Propositional primal logic with disjunction

Lev Beklemishev, Yuri Gurevich

March 2011

Abstract

Gurevich and Neeman introduced Distributed Knowledge Authorization Language (DKAL). The world of DKAL consists of communicating principals computing their own knowledge in their own states. DKAL is based on a new logic of information, the so-called *infon logic*, and its efficient subsystem called *primal logic*. In this paper we simplify Kripkean semantics of primal logic and study various extensions of it in search to balance expressivity and efficiency. On the proof-theoretic side we develop cut-free Gentzen-style sequent calculi for the original primal logic and its extensions.

1 Introduction

Our story starts with cloud computing and cloud security, not because these are fashionable buzzwords but because this paper was written in the framework of such a project (code-named Vidalia for the time being [1]). With the advent of cloud computing, the role of formal policies grows. The personnel of brick-and-mortar businesses often exercise their judgments; all that should be replaced with formal policies when businesses move to the cloud. The logic-based policy language DKAL (Distributed Knowledge Authorization Language) [19, 20, 12] was developed with such applications in mind. The feature that distinguishes DKAL from most preceding logic-based policy languages is that it is explicitly geared toward federated scenarios (with no central authority) where trust may be in short supply.

The world of DKAL consists of communicating principals computing their own knowledge in their own states. They communicate *infons*, pieces of information, and reason in terms of infons. In [20], the original developers of DKAL distilled the basic features of the logic of infons and introduced infon logic **qI** that is an extension of the $\{\rightarrow, \wedge\}$ fragment **I** of intuitionistic logic with quotation modalities $p\,\texttt{said}\,\varphi$ and $p\,\texttt{implied}\,\varphi$. In addition

they discovered a *primal fragment* **qP** of **qI** which is very efficient and yet sufficiently expressive for many purposes. In the case of bounded quotation depth, the derivation problem for **qP** is solvable in linear time. In particular, the quotation-free fragment **P** of **qP** is linear time in that sense. (Notations **I**, **qI**, **P** and **qP** are introduced in the present paper.)

The continuing development of DKAL (whose current implementation is found at [2]) requires further investigation of the logic of infons. That is exactly what we are doing here. We extend the four logics of [20] with one or both of disjunction and negation, and we determine the complexities of the extended logics. We provide a simpler semantics for the extension $\mathbf{P}[\vee]$ of **P** that we call *quasi-boolean*. This allows us to give efficient mutual translations between $\mathbf{P}[\vee]$ and classical propositional logic as well as an embedding of the appropriate classical modal logic into $\mathbf{qP}[\vee]$. On the proof-theoretic side we develop cut-free Gentzen-style sequent calculi for the extensions of primal logic **P** with some or all of disjunction, negation and quotations.

Related work. As we mentioned, infon logic emerged in the context of access control language DKAL. However, the present paper deals exclusively with infon logic itself. Accordingly we do not discuss access control literature here. The DKAL papers mentioned above include short discussions on the issue.

Technically, infon logic belongs to the family of *intuitionistic* (or *constructive*) *modal logics*. Such logics have been considered at least from the time of Bull [14, 15], see [29, 30, 27, 34, 35, 17]. Potential applications in Computer Science stimulated a growing interest in this topic, see e.g. [28, 16, 26, 10]. We would like to refer the reader to Simpson [31] and Wolter and Zakharyaschev [39] for comprehensive surveys. General results on decidability of intuitionistic modal logics have been considered in [38, 37, 5].

Infon logics of this paper are, in one important respect, simpler than typical intuitionistic modal logics found in the literature. Namely, they only have $\Box$-type modalities, though there are infinitely many of those. They have no $\Diamond$-type modalities.[1] The situation is similar for the other access control modal logics in the literature, where `says` operators play the role of modalities, see e.g. [4, 24, 6, 8, 13] and especially [3, 18]. The axioms of `said` and `implied` modalities in our systems correspond to basic modal logic **K**. Thus they do not admit the principles such as $\varphi \to q\,\mathtt{said}\,\varphi$ postulated for some of the typical access control logics and discussed in [3]. In this regard our systems are closer to the standard modal logics than to the so-called lax

[1] In intuitionistic modal logic diamonds are usually not expressible in terms of boxes.

logics.

An essential novelty of infon logic is the use of restricted (primal) implication introduced in [21] as a compromise between expressivity and practical efficiency. The goal of this paper is to better understand primal implication, also in relation to the modalities. Our conclusions are that this new connective is quite manageable and has good proof-theoretic and semantic properties. Avron and Lahav [7] consider a sequent calculus for primal logic (without modalities) and observe that it falls within their framework of constructive canonical systems, which implies a number of nice properties such as cut-elimination and semantic completeness. The semantics as well as the sequent calculus presented in this paper are somewhat different from the one in [7]. Namely, we deal with a multi-conclusion sequent calculus, and our quasi-boolean models are simpler than those of [21] and [7].

2 Infon logic: language and derivability

Language. The vocabulary of infon logic consists of a set $\mathcal{P}$ of constants denoting *principals* and of a set of propositional variables $P, Q, \ldots$ denoting *infons*, that is, any pieces of information that can be communicated between the principals. We can think of infons as declarative statements; the notion of infon is basic in DKAL.

Propositional infon logic introduced in [20, 21] is an extension of the fragment of propositional intuitionistic logic without disjunction and negation by two series of *quotation modalities* $p\,\texttt{said}$ and $p\,\texttt{implied}$, for each principal $p \in \mathcal{P}$.

Intuitively, logical connectives denote some natural ways of combining infons. Thus, conjunction $\varphi \wedge \psi$ means joining the information contained in φ and in ψ. The implication $\varphi \to \psi$ represents conditional information: the minimal information needed to infer ψ once one has φ. Logical constant $\top$ represents the *uninformative infon*, that is, something every principal knows.

The meaning of quotations is related to communication between the principals. The intuitive meaning of $q\,\texttt{said}\,\varphi$ (from the point of view of another principal p) is that φ can be inferred from the information directly said by q to p.[2] Here is the most typical DKAL scenario how a principal p learns that $q\,\texttt{said}\,\varphi$. Suppose that a principal q says φ to p (and p gets the

[2]DKAL avoids the logical omniscience problem by means of a mechanism of computing knowledge. On the level of logical systems, deduction is unrestricted.

message, and the message is properly signed by q so that there is no doubt that it is coming from q); then p learns $q\,\texttt{said}\,\varphi$.

The intuitive meaning of $q\,\texttt{implied}\,\varphi$ is that q indeed communicated (its support for) φ but predicated it on the knowledge of some proviso ψ. Here is the most typical scenario how a principal p learns $q\,\texttt{implied}\,\varphi$. Suppose that q communicates φ to p under condition that p knows ψ, and suppose that p knows the proviso ψ; then p learns $q\,\texttt{implied}\,\varphi$. The exact meaning of $q\,\texttt{said}\,\varphi$ and $q\,\texttt{implied}\,\varphi$ in DKAL is more involved but those details are irrelevant for our purposes in this paper. Intuitively, $q\,\texttt{said}\,\varphi$ is a version of $q\,\texttt{implied}\,\varphi$ where the communication was not predicated on any proviso. Technically, both kinds of modalities satisfy the rules of the basic modal logic **K** and the relation $(q\,\texttt{said}\,\varphi) \vdash (q\,\texttt{implied}\,\varphi)$.

Proof system. A proof system for infon logic could be equivalently stated in any of the familiar proof-theoretic formats, in particular, it has been formulated in a Hilbert-style format and in a natural deduction style format in [21]. In this paper we adopt the sequent-style natural deduction format from [21] as our basic definition of derivability relation. In Section 5 we also present an equivalent Gentzen-style calculus together with the corresponding cut-elimination theorem.

Let Γ, Δ denote sets of formulas; we abbreviate $\Gamma \cup \Delta$ as Γ, Δ and $\Gamma \cup \{\varphi\}$ as Γ, φ. Also, $q\,\texttt{said}\,\Gamma$ stands for $\{q\,\texttt{said}\,\varphi : \varphi \in \Gamma\}$.

We define the relation $\Gamma \vdash \varphi$ *'formula φ is provable from assumptions Γ'* as the minimal relation containing the following axioms and closed under the following inference rules.

Axioms: $\varphi \vdash \varphi$; $\quad \vdash \top$;

Inference rules: $\dfrac{\Gamma \vdash \varphi}{\Gamma, \Delta \vdash \varphi}$ (weakening)

$$\frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \varphi}\ (\wedge E_l) \qquad \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \psi}\ (\wedge E_r) \qquad \frac{\Gamma \vdash \varphi \quad \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi}\ (\wedge I)$$

$$\frac{\Gamma \vdash \varphi \to \psi \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi}\ (\to E) \qquad \frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi}\ (\to I)$$

$$\frac{\Gamma \vdash \varphi}{q\,\texttt{said}\,\Gamma \vdash q\,\texttt{said}\,\varphi}\ (\texttt{Said}) \qquad \frac{\Gamma, \Delta \vdash \varphi}{q\,\texttt{said}\,\Gamma,\ q\,\texttt{implied}\,\Delta \vdash q\,\texttt{implied}\,\varphi}\ (\texttt{Implied})$$

The intuitionistic propositional logic, and even its fragment in the language without disjunction and negation which we denote **I**, is known to be PSPACE-complete by a result of R. Statman [32] (see also [36]). The same result holds for the infon logic with quotations: it remains in the class PSPACE like many other natural modal logics [21]. This motivated Gurevich

and Neeman to introduce a weaker but still relatively expressive and much more efficient fragment of intuitionistic logic called *primal logic* **P**. Primal logic is obtained by restricting the $(\rightarrow I)$ rule as follows:

$$\frac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \rightarrow \psi}\ (\rightarrow I_p)$$

For **P**, there is a linear time algorithm deciding whether $\Gamma \vdash \varphi$ [21].

A logical connective satisfying the rules $(\rightarrow E)$ and $(\rightarrow I_p)$ can be called *quasi-implication*. Both the intuitionistic and classical implications are examples of such. The quasi-implication of **P** itself will be called the *primal implication*. Sometimes it would be convenient to denote it $\rightarrow_p$ to distinguish from the intuitionistic implication. One possible interpretation would be to say that $\varphi \rightarrow_p \psi$ denotes *an arbitrary* infon θ such that ψ yields θ and $\theta \wedge \varphi$ yields ψ. This reading will be supported by the formal notion of *primal model*, see below.

