Principles of Constructive Provability Logic

Robert J. Simmons **Bernardo Toninho**

December 10, 2010
CMU-CS-10-151

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

Abstract

We present a novel formulation of the modal logic **CPL**, a *constructive logic of provability* that is closely connected to the Gödel-Löb logic of provability. Our logical formulation allows modal operators to talk about both *provability* and *non-provability* of propositions at reachable worlds. We are interested in the applications of **CPL** to logic programming; however, this report focuses on the presentation of a minimal fragment (in the sense of minimal logic) of **CPL** and on the formalization of minimal **CPL** and its metatheory in the Agda programming language. We present both a natural deduction system and a sequent calculus for minimal **CPL** and show that the presentations are equivalent.

Support for this research was provided by an X10 Innovation Award from IBM, a National Science Foundation Graduate Research Fellowship for the first author, and by the Fundação para a Ciência e a Tecnologia (Portuguese Foundation for Science and Technology) through the Carnegie Mellon Portugal Program under Grants NGN-44 and SFRH / BD / 33763 / 2009. Any opinions, findings, conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of these supporting groups.

Keywords: modal logic, provability logic, judgmental reconstruction, natural deduction, sequent calculus, constructive type theory

1 Motivation

Consider the following propositions (where "$\supset$" represents implication):

$$\forall x.\, \forall y.\, \mathsf{edge}(x, y) \supset \mathsf{edge}(y, x)$$
$$\forall x.\, \forall y.\, \mathsf{edge}(x, y) \supset \mathsf{path}(x, y)$$
$$\forall x.\, \forall y.\, \forall z.\, \mathsf{edge}(x, y) \supset \mathsf{path}(y, z) \supset \mathsf{path}(x, z)$$

One way to think of these propositions is as rules in a *bottom-up logic program*. This gives them an operational meaning: given some known set of facts, a bottom-up logic program uses rules to derive more facts. If we start with the single fact $\mathsf{edge}(\mathsf{a}, \mathsf{b})$, we can derive $\mathsf{edge}(\mathsf{b}, \mathsf{a})$ by using the first rule (taking $x = \mathsf{a}$ and $y = \mathsf{b}$), and then, using this new fact, we can derive $\mathsf{path}(\mathsf{b}, \mathsf{a})$ by using the second rule (taking $x = \mathsf{b}$ and $y = \mathsf{a}$). Finally, from the original $\mathsf{edge}(\mathsf{a}, \mathsf{b})$ fact and the new $\mathsf{path}(\mathsf{b}, \mathsf{a})$ fact, we can derive $\mathsf{path}(\mathsf{a}, \mathsf{a})$ using the third rule (taking $x = \mathsf{a}$, $y = \mathsf{b}$, and $z = \mathsf{a}$). Once the only new facts we can derive are facts we already know, we say we have reached *saturation* — this will happen in our example when we have derived $\mathsf{edge}(\mathsf{a}, \mathsf{b})$, $\mathsf{edge}(\mathsf{b}, \mathsf{a})$, $\mathsf{path}(\mathsf{a}, \mathsf{b})$, $\mathsf{path}(\mathsf{b}, \mathsf{a})$, $\mathsf{path}(\mathsf{a}, \mathsf{a})$, and $\mathsf{path}(\mathsf{b}, \mathsf{b})$. Bottom-up logic programming is a very simple and intuitive kind of reasoning, and it has also shown to be an elegant and powerful way of declaratively specifying and efficiently solving many computational problems, especially in the field of program analysis (see [13] for a number of references).

Next, consider the following proposition:

$$\forall x.\, \forall y.\, \mathsf{path}(x, y) \supset \neg\mathsf{edge}(x, y) \supset \mathsf{noedge}(x, y)$$

Intuition says that this is a meaningful statement. In our example above, we can derive $\mathsf{path}(\mathsf{a}, \mathsf{a})$, but we can't possibly derive $\mathsf{edge}(\mathsf{a}, \mathsf{a})$, so we should be able to conclude $\mathsf{noedge}(\mathsf{a}, \mathsf{a})$. A bottom-up logic programming semantics based on *stratified negation* verifies this intuition. In a stratified logic program made up of the four previous rules, we can derive all the consequences of the first three rules until saturation is reached. At this point, we know everything there is to know about facts of the form $\mathsf{edge}(X, Y)$ and $\mathsf{path}(X, Y)$. When considering the negated premise $\neg\mathsf{edge}(x, y)$ in the fourth rule, we simply check the saturated database and conclude that the premise holds if the fact does not appear in the database.

Stratified negation would, however, disallow the addition of the following rule as paradoxical or contradictory:

$$\forall x.\, \forall y.\, \mathsf{path}(x, y) \supset \neg\mathsf{edge}(x, y) \supset \mathsf{edge}(x, y)$$

Why is this rule problematic? Operationally, the procedure we used for stratified negation no longer really makes sense: we reached saturation, then concluded that there was no way to prove $\mathsf{edge}(\mathsf{a}, \mathsf{a})$, then used that conclusion to prove $\mathsf{edge}(\mathsf{a}, \mathsf{a})$. But we had just concluded that it wasn't provable! Stratified negation ensures that we never use the fact that there is no proof of A to come up with a proof of A, either directly or indirectly. However, stratified negation is an odd property: the program consisting of the single rule $\neg\mathsf{prop1} \supset \mathsf{prop2}$ is stratified (we consider prop1 first, and then we consider prop2), and the program consisting of the single rule $\neg\mathsf{prop2} \supset \mathsf{prop1}$ is

also stratified (we consider prop2 first, and then we consider prop1), but the two rules cannot be combined as a single stratified logic program. This sort of problem is a large part of the reason why a general and proof-theoretic justification for stratified negation has been elusive.

This report considers the proof theory of a logical system, *constructive provability logic*, that we believe can be used to give a complete and satisfying justification for stratified negation in logic programming. However, logic programming will be used in this report only as a motivating example — the relationship between this logic and stratified logic programming will be left for future work.

1.1 Foundations, formalization, and Agda

It is always the case that the proof theory of a logic needs to be formalized using some metalogic — usually some assumed and largely informal notion of set-theory-based mathematics that admits, at minimum, induction. Any consistency results for the logic are obviously premised upon consistency of the metalogic; worrying about consistency of the metalogic is generally filed under the label "foundational issues." However, as we will see, in constructive provability logic the metalogic is interwoven with the proof theory in a way that is mostly foreign outside of dependent type theories,[1] making these sorts of foundational issues quite a bit more relevant. Therefore, it is desirable to be a little more precise about what our metalogic actually is to ensure that there are no unintentional shenanigans.

In our case, we make our foundational assumptions precise by formalizing the contents of this report in a proof assistant, Agda [8]. This has the effect of fixing our metalogic as the logic that Agda implements, intuitionistic type theory (unless, of course, there are bugs in Agda!).[2] The code from this formalization is available online in the CMU technical report archive and at `https://bitbucket.org/robsimmons/constructive-provability-logic`.

2 A judgmental introduction

We will introduce the principles of constructive provability logic in a manner consistent with Pfenning and Davies' judgmental reconstruction of modal logic [9] (itself an interpretation of Martin-Löf's 1983 Siena Lectures [7]). This section is not intended to be a complete introduction to the judgmental methodology, and we refer readers to the aforementioned papers for a more complete discussion.

The judgmental methodology carefully maintains a separation between propositions (which we write as A, B, etc.) and judgments J. Propositions are syntactic constructs that are built up from some set of *atomic propositions* ($\mathsf{edge}(\mathsf{a}, \mathsf{b})$ is an example of an atomic proposition) using connectives (implication $A \supset B$, conjunction $A \wedge B$, and disjunction $A \vee B$ are examples of connectives), and judgments are things that are proved using rules of inference. In this methodology, given a proposition A we can talk about giving a proof of the judgment $A\ \mathit{true}$ (i.e. "proving that A is true"), giving a proof of the judgment $A\ \mathit{false}$ (i.e. "proving that A is false"), or even giving a

[1] One exception is Zeilberger et al.'s recent work on higher-order focusing [5, 14].

