in $\mathbf{qT}_0$, then every $\mathbf{qT}_0$-formula in $\mathcal{P}$ is local to $\Gamma \cup \{y\}$.

Proof. For each node u in $\mathcal{P}$, we will prove that $F(u)$ is local to $\Gamma \cup \{y\}$. For the root, this is clear. Now, suppose that for u' we have that $F(u')$ is local and let u be a child of u'. There are several cases for L, the inference rule used to obtain $F(u')$. If L is either $(\wedge\mathrm{i})$ or $(\rightarrow\mathrm{i})$, then $F(u)$ is local as well, because $F(u)$ is local to $F(u')$. The other cases, $(\wedge\mathrm{e})$, $(\rightarrow\mathrm{e})$ and (trans*) require a careful inspection:

- Case $L = (\wedge\mathrm{e})$. In this case, the part of $\mathcal{P}$ where u and u' appear has the following form:

  $$(\wedge\mathrm{e})\ \dfrac{\dfrac{\vdots}{u : \mathtt{pref}\ \ (x \wedge y)}}{\dfrac{u' : \mathtt{pref}\ x}{\vdots}}$$

  We are assuming, without loss of generality, that $F(u') = \mathtt{pref}\ x$; the argument for $F(u') = y$ is similar. If u is a hypothesis, then, clearly, $\mathtt{pref}\ \ (x \wedge y)$ is local to Γ. Now, suppose u is the conclusion of an instance of an inference rule L. For each case for L, we will prove that $F(u)$ is a relevant component of some premise of that instance; this will imply $\mathtt{pref}\ \ (x \wedge y)$ is local to Γ by lemma 5. This is easily done for $L = (\wedge\mathrm{e})$ and $L = (\rightarrow\mathrm{e})$. Now, by the form of $F(u)$, L cannot be (trans) nor $(\rightarrow\mathrm{i})$. Finally, L cannot be $(\wedge\mathrm{i})$ either, otherwise we could shorten $\mathcal{P}$ in the following way:

  $$(\wedge\mathrm{e})\ \dfrac{(\wedge\mathrm{i})\ \dfrac{L''\ \dfrac{\vdots}{\mathtt{pref}\ x} \qquad \dfrac{\vdots}{\mathtt{pref}\ y}}{u : \mathtt{pref}\ (x \wedge y)}}{\dfrac{u' : \mathtt{pref}\ x}{\vdots}} \qquad \Rightarrow \qquad L''\ \dfrac{\vdots}{\dfrac{u' : \mathtt{pref}\ x}{\vdots}}$$

- Case $L = (\rightarrow\mathrm{e})$. This is a twofold case; u may be either the right or the left premise. Both cases are similar, so we will treat the left case only. The part of $\mathcal{P}$ where u and u' appear has the following form:

$$L\ \dfrac{\dfrac{\vdots}{u:\texttt{pref}\ x}\qquad \dfrac{\vdots}{v:\texttt{pref}\ (x\to y)}}{\dfrac{u':\texttt{pref}\ y}{\vdots}}$$

Again, we will use lemma 5 to show $F(v)$ is local to Γ.

We will show that for any case of L', $F(v)$ is a relevant component of some premise of L'. This is easy for L' = ($\wedge$e) and L' = ($\to$e). The case of L' = ($\wedge$ i) is not possible because of the form of $F(v)$. L' cannot be ($\to$i); otherwise, we could shorten $\mathcal{P}$ in the following way:

$$L=(\to\text{e})\ \dfrac{\dfrac{\vdots}{\texttt{pref}\ x}\qquad L'=(\to\text{i})\ \dfrac{L''\ \dfrac{\vdots}{\texttt{pref}\ y}}{u:\texttt{pref}\ (x\to y)}}{\dfrac{u':\texttt{pref}\ y}{\vdots}}\qquad\Rightarrow\qquad L''\ \dfrac{\vdots}{u':\texttt{pref}\ y}$$

Finally, if L' = (trans*), then $\mathcal{P}$ would have the following form:

$$\begin{matrix}L'' \\ (\to\text{e})\end{matrix}\ \dfrac{\dfrac{\vdots}{\texttt{pref}\ x}\qquad (\text{trans*})\ \dfrac{\dfrac{\vdots}{\texttt{pref}\ x\to\texttt{pref}\ x_1}\qquad \dfrac{\vdots}{\texttt{pref}\ (x_1\to x_2)\quad\ldots}\qquad \dfrac{\vdots}{\texttt{pref}\ (x_k\to y)}}{u:\texttt{pref}\ (x\to y)}}{\dfrac{u':\texttt{pref}\ y}{\vdots}}$$

But this contradicts our assumption that $\mathcal{P}$ is normal. We have successfully all possible cases for L'; hence, $\texttt{pref}\ (x\to y)$, and consequently, $\texttt{pref}\ x$ are local to Γ.

- Case L = (trans*). In this case, the part of $\mathcal{P}$ where u and u' appear has the following form:

$$(\text{trans*})\ \dfrac{\dfrac{\vdots}{\texttt{pref}\ (x_1\to x_2)\quad\ldots}\qquad \dfrac{\vdots}{u:\texttt{pref}\ (x_{i-1}\to x_i)}\qquad \dfrac{\vdots}{\ldots\quad\texttt{pref}\ (x_{k-1}\to x_k)}}{\dfrac{u':\texttt{pref}\ (x_1\to x_k)}{\vdots}}$$

If u is a hypothesis, then we are done; otherwise, u is the conclusion of some inference rule L'. Note L' cannot be ($\wedge$i). If $L' = (\to\text{i})$, then $\mathcal{P}$ would have the following form:

$$\text{(trans*)}\ \dfrac{\dfrac{\vdots}{\texttt{pref}\ (x_1 \to x_2)} \quad \ldots \quad (\to\text{i})\ \dfrac{\dfrac{\vdots}{\texttt{pref}\ x_i}}{u : \texttt{pref}\ (x_{i-1} \to x_i)} \quad \ldots \quad \dfrac{\vdots}{\texttt{pref}\ (x_{k-1} \to x_k)}}{\dfrac{u' : \texttt{pref}\ (x_1 \to x_k)}{\vdots}}$$