Let **qP** denote the *primal infon logic*, that is, the extension of primal logic to the language with quotations, when the rules (`Said`) and (`Implied`) are added. There is a linear time algorithm deciding whether $\Gamma \vdash \varphi$ provided Γ and φ have quotation depth bounded by a constant [21]. Despite its restrictions on the implication and quotation depth this logic turns out to be sufficiently expressive for many practical purposes.

Introducing disjunction and negation. Some scenarios we would like to formalize in DKAL presuppose the use of disjunction and negation. Disjunction is a way of combining information related to hiding it. When you say *'There is a coin in my left or in my right pocket'* you essentially communicate a disjunction of two pieces of information (you can have a coin in each pocket). The rules of handling disjunctions are the usual ones: the introduction rules

$$\frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi}\ (\vee I_l) \qquad \frac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \vee \psi}\ (\vee I_r)$$

are applied when wrapping an infon into a disjunction (they can be called *hiding rules*). The receiver can use disjunction $\theta \vee \psi$ by the following rule: if φ can be inferred separately from θ and from ψ, and disjunction $\theta \vee \psi$ is known, then one can infer φ. Proof-theoretically this amounts to the usual disjunction elimination rule:

$$\frac{\Gamma, \theta \vdash \varphi \quad \Gamma, \psi \vdash \varphi \quad \Gamma \vdash \theta \vee \psi}{\Gamma \vdash \varphi}\ (\vee E)$$

When speaking about disjunction in infon logic we will assume all three of the above rules. We also remark that the rule $(\vee E)$, as well as $(\rightarrow I)$, involves 'cancelation' of some hypotheses and, thus, it is not *hilbertian* in the sense of [11].

Introducing negation into the language of infon logic is a more delicate matter. Here we consider the most straightforward approach to negation in infon logic corresponding to intuitionistic negation. This has been sufficient in practice. As we gain more experience in the use of DKAL, we will see whether the other, possibly stronger, forms of negation are needed.

Negation $\neg\varphi$ in intuitionistic logic is often introduced as an abbreviation for $\varphi \rightarrow \bot$, where $\bot$ is the constant **false**. The other way around, $\bot$ can be introduced, for example, as $\neg\top$, once one has the negation. In intuitionistic logic, the constant $\bot$ satisfies the principle *ex contradictio*:

$$(\bot) \qquad \bot \vdash \varphi,$$

for any φ. When this axiom is not assumed, that is, when we just have a constant $\bot$ without postulating any logical laws for it, we obtain the so-called *minimal logic* (see [33]).

What should be the infon-logical interpretation of $\bot$? It is natural to assume that $\bot$ represents inconsistent information, that is, the information that should be interpreted as an error. Obtaining this information a principal should go into the error-handling mode rather than continue its usual mode of operation. This interpretation of $\bot$ seems to call for the minimal logic rather than the intuitionistic logic axioms. In fact, having $\bot \vdash \varphi$ as an axiom might lead in some scenarios to unwanted communication between the principals.

Technically, the intuitionistic and the minimal logics are very close to each other (see e.g. [33]). Therefore, until we gain more experience in the practical use of infon logic to favor one of the two logics, we will treat both of them in parallel. Since in the minimal logic $\bot$ is as good as any other variable, we shall ignore the difference between such logics and the logics without $\bot$ and negation.

We shall use the following notation for various logics. Our basic propositional logics are **I** and **P**. We denote their extensions by the rules for $\vee$ and/or the axiom $(\bot)$ as $\mathbf{P}[\vee]$, $\mathbf{I}[\vee, \bot]$, etc. The presence of quotations is indicated by a **q** in front of the logic name, for example, $\mathbf{qP}[\vee, \bot]$.

3 Primal logic with disjunction: semantics and complexity

A complete Kripke-style semantics for primal logic **P** was developed in [21]. Here we simplify it by showing that the completeness result holds for a very particular class of models that we call *quasi-boolean*. We define these models for the language with disjunction, that is, for $\mathbf{P}[\vee]$. In Section 5 this semantics is extended to the language with quotations.

A notable feature of primal logic is that it does not respect substitution of equivalents. For example, as we will see shortly, one cannot derive in **P**

$$Q \to (P \wedge P) \vdash Q \to P. \tag{1}$$

This means that a complete semantics for primal logic cannot be *compositional* in the sense that the meaning of an implication $\varphi \to \psi$ is determined by the meanings of the formulas φ and ψ. The quasi-boolean models defined below are a non-compositional analog of the usual $\{0,1\}$-valued semantics for classical propositional logic.

Definition 3.1 A *valuation* v is a map assigning 0 or 1 to each propositional variable, as well as to each implication $\varphi \to \psi$ of the language of primal logic (with disjunction). Valuation v naturally extends to all formulas by applying the usual truth tables for $\wedge$, $\vee$ and by letting $v(\top) = 1$. A formula φ is *valid under* v if $v(\varphi) = 1$, which is denoted $\vDash_v \varphi$. For a set of formulas Γ we write $\vDash_v \Gamma$ iff $\vDash_v \varphi$, for all $\varphi \in \Gamma$.

We say that v is *quasi-boolean* if, for each implication $\varphi \to \psi$,

(i) If $\vDash_v \psi$, then $\vDash_v (\varphi \to \psi)$;

(ii) If $\vDash_v (\varphi \to \psi)$, then either $\nvDash_v \varphi$ or $\vDash_v \psi$.

Notice that the classical material implication is defined by postulating an equivalence in (ii), whereas (i) is just a half of the converse implication.

Valuations satisfying

$$\vDash_v (\varphi \to \psi) \quad \text{iff} \quad (\nvDash_v \varphi \text{ or } \vDash_v \psi)$$

will be called *classical*. The following is a strong form of soundness and completeness theorem for primal logic.

Theorem 1 *$\Gamma \vdash \varphi$ holds in $\mathbf{P}[\vee]$ iff $\vDash_v \Gamma$ implies $\vDash_v \varphi$ for all quasi-boolean valuations v.*

Proof. The soundness part is a routine check. To show the completeness we apply a variant of the usual canonical model argument.

A set of formulas F is called a *theory* if, for all formulas ψ, $F \vdash \psi$ implies $\psi \in F$, that is, if F is deductively closed. The following lemma has a standard proof.

Lemma 3.2 *Any set of formulas Γ such that $\Gamma \nvdash \psi$ can be extended to a maximal theory $F \supseteq \Gamma$ such that $F \nvdash \psi$.*

Assume $\Gamma \nvdash \varphi$ and let F be a maximal theory such that $\Gamma \subseteq F$ and $F \nvdash \varphi$.

Lemma 3.3 *For all ψ_1, ψ_2,*

$$(\psi_1 \vee \psi_2) \in F \iff (\psi_1 \in F \text{ or } \psi_2 \in F).$$

Proof. ($\Leftarrow$) If $\psi_1 \in F$ then $F \vdash \psi_1 \vee \psi_2$ by $(\vee I)$, hence $(\psi_1 \vee \psi_2) \in F$, since F is deductively closed.

($\Rightarrow$) If $\psi_1, \psi_2 \notin F$, then $F, \psi_1 \vdash \varphi$ and $F, \psi_2 \vdash \varphi$ by maximality. Hence, $F, \psi_1 \vee \psi_2 \vdash \varphi$ by $(\vee E)$ contradicting $(\psi_1 \vee \psi_2) \in F$. $\boxtimes$

We define a valuation v by

$$v(A) = 1 \overset{\text{def}}{\iff} A \in F,$$

for each variable or implication A.

Lemma 3.4 *For every formula ψ, $\vDash_v \psi \iff \psi \in F$.*

Proof. Induction on the build-up of ψ. The claim is obvious if ψ is a variable, an implication, or the constant $\top$.

Suppose $\psi = (\psi_1 \wedge \psi_2)$. By the induction hypothesis we have:

$$\vDash_v \psi \iff (\vDash_v \psi_1 \text{ and } \vDash_v \psi_2) \iff (\psi_1 \in F \text{ and } \psi_2 \in F).$$

Since F is deductively closed, $\psi_1, \psi_2 \in F \iff (\psi_1 \wedge \psi_2) \in F \iff \psi \in F$.

Suppose $\psi = (\psi_1 \vee \psi_2)$. Then

$$\vDash_v \psi \iff (\vDash_v \psi_1 \text{ or } \vDash_v \psi_2) \iff (\psi_1 \in F \text{ or } \psi_2 \in F) \iff (\psi_1 \vee \psi_2) \in F,$$

by Lemma 3.3. $\boxtimes$

By this lemma we can conclude that $\vDash_v \Gamma$ and $\nvDash_v \varphi$. We can also easily check that v is quasi-boolean. Consider an implication $\theta \to \psi$.

(i) If $\models_v \psi$ then $\psi \in F$, hence $(\theta \to \psi) \in F$ by $(\to P)$ and $\models_v \theta \to \psi$.

(ii) If $\models_v \theta$ and $\models_v (\theta \to \psi)$, then $\theta, (\theta \to \psi) \in F$, hence $\psi \in F$ by $(\to E)$ and $\models_v \psi$.

This completes the proof of the theorem. $\boxtimes$

We remark that to define a quasi-boolean valuation v falsifying $\Gamma \vdash \varphi$ it is sufficient to only specify it on the variables and the implications contained in $\Gamma \cup \{\varphi\}$. We can illustrate the use of this semantics by exhibiting a quasi-boolean valuation falsifying (1). In fact, it is sufficient to put $v(P) = v(Q) = v(Q \to P) = 0$ and $v(Q \to (P \wedge P)) = 1$.

As an application of quasi-boolean semantics we prove that the primal logic shares with the intuitionistic logic its fundamental *disjunction property*. Our method of constructing a quasi-boolean model is similar to the so-called *Aczel slash*, see [33]. In some sense quasi-boolean models clarify this somewhat mysterious operation.

Recall that the set of *Harrop formulas* H is defined by the following grammar:

$$H ::= \top \mid P \mid H \wedge H \mid A \to H \qquad P \text{ a variable, } A \text{ a formula}$$

Theorem 2 (disjunction property) *If Γ is a set of Harrop formulas and $\Gamma \vdash \varphi \vee \psi$ in $\mathbf{P}[\vee]$, then $\Gamma \vdash \varphi$ or $\Gamma \vdash \psi$.*

Proof. For any set of formulas Γ we inductively define a valuation v (Aczel slash) as follows:

- $v(P) = 1 \iff \Gamma \vdash P$, if P is a variable;
- $v(\varphi \to \psi) = 1 \iff (\Gamma \vdash (\varphi \to \psi)$ and $(\not\models_v \varphi$ or $\models_v \psi))$.