[2] There is one caveat, which we discuss in Section 2.4.

proof of the judgment that A is true at some specific time t. It isn't really meaningful to "prove A" — if we say such a thing, we usually mean it as shorthand for proving that A is true.

A *hypothetical* judgment $J_1, \ldots, J_n \vdash J$ (where the sequence of J_i are called the *antecedents* and J is called the *consequent*) roughly expresses that the judgment J has a proof if we assume that there are proofs of the assumptions $J_1, \ldots, J_n$. However, a hypothetical judgment does not necessarily have a set meaning; rather, we *define* the meaning of a hypothetical judgment by defining three things: (1) a *hypothesis rule*, (2) a *weakening principle*, and a (3) a *substitution principle*. These defining principles should flow from our preexisting understanding of what the hypothetical judgment means. A rich family of logics (we call these the *structural logics*) obey a common set of defining principles (we use Ψ as an abbreviation for $J_1, \ldots, J_n$):

Definition of hypothetical judgment in structural logics:
- *Hypothesis rule*: If $J \in \Psi$, then $\Psi \vdash J$.
- *Weakening*[3] *principle*: If $\Psi \subseteq \Psi'$ and $\Psi \vdash J$, then $\Psi' \vdash J$.
- *Substitution principle*: If $\Psi \vdash J$ and $\Psi, J \vdash J'$, then $\Psi \vdash J'$.

These weakening and substitution principles have an interesting character. In one sense, they are the last thing we need to consider, as once the logic is fully defined, they are theorems that we have to prove about the logic as a whole. However, the position of the judgmental methodology is that such defining principles are also the *first* thing that we need to consider. On a philosophical level, this is because these defining principles should flow from our understanding of the meaning of the hypothetical judgment. On a practical level, the weakening and substitution principles are necessary to have on hand as we work through the two "sanity checks" on the meaning of logical connectives (more on that in a moment).

The meaning of a connective is defined by two sets of rules, the *introduction* and *elimination* rules. In the case of implication $A \supset B$, which we will use as an example, there is one introduction rule and one elimination rule. Introduction rules establish how we can obtain proof of a judgment about a certain proposition — they mention the connective in the conclusion.

$$\frac{\Psi, A\ true \vdash B\ true}{\Psi \vdash A \supset B\ true}\ \supset I$$

Elimination rules establish how we can use a proof of a judgment about that proposition — they mention the connective in a premise.

$$\frac{\Psi \vdash A \supset B\ true \quad \Psi \vdash A\ true}{\Psi \vdash B\ true}\ \supset E$$

The two sanity checks on these rules are usually called *local soundness* and *local completeness*. Local soundness ensures that the elimination rules are not too strong relative to the introduction

[3]The weakening principle actually generalizes the principle commonly called weakening (if $\Psi \vdash J$ then $\Psi, J' \vdash J$) as well as the principles commonly called exchange (if $\Psi, J_1, J_2, \Psi' \vdash J$ then $\Psi, J_2, J_1, \Psi' \vdash J$) and contraction (if $\Psi, J', J' \vdash J$ then $\Psi, J' \vdash J$). According to user "thecod" at `http://requestforlogic.blogspot.com/2010/11/totally-nameless-representation.html`, the presentation here is generally known as the "presheaf approach" and represents the action of the term functor on context renamings.

rules (or, conversely, that the introduction rules are not too weak).[4] Consider a proof $\mathcal{D}$ of the hypothetical judgment $\Psi \vdash C\ true$ where the "last" rule is an elimination rule. In the running example of implication, this means that the elimination rule is $\supset E$ and there are two subproofs: one proves $\Psi \vdash A \supset C\ true$ and the other proves $\Psi \vdash A\ true$. Call these two subproofs $\mathcal{D}_1$ and $\mathcal{D}_2$, respectively.

$$\dfrac{\begin{array}{cc}\mathcal{D}_1 & \mathcal{D}_2 \\ \Psi \vdash A \supset C\ true & \Psi \vdash A\ true\end{array}}{\Psi \vdash C\ true}\ \supset E$$

As the "last" rule was an elimination rule, one of the subproofs must mention the relevant connective (in this case $\mathcal{D}_1$). Local soundness is the property that, if the "last" rule in that premise is an *introduction* rule, then both the introduction rule and the elimination rule are unnecessary — we can reconstruct a proof of the ultimate conclusion $\Psi \vdash C\ true$ by using the premises of the introduction rule and any other premises of the elimination rule. In the case of implication, we can get $\mathcal{D}'$ by applying the substitution principle to the subproofs labeled $\mathcal{D}_2$ and $\mathcal{D}'_1$ below.

$$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}'_1 \\ \Psi, A\ true \vdash C\ true\end{array}}{\Psi \vdash A \supset C\ true}\ \supset I \quad \begin{array}{c}\mathcal{D}_2 \\ \Psi \vdash A\ true\end{array}}{\Psi \vdash C\ true}\ \supset E \qquad \Longrightarrow_R \qquad \begin{array}{c}\mathcal{D}' \\ \Psi \vdash C\ true\end{array}$$

Local completeness, on the other hand, ensures that the elimination rules are not too weak relative to the introduction rules (or, conversely, that the introduction rules are not too strong). Whereas local soundness has the form of a reduction or simplification, local completeness has the form of an expansion: we show that, given a proof of the connective, we can obtain enough evidence by applying elimination rules to re-apply the introduction rule and reconstruct the proof. In the expansion below, we get $\mathcal{D}'$ by applying the weakening principle to $\mathcal{D}$.

$$\begin{array}{c}\mathcal{D} \\ \Psi \vdash A \supset B\ true\end{array} \qquad \Longrightarrow_E \qquad \dfrac{\dfrac{\begin{array}{c}\mathcal{D}' \\ \Psi, A\ true \vdash A \supset B\ true\end{array} \quad \dfrac{}{\Psi, A\ true \vdash A\ true}\ hyp}{\Psi, A\ true \vdash B\ true}\ \supset E}{\Psi \vdash A \supset B\ true}\ \supset I$$

2.1 Intuitionistic Kripke semantics (a.k.a. "Simpson-style" modal logic)

Modal logic is an extension of regular logic that initially sought to deal with concepts like "possibility" and "necessity." A popular way of understanding and modeling modal logics is through *Kripke semantics*, which explain the meaning of possibility and necessity in terms of some set of *worlds* and some *accessibility relation*. An accessibility relation determines whether you can get

[4] Note that the fact that we call this property local **soundness** indicates a bias towards the introduction rules — local soundness proves that the elimination rules are (locally) sound with respect to the introduction rules, but it also proves the introduction rules are (locally) complete with respect to the elimination rules! Dummett labeled this bias towards the introduction rules the *verificationist* perspective and the opposite bias towards the elimination rules the *pragmatist* perspective [3].

from one world to another world. Then, the judgment "A is possibly true at world w" means that, from w, you can get to some world where A is true, and the judgment "A is necessarily true at world w" means that, from w, *everywhere* you can get to is a world where A is true.

The primary contribution of Alex Simpson's Ph.D. thesis was to show that many intuitionistic modal logics could be given proof-theoretic treatment that strongly resembles Kripke semantics by using a structural logic with two judgments [11]. The first judgment is $A[w]$, which expresses that A is true at a specific "world" w. The other judgment is $w \prec w'$, which expresses that, from world w, world w' is accessible. In Simpson's thesis, worlds are just syntactic things (much like propositions). One complication is that, in order to talk about the definition of the hypothetical judgment in Simpson-style modal logic, we must extend the form of the hypothetical judgment to account for the fact that we have as antecedents not only judgments $A[w]$ and $w \prec w'$, but also *world variables* ω.