But, this contradicts our assumption that $\mathcal{P}$ is normal. Lastly, L' cannot be (trans*) either; otherwise $\mathcal{P}$ would have the form

$$\text{(trans*)}\ \dfrac{\dfrac{\vdots}{\texttt{pref}\ (x_1 \to x_2)} \quad \ldots \quad \text{(trans*)}\ \dfrac{\dfrac{\vdots}{\texttt{pref}\ (x_{i-1} \to y_1)} \quad \dfrac{\vdots}{\ldots} \quad \dfrac{\vdots}{\texttt{pref}\ (y_m \to x_i)}}{j_0 : \texttt{pref}\ (x_{i-1} \to x_i)} \quad \dfrac{\vdots}{\ldots \quad \texttt{pref}\ (x_{k-1} \to x_k)}}{\dfrac{u' : \texttt{pref}\ (x_1 \to x_k)}{\vdots}}$$

and it could be shortened in the following way:

$$\text{(trans*)}\ \dfrac{\dfrac{\vdots}{\texttt{pref}\ (x_1 \to x_2) \quad \ldots} \quad \dfrac{\vdots}{\texttt{pref}\ (x_{i-1} \to y_1) \quad \ldots \quad \texttt{pref}\ (y_m \to x_i)} \quad \dfrac{\vdots}{\ldots \quad \texttt{pref}\ (x_{k-1} \to x_k)}}{\dfrac{u' : \texttt{pref}\ (x_1 \to x_k)}{\vdots}}$$

Note that this is the one and only case where we take advantage of the greater generality of (trans*) comparative to (trans). To summarise, there are only two possible cases for L': ($\wedge$e) and ($\to$e). For these two, $F(u)$ is a relevant component of some premise of L', therefore $F(u)$ is local to Γ by lemma 5. This completes the analysis when $L =$ (trans*).

All cases for L have been exhausted; therefore, we conclude that every $\mathbf{qT}_0$-formula in a minimal normal proof of y from Γ is local to $\Gamma \cup \{y\}$.

$\square$

4.2 The algorithm

The algorithm for $MD\,(\mathsf{qT}_0)$ is an extension of the algorithm presented in [10] for the multi-derivability problem for primal infon logic. We explain how the algorithm in [10] works. First, mark all formulas in Γ and insert them in a queue. Let x be the first formula in the queue. Mark and insert in the queue all those formulas in S that can be proved with the aid of x. Then, remove x from the queue, and repeat this with the next formula in the queue. When this queue empties, all the formulas in S that are provable from Γ will have been marked. Finally, output those formulas in Δ that were marked.

Theorem 7. There is a quadratic-time algorithm for $MD\,(\mathsf{qT}_0)$.

Proof. The parse-tree and homonymy-originals stages are the same as in the algorithm for $MD(\mathsf{PIL})$. In the preprocessing stage, each node has a record $T(u)$ with five fields S, $(\wedge$, left), $(\wedge$, right), $(\to$, left) and $(\to$, right). We need a new record $N(u)$, which is the ordinal number (among the homonymy originals) in the depth-first traversal of the parse tree. A possible way to initialize N is the following. Set a counter $i = 1$ and set all $N(u) = -1$. Traverse the parse tree in the depth-first manner and let u be the current node. If $N(H(u)) = -1$, then set $N(H(u)) = i$ and increase i by 1.

We introduce here the auxiliary relations *Suc* and *Pred*. For nodes u, v and quotation prefix `pref` (possible empty), we say that

$$v\; Suc_{\texttt{pref}}\; u :\Longleftrightarrow u\; Pred_{\texttt{pref}}\; v :\Longleftrightarrow \begin{cases} \texttt{pref}\ (u \to v) \text{ is local to } \Gamma \cup Q \text{ and} \\ \texttt{pref}\ (u \to v) \text{ is pending or processed.} \end{cases}$$

For example, suppose

$$\Gamma \cup Q = \{p\ \texttt{said}\ q\ \texttt{said}\ x \to y, q\ \texttt{said}\ p\ \texttt{said}\ y \to z, p\ \texttt{said}\ q\ \texttt{said}\ y \to w\}\,.$$

Assume also that all of them are raw, except $p\ \texttt{said}\ q\ \texttt{said}\ x \to y$ and $p\ \texttt{said}\ q\ \texttt{said}\ y \to z$ which are pending. Then,

$$x\; Pred_{p\ \texttt{said}\ q\ \texttt{said}}\; y \text{ and } z\; Suc_{q\ \texttt{said}\ p\ \texttt{said}}\; y.$$

Note it is not true that $x\; Pred_{q\ \texttt{said}}\; y$, because $q\ \texttt{said}\ (x \to y)$ is not local to $\Gamma \cup Q$; neither is $w\; Suc_{p\ \texttt{said}\ q\ \texttt{said}}\, y$, because $p\ \texttt{said}\ q\ \texttt{said}\ (y \to w)$ is not pending nor processed yet.

After the preprocessing stage comes the processing stage. This stage consists of processing all pending homonymy originals. For each pending u in T, we instantiate all rules in which u may act as premise. For each rule different from (trans*), the instantiation works exactly as described in the algorithm for $MD(\mathsf{PIL})$. The presence of (trans*) in $\mathcal{H}^*$ demands an additional step in the processing of each pending node:

- **Step** (trans*) This requires $L(u)$ has the form $\texttt{pref}\ (L(v') \to L(v''))$ for some nodes v' and v''. Let $\bar{u}$ be the descendant of u such that $L(\bar{u}) = L(v') \to L(v'')$. For each node w' reachable from v' by $Suc_{\texttt{pref}}$ and each node w'' reachable from v'' by $Pred_{\texttt{pref}}$, if $\texttt{pref}\ (w' \to w'')$ is raw, then make it pending. We will explain how to implement this:

  1. Let m be the number of homonymy originals and let $R_{suc}\,[1..m]$ and $R_{pred}\,[1..m]$ be two auxiliary arrays whose values are initially set to 0.
  2. Make a breadth-first search through the connected component of v' in the graph generated by the homonymy originals and the relation $Suc_{\texttt{pref}}$. For each visited node w, set $R_{suc}\,[N(w)] = 1$.
  3. Do the same for v'', but in this case, the graph is that generated by the relation $Pred_{\texttt{pref}}$.
  4. Traverse T and for each u, if
     - $L(u) = \texttt{pref}\ L(w') \to L(w'')$,
     - $R_{suc}\,[N(H(w'))] = R_{pred}\,[N(H(w''))] = 1$ and
     - $S(u) = 1$ (i.e. u is raw),

     then set $S(u) = 2$.