We remark that $\models_v \varphi$ is usually written as $\Gamma | \varphi$ in the intuitionistic literature. It is easy to check the following property by induction on the build-up of φ.

Lemma 3.5 *If $\models_v \varphi$ then $\Gamma \vdash \varphi$, for any formula φ.*

As an immediate corollary we obtain that v is quasi-boolean. In fact, condition (i) holds because $\models_v \psi$ implies $\Gamma \vdash \psi$ and hence $\Gamma \vdash \varphi \to \psi$; therefore $v(\varphi \to \psi) = 1$. Condition (ii) is immediate from the definition of v.

Next we show that Harrop formulas are well-behaved in this model.

Lemma 3.6 *If φ is Harrop, then*

$$\models_v \varphi \iff \Gamma \vdash \varphi.$$

Proof. The implication ($\Rightarrow$) always holds by the previous lemma. To prove ($\Leftarrow$) we argue by induction on the build-up of φ. The cases when φ is $\top$, a variable or a conjunction are easy. Suppose $\varphi = (\theta \to \psi)$ with ψ Harrop. We have to show that $\nvDash_v \theta$ or $\vDash_v \psi$. Suppose $\vDash_v \theta$, then $\Gamma \vdash \theta$. Since we also assume $\Gamma \vdash (\theta \to \psi)$ we have $\Gamma \vdash \psi$ and by the induction hypothesis $\vDash_v \psi$. $\boxtimes$

Now suppose Γ is Harrop and $\Gamma \vdash \varphi \vee \psi$. For any $\theta \in \Gamma$ we have $\Gamma \vdash \theta$, hence $\vDash_v \theta$ by Lemma 3.6. By the soundness theorem it follows that $\vDash_v \varphi \vee \psi$, hence $\vDash_v \varphi$ or $\vDash_v \psi$. By Lemma 3.5 this implies $\Gamma \vdash \varphi$ or $\Gamma \vdash \psi$. $\boxtimes$

Remark 3.7 All of the above works for the logic $\mathbf{P}[\vee, \bot]$. One only has to stipulate in this case that $\bot$ is always evaluated as 0.

4 Reductions between primal and classical logic

In spite of the above, the quasi-boolean semantics shows that primal logic is in some respects akin to classical logic. We define polynomial translations from one logic to the other assuming disjunction to be present in the language. This shows, in particular, that the derivability problem for $\mathbf{P}[\vee]$ is co-NP-complete.

We assume that classical logic $\mathbf{C}$ is formalized in the language of $\mathbf{P}[\vee]$ with a distinguished variable $\bot$ for falsity. For a given formula A let $H(A)$ denote the conjunction of the following formulas:

(i) $\varphi \vee (\varphi \to \psi)$, for all subformulas $\varphi \to \psi$ of A;

(ii) $\bot \to Q$, for all variables Q of A.

Proposition 4.1 $\mathbf{C} \vdash A$ *iff* $H(A) \vdash A$ *is provable in* $\mathbf{P}[\vee]$.

Proof. The (if) part is clear, since $H(A)$ is classically valid.

(only if) Suppose $H(A) \nvdash A$. There is a quasi-boolean valuation for which $\vDash H(A)$ and $\nvDash A$. We have to show that it is, in fact, a classical boolean valuation. For each subformula $\varphi \to \psi$ of A we have:

$$\vDash (\varphi \to \psi) \iff (\nvDash \varphi \text{ or } \vDash \psi).$$

Indeed, the implication ($\Rightarrow$) always holds, and $\vDash \psi$ implies $\vDash \varphi \to \psi$. If $\nvDash \varphi$ then, since $\vDash (\varphi \to \psi) \vee \varphi$, we also have $\vDash \varphi \to \psi$.

It remains for us to check that $\bot$ is evaluated as 0. By induction on the build-up of an arbitrary formula ψ (of positive logic) it is easy to show that

$\models \psi$ whenever $\models Q$, for each variable Q of ψ. Since we have $\not\models A$, this means that some variable P of A must be false. But the formula $\bot \to P$ is true, hence $\bot$ is false. $\boxtimes$

Theorem 3 *The derivability problem for primal logic with disjunction is* co-NP*-complete.*

Proof. Since the length of $H(A)$ is polynomial in the length of A, the hardness follows from the above proposition. It is also clear that the non-derivability problem for primal logic is in NP. In fact, we can verify $\Gamma \not\vdash \varphi$ by non-deterministically guessing a quasi-boolean valuation, which is polynomial in the size of φ, then checking that it satisfies the conditions of being quasi-boolean, and computing the truthvalues of Γ and φ. $\boxtimes$

Remark 4.2 The same result can be obtained by a somewhat simpler translation: $\mathbf{C} \vdash A$ iff $H_0(A) \vdash A \vee \bot$ in primal logic, where $H_0(A)$ only consists of formulas (i) in the definition of $H(A)$.

Remark 4.3 The use of disjunction is necessary for such an effective reduction, because of the linear time complexity bound established for $\mathbf{P}$ in [21].

Next we show that $\mathbf{P}[\vee, \bot]$ (and hence $\mathbf{P}[\vee]$) is effectively reducible to $\mathbf{C}$, and $\mathbf{P}$ is effectively reducible to the Horn fragment of $\mathbf{C}$.

Suppose we want to check whether $\Gamma \vdash A$ in primal logic. We introduce a fresh variable P_φ for each subformula φ of a formula in $\Gamma \cup \{A\}$. Let Φ be the union of the following sets of formulas:

1. $\left\{ \begin{array}{l} P_{\varphi\to\psi} \wedge P_\varphi \to P_\psi \\ P_\psi \to P_{\varphi\to\psi} \end{array} \right.$, for each subformula $\varphi \to \psi$ of A;
2. $\left\{ \begin{array}{l} P_{\varphi\wedge\psi} \to P_\varphi, \quad P_{\varphi\wedge\psi} \to P_\psi, \\ P_\varphi \wedge P_\psi \to P_{\varphi\wedge\psi} \end{array} \right.$, for each subformula $\varphi \wedge \psi$ of A;
3. $\left\{ \begin{array}{l} P_\varphi \to P_{\varphi\wedge\psi}, \quad P_\psi \to P_{\varphi\vee\psi}, \\ P_{\varphi\vee\psi} \to (P_\varphi \vee P_\psi), \end{array} \right.$, for each subformula $\varphi \vee \psi$ of A;
4. $P_\top; \quad P_\bot \to P_A$.

Let φ^* denote P_φ, and let $\Gamma^* = \{P_\varphi : \varphi \in \Gamma\}$.

Proposition 4.4 $\Gamma \vdash A$ *in* $\mathbf{P}[\vee, \bot]$ *iff* $\Gamma^*, \Phi \vdash A^*$ *in* $\mathbf{C}$.

Proof. ($\Leftarrow$) Suppose $\Gamma \not\vdash A$. Let v be a quasi-boolean valuation such that $\models_v \Gamma$ and $\not\models_v A$. Define a classical valuation v' on propositional variables P_φ by $v'(P_\varphi) := v(\varphi)$. Obviously, $\models_{v'} \Gamma^*$ and $\not\models_{v'} A^*$. Since v is quasi-boolean, we also have $\models_{v'} \Phi$. Hence, $\Gamma^*, \Phi \not\vdash A^*$ in classical logic.

($\Rightarrow$) Suppose $\Gamma^*, \Phi \not\vdash A^*$ in $\mathbf{C}$. Let v be a classical valuation such that $\models_v \Gamma^*, \Phi$ and $\not\models_v A^*$. Define a valuation v' by $v'(\psi) := v(\psi^*)$, for each variable or implication ψ.

Let θ be a subformula of a formula in $\Gamma \cup \{A\}$. We claim that

$$v'(\theta) = v(\theta^*).$$

The claim is proved by a straightforward induction on the build-up of θ. It is obvious if θ is $\top$, a variable or an implication.

If θ is $\bot$ we have $\models_v (\bot^* \to A^*)$, since $\bot^* \to A^*$ is in Φ. Since $\not\models_v A^*$ we have $v(\bot^*) = 0 = v'(\bot)$.

If θ is a conjunction or a disjunction we use the validity of parts 2 and 3 of Φ, respectively.

Finally, using the validity of part 1 of Φ we check that v' is quasi-boolean. Suppose $\varphi \to \psi$ is a subformula of a formula in $\Gamma \cup \{A\}$.

(i) If $\models_{v'} \psi$ then $\models_v \psi^*$ by the claim. We have $\models_v (\varphi \to \psi)^*$ by the second part of 1, hence $\models_{v'} (\varphi \to \psi)$.

(ii) Similarly, if $\models_{v'} (\varphi \to \psi)$ then $\models_v (\varphi \to \psi)^*$. By the first part of 1, either $\not\models_v \varphi^*$ or $\models_v \psi^*$. Hence, $\not\models_{v'} \varphi$ or $\models_{v'} \psi$. $\boxtimes$

Next we remark that the above reduction is quite efficient. As usual, we consider linear time computations within the PRAM model. We denote by $\Gamma \Rightarrow A$ a formal expression consisting of a finite set of hypotheses Γ followed by conclusion A.

Lemma 4.5 *There is a linear-time algorithm producing on input $\Gamma \Rightarrow A$ the output $\Gamma^*, \Phi \Rightarrow A^*$.*

Proof. Run a parser on the input string (of length n) producing a parse tree. The subtrees of the formulas in Γ and the one of A hang immediately under the root. Each node of the parse tree has a label representing a variable or a connective. The label length can be assumed to be $O(\log(n))$. Extra tags mark the hypotheses in Γ and the query A.

Each variable P_φ in the translation will be represented by (the name of) a node of the parse tree, except for the root. Thus, we consider an obvious variant of the translation in Proposition 4.4 where new variables

are assigned to all *occurrences* of subformulas in $\Gamma \cup \{A\}$ rather than to subformulas themselves.

Run through the parse tree visiting each node once (in whatever order). For each node write down the formulas of the groups 1–4 depending on the label of the node. Notice that each variable P_ψ occurs in Φ no more than 6 times: at most 3 times in a group where P_ψ is the main variable, and at most 3 times in a group where it is a secondary variable. Hence, the total number of steps needed to write down Φ is linear in the sum of the lengths of all new variables. The latter, however, does not exceed the total size of the representation of the tree, which is linear in the size n of the original input. $\boxtimes$

Recall that a *Horn clause* is a variable or a formula of the form $P_1 \wedge P_2 \wedge \cdots \wedge P_n \to Q$, where $P_1, \ldots, P_n, Q$ are variables. We notice that if Γ and A are in the language without disjunction, then the translation $\Gamma^*, \Phi \Rightarrow A^*$ consists of Horn clauses. It is well-known that the satisfiability problem for a set of Horn clauses in classical logic is solvable in linear time (see [25]). As a corollary we obtain that the derivability problem for primal logic is in linear time. This fact was proved by Gurevich and Neeman [21] using a different method.