A general introduction to hypothetical judgments parametrized by variables would lead us too far astray; Harper has a complete discussion elsewhere [4, Chapter 4]. Specialized to our needs, the form of the hypothetical judgment is $\Phi \vdash_\Sigma J$, where $\Sigma = \omega_1 \ldots \omega_k$, $\Phi = J_1, \ldots, J_n$, and J along with each of the J_i are either $A[w]$ or $w \prec w'$.

Definition of hypothetical judgment in Simpson-style modal logic:

— *Hypothesis rule*: If $J \in \Phi$, then $\Phi \vdash_\Sigma J$.
— *Weakening principle*: If $\Sigma \subseteq \Sigma'$ and $\Phi \subseteq \Phi'$ and $\Phi \vdash_\Sigma J$, then $\Phi' \vdash_{\Sigma'} J$.
— *Variable substitution principle*: If $\Phi \vdash_{\Sigma,\omega} J$, then $\Phi[w/\omega] \vdash_\Sigma J[w/\omega]$.
— *Substitution principle 1*: If $\Phi \vdash_\Sigma A[w]$ and $\Phi, A[w] \vdash_\Sigma J$, then $\Phi \vdash J$.
— *Substitution principle 2*: If $\Phi \vdash_\Sigma w \prec w'$ and $\Phi, w \prec w' \vdash_\Sigma J$, then $\Phi \vdash J$.

The hypothetical judgment is only well-formed if every world variable mentioned in Φ or J also appears in Σ. This restricts the weakening and variable substitution principles — it isn't possible to weaken the hypothetical judgment $A[\omega_1] \vdash_{\omega_1} C[\omega_1]$ to $A[\omega_1], \omega_1 \prec \omega_3 \vdash_{\omega_1,\omega_2} C[\omega_1]$ because $\omega_3 \notin \{\omega_1, \omega_2\}$, for instance. It is also not possible to use variable substitution to replace $A[\omega_2] \vdash_{\omega_1,\omega_2} C[\omega_2]$ with $A[\omega_3] \vdash_{\omega_1} C[\omega_3]$, and for the same reason.

Now we can define the meaning of connectives and reason about their soundness and completeness in the same way as we did before. The rules for implication are nearly unchanged, and the local soundness and completeness checks behave much as they did before, so we will not repeat them.

$$\frac{\Phi, A[w] \vdash_\Sigma B[w]}{\Phi \vdash_\Sigma A \supset B[w]} \supset I \qquad \frac{\Phi \vdash_\Sigma A \supset B[w] \quad \Phi \vdash_\Sigma A[w]}{\Phi \vdash_\Sigma B[w]} \supset E$$

The point of this new infrastructure is that it allows us to define new connectives, such as *modal possibility*, written $\Diamond A$. The intended meaning of $\Diamond A$ is that it should be true at a given world if there is some accessible world where A is true.

$$\frac{\Phi \vdash_\Sigma w \prec w' \quad \Phi \vdash_\Sigma A[w']}{\Phi \vdash_\Sigma \Diamond A[w]} \Diamond I \qquad \frac{\Phi \vdash_\Sigma \Diamond A[w] \quad \Phi, w \prec \omega'', A[\omega''] \vdash_{\Sigma,\omega''} C[w']}{\Phi \vdash_\Sigma C[w']} \Diamond E$$

The introduction rule just follows our informal definition above: if a world w' is accessible from a world w and A is true at w', then $\Diamond A$ is true at w. The elimination rule is slightly more complicated. If $\Diamond A$ is true at w and we are trying to prove C at some (potentially different) world w', then it suffices to prove $C[w']$ under the additional assumption that A is true at ω'', where ω'' is a newly introduced world variable that represents an arbitrary world accessible from w.

Local soundness for modal possibility is straightforward, though it uses all three substitution principles: from $\mathcal{D}_3$, variable substitution gives us $\Phi, w_1 \prec w_2, A[w_2] \vdash_\Sigma C[w_3]$. Then, from the first substitution principle along with $\mathcal{D}_2'$ (which is $\mathcal{D}_2$ after the weakening principle is used to add the premise $w_1 \prec w_2$), we get $\Phi, w_1 \prec w_2 \vdash_\Sigma C[w_3]$. Finally, the second substitution principle along with $\mathcal{D}_1$ gives us $\mathcal{D}'$, a proof of $\Phi \vdash_\Sigma C[w_3]$.

$$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}_1\\ \Phi \vdash_\Sigma w_1 \prec w_2\end{array} \quad \begin{array}{c}\mathcal{D}_2\\ \Phi \vdash_\Sigma A[w_2]\end{array}}{\Phi \vdash_\Sigma \Diamond A[w_1]}\Diamond I \quad \begin{array}{c}\mathcal{D}_3\\ \Phi, w_1 \prec \omega, A[\omega] \vdash_{\Sigma,\omega} C[w_3]\end{array}}{\Phi \vdash_\Sigma C[w_3]}\Diamond E \quad \Longrightarrow_R \quad \begin{array}{c}\mathcal{D}'\\ \Phi \vdash C[w_3]\end{array}$$

Local completeness for modal possibility is straightforward: the two new pieces of information provided by the $\Diamond E$ rule are precisely what we need to apply the $\Diamond I$ rule.

$$\begin{array}{c}\mathcal{D}\\ \Phi \vdash \Diamond A[w]\end{array} \Longrightarrow_E$$

$$\dfrac{\begin{array}{c}\mathcal{D}\\ \Phi \vdash \Diamond A[w]\end{array} \quad \dfrac{\dfrac{}{\Phi, w \prec \omega', A[\omega'] \vdash_{\Sigma,\omega'} w \prec \omega'}\,hyp \quad \dfrac{}{\Phi, w \prec \omega', A[\omega'] \vdash_{\Sigma,\omega'} A[\omega']}\,hyp}{\Phi, w \prec \omega', A[\omega'] \vdash_{\Sigma,\omega'} \Diamond A[w]}\Diamond I}{\Phi \vdash \Diamond A[w]}\Diamond E$$

2.2 Reflection over the accessibility relation

Consider a very simple accessibility relation: there are two worlds α and β, and from α, β is accessible (again, we write this $\alpha \prec \beta$). Then assume that $\Diamond A$ is true at α and that $A \supset B$ is true at β. Should we be able to conclude that B is true at β?

We can represent this question by asking whether the following judgment has a proof:

$$\alpha \prec \beta, \Diamond A[\alpha], A \supset B[\beta] \vdash_{\alpha,\beta} B[\beta]$$

At the level of a word problem, this seems plausible: $\Diamond A$ is true at α, meaning that A is true at some world accessible from α. As β is the only world accessible from α, you could argue that this means A must be true at β, at which point the rest follows by implication elimination:

$$\dfrac{\dfrac{}{\ldots, A[\beta], A \supset B[\beta] \vdash_{\alpha,\beta} A \supset B[\beta]}\,hyp \quad \dfrac{}{\ldots, A[\beta], A \supset B[\beta] \vdash_{\alpha,\beta} A[\beta]}\,hyp}{\ldots, A[\beta], A \supset B[\beta] \vdash_{\alpha,\beta} B[\beta]}\supset E$$

This reasoning, however, is inconsistent with the defining principles of the logic. If we can prove the judgment $\alpha \prec \beta, \Diamond A[\alpha], A \supset B[\beta] \vdash_{\alpha,\beta} B[\beta]$, the weakening principle says that we must

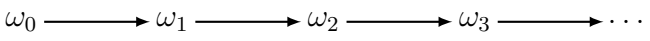
also be able to prove the judgment $\alpha \prec \beta, \alpha \prec \gamma, \Diamond A[\alpha], A \supset B[\beta] \vdash_{\alpha,\beta,\gamma} B[\beta]$. By weakening the previous hypothetical judgment, there are are now two worlds accessible from α, both β and γ. This no longer seems like a hypothetical judgment that should have a proof, as it might be the case that A was true at γ but not at β. In other words, we should hope that the Simpson-style modal logic doesn't allow us to prove this hypothetical judgment[5] — if it did, that would indicate a problem with the weakening principle we started with!