The rest of the processing stage is identical to that for $MD(\textsf{PIL})$.

Proof of correctness Let x be a formula local to $\Gamma \cup Q$ and let u be the homonymy original such that $L(u) = x$. It suffices to show that u becomes pending iff x is provable from Γ in $\textsf{qT}_0$. The $(\Rightarrow)$-part is obtained by a straightforward inspection of the algorithm. We prove the $(\Leftarrow)$-part by induction on $\mathcal{P}$, a normal proof of minimal size of x from Γ. If $\texttt{pref}\ x$ is a hypothesis, then u will become pending at the preprocessing phase; otherwise, x is the conclusion of an instance of an inference rule L. Several cases arise for L. All cases are similar, so we will explain only when $L =$ (trans*). Let us pressume that $x = \texttt{pref}\ (x_1 \to x_k)$ and that $S = \{\texttt{pref}\ (x_1 \to x_2), \texttt{pref}\ (x_2 \to x_3), \ldots, \texttt{pref}\ (x_{k-1} \to x_k)\}$ are the premises of L in $\mathcal{P}$. For some $i < k$, formula $\texttt{pref}\ (x_i \to x_{i+1})$ will be the last among S in the processing queue. Let us inspect what the algorithm will do when it processes $\texttt{pref}\ (x_i \to x_{i+1})$. By this time, we must have the following:

$$x_i\ Suc_{\texttt{pref}}\ x_{i-1}\ Suc_{\texttt{pref}}\ x_{i-2}\ Suc_{\texttt{pref}}\ \ldots\ Suc_{\texttt{pref}}\ x_2\ Suc_{\texttt{pref}}\ x_1,$$

and

$$x_{i+1}\ Pred_{\texttt{pref}}\ x_{i+2}\ Pred_{\texttt{pref}}\ x_{i+3}\ Pred_{\texttt{pref}}\ \ldots\ Pred_{\texttt{pref}}\ x_{k-1}\ Pred_{\texttt{pref}}\ x_k.$$

This implies that when the algorithm evaluates (trans*) as a potential rule for instantiation, it will obtain that $R_{suc}\,[N(x_1)] = R_{pred}\,[N(x_k)] = 1$. Thus, u will become pending if it was raw.

Time complexity An inspection of the algorithm shows that the parse-tree, homonymy-originals and preprocessing stages take linear time. It suffices to prove, then, that the processing stage takes time $O(n^2)$.

In [10], it is proved that the processing stage takes linear time by showing that the total number of steps in the evaluation of all the rules for all the nodes is $O(n)$. Since our algorithm for qT_0 consists of one additional step for each node in the processing stage; it is enough to verify that, for a homonymy original, the additional time due to **Step** (trans*) is $O(n)$. To explain this, note that this step consists of the following substeps:

1. Initialization of $R_{pred}\,[1..m]$ and $R_{suc}\,[1..m]$.

2. Two breadth-first searches.

3. Traversal and updating of T.

Each breadth-first search takes linear time. To see this, recall that a breadth-first search in a graph where the edges are implemented by adjacency lists takes time $O(n+e)$, where e is the number of edges; but in our case, $e = O(n)$. Then each substep takes linear time, thus **Step** (trans*) takes altogether $O(n)$. We conclude that this algorithm works in time $O(n^2)$. □

5 Semantics for qT

Semantics for primal infon logic **PIL** uses a version of Kripke semantics in which connectives p `said` are interpreted as modal operators. The replacement of the classical deduction theorem with the weaker rule (→i) gives rise to requirement:

- If y holds in w, then $x \to y$ must hold as well.

Also, rule (→e) gives rise to requirement:

- If x holds, but y does not; then, $x \to y$ does not hold.

But, what should happen if neither x nor y holds, should $x \to y$ hold or not? This turns out to be irrelevant; models that satisfy only the previous two requirements form a complete semantics for **PIL**.

The presence of (trans) and (x2x) in **qT** imposes additional constraints on the validity of $x \to y$ in a world:

- $x \to x$ holds for every world.

- if $x \to y$ and $y \to z$ hold in w, then $x \to z$ must hold as well.

The obvious solution is to insert these new conditions in the definition of semantics for **qT**, but this makes difficult to construct Kripke models for **PIL**, for one has to be careful to be complying with all the requirements above. It is much simpler if we define validity of a formula x in a world w by induction on the complexity of x, so we only set validity for variables and let this unfold to all the formulas. The question is how to define validity of $x \to y$ in terms of x and y; more specifically, when x and y does not hold in w. This is not trivial anymore since we have to assure that the requirements forced by (trans) and (x2x) are met. We solve this by equipping each world w with a quasi-order on the formulas $\preceq_w$. Validity of $x \to y$ in a world w is defined as usual except when x and y does not hold, in this case $x \to y$ holds if and only if $x \preceq_w y$. The purpose of this section is to show that these models form a complete semantics for **qT**.

Definition 5. Let P be the set of all principal constants. A *Kripke frame* is a structure $\left\langle W, \leq, (S_q)_{q \in P} \right\rangle$ such that:

- The pair $\langle W, \leq \rangle$ is a non-empty partially ordered set, whose elements are called *worlds*.
- For q a principal constant, S_q is a binary relation on W such that for $u, v, w \in W$, if $u \leq v$ and $v \, S_q \, w$, then $u \, S_q \, w$.