Corollary 4.6 *For the language without disjunction, there is a linear time algorithm to determine whether* $\Gamma \vdash A$ *in* $\mathbf{P}$.

5 Primal logic with disjunction and quotations: sequent calculus and cut-elimination

In this section we study the logic $\mathbf{qP}[\vee, \bot]$. We introduce a Gentzen-style sequent calculus and a Kripke-style semantics, and we prove a cut-elimination theorem as well as a soundness and completeness theorem. Gentzen-style systems without $\bot$, $\vee$ or the quotations can be obtained by ignoring the respective connectives everywhere below.

Sequents are objects of the form $\Gamma \Rightarrow \Delta$, where Γ and Δ are finite sets of formulas. The rules of primal, intuitionistic and classical sequent calculus are all the same, except for the rules $(\to R)$ of introduction of implication to the right.

Axioms: $\varphi \Rightarrow \varphi$; $\quad \Rightarrow \top$; $\quad \bot \Rightarrow$;

Inference rules:

$$\frac{\Gamma \Rightarrow \Delta, \varphi \quad \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \wedge \psi}\ (\wedge R) \qquad \frac{\Gamma, \varphi, \psi \Rightarrow \Delta}{\Gamma, \varphi \wedge \psi \Rightarrow \Delta}\ (\wedge L)$$

$$\frac{\Gamma, \varphi \Rightarrow \Delta \quad \Gamma, \psi \Rightarrow \Delta}{\Gamma, \varphi \vee \psi \Rightarrow \Delta} \ (\vee L) \qquad \frac{\Gamma \Rightarrow \Delta, \varphi, \psi}{\Gamma \Rightarrow \Delta, \varphi \vee \psi} \ (\vee R)$$

$$\frac{\Gamma, \psi \Rightarrow \Delta \quad \Gamma \Rightarrow \Delta, \varphi}{\Gamma, \varphi \to \psi \Rightarrow \Delta} \ (\to L)$$

The $(\to R)$ rules for the three logics respectively are

$$\frac{\Gamma \Rightarrow \psi, \Delta}{\Gamma \Rightarrow \varphi \to \psi, \Delta} \ (\to R_p) \qquad \frac{\Gamma, \varphi \Rightarrow \psi}{\Gamma \Rightarrow \varphi \to \psi} \ (\to R_i) \qquad \frac{\Gamma, \varphi \Rightarrow \psi, \Delta}{\Gamma \Rightarrow \varphi \to \psi, \Delta} \ (\to R_c)$$

Within this framework, the rules for quotations look the same as the corresponding natural deduction-style rules:

$$\frac{\Gamma \Rightarrow \varphi}{q\,\texttt{said}\,\Gamma \Rightarrow q\,\texttt{said}\,\varphi} \ (\texttt{Said}) \qquad \frac{\Gamma, \Delta \Rightarrow \varphi}{q\,\texttt{said}\,\Gamma,\ q\,\texttt{implied}\,\Delta \Rightarrow q\,\texttt{implied}\,\varphi} \ (\texttt{Implied})$$

We also posit the rules of weakening and cut:

$$\frac{\Gamma \Rightarrow \Delta}{\Gamma, \Gamma_1 \Rightarrow \Delta, \Delta_1} \ (\texttt{Weaken}) \qquad \frac{\Gamma \Rightarrow \Delta, \varphi \quad \varphi, \Gamma_1 \Rightarrow \Delta_1}{\Gamma, \Gamma_1 \Rightarrow \Delta, \Delta_1} \ (\texttt{Cut})$$

The systems described above will be denoted **GP** (primal), **GI** (intuitionistic), and **GC** (classical). Checking that they axiomatize the respective logics under the interpretation of $\Gamma \Rightarrow \Delta$ as $\Gamma \vdash \bigvee \Delta$ is routine. The cut-rule can be eliminated in all these systems. This can be done both syntactically and semantically. The syntactical argument (in either case) is more tedious, but it is constructive and differs only slightly from the standard proof of the cut-elimination theorem due to Gentzen, see [9] for some details. In contrast, the semantical argument also delivers completeness theorems for these calculi and shall be presented (for the case of primal logic) in the next section.

Theorem 4 *Let L be any of the Gentzen-style systems* **GP**, **GI** *or* **GC**. *A sequent $\Gamma \Rightarrow \Delta$ is provable in L iff it is provable in L without a cut.*

Proof. We essentially follow the standard proof-reduction strategy due to Gentzen. It is sufficient to show that cuts can be eliminated in any proof containing a single cut as the last inference rule. The *grade* $g(d)$ and the *rank* $r(d)$ of such a proof d are defined as usual: Let $|\psi|$ denote the height of the parse tree of a formula ψ. Then $g(d) := |\theta|+1$ where θ is the cut-formula in d, and $r(d)$ is the sum of heights of the right and the left proof subtrees of d.

The proof of cut-elimination goes by induction on the grade and a subsidiary induction on the rank of d. If θ has not been introduced in d on both sides of the cut-rule immediately before the cut, we can obviously decrease

the rank of d. If θ is on the one side part of an axiom or is introduced by weakening, the rank of the proof can also be decreased. The proof transformations in the cases when θ is a conjunction, a disjunction or an implication (in the cases of classical and intuitionistic logics) are standard. Thus, it is sufficient to consider the case $\theta = (\varphi \to \psi)$ for **GP**, and the cases of quotations $\theta = q\,\texttt{said}\,\varphi$ and $\theta = q\,\texttt{implied}\,\varphi$ which in all three logics are treated in the same way.

If $\theta = (\varphi \to \psi)$ the end-piece of the proof d must have the form

$$\dfrac{\dfrac{\Gamma \Rightarrow \psi, \Delta}{\Gamma \Rightarrow \varphi \to \psi, \Delta}\,(\to R_p) \quad \dfrac{\Gamma_1, \psi \Rightarrow \Delta_1 \quad \Gamma_1 \Rightarrow \Delta_1, \varphi}{\Gamma_1, \varphi \to \psi \Rightarrow \Delta_1}\,(\to L)}{\Gamma, \Gamma_1 \Rightarrow \Delta, \Delta_1}\,(\texttt{Cut})$$

We can reduce it to a proof-tree with a lower grade to which the induction hypothesis is applicable:

$$\dfrac{\Gamma \Rightarrow \psi, \Delta \quad \Gamma_1, \psi \Rightarrow \Delta_1}{\Gamma, \Gamma_1 \Rightarrow \Delta, \Delta_1}\,(\texttt{Cut})$$

To enhance the readability we shall locally write $\Box$ and $\triangle$ for $q\,\texttt{said}$ and $q\,\texttt{implied}$, respectively.

If $\theta = \Box\varphi$ is introduced on both sides of the cut, the left rule must be (`Said`) and the right one either (`Said`) or (`Implied`). Both cases are similar, so we only consider the latter. Then the end-piece of d has the form

$$\dfrac{\dfrac{\Gamma \Rightarrow \varphi}{\Box\Gamma \Rightarrow \Box\varphi}\,(\texttt{Said}) \quad \dfrac{\varphi, \Gamma_1, \Gamma_2 \Rightarrow \psi}{\Box\varphi, \Box\Gamma_1, \triangle\Gamma_2 \Rightarrow \triangle\psi}\,(\texttt{Implied})}{\Box\Gamma, \Box\Gamma_1, \triangle\Gamma_2 \Rightarrow \triangle\psi}\,(\texttt{Cut})$$

We reduce this proof to the following one of lower grade:

$$\dfrac{\dfrac{\Gamma \Rightarrow \varphi \quad \varphi, \Gamma_1, \Gamma_2 \Rightarrow \psi}{\Gamma, \Gamma_1, \Gamma_2 \Rightarrow \psi}\,(\texttt{Cut})}{\Box\Gamma, \Box\Gamma_1, \triangle\Gamma_2 \Rightarrow \triangle\psi}\,(\texttt{Implied})$$

The case $\theta = \triangle\varphi$ is similar; the end-piece of d must have the form

$$\dfrac{\dfrac{\Sigma_1, \Sigma_2 \Rightarrow \varphi}{\Box\Sigma_1, \triangle\Sigma_2 \Rightarrow \triangle\varphi}\,(\texttt{Implied}) \quad \dfrac{\varphi, \Gamma_1, \Gamma_2 \Rightarrow \psi}{\triangle\varphi, \Box\Gamma_1, \triangle\Gamma_2 \Rightarrow \triangle\psi}\,(\texttt{Implied})}{\Box\Sigma_1, \triangle\Sigma_2, \Box\Gamma_1, \triangle\Gamma_2 \Rightarrow \triangle\psi}\,(\texttt{Cut})$$

We reduce this proof to the following one of lower grade:

$$\dfrac{\dfrac{\Sigma_1, \Sigma_2 \Rightarrow \varphi \quad \varphi, \Gamma_1, \Gamma_2 \Rightarrow \psi}{\Sigma_1, \Sigma_2, \Gamma_1, \Gamma_2 \Rightarrow \psi}\,(\texttt{Cut})}{\Box\Sigma_1, \triangle\Sigma_2, \Box\Gamma_1, \triangle\Gamma_2 \Rightarrow \triangle\psi}\,(\texttt{Implied})$$

This completes our sketch of a proof of Theorem 4. ⊠

We note some standard corollaries. Firstly, **GP** without cut enjoys the subformula property: if $\Gamma \Rightarrow \Delta$ occurs in a cut-free derivation of $\Gamma_0 \Rightarrow \Delta_0$, then Γ and Δ only contain the subformulas of the formulas in $\Gamma_0 \cup \Delta_0$. In fact, the set of all subformulas here can be replaced by a somewhat narrower set of *primal subformulas*.

Definition 5.1 We define the sets of the *left* $L(\varphi)$ and the *right* $R(\varphi)$ primal subformulas of a formula φ. (These are subsets of the sets of the negatively and of the positively occurring subformulas of φ, respectively.)