2.2.1 Modal logic with a pre-defined accessibility relation

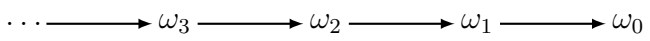
One of the reasons that we formalize logic in the first case is to capture and mechanize patterns of natural reasoning. Perhaps we want to be able to formalize the informal reasoning above. It is immediately clear that any logic that captures this argument will have defining principles that differ from the defining principles of Simpson-style modal logic. In particular, the weakening principle cannot apply in the same way to judgments about accessibility — if we add new worlds or new connections in the accessibility relation, previously provable judgments may become unprovable.

The way we will deal with this is by completely separating reasoning about accessibility and reasoning about truth-at-a-given-world; we will just assume that there is some preexisting set of worlds w and some preexisting accessibility judgment $w \prec w'$ that the logic inherits. The simple accessibility relation that only has $\alpha \prec \beta$ is one possible accessibility relation, and another is represented by the following diagram, where the arrow from α to β indicates that $\alpha \prec \beta$:

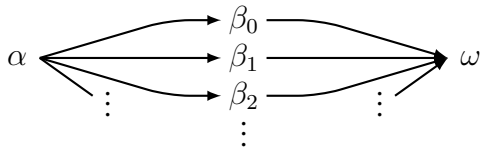
Another accessibility relation might have two worlds and a complete accessibility relation ($\alpha \prec \beta$, $\alpha \prec \alpha$, $\beta \prec \alpha$, $\beta \prec \beta$), and others might have an infinite number of worlds. For instance, the "count-up" accessibility relation has countably infinite worlds arranged like this:



The "count-down" accessibility relation has countably infinite worlds arranged like this:



Yet another possibility is this "infinite options" accessibility relation, where α has countably infinite successors and ω countably infinite predecessors:



[5] It doesn't.

Whatever accessibility relation we use, judgments about accessibility no longer need to appear in the hypothetical judgment, so we can once again define a structural logic. Specializing the original definition to our current logic, we let $\Gamma = A_1[w_1], \ldots, A_n[w_n]$.

Definition of hypothetical judgment in modal logic with a predefined accessibility relation:
— *Hypothesis rule*: If $A_i[w_i] \in \Gamma$, then $\Gamma \vdash A_i[w_i]$.
— *Weakening principle*: If $\Gamma \subseteq \Gamma'$ and $\Gamma \vdash A[w]$ then $\Gamma' \vdash A[w]$.
— *Substitution principle*: If $\Gamma \vdash A[w]$ and $\Gamma, A[w] \vdash C[w']$ then $\Gamma \vdash C[w']$.

2.2.2 Higher-order formulations of rules

Having set out the defining principles of the logic, we can talk about connectives. As we will see, this requires us to introduce a significant new idea: rules with premises that are "higher-order." Non-modal connectives (like implication) can be preserved from the Simpson-style modal logic, but the modal operators will, unsurprisingly, need to change. A reasonable introduction rule for modal possibility $\Diamond A$ looks much like it did before, but now the first premise $w \prec w'$ just refers to the predefined accessibility relation:

$$\frac{w \prec w' \quad \Gamma \vdash A[w']}{\Gamma \vdash \Diamond A[w]}\ \Diamond I$$

The elimination rules make things a bit more complicated. Say we're dealing with this accessibility relation:

In a sense, we want our elimination rules to be specific to the world. If we have a proof of $\Diamond A[\alpha]$, we know that at one of the two worlds accessible from α (namely β and ω), A must be true. Therefore, if we can prove $C[w']$ assuming $A[\beta]$, **and** if we can prove $C[w']$ assuming $A[\omega]$, then C is true at w'. This is captured by the following elimination rule:

$$\frac{\Gamma \vdash \Diamond A[\alpha] \quad \Gamma, A[\beta] \vdash C[w'] \quad \Gamma, A[\omega] \vdash C[w']}{\Gamma \vdash C[w']}\ \Diamond E_\alpha$$

Following this strategy, we need an elimination rule for proofs of $\Diamond A$ at each of the other worlds:

$$\frac{\Gamma \vdash \Diamond A[\beta] \quad \Gamma, A[\omega] \vdash C[w']}{\Gamma \vdash C[w']}\ \Diamond E_\beta \qquad \frac{\Gamma \vdash \Diamond A[\gamma] \quad \Gamma, A[\omega] \vdash C[w']}{\Gamma \vdash C[w']}\ \Diamond E_\gamma \qquad \frac{\Gamma \vdash \Diamond A[\omega]}{\Gamma \vdash C[w']}\ \Diamond E_\omega$$

For a logic defined under the accessibility relation above, the introduction rule $\Diamond I$ and the four elimination rules $\Diamond E_\alpha$, $\Diamond E_\beta$, $\Diamond E_\gamma$, and $\Diamond E_\omega$ are, in fact, locally sound and complete. However, it should be obvious that this is not a feasible or scalable way to put together a logic; for instance, we'd need to have an infinite number of rules to handle accessibility relations with an infinite

number of worlds! (Performing an infinite number of checks for local soundness and completeness is nobody's idea of a good time.)

However, the elimination rules that we wrote for $\Diamond E$ can be generically represented using a *higher-order formulation*. The higher-order formulation of the $\Diamond E$ rule looks like this:

$$\frac{\Gamma \vdash \Diamond A[w] \quad \forall w'.\, w \prec w' \longrightarrow \Gamma, A[w'] \vdash C[w'']}{\Gamma \vdash C[w'']}\ \Diamond E$$

The second premise quantifies over all worlds w' such that $w \prec w'$ and demands that a proof of $\Gamma, A[w'] \vdash C[w'']$ be given for each such w'. We refer to this higher-order formulation as *reflection* over proofs of another judgment — in this case, we are reflecting over the definition of the accessibility relation. Higher-order formulations are only permissible when we can give a complete definition of the judgment we're reflecting over before we discuss the judgment that uses reflection. In this case, we have already established that we can give a complete definition of the judgment $w \prec w'$ before we say anything about proofs of $\Gamma \vdash A[w]$, so the higher-order formulation is permissible.

If we so desire, we can imagine that the second premise of $\Diamond E$ just takes a given accessibility relation and "macro expands" into as many rules as there are worlds in the accessibility relation. In some cases (the "infinite options" accessibility relation is an example), this means that some rules have an infinite number of premises. In the experience of these authors, that is a difficult concept to wrap one's head around, and it means that even establishing simple properties like local soundness and completeness involve dealing with infinite objects in a way that can be delicate at best. However, it's also not necessary: we can instead treat the arrow "$\longrightarrow$" as "implies" and then write down a proof of the implication. We will give an example to illustrate what we mean.