A *Kripke model for* **qT** is a triple $\mathfrak{M} = (\mathfrak{F}, Q, V)$ such that the first component $\mathfrak{F}$ is a Kripke frame, the second component Q is a function assigning a quasi-order on the formulas $\preceq_w$ to each world w in $\mathfrak{F}$, and the last component V assigns to each variable v a subset $V(v)$ of worlds of $\mathfrak{F}$ such that:

$$\text{if } w \in V(v) \text{ and } w \leq w', \text{ then } w' \in V(v).$$

Let w be a world of a Kripke model $\mathfrak{M} = (\mathfrak{F}, Q, V)$. For a formula x we define the notion $w \vDash x$ by induction on x:

$$\begin{array}{rcll}
[\mathbf{K\text{-}Var}] & w \vDash v & \text{iff} & w \in V(v), \text{ where } v \text{ is a variable.} \\
[\mathbf{K\text{-}}\top] & w \vDash \top. & & \\
[\mathbf{K\text{-}}\wedge] & w \vDash x \wedge y & \text{iff} & w \vDash x \text{ and } w \vDash y. \\
[\mathbf{K\text{-}}\to] & w \vDash x \to y & \text{iff} & \text{for any } w' \text{ such that } w \leq w', \\
 & & & \quad (x \preceq_{w'} y \text{ and } w' \nvDash x) \text{ or } w' \vDash y. \\
[\mathbf{K\text{-}}\mathtt{said}] & w \vDash q \;\mathtt{said}\; x & \text{iff} & w' \vDash x \text{ for all } w' \text{ such that } w \, S_q \, w'.
\end{array}$$

Definition $[\mathbf{K\text{-}}\to]$ seems complicated. The following table will clarify what it means.

$w' \vDash x$	$w' \vDash y$	$w' \vDash x$ implies $w' \vDash y$	$(x \preceq_{w'} y$ and $w' \nvDash x)$ or $w' \vDash y$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	$x \preceq_{w'} y$

This explains that [**K-**$\rightarrow$] is almost exactly as the intuitionistic definition of $w \vDash x \rightarrow y$. The only change is when in a future world w', we have $w' \nvDash x$ and $w' \nvDash y$; in this case, we require in addition that $x \preceq_{w'} y$.

Lastly, we say that x *holds* in w if $w \vDash x$ and that x *fails* in w otherwise. Also, we say that Γ *holds* in w if x holds in every world of $\mathfrak{M}$ for all $x \in \Gamma$. $\triangle$

5.1 Soundness and completeness

Theorem 8. Let Γ be a finite set of formulas. A formula y is provable from Γ in **qT** iff for any Kripke model, y holds in every world in which Γ holds.

Proof. ($\Rightarrow$) Let $\mathfrak{M}$ be a Kripke model and let w be a world such that $w \vDash \Gamma$. We prove that $w \vDash y$ by induction on the proof of y from Γ. For the base case it suffices to prove three things:

- If $y \in \Gamma$, then y holds in w; but this is obvious.

- $w \vDash \texttt{pref}\ \top$ for any quotation prefix $\texttt{pref}$. Suppose first that $\texttt{pref} = p\,\texttt{said}$. It is easy to see that $w \vDash p\ \texttt{said}\ \top$ is always true because $w' \vDash \top$ for every world w', in particular, for those, if any, such that wS_pw'. Therefore, $w \vDash p\ \texttt{said}\ \top$. The argument is easily extended for any quotation prefix $\texttt{pref}$.

- $w \vDash \texttt{pref}\,(x \rightarrow x)$ for any quotation prefix $\texttt{pref}$ and any formula x. Again, we will explain this for the case $\texttt{pref} = p\ \texttt{said}\ (x \rightarrow x)$, since the argument presented can be easily extended to any quotation prefix. Note that $w' \vDash x \rightarrow x$ is always true for any world w', because for any $w'' \geq w'$, the reflexitivy of $\preceq_{w''}$ allows to us to assert that:

$$(x \preceq_{w''} x \text{ and } w'' \nvDash x) \text{ or } w'' \vDash x.$$

This implies $w' \vDash x \rightarrow x$. In particular, this is true for all w', if any, such that $w\,S_p\,w'$. Hence, $w \vDash p\ \texttt{said}\ (x \rightarrow x)$.

This concludes the base case. Now, suppose that y was obtained from $x_1, x_2, \ldots, x_n$ by an instance of an inference rule L and that for each i, we have $w \vDash x_i$. An inspection of all the cases for L will show that $w \vDash y$ as well. Since all cases are similar, we will explain only two of them:

- Case $L = (\rightarrow\text{e})$. In this case, $n = 2$ and $x_2 = x_1 \rightarrow y$. Since $w \vDash x_1 \rightarrow y$, either $w \vDash y$ or $w \nvDash x_1$; but the latter cannot be, for $w \vDash x_1$. We conclude that $w \vDash y$.

- Case $L =$ (trans). In this case, $n = 2$, $x_1 = y_1 \rightarrow y_2$, $x_2 = y_2 \rightarrow y_3$ and $y = y_1 \rightarrow y_3$. To prove that $w \vDash y_1 \rightarrow y_3$, we have to prove that for any $w' \geq w$,

$$(y_1 \preceq_{w'} y_3 \text{ and } w' \nvDash y_1) \text{ or } w' \vDash y_3. \tag{1}$$

So, let $w' \geq w$. Recall we are assuming that $w \vDash y_1 \rightarrow y_2$ and $w \vDash y_2 \rightarrow y_3$, which implies that

$$\begin{array}{l}(y_1 \preceq_{w'} y_2 \text{ and } w' \nvDash y_1) \text{ or } w' \vDash y_2\text{, and} \\ (y_2 \preceq_{w'} y_3 \text{ and } w' \nvDash y_2) \text{ or } w' \vDash y_3\end{array}$$

If $w' \nvDash y_i$ for all $i \leq 3$, then we must have $y_1 \preceq_{w'} y_2 \preceq_{w'} y_3$. This implies that

$$(y_1 \preceq_{w'} y_3 \text{ and } w' \nvDash y_1),$$

which implies expression (1). Now, suppose $w' \vDash y_i$ for some $i \leq 3$. If $w' \vDash y_3$, then we immediately have expression (1). If $w' \vDash y_1$, then, since $w \vDash y_1 \rightarrow y_2$, we must have $w' \vDash y_2$, and since $w \vDash y_2 \rightarrow y_3$, we must have $w' \vDash y_3$, which implies again expression (1). In a similar way it is checked that $w' \vDash y_2$ implies (1).