- $L(\varphi) = \varnothing$ and $R(\varphi) = \{\varphi\}$, if φ is a variable or a constant;
- If $\varphi = (\varphi_1 \wedge \varphi_2)$ or $\varphi = (\varphi_1 \vee \varphi_2)$, then

$$\begin{aligned} L(\varphi) &= L(\varphi_1) \cup L(\varphi_2), \\ R(\varphi) &= \{\varphi\} \cup R(\varphi_1) \cup R(\varphi_2); \end{aligned}$$

- If $\varphi = (\varphi_1 \to \varphi_2)$ then

$$\begin{aligned} L(\varphi) &= R(\varphi_1) \cup L(\varphi_2), \\ R(\varphi) &= \{\varphi\} \cup R(\varphi_2). \end{aligned}$$

- If $\varphi = (q\,\texttt{said}\,\varphi_1)$ or $\varphi = (q\,\texttt{implied}\,\varphi_1)$ then

$$L(\varphi) = L(\varphi_1), \quad R(\varphi) = \{\varphi\} \cup R(\varphi_1).$$

For a set of formulas Γ define

$$\begin{aligned} L(\Gamma) &= \bigcup\{L(\varphi) : \varphi \in \Gamma\}, \\ R(\Gamma) &= \bigcup\{R(\varphi) : \varphi \in \Gamma\}. \end{aligned}$$

A *primal subformula* of φ is either its left or its right primal subformula.

Proposition 5.2 *If* $\Gamma \Rightarrow \Delta$ *occurs in a cut-free derivation in* **GP** *of a sequent* $\Gamma_0 \Rightarrow \Delta_0$*, then* $\Delta \subseteq L(\Gamma_0) \cup R(\Delta_0)$ *and* $\Gamma \subseteq R(\Gamma_0)$*.*

Proof. The proof goes by a routine induction on the length of a cut-free proof of $\Gamma_0 \Rightarrow \Delta_0$. We only treat the cases of the implication and the quotation rules.

Suppose $\Delta_0 = \Delta_1, \varphi \to \psi$ and the last application of a rule in the derivation of $\Gamma_0 \Rightarrow \Delta_0$ has the form

$$\frac{\Gamma_0 \Rightarrow \Delta_1, \psi}{\Gamma_0 \Rightarrow \Delta_1, \varphi \to \psi}\ (\to R)$$

If $\Gamma \Rightarrow \Delta$ coincides with $\Gamma_0 \Rightarrow \Delta_0$, the claim is obvious. Otherwise, $\Gamma \Rightarrow \Delta$ occurs in the proof of $\Gamma_0 \Rightarrow \Delta_1, \psi$. By the induction hypothesis $\Gamma \subseteq R(\Gamma_0)$ and $\Delta \subseteq L(\Gamma_0) \cup R(\Delta_1) \cup R(\psi)$. However, $R(\psi) \subseteq R(\varphi \to \psi) \subseteq R(\Delta_0)$. Hence, the claim.

Suppose $\Gamma_0 = \Gamma_1, \varphi \to \psi$ and the last application of a rule in the derivation of $\Gamma_0 \Rightarrow \Delta_0$ has the form

$$\frac{\Gamma_1 \Rightarrow \Delta_0, \varphi \quad \Gamma_1, \psi \Rightarrow \Delta_0}{\Gamma_1, \varphi \to \psi \Rightarrow \Delta_0}\ (\to L)$$

Suppose $\Gamma \Rightarrow \Delta$ occurs in the proof of $\Gamma_1 \Rightarrow \Delta_0, \varphi$. By the induction hypothesis $\Gamma \subseteq R(\Gamma_1)$ and $\Delta \subseteq L(\Gamma_1) \cup R(\Delta_0) \cup R(\varphi)$. However, $R(\varphi) \subseteq L(\varphi \to \psi) \subseteq L(\Gamma_0)$. Hence, $\Delta \subseteq L(\Gamma_0) \cup R(\Delta_0)$.

If $\Gamma \Rightarrow \Delta$ occurs in the proof of $\Gamma_1, \psi \Rightarrow \Delta_0$, then by the induction hypothesis $\Gamma \subseteq R(\Gamma_1) \cup R(\psi)$ and $\Delta \subseteq L(\Gamma_1) \cup R(\Delta_0) \cup L(\psi)$. We have $R(\psi) \subseteq R(\varphi \to \psi) \subseteq R(\Gamma_0)$, hence $\Gamma \subseteq R(\Gamma_0)$. On the other hand, $L(\psi) \subseteq L(\varphi \to \psi) \subseteq L(\Gamma_0)$, hence $\Delta \subseteq L(\Gamma_0) \cup R(\Delta_0)$.

Suppose the last inference in the proof is

$$\frac{\Gamma_1, \Delta_1 \Rightarrow \varphi}{q\,\mathtt{said}\,\Gamma_1, q\,\mathtt{implied}\,\Delta_1 \Rightarrow q\,\mathtt{implied}\,\varphi}$$

Here $\Gamma_0 = q\,\mathtt{said}\,\Gamma_1,\ q\,\mathtt{implied}\,\Delta_1$ and $\Delta_0 = \{q\,\mathtt{implied}\,\varphi\}$.

Suppose $\Gamma \Rightarrow \Delta$ occurs in the proof of $\Gamma_1, \Delta_1 \Rightarrow \varphi$. By the induction hypothesis $\Gamma \subseteq R(\Gamma_1) \cup R(\Delta_1)$ and $\Delta \subseteq L(\Gamma_1) \cup L(\Delta_1) \cup R(\varphi)$. Since $R(\Gamma_1) \subseteq R(q\,\mathtt{said}\,\Gamma_1)$ and $R(\Delta_1) \subseteq R(q\,\mathtt{implied}\,\Delta_1)$, we have $\Gamma \subseteq R(\Gamma_0)$. On the other hand, $L(\Gamma_1) \subseteq L(q\,\mathtt{said}\,\Gamma_1)$, $L(\Delta_1) \subseteq L(q\,\mathtt{implied}\,\Delta_1)$ and $R(\varphi) \subseteq R(q\,\mathtt{implied}\,\varphi)$. Hence, $\Delta \subseteq L(\Gamma_0) \cup R(\Delta_0)$.

All the other rules are treated similarly. ⊠

The standard proof-search procedure for a cut-free derivation in **GP** provides a PSPACE algorithm solving the derivability problem.

Corollary 5.3 *The derivability problem for* $\mathbf{qP}[\vee, \bot]$ *is in* PSPACE.

Proof. Here it is sufficient to notice that the number of nodes in any branch in a cut-free derivation of a sequent $\Gamma_0 \Rightarrow \Delta_0$ is bounded by the length n of that sequent, and the length of any sequent $\Gamma \Rightarrow \Delta$ occurring at any node in the proof-tree is polynomial in n by the subformula property. ⊠

6 Primal logic with disjunction and quotations: semantics and a completeness proof

Kripke semantics for the intuitionistic and primal infon logic was introduced in [21]. We define simpler Kripke models for primal infon logic.

Definition 6.1 A tuple $\mathcal{W} = (W, (S_q)_{q\in\mathcal{P}}, (I_q)_{q\in\mathcal{P}}, v)$ is called a primal Kripke *pre-model*, if $\mathcal{P}$ is the set of principals in the language and W is a non-empty set (of worlds). For each $q \in \mathcal{P}$, S_q and I_q are binary relations on W such that $S_q \subseteq I_q$; they correspond to modalities `said` and `implied`, respectively. v is a map assigning to each $x \in W$ a valuation v_x. In turn, v_x is a map assigning 0 or 1 to all the variables and implications of the language of primal logic with quotations.

Given a pre-model $\mathcal{W}$, the *validity relation* $x \vDash \varphi$ is defined, for each $x \in W$ and each formula φ, as follows:

1. $x \vDash \varphi \iff v_x(\varphi) = 1$, if φ is a variable or an implication;
2. $x \vDash \top, \quad x \nvDash \bot$;
3. $x \vDash \theta \wedge \psi \iff (x \vDash \theta \text{ and } x \vDash \psi)$;
4. $x \vDash \theta \vee \psi \iff (x \vDash \theta \text{ or } x \vDash \psi)$;
5. $x \vDash q\,\texttt{said}\,\psi \iff \forall y\,(xS_qy \Rightarrow y \vDash \psi)$;
6. $x \vDash q\,\texttt{implied}\,\psi \iff \forall y\,(xI_qy \Rightarrow y \vDash \psi)$.

We require that the validity relation satisfies the conditions of being quasi-boolean, for each $x \in W$:

(i) If $x \vDash \psi$ then $x \vDash (\varphi \to \psi)$;

(ii) If $x \vDash (\varphi \to \psi)$ then $(x \nvDash \varphi \text{ or } x \vDash \psi)$.

If the two conditions are satisfied for a given pre-model $\mathcal{W}$, we say that $\mathcal{W}$ is a *primal Kripke model*. A sequent $\Gamma \Rightarrow \Delta$ is *valid in* $\mathcal{W}$ if

$$\forall x \in W\,(x \vDash \bigwedge \Gamma \Rightarrow x \vDash \bigvee \Delta).$$

Remark 6.2 Even though the meaning of implication in primal logic is not compositional, Conditions (i) and (ii) relate the validity of an implication $\varphi \to \psi$ only to the validity of its simpler constituents φ and ψ. This allows to define a quasi-boolean valuation of implications from any given valuation

of variables selecting their values in any order respecting the subformula order on the implications. There is a lot of freedom in doing this. One possibility is the usual classical valuation. Another one is to always define $v(\varphi \to \psi) = v(\psi)$, which corresponds, in a sense, to the strongest quasi-implication. But there is a host of intermediate cases.

Theorem 5 *The following statements are equivalent:*

(i) $\Gamma \vdash \bigvee \Delta$ *holds in* $\mathbf{qP}[\vee, \bot]$*;*

(ii) $\Gamma \Rightarrow \Delta$ *is provable in* $\mathbf{GP}$*;*

(iii) $\Gamma \Rightarrow \Delta$ *is provable in* $\mathbf{GP}$ *without cut;*

(iv) $\Gamma \Rightarrow \Delta$ *is valid in all finite primal Kripke models;*

(v) $\Gamma \Rightarrow \Delta$ *is valid in all primal Kripke models.*

Proof. The implications (iii)⇒(ii), (ii)⇒(i), (v)⇒(iv), and (i)⇒(v) are routine. We only prove (iv)⇒(iii).

Suppose $\Gamma_0 \Rightarrow \Delta_0$ is not cut-free provable. We are going to construct a finite primal Kripke model $\mathcal{W}$ such that $\Gamma_0 \Rightarrow \Delta_0$ is not valid in $\mathcal{W}$.