2.2.3 Example

In this example, we will use the rules defined above and the four-world accessibility relation given in the previous section. Let $\Gamma_0 = \Diamond A[\alpha], A \supset C[\beta], A \supset B[\omega], B \supset C[\omega]$; we will prove that $\Gamma_0 \vdash \Diamond C[\alpha]$. First, we prove the following theorem:

Theorem 1. *For all w', if $\alpha \prec w'$, then $\Gamma_0, A[w'] \vdash \Diamond C[\alpha]$*

Proof. By case analysis on the accessibility relation, either $w' = \beta$ or $w' = \omega$. If $w' = \beta$, we have the following proof:

$$\dfrac{\dfrac{}{\alpha \prec \beta}\ axiom \quad \dfrac{\dfrac{}{\Gamma_0, A[\beta] \vdash A \supset C[\beta]}\ hyp \quad \dfrac{}{\Gamma_0, A[\beta] \vdash A[\beta]}\ hyp}{\Gamma_0, A[\beta] \vdash C[\beta]}\ \supset E}{\Gamma_0, A[\beta] \vdash \Diamond C[\alpha]}\ \Diamond I$$

If $w' = \omega$, we have the following proof:

$$\dfrac{\dfrac{}{\alpha \prec \omega}\ axiom \quad \dfrac{\dfrac{}{\Gamma_0, A[\omega] \vdash B \supset C[\omega]}\ hyp \quad \dfrac{\dfrac{}{\Gamma_0, A[\omega] \vdash A \supset B[\omega]}\ hyp \quad \dfrac{}{\Gamma_0, A[\omega] \vdash A[\omega]}\ hyp}{\Gamma_0, A[\omega] \vdash B[\omega]}\ \supset E}{\Gamma_0, A[\omega] \vdash C[\omega]}\ \supset E}{\Gamma_0, A[\omega] \vdash \Diamond C[\alpha]}\ \Diamond I$$

This completes the case analysis, and hence the proof. □

Having proved this theorem, we can complete the proof that $\Gamma_0 \vdash \Diamond C[\alpha]$:

$$\dfrac{\dfrac{}{\Gamma_0 \vdash \Diamond A[\alpha]}\ hyp \qquad \begin{array}{c}(Theorem\ 1)\\ \forall w'.\, \alpha \prec w' \longrightarrow \Gamma_0, A[w'] \vdash \Diamond C[\alpha]\end{array}}{\Gamma_0 \vdash \Diamond C[\alpha]}\ \Diamond E$$

The most significant thing to notice here is that proofs aren't simple tree-like structures anymore; the second premise of $\Diamond E$ in the proof tree above is satisfied not by another proof tree but by a *theorem*. This particular way of understanding higher-order formulations of judgments is not new; our use of it follows Noam Zeilberger's. To slightly misquote Zeilberger's "Focusing and Higher-Order Abstract Syntax",

> "We hope to make the case that this higher-order formulation should be taken at face value — interpreted constructively, it demands a mapping from proofs of $w \prec w'$ to proofs of $\Gamma, A[w'] \vdash C[w]$" (see [14, p. 361] for the original quote).

This is exactly the point that the example above tries to draw out: the way we prove that there is a mapping from proofs of the judgment $w \prec w'$ to proofs of the judgment $\Gamma, A[w'] \vdash C[w]$ is to, well, prove the statement "for all w', if $w \prec w'$, then $\Gamma, A[w'] \vdash C[w]$." However, because we get to prove this statement using all the familiar machinery of whatever logic we use to prove theorems, our notion of "proof" has gone from a fairly innocent set of trees to something much more complex. This is what we were foreshadowing in the introduction when we said "the metalogic is interwoven with the proof theory." Luckily, the foundation for this kind of system can be found in Martin Löf's theory of *iterated inductive definitions* [6], and these sorts of logical systems can be represented and reasoned about straightforwardly in logical frameworks like Agda. In fact, we would claim that many of the proofs in this paper can be expressed in Agda more naturally (and certainly more concisely) than they can be expressed on paper.

2.3 Reflection over provability

In the previous section, we considered what it took to reflect over the accessibility relation within a still more-or-less Simpson-style modal logic. In this section, we consider a style of reasoning that involves reflection over *provability at different worlds*. Consider again the simple accessibility relation where $\alpha \prec \beta$ and nothing else. If Q_1 and Q_2 are distinct atomic propositions, then it is not the case that we can prove $(Q_1 \supset Q_2)$ at the world β. In other words:

Theorem 2. *For distinct atomic propositions Q_1 and Q_2, it is not the case that $\cdot \vdash Q_1 \supset Q_2[\beta]$.*

Proving this sort of theorem is usually facilitated by the use of a *sequent calculus* presentation of logic rather than the natural deduction presentation we have considered so far; this is a topic that we will consider later on in Section 4. The way we prove this theorem in constructive logic is to prove that, if $\cdot \vdash Q_1 \supset Q_2[\beta]$, then we have a contradiction. While we will delay proving Theorem 2 for now, we can use the theorem to prove that it is not the case that $Q_1[\beta] \vdash Q_2[\beta]$.

To do this, we assume $Q_1[\beta] \vdash Q_2[\beta]$ and have to prove a contradiction; by rule $\supset I$ we prove $\cdot \vdash Q_1 \supset Q_2[\beta]$, and then from Theorem 2 we can then prove a contradiction! We can prove anything from a contradiction (*ex falso quodlibet*); so for instance, for a third distinct atomic proposition Q_3, if $Q_1[\beta] \vdash Q_2[\beta]$, then $Q_1[\beta] \vdash Q_3[\beta]$ – we assume $Q_1[\beta] \vdash Q_2[\beta]$, obtain a contradiction, and then use that contradiction to prove $Q_1[\beta] \vdash Q_3[\beta]$.

We just showed that, if $Q_1[\beta] \vdash Q_2[\beta]$, then $Q_1[\beta] \vdash Q_3[\beta]$; however, it is not the case that $Q_1[\beta] \vdash Q_2 \supset Q_3[\beta]$. The former statement is a *meta-theorem*, a statement *about* the logic (given one statement in the logic, $Q_1[\beta] \vdash Q_2[\beta]$, we can get another, $Q_1[\beta] \vdash Q_3[\beta]$). The second is a statement *within* the logic ($Q_1[\beta] \vdash Q_2 \supset Q_3[\beta]$). The goal of constructive provability logic (and the goal of previous work in classical provability logic discussed in the conclusion) is to use modal logic to allow meta-theorems (statements *about* the logic), to be reflected under the modal operators as statements *within* the logic. In our setting, this means that we want to reflect meta-theorems about world β as statements within the logic at world α; in particular, while we cannot prove $Q_1[\beta] \vdash Q_2 \supset Q_3[\beta]$, we *do* want to be able to prove $Q_1[\beta] \vdash \Diamond Q_2 \supset Q_3[\alpha]$.[6] In fact, we will be able to prove $Q_1[\beta] \vdash \Diamond Q_2 \supset C[\alpha]$ for any proposition C; this internalizes the notion that, if we only have a single assumption $Q_1[\beta]$, it is *not* the case that $Q_2[\beta]$ is true under our current assumptions; assuming that it is (by assuming $\Diamond Q_2[\alpha]$) is contradictory and allows us to prove anything.

Let's think about the judgmental principles this entails. We can prove that $Q_1[\beta] \vdash Q_2[\beta]$ is not the case, but we can prove the weakened hypothetical judgment $Q_1[\beta], Q_2[\beta] \vdash Q_2[\beta]$. By our discussion above, the hypothetical judgment $Q_1[\beta] \vdash \Diamond Q_2 \supset C[\alpha]$ should have a proof. On the other hand, the "weakened" judgment $Q_1[\beta], Q_2[\beta] \vdash \Diamond Q_2 \supset C[\alpha]$ *should not* have a proof, at least not for an arbitrary C, because if we have assumed $Q_1[\beta]$ *and* $Q_2[\beta]$ it is no longer contradictory to assume that Q_2 is provable at β. Weakening shouldn't take a provable hypothetical judgment and make it unprovable (hence the scare quotes), so weakening "at α" (that is, weakening when the consequent is $A[\alpha]$ for some A) clearly cannot add new antecedents of the form $A[\beta]$. If we define a restricted partial order on contexts $\Gamma \subseteq_w \Gamma'$ which requires that every antecedent in Γ be in Γ' *and* requires that every antecedent Γ' not of the form $A[w]$ be in Γ, then we can state a reasonable weakening principle in light of this observation:

— *Weakening principle*: If $\Gamma \subseteq_w \Gamma'$ and $\Gamma \vdash A[w]$, then $\Gamma' \vdash A[w]$.