($\Leftarrow$) We prove the counterpositive: if y is not provable from Γ in **qT**, then there is a Kripke model $\mathfrak{M}$ in which, at some world, Γ holds but y does not. First, we describe the underlying Kripke frame of $\mathfrak{M}$:

- The set of worlds W is the set of quotation prefixes `pref` such that there is a formula of the form `pref` x local to $\Gamma \cup \{y\}$.
- Relation $\leq$ is the identity relation on W.
- For $\texttt{pref}, \texttt{pref}' \in W$, define:

$$\texttt{pref}\ S_q\ \texttt{pref}' \text{ iff } \texttt{pref}' = \texttt{pref}\ q\ \texttt{said}\ .$$

Next, we define the quasi-order for each world and the valuation for each variable:

- For $\texttt{pref} \in W$, define

$$x \preceq_{\texttt{pref}} y \text{ iff } \Gamma \vdash \texttt{pref}\ \ (x \rightarrow y) \text{ (i.e. } \texttt{pref}\ \ (x \rightarrow y) \text{ is provable from } \Gamma).$$

- For $\texttt{pref} \in W$ and v a variable, define

$$\texttt{pref} \in V(v) \text{ iff } \Gamma \vdash \texttt{pref}\ v \text{ (i.e. } \texttt{pref}\ v \text{ is provable from } \Gamma).$$

We will show that for any formula `pref` x local to $\Gamma \cup \{y\}$, we have $\texttt{pref} \vDash x$ iff $\Gamma \vdash \texttt{pref}\ x$. We do this by induction on the complexity of x:

- Case x is a variable. This follows from the defintion.

- Case $x = \top$. Clearly, for any $\texttt{pref} \in W$, we have that $\texttt{pref} \vDash \top$ and $\Gamma \vdash \texttt{pref}\ \top$.
- Case $x = x_1 \wedge x_2$.

$$\begin{aligned}
\texttt{pref} \vDash x_1 \wedge x_2 &\Leftrightarrow \texttt{pref} \vDash x_1 \text{ and } \texttt{pref} \vDash x_2 \\
&\Leftrightarrow \Gamma \vdash x_1 \text{ and } \Gamma \vdash x_2 && \text{Induction hypothesis.} \\
&\Leftrightarrow \Gamma \vdash x_1 \wedge x_2 && \text{Rules } (\wedge\text{i}) \text{ and } (\wedge\text{e}).
\end{aligned}$$

- Case $x = x_1 \to x_2$. By the definitions and the induction hypothesis, we have:

$$\begin{aligned}
&\texttt{pref} \vDash x_1 \to x_2 \\
\Leftrightarrow\ &\text{for all } \texttt{pref}' \geq \texttt{pref}\ \left[\left(x_1 \preceq_{\texttt{pref}'} x_2 \text{ and } \texttt{pref}' \nvDash x_1\right) \text{ or } \texttt{pref}' \vDash x_2\right] \\
\Leftrightarrow\ &\left(x_1 \preceq_{\texttt{pref}} x_2 \text{ and } \texttt{pref} \nvDash x_1\right) \text{ or } \texttt{pref} \vDash x_2 \\
\Leftrightarrow\ &(\Gamma \vdash \texttt{pref}\ \ (x_1 \to x_2) \text{ and } \Gamma \nvdash \texttt{pref}\ x_1) \text{ or } \Gamma \vdash \texttt{pref}\ x_2.
\end{aligned}$$

So, we have to prove that:

$$\begin{aligned}
(\Gamma \vdash \texttt{pref}\ \ (x_1 \to x_2) \text{ and } \Gamma \nvdash \texttt{pref}\ x_1) \text{ or } \Gamma \vdash \texttt{pref}\ x_2 \\
\Longleftrightarrow \Gamma \vdash \texttt{pref}\ \ (x_1 \to x_2).
\end{aligned}$$

The ($\Rightarrow$) part follows easily by rule ($\to$i). For the ($\Leftarrow$) part, suppose $\Gamma \vdash \texttt{pref}\ \ (x_1 \to x_2)$. On one hand, if $\Gamma \vdash \texttt{pref}\ x_1$, then by ($\to$e) we have $\Gamma \vdash \texttt{pref}\ x_2$. On the other hand, if $\Gamma \nvdash \texttt{pref}\ x_1$, then we immediately have the result.

- Case $x = q\ \texttt{said}\ x'$.

$$\begin{aligned}
&\texttt{pref} \vDash q\ \texttt{said}\ x' \\
\Leftrightarrow\ &\texttt{pref}' \vDash x' \quad \forall \texttt{pref}' \, (\texttt{pref}\ S_q\ \texttt{pref}') \\
\Leftrightarrow\ &\texttt{pref}\ q\ \texttt{said}\ \vDash x' && \texttt{pref}\ S_q\ \texttt{pref}' \text{ iff } \texttt{pref}' = \texttt{pref}\ q\, \texttt{said} \\
\Leftrightarrow\ &\Gamma \vdash \texttt{pref}\ q\ \texttt{said}\ x' && \text{Induction hypothesis.}
\end{aligned}$$

All cases have been exhausted; therefore, if $\texttt{pref}\ x$ is local to $\Gamma \cup Q$, then $\texttt{pref} \vDash x$ iff $\Gamma \vdash \texttt{pref}\ x$. Applying this result with ϵ, the empty prefix, we have that $\epsilon \vDash \Gamma$, but $\epsilon \nvDash y$, which was what we wanted.

□

Lastly, a remark on the size of the model $\mathfrak{M}$ built in this proof. For a formula x, we define its *size* $|x|$ in the natural way:

- For a variable v, we have $|v| = 1$.
- For x and y formulas, we have

$$\begin{aligned} |x \wedge y| &= |x| + |y| + 1, \\ |x \to y| &= |x| + |y| + 1, \text{ and} \\ |q \texttt{ said } x| &= 2 + |x| . \end{aligned}$$

For a set of formulas Δ, we define its size as the sum of all the sizes of its elements.

A prefix `pref` is said to be *local* to a formula z if there exists a formula x such that `pref` x is local to z. A prefix is local to a set of formulas Δ if it is local to some formula $z \in \Delta$.

Lemma 9. For a formula x, the number of non-empty prefixes local to x is less than $|x|/2$.