Let $\mathcal{F}$ be the set of all subformulas of $\Gamma_0 \cup \Delta_0$. Sequents $\Gamma \Rightarrow \Delta$ with $\Gamma, \Delta \subseteq \mathcal{F}$ will be called *$\mathcal{F}$-sequents.*

Definition 6.3 Let $\Gamma \Rightarrow \Delta$ be an $\mathcal{F}$-sequent. $\Gamma \Rightarrow \Delta$ is called *saturated* if the following conditions hold for all $\varphi, \psi \in \mathcal{F}$:

1. $\varphi \wedge \psi \in \Gamma \Rightarrow \varphi, \psi \in \Gamma$;
2. $\varphi \wedge \psi \in \Delta \Rightarrow (\varphi \in \Delta$ or $\psi \in \Delta)$;
3. $\varphi \vee \psi \in \Gamma \Rightarrow (\varphi \in \Gamma$ or $\psi \in \Gamma)$;
4. $\varphi \vee \psi \in \Delta \Rightarrow \varphi, \psi \in \Delta$;
5. $(\varphi \to \psi) \in \Gamma \Rightarrow (\psi \in \Gamma$ or $\varphi \in \Delta)$;
6. $(\varphi \to \psi) \in \Delta \Rightarrow \psi \in \Delta$;
7. $\top \in \Gamma$, $\bot \in \Delta$.

Lemma 6.4 *Suppose $\Gamma \Rightarrow \Delta$ is an $\mathcal{F}$-sequent unprovable in* $\mathbf{GP}$ *without cut. Then there is a saturated $\mathcal{F}$-sequent $\Gamma' \Rightarrow \Delta'$ such that $\Gamma \subseteq \Gamma'$, $\Delta \subseteq \Delta'$ and $\Gamma' \Rightarrow \Delta'$ is unprovable without cut.*

Proof. The closure conditions 1–6 correspond to the inference rules of **GP** being read bottom-up. Therefore, these statements directly follow from the logical form of the rules in our Gentzen-style sequent calculus. In the case of 7 we have show that $\Gamma \Rightarrow \Delta$ is cut-free derivable if (and only if) so is $\Gamma, \top \Rightarrow \Delta$. This is easily checked by induction on the height of the cut-free derivation of $\Gamma, \top \Rightarrow \Delta$. The case of $\bot$ is similar. $\boxtimes$

Now we introduce the following notation. Let $s = (\Gamma \Rightarrow \Delta)$ be a sequent. Then s_0 denotes Γ and s_1 denotes Δ.

We define a Kripke model $\mathcal{W} = (W, (S_q)_{q \in \mathcal{P}}, (I_q)_{q \in \mathcal{P}}, v)$ as follows:

- W is the set of all cut-free unprovable saturated $\mathcal{F}$-sequents; further, for all $r, s \in W$,
- $sS_q r \iff^{\text{def}} \forall \varphi \, (q \, \texttt{said} \, \varphi \in s_0 \Rightarrow \varphi \in r_0)$;
- $sI_q r \iff^{\text{def}} \forall \varphi \, (q \, \texttt{implied} \, \varphi \in s_0 \Rightarrow \varphi \in r_0)$ and $sS_q r$.

The valuation v on $\mathcal{W}$ is defined by induction on the complexity of formulas. We introduce the following measure of formula complexity.

- $c(\varphi) = 0$, if φ is a variable or a constant;
- $c(\varphi \to \psi) = c(\psi) + 1$;
- $c(\varphi \wedge \psi) = c(\varphi \vee \psi) = \max(c(\varphi), c(\psi))$;
- $c(q \, \texttt{said} \, \varphi) = c(q \, \texttt{implied} \, \varphi) = c(\varphi)$.

By a *partial n-valuation* we mean a map assigning 0 or 1 to all variables and implications of complexity at most n at each node $s \in W$. If such a partial n-valuation is given, the corresponding validity relation $x \vDash_n \varphi$ is uniquely defined, for all formulas φ such that $c(\varphi) \leqslant n$, according to the clauses of Definition 6.1.

Therefore, by induction on n we can define partial n-valuations v^n on $\mathcal{W}$ as follows: for all $s \in W$,

- $v^n_s(P) = 1 \iff^{\text{def}} P \in s_0$, if P is a variable;
- $v^n_s(\varphi \to \psi) = 1 \iff^{\text{def}} ((\varphi \to \psi) \in s_0$ or $s \vDash_{n-1} \psi)$, if $c(\varphi \to \psi) \leqslant n$.

We notice that with n increasing the partial valuations v^n extend each other. Hence, in the limit we obtain a valuation v on $\mathcal{W}$ such that, for all $s \in W$ and all formulas φ, ψ (not necessarily from $\mathcal{F}$),

- $v_s(P) = 1 \stackrel{\text{def}}{\iff} P \in s_0$, if P is a variable;
- $v_s(\varphi \to \psi) = 1 \stackrel{\text{def}}{\iff} ((\varphi \to \psi) \in s_0 \text{ or } s \vDash \psi)$. $(*)$

This completes the definition of the model $\mathcal{W}$. Before showing that this model is, in fact, primal we prove the following lemma.

Lemma 6.5 *For all $s \in W$ and $\varphi \in \mathcal{F}$,*

(i) $\varphi \in s_0 \Rightarrow s \vDash \varphi$;

(ii) $\varphi \in s_1 \Rightarrow s \nvDash \varphi$.

Proof. If φ is a variable or a constant, both (a) and (b) are obvious.

Suppose $\varphi = (\theta \to \psi)$. If $(\theta \to \psi) \in s_0$ then trivially $s \vDash (\theta \to \psi)$ by $(*)$.

If $(\theta \to \psi) \in s_1$ then $\psi \in s_1$ since s is saturated. Hence, $s \nvDash \psi$ by the induction hypothesis. We also have $(\theta \to \psi) \notin s_0$, otherwise s would be provable. Thus, $s \vDash (\theta \to \psi)$ by $(*)$.

Suppose $\varphi = (\theta \wedge \psi)$. If $(\theta \wedge \psi) \in s_0$ then $\theta, \psi \in s_0$ by saturation, hence $s \vDash \psi, \theta$ and $s \vDash \theta \wedge \psi$ by the induction hypothesis.

If $(\theta \wedge \psi) \in s_1$ then $\theta \in s_1$ or $\psi \in s_1$ by saturation. Hence, $s \nvDash \psi$ or $s \nvDash \theta$, which implies $s \nvDash \theta \vee \psi$.

Suppose $\varphi = (\theta \vee \psi)$. If $(\theta \vee \psi) \in s_0$ then $\theta \in s_0$ or $\psi \in s_0$ by saturation. Hence, $s \vDash \psi$ or $s \vDash \theta$, which implies $s \vDash \theta \vee \psi$.

If $(\theta \vee \psi) \in s_1$ then $\theta, \psi \in s_1$ by saturation, hence $s \nvDash \psi, \theta$ and $s \nvDash \theta \vee \psi$.

Suppose $\varphi = (q \,\mathtt{said}\, \psi)$. (a) By definition of S_q, if sS_qr and $q \,\mathtt{said}\, \psi \in s_0$, then $\psi \in r_0$ and $r \vDash \psi$ by the induction hypothesis. Since this holds for any r, we obtain $s \vDash q \,\mathtt{said}\, \psi$ whenever $q \,\mathtt{said}\, \psi \in s_0$.

(b) Assume $q \,\mathtt{said}\, \psi \in s_1$. Let $\Gamma := \{\theta : q \,\mathtt{said}\, \theta \in s_0\}$. We claim that $\Gamma \Rightarrow \psi$ is cut-free unprovable. Otherwise, from $\Gamma \Rightarrow \psi$ one could infer

$$q \,\mathtt{said}\, \Gamma \Rightarrow q \,\mathtt{said}\, \psi,$$

and therefore s would be provable by weakening (we have $q \,\mathtt{said}\, \Gamma \subseteq s_0$ and $q \,\mathtt{said}\, \psi \in s_1$).

Let r be any saturated unprovable sequent with $\Gamma \subseteq r_0$ and $\psi \in r_1$. We have sS_qr by the definition of S_q and $r \nvDash \psi$ by the induction hypothesis. It follows that $s \nvDash q \,\mathtt{said}\, \psi$.

Suppose $\varphi = (q\,\mathtt{implied}\,\psi)$. Part (a) is similar to the previous case. We prove (b). Assume $q\,\mathtt{implied}\,\psi \in s_1$. Let

$$\Gamma := \{\theta : q\,\mathtt{said}\,\theta \in s_0 \text{ or } q\,\mathtt{implied}\,\theta \in s_0\}.$$

We claim that $\Gamma \Rightarrow \psi$ is cut-free unprovable. Otherwise, from $\Gamma \Rightarrow \psi$ by the rule (`Implied`) we could infer

$$\{q\,\mathtt{said}\,\theta, q\,\mathtt{implied}\,\xi : q\,\mathtt{said}\,\theta,\ q\,\mathtt{implied}\,\xi \in s_0\} \Rightarrow q\,\mathtt{implied}\,\psi,$$

from which s follows by weakening. Let r be an unprovable saturation of $\Gamma \Rightarrow \psi$. We have $sI_q r$ and $\psi \in r_1$, hence $s \nvDash q\,\mathtt{implied}\,\psi$. $\boxtimes$

Now we can check that $\mathcal{W}$ satisfies the conditions of being primal.

Lemma 6.6 *For any $(\varphi \to \psi) \in \mathcal{F}$ and any $s \in W$,*

(i) *if $s \vDash \psi$ then $s \vDash (\varphi \to \psi)$;*

(ii) *if $s \vDash (\varphi \to \psi)$ then ($s \nvDash \varphi$ or $s \vDash \psi$).*

Proof. Statement (i) is immediate from $(*)$. We prove (ii).

Suppose $s \vDash \varphi \to \psi$. Then, by $(*)$, either $(\varphi \to \psi) \in s_0$ or $s \vDash \psi$. If $s \vDash \psi$ we are done. If $(\varphi \to \psi) \in s_0$ then $\psi \in s_0$ or $\varphi \in s_1$ by the saturation of s. Hence, either $s \vDash \psi$ or $s \nvDash \varphi$ by the previous lemma. $\boxtimes$

To complete the proof of Theorem 5 recall that the given sequent $\Gamma_0 \Rightarrow \Delta_0$ is not cut-free provable. Let s be an unprovable saturation of $\Gamma_0 \Rightarrow \Delta_0$. By Lemma 6.5 we obtain $s \vDash \bigwedge \Gamma_0$ and $s \nvDash \bigvee \Delta_0$. Hence, $\Gamma_0 \Rightarrow \Delta_0$ is not valid in $\mathcal{W}$. $\boxtimes$

As an application of semantical completeness we now establish the disjunction property for $\mathbf{qP}[\vee, \bot]$. In fact, the Aczel slash method works here with just a few modifications.