So, how can we define $\Diamond A$ such that it has the meaning we desire? We can keep the rule for $\Diamond$ introduction the same as it was before, because it continues to be the case that the way we prove $\Diamond A$ at world w is by picking a world w' accessible from w and proving $\Gamma \vdash A[w']$ there.

$$\frac{w \prec w' \quad \Gamma \vdash A[w']}{\Gamma \vdash \Diamond A[w]}\ \Diamond I$$

It is the elimination rule for $\Diamond$ that we will want to change. Recall the definition of $\Diamond E$ that allowed us to reflect over the accessibility relation:

$$\frac{\Gamma \vdash \Diamond A[w] \quad \forall w'.\, w \prec w' \longrightarrow \Gamma, A[w'] \vdash C[w]}{\Gamma \vdash C[w]}\ \Diamond E$$

[6] The unary connectives always bind the most tightly; we disambiguate $\Diamond A \supset B$ as $(\Diamond A) \supset B$

If we're going to prove $Q_1[\beta] \vdash \Diamond Q_2 \supset C[\alpha]$, the proof is going to need to look like this:

$$\dfrac{\dfrac{\dfrac{}{Q_1[\beta], \Diamond Q_2[\alpha] \vdash \Diamond Q_2[\alpha]}\, hyp \quad ???}{Q_1[\beta], \Diamond Q_2[\alpha] \vdash C[\alpha]}\, \Diamond E}{Q_1[\beta] \vdash \Diamond Q_2 \supset C[\alpha]}\, \supset I$$

Because it is not the case that $Q_1[\beta], \Diamond Q_2[\alpha] \vdash Q_2[\beta]$, assuming $Q_1[\beta], \Diamond Q_2[\alpha] \vdash Q_2[\beta]$ is contradictory. Therefore, such an assumption allows us to prove anything, and in particular it allows us to prove $Q_1[\beta], \Diamond Q_2[\alpha] \vdash C[\alpha]$. In other words, for every world accessible from α, it is the case that $Q_1[\beta], \Diamond Q_2[\alpha] \vdash Q_2[\beta]$ implies $Q_1[\beta], \Diamond Q_2[\alpha] \vdash C[\alpha]$. We can try to use this instance as the template for filling in those question marks, giving us the following $\Diamond E$ rule:

$$\dfrac{\Gamma \vdash \Diamond A[w] \quad \forall w'.\, w \prec w' \longrightarrow \Gamma \vdash A[w'] \longrightarrow \Gamma \vdash C[w'']}{\Gamma \vdash C[w'']}\, \Diamond E$$

Warning: this definition breaks the consistency of logic.

The above rule is, it will turn out, very nearly the one we want, but without some additional restrictions it results in logical inconsistency, which is Very Bad. The blame falls on the use of $\Gamma \vdash A[w']$ in the premise of $\Diamond E$. When we introduced the higher-order formulation of reflection over the accessibility relation, we emphasized that we could only do so because the accessibility relation could be completely defined before the meaning of the hypothetical judgment $\Gamma \vdash A[w]$ was discussed. This is therefore an illegitimate "higher-order formulation," because we are using logical reflection on the definition of $\Gamma \vdash A[w]$ to define $\Gamma \vdash A[w]$. Within such self-reference, contradiction frequently lurks.

To rescue the our logic from this inconsistency, we first observe that $\Diamond E$ is reflecting on the definition of $\Gamma \vdash A[w']$ when defining $\Gamma \vdash C[w'']$. Therefore, if we can completely define "A true at w'" before discussing the meaning of "C is true at w''," the $\Diamond E$ rule can be again considered sensible. This means that we will define provability at some worlds w' *before* we define provability at other worlds w, and we need some way of describing which worlds get defined first. For this, we will use the accessibility relation.

In our previous example where $\alpha \prec \beta$, we wanted to prove $\Diamond Q_2 \supset C$ at world α by reflecting over provability at β; this means that provability at β had to be defined first. In general, when we define provability at a particular world w, we must previously and independently be able to define provability at all the worlds w' accessible from w' – and to do *that* we must previously be able to define provability at all the worlds accessible from one of *those* worlds, and so on. This obviously means that our accessibility relation can have no cycles, but it also implies something stronger – the accessibility relation must be *converse well-founded* (sometimes called *upwards well-founded*) – there must be no infinite ascending chains $w_0 \prec w_1 \prec w_2 \ldots$ The "count-up" accessibility relation that we considered earlier is incompatible with the $\Diamond E$ rule – it is well-founded but not converse

well-founded. On the other hand, the "count-down" accessibility relation is not well-founded, but it is converse well-founded, and the "infinite options" accessibility relation, as well as all of the non-reflexive finite accessibility relations we have considered, are all converse well-founded.

Even with a converse well-founded accessibility relation, we still can't use the $\Diamond E$ rule above, because it reflects on provability at w' when defining $\Gamma \vdash C[w'']$ for some potentially unrelated world w''. We do, however, know that provability at world w can reflect over provability at world w', so our solution is to require the premise (where we use $\Diamond A$) and the conclusion (where we prove C) to mention the *same* world w.[7] Our new $\Diamond E$ rule looks like this:

$$\frac{\Gamma \vdash \Diamond A[w] \quad \forall w'.\, w \prec w' \longrightarrow \Gamma \vdash A[w'] \longrightarrow \Gamma \vdash C[w]}{\Gamma \vdash C[w]}\ \Diamond E$$

Now that we have restricted the accessibility relation and tethered the $\Diamond E$ rule, one additional requirement, which we express as a defining principle of the logic, ensures that rules such as $\Diamond E$ are sensible. If $\alpha \prec \beta$, then keeping with the idea that provability at β has to be completely defined before provability at α is discussed, $\Gamma \vdash C[\beta]$ needs to be unaffected by assumptions of the form $A[\alpha]$ in Γ. We say that $\Gamma =_w \Gamma'$ if, for every A and every w' accessible from w in zero or more steps, $A[w']$ is in Γ if and only if it is in Γ'. This allows us to state a *strengthening principle* which emphasizes that only the hypotheses at current or (transitively) accessible worlds are relevant to provability at a given world.

— *Strengthening principle*: If $\Gamma =_w \Gamma'$ and $\Gamma \vdash A[w]$, then $\Gamma' \vdash A[w]$.

Because $\Gamma, A[\alpha] =_\beta \Gamma$ in our example above, this defining principle establishes that, if we can prove $\Gamma, A[\alpha] \vdash C[\beta]$, then the $A[\alpha]$ was not necessary for the proof and we can prove $\Gamma \vdash C[\beta]$.

To finish our discussion of the defining principles of constructive provability logic, we need only to discuss the substitution principle. It is not obvious that there is any problem with the general substitution principle that we have used so far: if $\Gamma \vdash A[w]$ and $\Gamma, A[w] \vdash C[w']$ then $\Gamma \vdash C[w']$. We believe that this strong substitution principle is, in fact, true; however, we have been unable to prove it. Therefore, we instead use a weaker "tethered" substitution principle that is nevertheless sufficient for our purposes.