Proof. Let $LP(x)$ be the number of non-empty prefixes local to x. This lemma is easily proved by induction on the complexity of x. For the case $x = q \texttt{ said } x'$, note that the non-empty local prefixes of x are $q\texttt{ said}$ plus all the prefixes of the form $q \texttt{ said pref}$, where `pref` is non-empty and local to x'. Hence,

$$\begin{aligned} LP(q \texttt{ said } x') = 1 + LP(x') < 1 + |x'|/2 &= (2 + |x'|)/2 \\ &= |q \texttt{ said } x'|/2. \end{aligned}$$

□

It turns out that the model $\mathfrak{M}$ built above is relatively small. Its size (i.e. the number of worlds of the underlying Kripke structure) is less than $|\Gamma \cup \{y\}|/2{+}1$. To see this, recall that the worlds of the underlying Kripke structure of $\mathfrak{M}$ are all prefixes local to $\Gamma \cup \{y\}$. The previous lemma implies that the number of non-empty prefixes local to a set of formulas Δ is less than $|\Delta|/2$; so the number of prefixes local to Δ is less than $|\Delta|/2 + 1$. Hence, the size of $\mathfrak{M}$ is less than $|\Gamma \cup \{y\}|/2 + 1$. The 1/2 bound cannot be improved. Consider the formula

$$z = p_1 \texttt{ said } p_2 \texttt{ said } \ldots p_k \texttt{ said } v,$$

where v is a variable. Its size is $2k + 1$ and the number of non-empty local prefixes is k. So you can get as close as possible to $1/|z|$.

6 Transitive primal logic

If we forget about quotations in **qT**, we obtain a fragment of propostitional intuitionistic logic decidable in quadratic-time.

Hilbert calculus $\mathcal{H}p^{\mathsf{T}}$

Axiom

$$(\top) \quad \top \qquad\qquad (\text{x2x}) \quad x \to x$$

Inference rules

$$(\wedge\text{i}) \quad \frac{x \qquad y}{x \wedge y} \qquad (\wedge\text{e}) \quad \frac{x \wedge y}{x} \qquad \frac{x \wedge y}{y}$$

$$(\to\text{i}) \quad \frac{y}{x \to y} \qquad (\to\text{e}) \quad \frac{x \qquad x \to y}{y}$$

$$(\text{trans}) \ \frac{x \to y \qquad y \to z}{x \to z}$$

Consider the set of formulas built only from propositional variables, $\wedge$, $\to$ and the constant $\top$. This set and calculus $\mathcal{H}_p{}^{\mathsf{T}}$ gives rise to a logic which we call *transitive primal logic* and denote by T.

Since quotations do not exist in T, the formulas local to z are exactly the subformulas of z. The following theorem is a direct consequence of theorem 6.

Theorem 10. A minimal normal proof of y from Γ in T is composed only of subformulas of $\Gamma \cup \{y\}$.

Further, we can modify the algorithm presented in 7 so it solves $MD\,(\mathsf{T})$.

Theorem 11. There is a quadratic-time algorithm for the multiple derivability problem for T.

The semantics for T is a simplification of that for qT.

Definition 6. A *Kripke model* for T is a structure $\langle W, \leq, Q, V\rangle$ such that:

- The pair $\langle W, \leq\rangle$ is a non-empty partially ordered set, whose elements are called *worlds*.
- Function Q assigns to each world in W a quasi-order $\preceq_w$ on the infon formulas.
- V is a function assigning to each infon variable a set of worlds in W.

Let w be a world of a Kripke model $\mathfrak{M} = (W, \leq, Q, V)$. For a formula x we define the notion $w \vDash x$ by induction on x:

$$\begin{array}{rlll}
[\textbf{K-Var}] & w \vDash v & \text{iff} & w \in V(v), \text{ where } v \text{ is a variable.} \\
[\textbf{K-}\top] & w \vDash \top. & & \\
[\textbf{K-}\wedge] & w \vDash x \wedge y & \text{iff} & w \vDash x \text{ and } w \vDash y. \\
[\textbf{K-}\!\to] & w \vDash x \to y & \text{iff} & \text{for all } w' \geq w, \\
 & & & \quad (x \preceq_{w'} y \text{ and } w' \nvDash x) \text{ or } w' \vDash y.
\end{array}$$

We say that x *holds* in w if $w \vDash x$ and that x *fails* in w otherwise. Also, we say that Γ *holds* in w if x holds in every world of $\mathfrak{M}$ for all $x \in \Gamma$. △

Theorem 12. (Soundness and completeness) Let Γ be a set of formulas and y be a formula. The following are equivalent:

1. y is provable from Γ.

2. For any Kripke model, y holds in every world in which Γ holds.

3. For any Kripke model with only one world w, if Γ holds in w, then so does y.

Proof. (1) ⇒ (2) Let w be a world in a Kripke world such that Γ holds in w. We prove that y holds in w by induction on a proof of y from Γ. For the axioms, we have to prove that $w \vDash \top$ and $w \vDash x \to x$. The first one is obvious, and the second follows from the following observation:

$$\text{for all } w' \geq w \;:\; (x \preceq_{w'} x \text{ and } w' \nvDash x) \text{ or } w' \vDash x.$$

Now, suppose y is the conclusion of an inference rule L. It is easily proven that $w \vDash y$ by case analysis of L. We present the case of $L =$ (trans) only. Suppose that the premises are $y_1 \to y_2$ and $y_2 \to y_3$, so $y = y_1 \to y_3$. By induction hypothesis, we have that $w \vDash y_1 \to y_2$ and $w \vDash y_2 \to y_3$. We have to show that $w \vDash y_1 \to y_3$, that is, for all $w' \geq w$

$$(y_1 \preceq_{w'} y_3 \text{ and } w' \nvDash y_1) \text{ or } w' \vDash y_3. \tag{2}$$

So, let $w' \geq w$. If $w' \nvDash y_i$ for $i \leq 3$, then we must have $y_1 \preceq_{w'} y_2 \preceq_{w'} y_3$. Therefore,

$$y_1 \preceq_{w'} y_3 \text{ and } w' \nvDash y_1,$$

which implies expression (2). Now, suppose $w' \vDash y_i$ for some $i \leq 3$. If $w' \vDash y_3$, then clearly (2) follows. Since $w \vDash y_2 \to y_3$, we have that if $w' \vDash y_2$, then, $w' \vDash y_3$, and (2) follows. Analogously, since $w \vDash y_1 \to y_2$, we have that $w' \vDash y_1$ implies (2).

(2) ⇒ (3) Obvious.