The set of Harrop formulas for the language with quotations is now defined by the following grammar:

$$H ::= \top \mid \bot \mid P \mid H \wedge H \mid A \to H \mid q\,\mathtt{said}\,A \mid q\,\mathtt{implied}\,A$$

Here P is a variable, A is a formula, and q is a principal constant.

Theorem 6 (disjunction property) *If Γ is a set of Harrop formulas and $\Gamma \vdash \varphi \vee \psi$ in $\mathbf{qP}[\vee, \bot]$, then $\Gamma \vdash \varphi$ or $\Gamma \vdash \psi$.*

Proof. As in the proof of Theorem 2, with a given set Γ we inductively associate a valuation $v = v_\Gamma$ on the set of formulas of the language of $\mathbf{qP}[\vee, \bot]$:

- $v(\varphi) = 1 \iff \Gamma \vdash \varphi$, if φ is a variable or has the form $q\,\mathtt{said}\,\psi$ or $q\,\mathtt{implied}\,\psi$;
- $v(\varphi \to \psi) = 1 \iff (\Gamma \vdash (\varphi \to \psi)$ and $(\nvDash_v \varphi$ or $\vDash_v \psi))$;

In other words, we treat all formulas of the form $q\,\mathtt{said}\,\psi$ or $q\,\mathtt{implied}\,\psi$ as propositional atoms. We further proceed as in the proof of Theorem 2. Firstly, by an easy induction on φ we obtain

Lemma 6.7 *For any formula φ, if $\vDash_v \varphi$ then $\Gamma \vdash \varphi$.*

Then we establish the soundness lemma for provability in $\mathbf{qP}[\vee, \bot]$.

Lemma 6.8 *If $\Delta \vdash A$ and $\vDash_v \Delta$, then $\vDash_v A$.*

Proof. This is proved by a straightforward induction on the length of the proof of $\Delta \vdash A$. We only treat the cases of implication and quotation rules.

Suppose $\Delta \vdash (\varphi \to \psi)$ is obtained from $\Delta \vdash \psi$. If $\vDash_v \Delta$, by the induction hypothesis we have $\vDash_v \psi$ and by the previous lemma $\Gamma \vdash \psi$. It follows that $\Gamma \vdash (\varphi \to \psi)$ and by the definition of v we obtain $\vDash_v (\varphi \to \psi)$.

Suppose that $\vDash_v \Delta$ and $\Delta \vdash \psi$ is obtained from $\Delta \vdash (\varphi \to \psi)$. If $\Delta \vdash \varphi$, by the induction hypothesis we have $\vDash_v (\varphi \to \psi)$ and $\vDash_v \varphi$. However, $\vDash_v (\varphi \to \psi)$ implies that $\nvDash_v \varphi$ or $\vDash_v \psi$, by the definition of v. The first is false, hence $\vDash_v \psi$.

Suppose $\Delta = q\,\mathtt{said}\,\Delta_1$, $A = q\,\mathtt{said}\,\varphi$ and the last inference is

$$\frac{\Delta_1 \vdash \varphi}{q\,\mathtt{said}\,\Delta_1 \vdash q\,\mathtt{said}\,\varphi}$$

Assume $\vDash_v q\,\mathtt{said}\,\Delta_1$. This means $\Gamma \vdash q\,\mathtt{said}\,\psi$, for each $\psi \in \Delta_1$. Since $q\,\mathtt{said}\,\Delta_1 \vdash q\,\mathtt{said}\,\varphi$, we also have $\Gamma \vdash q\,\mathtt{said}\,\varphi$, which means $\vDash_v q\,\mathtt{said}\,\varphi$ by the definition of v. So, in this case we do not even have to use the induction hypothesis.

The case of the rule `(Implied)` is similar. $\boxtimes$

The analogue of Lemma 3.6 works without any change.

Lemma 6.9 *If φ is Harrop, then*

$$\vDash_v \varphi \iff \Gamma \vdash \varphi.$$

Now suppose Γ is Harrop and $\Gamma \vdash \varphi \vee \psi$. For any $\theta \in \Gamma$ we have $\Gamma \vdash \theta$, hence $\vDash_v \theta$ by Lemma 6.9. By Lemma 6.8 it follows that $\vDash_v \varphi \vee \psi$, hence $\vDash_v \varphi$ or $\vDash_v \psi$. By Lemma 6.7 this implies $\Gamma \vdash \varphi$ or $\Gamma \vdash \psi$. $\boxtimes$

7 Complexity bounds

Next we show that there is a reduction of classical modal logic to primal logic with quotations. This gives suitable complexity bounds for the fragments of the primal logic with disjunction and quotations.

Let us call a *prefix* a sequence of modalities of the form $q_i\,\mathtt{said}$ or $q_j\,\mathtt{implied}$, for example, $q_1\,\mathtt{said}\,q_3\,\mathtt{implied}\,q_1\,\mathtt{said}$ is a prefix of length three. We say that a subformula φ *occurs in* A *under a prefix* σ, if in the parse tree of A there is a branch leading to an occurrence of φ such that reading the modalities top down along this branch yields σ. Of course, for a given occurrence of φ this prefix is uniquely defined. *Modal depth* of A can be defined as the maximal length of prefixes of subformula occurrences in A.

Let $H(A)$ denote the set of all formulas of the form $\sigma(\varphi \vee (\varphi \to \psi))$, where $\varphi \to \psi$ occurs in A under a prefix σ. We note that the length of $H(A)$ is polynomial in the length of A.

Let **qC** denote the extension of classical logic by quotations.

Proposition 7.1 *For any formula* A, $\mathbf{qC} \vdash A$ *iff* $H(A) \vdash A$ *in* $\mathbf{qP}[\vee, \bot]$.

Proof. The implication from right to left is obvious, since $H(A)$ is provable in **qC** for any A.

For the opposite implication we give a syntactic proof based on our Gentzen-style sequent calculus for primal logic. Given a set of formulas Γ define $H(\Gamma)$ to be the union of all $H(\varphi)$, for all $\varphi \in \Gamma$. By induction on the length of derivation we show that $H(\Gamma, \Delta), \Gamma \Rightarrow \Delta$ is provable in **GP** whenever $\Gamma \Rightarrow \Delta$ is provable in **GC**.

We only have to treat the cases of the modal rules and the rule $(\to R)$. Suppose the last rule applied in the classical derivation of $\Gamma \Rightarrow \Delta$ is $(\to R)$, that is, the last inference has the form

$$\frac{\Gamma, \varphi \Rightarrow \Delta', \psi}{\Gamma \Rightarrow \Delta', \varphi \to \psi}$$

By the induction hypothesis we obtain a derivation of $H, \Gamma, \varphi \Rightarrow \Delta', \psi$ in **GP** where $H = H(\Gamma, \varphi, \Delta', \psi)$. We notice that

$$H(\Gamma, \Delta) = H(\Gamma, \Delta', \varphi \to \psi) = H \cup \{\varphi \vee (\varphi \to \psi)\}.$$

Then we consider the following proof tree:

$$\dfrac{\dfrac{H, \varphi, \Gamma \Rightarrow \Delta', \psi}{H, \varphi, \Gamma \Rightarrow \Delta', \varphi \to \psi}\,(\to R_p) \qquad H, \varphi \to \psi, \Gamma \Rightarrow \Delta', \varphi \to \psi}{H, \varphi \vee (\varphi \to \psi), \Gamma \Rightarrow \Delta', \varphi \to \psi}\,(\vee L)$$

The leaves of this tree are provable in primal logic, the left one by the induction hypothesis and the right one for trivial reasons. Hence, we obtain the required derivation.

Suppose the last inference has the form

$$\frac{\Gamma' \Rightarrow \varphi}{q\,\mathtt{said}\,\Gamma' \Rightarrow q\,\mathtt{said}\,\varphi}\ (\mathtt{Said})$$

Let $H := H(\Gamma', \varphi)$, then clearly

$$H(q\,\mathtt{said}\,\Gamma', q\,\mathtt{said}\,\varphi) = \{q\,\mathtt{said}\,\psi : \psi \in H\} =: q\,\mathtt{said}\,H.$$

By the induction hypothesis $H, \Gamma' \Rightarrow \varphi$ is provable in primal logic. Hence, we obtain the required derivation

$$\frac{H, \Gamma' \Rightarrow \varphi}{q\,\mathtt{said}\,H, q\,\mathtt{said}\,\Gamma' \Rightarrow q\,\mathtt{said}\,\varphi.}$$

Suppose the last inference has the form

$$\frac{\Sigma, \Pi \Rightarrow \varphi}{q\,\mathtt{said}\,\Sigma, q\,\mathtt{implied}\,\Pi \Rightarrow q\,\mathtt{implied}\,\varphi}\ (\mathtt{Implied})$$

Let $H := H(\Sigma, \Pi, \varphi) = H(\Sigma) \cup H(\Pi, \varphi)$. Then

$$\begin{aligned} H(q\,\mathtt{said}\,\Sigma, q\,\mathtt{implied}\,\Pi, q\,\mathtt{implied}\,\varphi) &= H(q\,\mathtt{said}\,\Sigma) \cup H(q\,\mathtt{implied}\,\Pi, q\,\mathtt{implied}\,\varphi) \\ &= q\,\mathtt{said}\,H(\Sigma) \cup q\,\mathtt{implied}\,H(\Pi, \varphi). \quad (2) \end{aligned}$$

By the induction hypothesis $H, \Sigma, \Pi \Rightarrow \varphi$ is provable in primal logic. Hence, we obtain the required derivation

$$\frac{H(\Sigma), H(\Pi, \varphi), \Sigma, \Pi \Rightarrow \varphi}{q\,\mathtt{said}\,H(\Sigma), q\,\mathtt{implied}\,H(\Pi, \varphi), q\,\mathtt{said}\,\Sigma, q\,\mathtt{implied}\,\Pi \Rightarrow q\,\mathtt{implied}\,\varphi.}$$

The cases of all the other rules and axioms are obvious. ⊠

It follows from the well-known work of Ladner [23] that the derivability problem for **qC** is PSPACE-hard. Hence, Proposition 7.1 together with Theorem 3 imply the following theorem.

Theorem 7 *The derivability problem for* $\mathbf{qP}[\vee, \bot]$ *is* PSPACE*-complete.*

On the other hand, Halpern [22] showed that the derivability problem for the bounded-modal-depth fragment of modal logic **K** is CO-NP-complete. The situation for $\mathbf{qP}[\vee, \bot]$ is similar.