Definition of hypothetical judgment for constructive provability logic:
— *Hypothesis rule*: If $A_i[w_i] \in \Gamma$, then $\Gamma \vdash A_i[w_i]$.
— *Weakening principle*: If $\Gamma \subseteq_w \Gamma'$ and $\Gamma \vdash A[w]$, then $\Gamma' \vdash A[w]$.
— *Strengthening principle*: If $\Gamma =_w \Gamma'$ and $\Gamma \vdash A[w]$, then $\Gamma' \vdash A[w]$.
— *Substitution principle*: If $\Gamma \vdash A[w]$ and $\Gamma, A[w] \vdash C[w]$, then $\Gamma \vdash C[w]$.

2.4 Agda and consistency

We said that the original $\Diamond E$ rule lead to logical inconsistency if used without restrictions; we have demonstrated this in Agda (see `Inconsistency.agda`). The example works like this: if Q is

[7] This process has been called *tethering* the modal logic.

an atomic proposition and there is only one world α such that $\alpha \prec \alpha$ (obviously this means that the accessibility relation is not converse well-founded), then we can both give a proof of $\Diamond Q[\alpha] \vdash Q[\alpha]$ *and* a proof that it is not the case that $\Diamond Q[\alpha] \vdash Q[\alpha]$. Since "it is not the case that" is shorthand for "implies a contradiction," from modus ponens we can then get a closed proof of a contradiction, which we can use to prove anything. And note that "anything" doesn't just mean "$\Gamma \vdash J$ for any Γ and any J," it means that $2 + 2 = 5$, that every Turing machine halts, and that the harmonic series converges. The $\Diamond E$ rule makes *Agda* inconsistent.

Doesn't this mean that Agda is inconsistent as a logic? No, because in order to get Agda to accept this file, we had to turn off the "positivity check," Agda's way of ensuring that higher-order formulations of rules do not create precisely the kind of catastrophic self-reference that `Inconsistency.agda` demonstrates. However, we *also* turn off the positivity check in our formalization of constructive provability logic! How do we know that this does not lead to the same kind of inconsistency?

In the discussion above, we relied on the converse well-foundedness of the accessibility relation to ensure that, when $w \prec w'$, we can completely define $\Gamma \vdash A[w']$ before discussing $\Gamma \vdash A[w]$. Our Agda formalization defines provability in a convenient, generic fashion, parametrized over an arbitrary converse well-founded accessibility relation. Unfortunately, Agda's automatic, conservative positivity checker does not have the sophistication necessary to "understand" our claim that the converse well-founded accessibility relation makes the definition reasonable; by turning off the positivity checker, we declare that we are striking out on our own authority.

Of course, one of the reasons for using Agda in the first place was to fix the metalogic and thereby reduce reliance on our own authority! If we want to take this view seriously, then there are two subsystems of constructive provability logic that can rely fully on Agda – systems with finite accessibility relations and those with finitely branching accessibility relations. Using Agda's module system, it is possible to parametrize the definition of provability at a world w over provability at all worlds w' accessible from w. If we use this module-based definition, we can instantiate the logic "by hand" as long as the accessibility relation is finite, so for finite accessibility relations Agda will fully accept the definition of constructive provability logic. Similarly, if we have an accessibility relation where only finitely many worlds are accessible from any given world, then given a world w it is a finite and mechanical process to instantiate constructive provability logic at w and at all the worlds accessible from w (and all the worlds accessible from those worlds ...). Even though we cannot instantiate *all* of constructive provability logic for the "count-down" accessibility relation in this manner, we can fully instantiate constructive provability logic for any particular world w_i.

This discussion leaves infinitely branching but converse well-founded accessibility relations (such as the "infinite options" accessibility relation) tainted with suspicion, and, as we will see in the later discussion of the $\Box E$ rule, there are other reasons to be somewhat dubious of infinitely branching accessibility relations. A better understanding of the choices involved in the use of infinitely branching accessibility relations is definitely an interesting avenue for future investigation.

3 Natural deduction

Now that we have presented the judgmental principles and intuitions behind constructive provability logic, we will present natural deduction for minimal **CPL**, discussing local soundness and completeness for each connective. The Agda formalization of the rules introduced in Section 3.1 through Section 3.4 can be found in `MinimalCPL/Core.agda`.

3.1 Implication

The rules for implication introduction and elimination are unsurprisingly identical to those from the Simpson-style presentation, and the arguments for local soundness and completeness are again unchanged.

$$\frac{\Gamma, A[w] \vdash B[w]}{\Gamma \vdash A \supset B[w]} \supset I \qquad \frac{\Gamma \vdash A \supset B[w] \quad \Gamma \vdash A[w]}{\Gamma \vdash B[w]} \supset E$$

3.2 Modal possibility $\Diamond A$

As discussed in the previous section, modal possibility $\Diamond A$ is defined as follows: we can prove $\Diamond A[w]$ if, for a world w' that is accessible from w (in our predetermined accessibility relation), we can prove $A[w']$. We can make use of a proof of $\Diamond A[w]$ to prove $C[w]$ if we can produce a mapping from worlds w' accessible from w and proofs of A at w' to proofs of C at w.

$$\frac{w \prec w' \quad \Gamma \vdash A[w']}{\Gamma \vdash \Diamond A[w]} \Diamond I \qquad \frac{\Gamma \vdash \Diamond A[w] \quad \forall w'.\, w \prec w' \longrightarrow \Gamma \vdash A[w'] \longrightarrow \Gamma \vdash C[w]}{\Gamma \vdash C[w]} \Diamond E$$

Again, this definition is only reasonable because we require that the accessibility relation to be converse well-founded so that provability at the accessible world w' can be defined *a priori* and independently from provability at w. We will now perform our sanity checks of local soundness and completeness. To show local soundness we present the relevant local reduction.

$$\frac{\dfrac{\begin{array}{c}\mathcal{D}_w \\ w \prec w'\end{array} \quad \begin{array}{c}\mathcal{D}_1 \\ \Gamma \vdash A[w']\end{array}}{\Gamma \vdash \Diamond A[w]} \Diamond I \qquad \begin{array}{c}\mathcal{D}_2 \\ \forall w'.\, w \prec w' \longrightarrow \Gamma \vdash A[w'] \longrightarrow \Gamma \vdash C[w]\end{array}}{\Gamma \vdash C[w]} \Diamond E \quad \Longrightarrow_R \quad \begin{array}{c}(\mathcal{D}_2\ \mathcal{D}_w)\ \mathcal{D}_1 \\ \Gamma \vdash C[w]\end{array}$$

Recalling that $\mathcal{D}_2$ is actually a theorem in the metalogic, the local reduction is performed by meta-level theorem application. We use a notation of function application since we view $\mathcal{D}_2$ as a mapping, therefore we need to supply a proof of $w \prec w'$ (in this case $\mathcal{D}_w$) and a proof of $\Gamma \vdash A[w']$ (which is exactly $\mathcal{D}_1$) to produce the required result.

The local expansion that is evidence of local completeness might be slightly surprising:

$$\begin{array}{c}\mathcal{D} \\ \Gamma \vdash \Diamond A[w]\end{array} \quad \Longrightarrow_E \quad \frac{\begin{array}{c}\mathcal{D} \\ \Gamma \vdash \Diamond A[w]\end{array} \quad \Diamond I}{\Gamma \vdash \Diamond A[w]} \Diamond E$$

We expand the proof of $\Diamond A[w]$ by applying $\Diamond E$ to the initial derivation $\mathcal{D}$ and to the actual rule of $\Diamond$ introduction. The second premise for $\Diamond E$ requires a higher-order mapping of proofs $w \prec w'$ (for all w') and $A[w']$ to proofs of $\Diamond A[w]$, but that is exactly the definition of $\Diamond I$. Put another way, the proof of the theorem *If* $w \prec w'$ *and* $\Gamma \vdash A[w']$ *then* $\Gamma \vdash \Diamond A[w]$ is just "by application of the rule $\Diamond I$ to the assumptions," and we have already established that the way we satisfy a higher-order premise is with a theorem. The notation here is admittedly problematic; it is actually somewhat more natural in the Agda development where proofs do not have the tree-like two-dimensional structure that we use on paper.