(3) ⇒ (1) We prove the counterpositive, if y does not follow from Γ in T, then there exists a Kripke model with exactly one world w in which Γ holds but y does not. Consider a one-element Kripke model in which $\leq$ is the identity relation and $\preceq_w$ is defined by the following:

$$x \preceq_w y \text{ iff } \Gamma \vdash x \to y.$$

In a Kripke model with exactly one world, V takes only two values: $\emptyset$ or $\{w\}$. For a variable v, we define V as follows

$$V(v) = \begin{cases} \{w\}\,, & \text{if } \Gamma \vdash v \\ \emptyset, & \text{otherwise} \end{cases}.$$

Now, we show that for any formula x, we have $w \vDash x$ iff $\Gamma \vdash x$. This is done by induction on the complexity of x.

- Case x is either $\top$ or a variable. This is obvious from the definitions.
- Case $x = x_1 \wedge x_2$. This follows from rules ($\wedge$i) and ($\wedge$e) and [**K-**$\wedge$].
- Case $x = x_1 \to x_2$. Since $\leq$ is the identity relation. We have to prove $\Gamma \vdash x_1 \to x_2$ iff

  $$(x_1 \preceq_w x_2 \text{ and } w \nvDash x_1) \text{ or } w \vDash x_2. \tag{3}$$

  Suppose $\Gamma \vdash x_1 \to x_2$, then $x_1 \preceq_w x_2$ by definition. If, in addition, $\Gamma \vDash x_1$ then $\Gamma \vDash x_2$. By induction hypothesis, this means that if $w \vDash x_1$, then $w \vDash x_2$; in other words, either $w \nvDash x_1$ or $w \nvDash x_2$. We conclude that if $\Gamma \vdash x_1 \to x_2$, then (3) holds. The converse follows easily.

Finally, we check this is the desired model. Clearly, for any $x \in \Gamma$, we have $w \vDash x$; and since $\Gamma \nvdash y$, we have $w \nvDash y$. □

7 Related Work

The unary connectives "p `said`" of primal logic can be viewed as necessity operators. Thus primal logic and transitive primal logic are multimodal extensions of the primal fragment propositional intuitionistic logic. We refer the reader to [25] for a presentation of intuitionistic modal logic and to Chapter 1 of [9] for a presentation of multimodal logics.

Recall that the derivability problem for a logic is the problem of deciding whether a given formula is provable from a given set of formulas, and the validity problem is the problem of deciding whether a given formula is valid. Clearly, the second is a particular case of the first, and these two problems are the same when the deduction theorem holds for the logic.

There seems to be very few known natural fragments of intuitionistic logic, let alone its modal extensions, with polynomial-time decidable validity problem. But first let us mention some loosely related tractability results on modal and description logics. Halpern proved that the validity problem for $\mathbf{K}_n$, $\mathbf{T}_n$, $\mathbf{S4}_n$ and $\mathbf{K45}_n$, $\mathbf{KD45}_n$, $\mathbf{S5}_n$ can be decided in linear time if the nesting of modal operators and propositional variables is restricted [13]. See articles [14, 15] for the analysis of fragments of description logic $\mathcal{EL}$ (and some of its extensions) whose validity problem can be solved in polynomial time.

Now let us turn attention to fragments of propositional intuitionistic logic. The best known fragment with decidable derivability problem is the Horn fragment. In fact, the derivability problem for the Horn fragment is solvable in linear time [7, 8, 17]. Mints [18] found another fragment whose validity problem is decided in polynomial time.

The derivability problem for the primal fragment is linear-time decidable as well [10]. Propositional primal infon logic is an extension of the primal fragment of intuitionistic logic with quotation connectives. Originally there were two series of quotation connectives, "p `said`" and "p `implied`" where p ranges over an infinite list of principal constants; the associated derivability problem is linear-time decidable in the case of bounded quotation depth [10]. Later the `implied` series was removed. The derivability problem for the redefined logic is decidable in linear time (with no restriction on the quotation depth) [11].

Finally, let us consider the NNIL fragment of propositional intuitionistic logic [23]. Recall that negation in intuitionistic logic is defined by the following: $\neg\varphi := \varphi \to \bot$. Also, recall that the implicational complexity $\rho(\varphi)$ of a formula φ is defined as follows:

- $\rho(\top) = \rho(\bot) = \rho(v) = 0$, where v is a variable.
- $\rho(\varphi_1 \wedge \varphi_2) = \rho(\varphi_1 \vee \varphi_2) = \max\{\rho(\varphi_1), \rho(\varphi_2)\}$.
- $\rho(\varphi_1 \to \varphi_2) = \max\{\rho(\varphi_1) + 1, \rho(\varphi_2)\}$.

NNIL comprises the formulas with implicational complexity ≤ 1. We say that an NNIL formula φ is without *premise disjunctions* if, for every implication subformula $\alpha \to \beta$ of ϕ, disjunction does not occur in α.

Theorem 13.

1. The validity problem for NNIL formulas without premise disjunction is decidable in polynomial time [24].
2. The validity problem for NNIL is coNP-complete.

Proof.

1. Validity of NNIL formulas without premise disjunctions can be decided inductively as follows:
   - Constant $\top$ is valid, constant $\bot$ is not valid and a variable is not valid.
   - A conjunction is valid iff both conjuncts are valid.
   - A disjunction is valid iff at least one disjunct is valid.
   - For an implication $\varphi_1 \to \varphi_2$, since φ_1 does not have disjunctions, it must have the form $p_1 \wedge p_2 \wedge \ldots \wedge p_k$, where each p_i is a variable. Then, $\varphi_1 \to \varphi_2$ is valid iff $\varphi_2[p_1 := \top, p_2 := \top, \ldots, p_k := \top]$ is valid.

This gives rise to a validity checking algorithm. It is easy to see that the algorithm runs in polynomial time.

2. A formula $(\varphi_1 \vee \varphi_2) \to \psi$ is valid iff both $\varphi_1 \to \psi$ and $\varphi_2 \to \psi$ are valid. Note that this doubles the amount of work. But if we guess one disjunct φ_i and show that $\varphi_i \to \psi$ is not valid, then we have that $(\varphi_1 \vee \varphi_2) \to \psi$ is not valid. This idea leads to a non-deterministic algorithm for deciding whether a NNIL formula φ is not valid. First, for every disjunction occurring in a premise of some implication, make a guess and replace the disjunction with one of the disjuncts. Then, apply the polynomial-time procedure described in (1). Hence, the validity problem for NNIL is coNP.