Theorem 8 (i) *If* $\Gamma \nvdash A$ *in* $\mathbf{qP}[\vee, \bot]$ *and* Γ, A *have modal depth bounded by a constant* d, *there is a primal model* $\mathcal{W}$ *of size polynomial in the length of* Γ *and* A *such that, for some* $x \in \mathcal{W}$, $x \vDash \Gamma$ *but* $x \nvDash A$.

(ii) *For each* d, *the derivability problem for modal depth* d *fragment of* $\mathbf{qP}[\vee, \bot]$ *is* CO-NP*-complete.*

Clause (ii) follows from (i) and Theorem 3. Clause (i) can be proved by adapting the standard methods of [22]. We prove the following main lemma, which is a more specific version of (i). We call a primal model *treelike*, if its I_q relations are finite trees (and hence, so are its S_q relations).

Lemma 7.2 *Suppose* $\Gamma \Rightarrow \Delta$ *is unprovable in* **GP** *and has modal depth bounded by* d. *Then there is a treelike primal model* $\mathcal{W}$ *of depth* d *and branching bounded by the length of* $\Gamma \Rightarrow \Delta$ *such that* $\Gamma \Rightarrow \Delta$ *is false at the root* r *of* $\mathcal{W}$.

Proof. We argue by induction on d. If $d = 0$ the model $\mathcal{W}$ will consist of a single root, by Theorem 1. Suppose the modal depth of $\Gamma \Rightarrow \Delta$ is $d + 1$. Let $\mathcal{F}$ denote the set of all subformulas of $\Gamma \Rightarrow \Delta$. We write $u \vDash \Gamma \Rightarrow \Delta$ as a shorthand for $u \vDash \bigwedge \Gamma \to \bigvee \Delta$.

Consider any primal model $\mathcal{U}$ and a point $u \in \mathcal{U}$ such that $u \nvDash \Gamma \Rightarrow \Delta$. For each q let

$$\begin{aligned} \Gamma_q &:= \{\varphi \in \mathcal{F} : u \vDash q\,\mathtt{said}\,\varphi\} \\ \Delta_q &:= \{\varphi \in \mathcal{F} : u \vDash q\,\mathtt{implied}\,\varphi\} \end{aligned}$$

Further, let $\varphi_1^q, \ldots, \varphi_n^q$ be all the formulas $\varphi \in \mathcal{F}$ such that $u \nvDash q\,\mathtt{said}\,\varphi$, and let $\psi_1^q, \ldots, \psi_m^q$ be all the formulas $\varphi \in \mathcal{F}$ such that $u \nvDash q\,\mathtt{implied}\,\varphi$.

We notice that each of the sequents $\Gamma_q \Rightarrow \varphi_i^q$, for $i = 1, \ldots, n$, is false at some node $u_i^q \in \mathcal{W}$ such that $uS_q u_i^q$. Similarly, each of the sequents $\Gamma_q, \Delta_q \Rightarrow \psi_j^q$, for $j = 1, \ldots, m$, is false at some node $v_j^q \in \mathcal{U}$ such that $uI_q v_j^q$. The modal depth of all these sequents is bounded by d, so by the induction hypothesis we obtain treelike models $\mathcal{W}_i^q$ with the roots r_i^q, and $\mathcal{V}_j^q$ with the roots t_j^q such that

$$r_i^q \nvDash \Gamma_q \Rightarrow \varphi_i^q \text{ and } t_j^q \nvDash \Gamma_q, \Delta_q \Rightarrow \psi_i^q.$$

The required model $\mathcal{W}$ will consist of the disjoint union of all these models $\mathcal{W}_i^q$ and $\mathcal{V}_j^q$ together with a new root r. The root r is only connected to the points r_i^q by S_q and to the points t_j^q by I_q, for all q. The valuation

at the root r (on the variables and the implications) coincides with that at $u \in \mathcal{U}$.

CLAIM. For each formula $\varphi \in \mathcal{F}$, $u \vDash \varphi$ holds in $\mathcal{U}$ iff $r \vDash \varphi$ holds in $\mathcal{W}$.

This claim is proved by a straightforward induction which we omit. It follows that $r \nvDash \Gamma \Rightarrow \Delta$. We finally remark that the depth of $\mathcal{W}$ is bounded by $d + 1$, and that the branching at r is bounded by the total number of formulas in $\mathcal{F}$, hence by the length of $\Gamma \Rightarrow \Delta$. This concludes the proof of Lemma and thereby of Theorem 8. $\boxtimes$

References

[1] About Vidalia: http://www.infoworld.com/d/cloud-computing/microsoft-adds-access-controls-sql-azure-online-database-905.

[2] DKAL at CodePlex: http://dkal.codeplex.com/.

[3] M. Abadi. Variations in access control logic. In R. van der Meyden and L. van der Torre, editors, *DEON 2008, LNAI 5076*, pages 96–109. 2008.

[4] M. Abadi, M. Burrows, B. Lampson, and G. Plotkin. A calculus for access control in distributed systems. *ACM Transactions on Programming Languages and Systems*, 15(4):706–734, 1993.

[5] N. Aleshina and D. Shkatov. A general method for proving decidability of intuitionistic modal logics. *Journal of Applied Logic*, 4:219–230, 2006.

[6] A.W. Appel and E.W. Felten. Proof-carrying authentication. In *Proc. of the 6-th ACM Conference on Computer and Communications Security*, pages 52–62, 1999.

[7] A. Avron and O. Lahav. Strict canonical constructive systems. In A. Blass et al., editor, *Fields of Logic and Computation, LNCS 6300*, pages 75–94. Springer, 2010.

[8] M.Y. Becker, C. Fournet, and A.D. Gordon. Design and semantics of a decentralized authorization language. In *20th IEEE CSF Symposium*, pages 3–15. 2007.

[9] L. Beklemishev and Y. Gurevich. Exploring primal logic. Unpublished manuscript. http://www.mi.ras.ru/∼bekl/Papers/primlog.pdf, February 2011.

[10] N. Benton, G. Bierman, and V. de Paiva. Computational types from a logical perspective. *J. Funct. Programming*, 8(2):177–193, 1998.

[11] A. Blass and Y. Gurevich. Hilbertian Deductive Systems, Infon Logic, and Datalog. *Bulletin of Euro. Assoc. for Theor. Computer Science*, 102:122–150, October 2010.

[12] A. Blass, Y. Gurevich, M. Moskal, and I. Neeman. Evidential authorization. In S. Nanz, editor, *The Future of Software Engineering*, pages 77–99. Springer, 2011.

[13] G. Boella, D.M. Gabbay, V. Genovese, and L. van Torre. Fibred security language. *Studia Logica*, 92:395436, 2009.

[14] R. Bull. A modal extension of intuitionistic logic. *Notre Dame Journal of Formal Logic*, 6:142–146, 1965.

[15] R. Bull. MIPC as the formalization of an intuitionist concept of modality. *The Journal of Symbolic Logic*, 31:609–616, 1966.

[16] R. Davies and F. Pfenning. A modal analysis of staged computations. *Journal of ACM*, 48(3):555–604, 2001.

[17] K. Došen. Models for stronger intuitionistic modal logics. *Studia Logica*, 44:39–70, 1985.

[18] D. Garg and M. Abadi. A modal deconstruction of access control logics. In R. Amadio, editor, *FOSSACS 2008, LNCS 4962*, pages 216–230. Springer, 2008.

[19] Y. Gurevich and I. Neeman. DKAL: Distributed-Knowledge Authorization Language. In *Proc. of CSF 2008*, pages 149–162. IEEE Computer Society, 2008.

[20] Y. Gurevich and I. Neeman. DKAL 2 — A Simplified and Improved Authorization Language. Technical Report MSR-TR-2009-11, Microsoft Research, February 2009.

[21] Y. Gurevich and I. Neeman. Logic of Infons: the propositional case. *ACM Transactions on Computational Logic*, 12(2), 2011.

[22] J. 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.

[23] R.E. Ladner. The computational complexity of provability in systems of modal propositional logic. *SIAM Journal on Computing*, 6(3):467–480, 1977.

[24] N. Li, B.N. Grosof, and J. Feigenbaum. Delegation logic: A logic-based approach to distributed authorization. *ACM Transactions on Information and System Security*, 6(1):128–171, 2003.

[25] M. Minoux. LTUR: A simplified unit-resolution algorithm for Horn formulae and computer implementation. *Information Processing Letters*, 29:1–12, 1988.

[26] E. Moggi. Notions of computation and monads. *Information and Computation*, 93(1):55–92, 1991.

[27] H. Ono. On some intuitionistic modal logics. *Publ. Res. Institute for Mathematical Science*, 13:55–67, 1977.

[28] G. Plotkin and C. Stirling. A framework for intuitionistic modal logic. In J. Halpern, editor, *Theoretical Aspects of Reasoning about Knowledge*. 1986.

[29] G. Fischer Servi. On modal logic with an intuitionist base. *Studia Logica*, pages 141–149, 1977.

[30] G. Fischer Servi. Semantics for a class of intuitionist modal calculi. In M.-L. dalla Chiara, editor, *Italian Studies in the Philosophy of Science*, pages 59–72. Reidel, Dordrecht, 1981.

[31] A. Simpson. *The Proof Theory and Semantics of Intuitionistic Modal Logic*. PhD thesis, University of Edinburgh, 1994.

[32] R. Statman. Intuitionistic propositional logic is polynomial-space complete. *Theoretical Computer Science*, 9:67–72, 1979.

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

[34] D.I. Vakarelov. Intuitionistic modal logics incompatible with the law of the excluded middle. *Studia Logica*, 40(2):103–111, 1981.

[35] D.I. Vakarelov. An application of Rieger-Nishimura formulas to the intuitionistic modal logics. *Studia Logica*, 44(7):79–85, 1985.

[36] V. Švejdar. On the polynomial-space completeness of intuitionistic propositional logic. *Archive for Mathematical Logic*, 42:711–716, 2003.

[37] F. Wolter and M. Zakharyaschev. Intuitionistic modal logics as fragments of classical bimodal logics. In E. Orlowska, editor, *Logic at Work*, pages 168–186. Kluwer, 1997.

[38] F. Wolter and M. Zakharyaschev. On the relation between intuitionistic and classical modal logics. *Algebra and Logic*, 36:73–92, 1997.

[39] F. Wolter and M. Zakharyaschev. Intuitionistic modal logics. In A. Cantini, E. Casari, and P. Minari, editors, *Logic and Foundations of Mathematics*, pages 227–238. 1999.