   Now, we prove the coNP-hardness by a reduction from the non-three-coloring problem. Given a graph $G = (V, E)$, write a NNIL formula α such that G is 3-colorable iff α is not intuitionistically valid. Let A, B and C be unary relations and define $\alpha = \beta \to (\gamma \vee \delta)$, where

$$\begin{aligned}
\beta &= \bigwedge \{A(v) \vee B(v) \vee C(v) \ : \ v \in V\} \\
\gamma &= \bigvee \{(A(v) \wedge B(v)) \vee (B(v) \wedge C(v)) \vee (A(v) \vee C(v)) \ : \ v \in V\} \\
\delta &= \bigvee \{(A(u) \vee A(v)) \wedge (B(u) \vee B(v)) \wedge (C(u) \vee C(v)) \ : \ (u,v) \in E\} .
\end{aligned}$$

   Indeed, if G is 3-colorable then β is true while γ and δ are false. So α is not valid classicaly and, therefore, it is not valid intuitionistically. For the converse, if α is not valid intuitionistically, then there is a Kripke model with a world in which α does not hold. Hence, in this world, β is true while γ and δ are false; which implies that A, B and C represents a 3-coloring for G. Since the 3-coloring problem is NP-complete, we conclude that the validity problem for NNIL is coNP-hard, and hence, it is coNP-complete.

□

References

[1] Aaron Avron and Ori Lahav, *Strict Canonical Constructive Systems.* In Fields of Logic and Computation: Essays Dedicated to Yuri Gurevich on the Occasion of His 70th Birthday, (Andreas Blass, Nachum Dershowitz, and Wolfgang Reisig, editors), 7594 Lecture Notes in Computer Science, volume 6300, Springer-Verlag, 2010.

[2] Lev Beklemishev and Yuri Gurevich, *Propositional Primal Logic with Disjunction*, Microsoft Research Technical Report MSR-TR-2011-35, March 2011.

[3] Andreas Blass and Yuri Gurevich, *Hilbertian Deductive Systems and Datalog*, Microsoft Research Technical Report MSR-TR-2011-81, June 2011.

[4] Nikolaj Bjørner, Guido de Caso, and Yuri Gurevich, *From Primal Infon Logic with Variables to Datalog*, Microsoft Research Technical Report MSR-TR-2011-84, July 2011.

[5] Andreas Blass, Yuri Gurevich, Michal Moskałand Itay Neeman, *Evidential Authorization*, in *The Future of Software Engineering*, Sebastian Nanz (ed.), Springer, 2011, 77–99.

[6] Alexander Chagrov and Mikhail Rybakov, *How Many Variables Does One Need to Prove PSPACE-hardness of Modal Logics?* Advances in Modal Logic Vol. 4. 71-82, 2003.

[7] Evgeny Dantzin, Thomas Eiter, George Gottlob and Andrei Voronkov, *Complexity and Expressive Power of Logic Programming*, ACM Computing Sureveys 33:3, 374425, 2001.

[8] William Dowling and Jean Gallier, *Linear-time algorithms for testing the satisfiability of propositional Horn formulae*, J. Logic Programming 1, 267-284, 1984.

[9] Dov Gabbay, Agi Kurucz, Franz Wolter and Michael Zakharyaschev, *Many-dimensional modal logics: theory and applications*. Elsevier 2003.

[10] Yuri Gurevich and Itay Neeman, *The Logic of Infons*, Bulletin of European Association for Theoretical Computer Science Number 98, June 2009.

[11] Yuri Gurevich, *Two notes on propositional primal logic*, Technical Report MSR-TR-2011-70, Microsoft Research, May 2011.

[12] Yuri Gurevich and Itay Neeman, *DKAL: Distributed-Knowledge Authorization Language*, In Proc. of CSF 2008, pages 149-162. IEEE Computer Society, 2008.

[13] Joseph Halpern, *The effect of bounding the number of primitive propositions and the depth of nesting on the complexity of modal logic*. Artificial Intelligence, 75(2):361-372, 1995.

[14] Agi Kurucz, Frank Wolter and Michael Zakharyaschev, *Islands of tractability for relational constraints: towards dichotomy results for the description logic EL*, In L. Beklemishev, V. Goranko and V. Shehtman, editors, Advances in Modal Logic Vol 8, 271-291, 2010.

[15] Agi Kurucz, Frank Wolter and Michael Zakharyaschev, *On P/NP Dichotomies for EL Subsumption under Relational Constraints*, In Proceedings of DL 2011.

[16] Richard Ladner, *The Computational Complexity of Provability in Systems of Modal Propositional Logic*. SIAM Journal of Computing Vol. 6, No. 3, 467-480, 1977.

[17] Michel Minoux, *LTUR: A simplified linear-time unit resolution algorithm for Horn formulae and computer implementation*, Information Processing Letters 29:1, 1-12, 1988.

[18] Grigori Mints, *Complexity of Subclasses of the Intuitionistic Propositional Calculus*. BIT 32, 64-69, 1992.

[19] Mikhail Rybakov, *Complexity of Intuitionistic and Visser's Basic and Formal Logics in Finitely Many Variables.* Advances in Modal Logic, Vol. 6. 393-411, 2006.

[20] Mikhail Rybakov, *Complexity of Intuitionistic Propositional Logic and its Fragments.* Journal of Applied Non-Classical Logics, 267-292, 2008.

[21] Yury Savateev, *Investigation of primal logic*, unpublished manuscript, 2009.

[22] Richard Statman, *Intuitionistic Propositional Logic is Polynomial- Space Complete*, Theoretical Computer Science 9:1, 67-72, 1979.

[23] Alfred Visser, Johan van Benthem, Dick de Jongh and Gerard Renardel de Lavalette, *NNIL, a study in intuitionistic propositional logic*, Logic Group Preprint Series, Volume: 111, 2008.

[24] Alfred Visser, Personal communication, January 7, 2012.

[25] Frank Wolter and Michael Zakharyaschev, *Intuitionistic modal logic*. In A. cantini, E. Casari, and P. Minari, editors, Logic and Foundations of Mathematics, Kluwer Academic Publishers, 227-238, 1999.