3.3 Modal necessity

We now proceed to modal necessity $\Box A$. Even though our examples in the previous section exclusively used possibility as a motivating example, it is straightforward to define modal necessity in Simpson-style modal logics. Whereas modal possibility usually is thought of as having an "existential character" (there *exists* some accessibly world where A is true), modal necessity has a "universal character" (at *every* accessible world, A is true). This is reflected in the introduction rule for modal possibility:

$$\frac{\forall w'.\, w \prec w' \longrightarrow \Gamma \vdash A[w']}{\Gamma \vdash \Box A[w]}\ \Box I$$

If the introduction rule requires a proof of A at every accessible world, a reasonable elimination rule might ask that we select some accessible world w' and assume that A is provable at that world. A rule capturing this intuition, which resembles the $\Box E$ rule in Simpson-style modal logic, looks like this:

$$\frac{\Gamma \vdash \Box A[w] \quad w \prec w' \quad \Gamma \vdash A[w'] \longrightarrow \Gamma \vdash C[w]}{\Gamma \vdash C[w]}\ \Box E'$$

This rule is locally sound, as we can see from the following local reduction:

$$\frac{\dfrac{\begin{matrix}\mathcal{D}_1\\ \forall w'.\, w \prec w' \longrightarrow \Gamma \vdash A[w']\end{matrix}}{\Gamma \vdash \Box A[w]}\ \Box I \qquad \begin{matrix}\mathcal{D}_w & & \mathcal{D}_2\\ w \prec w' & \Gamma \vdash A[w'] & \longrightarrow \Gamma \vdash C[w]\end{matrix}}{\Gamma \vdash C[w]}\ \Box E' \quad \Longrightarrow_R \quad \begin{matrix}\mathcal{D}_2\ (\mathcal{D}_1\ \mathcal{D}_w)\\ \Gamma \vdash C[w]\end{matrix}$$

We reduce the proof of $C[w]$ through two meta-level theorem applications. We first apply $\mathcal{D}_1$ to $\mathcal{D}_w$ to obtain a proof of A at w', which we then supply to $\mathcal{D}_2$ to obtain the required proof of C at w.

However, as we will now see, the elimination rule is not locally complete for an arbitrary converse well-founded accessibility relation. If we consider our example accessibility relation:

we can always reconstruct a proof of $\Box A[w]$ since there are only a finite number of successors for each world. We need only exhaustively apply $\Box E'$ for each possible successor of w. Let's see how this works at two representative worlds:

Local completeness at ω. We have a proof $\mathcal{D}$ of $\Gamma \vdash C[\omega]$. It is a simple lemma that $\forall w'.\, \omega \prec w' \longrightarrow \Gamma \vdash A[w']$: we perform case analysis on the accessibility relation, which is trivial because there are no worlds w' accessible from ω.

With this lemma, we can give the local expansion at ω:

$$\dfrac{\dfrac{}{\forall w'.\, \omega \prec w' \longrightarrow \Gamma \vdash A[w']}\ \textit{(aforementioned lemma)}}{\Gamma \vdash A[\omega]}\ \Box I$$

Note that the expansion doesn't mention the proof $\mathcal{D}$ at all; this is similar to the local expansion of the trivially true proposition $\top$.

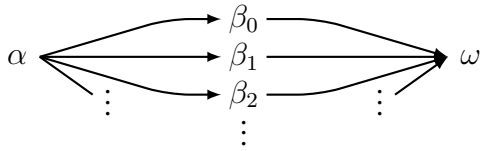
Local completeness at α. We have a proof $\mathcal{D}$ of $\Gamma \vdash C[\alpha]$. It is a simple lemma that, if $\Gamma \vdash A[\beta]$ and if $\Gamma \vdash A[\omega]$, then $\forall w'.\, \alpha \prec w' \longrightarrow \Gamma \vdash A[w']$: we perform case analysis on the accessibility relation; if $w' = \beta$ then we use the first premise and if $w' = \omega$ then we use the second premise.

With this lemma, we can give the local expansion at ω:

$$\dfrac{\dfrac{\overset{\mathcal{D}}{\Gamma \vdash \Box A[\alpha]} \quad \dfrac{}{\alpha \prec \beta}\ \textit{axiom}}{\Gamma \vdash \Box A[\alpha]}\ \Box E'_{\mathcal{D}_1} \quad \dfrac{\overset{\mathcal{D}}{\Gamma \vdash \Box A[\alpha]} \quad \dfrac{}{\alpha \prec \omega}\ \textit{axiom}}{\Gamma \vdash \Box A[\alpha]}\ \Box E'_{\mathcal{D}_2} \quad \dfrac{\forall w'.\, \alpha \prec w' \longrightarrow \Gamma \vdash A[w']}{\Gamma \vdash \Box A[\alpha]}\ \Box I\ (\textit{(aforementioned lemma)}\ \mathcal{D}_1)\ \mathcal{D}_2}$$

The third premise of $\Box E'_{\mathcal{D}_1}$ introduces a new scoped assumption $\mathcal{D}_1 :: \Gamma \vdash A[\beta]$, and the third premise of $\Box E'_{\mathcal{D}_2}$ introduces a scoped assumption $\mathcal{D}_2 :: \Gamma \vdash A[\omega]$. This is another instance where the traditional two-dimensional notation for proofs comes close to breaking down; the Agda code for both of these local expansions is in `AltBoxE.agda`.

The previous examples sufficed to illustrate the general structure of a local expansion with $\Box E'$ – from the bottom to top, we use one instance of $\Box E'$ for each of the worlds accessible from the current world w. Having done this, we have a scoped assumption $\Gamma \vdash A[w']$ for each $w \prec w'$, which allows us to apply the $\Box I$ rule. This works in cases when only finitely many worlds are accessible from a given world, but breaks down if we consider the "infinite options" accessibility relation:



We have a situation where α has infinitely many successors and ω has infinitely many predecessors. In this case, we cannot expand a proof of $\Box A[\alpha]$ using $\Box E'$ since we would need to apply the rule infinitely many times to obtain enough information to construct the necessary mapping to apply $\Box I$. We fix this by adopting a different elimination rule that does not require us to select some individual accessible world w'. Instead, we precisely capture all the information present in the

introduction of $\Box A[w]$ by assuming we have a mapping from proofs of all w' accessible from w to proofs of A at w', which we can then use to prove C at w.

$$\frac{\Gamma \vdash \Box A[w] \quad (\forall w'.\, w \prec w' \longrightarrow \Gamma \vdash A[w']) \longrightarrow \Gamma \vdash C[w]}{\Gamma \vdash C[w]}\ \Box E$$

This is an unusual rule. It defies the intuitive "universal character" of modal necessity that we can see in the $\Box E'$ rule, and it is also the first *third-order* formulation we have used (previously we have only used "second-order" higher-order formulations where implications were not nested to the left of other implications). However, we can take some comfort in the fact that $\Box E$ and $\Box E'$ are actually inter-derivable as long as the accessibility relation is finitely branching – one direction of this proof can be found in `MinimalCPL/Core.agda`, and the other in `AltBoxE.agda`.

Furthermore, as we will now see, our new definition of introduction and elimination for $\Box$ is locally sound and complete. Local soundness is witnessed by a local reduction that makes use of the higher-order formulation by applying the mapping $\mathcal{D}_2$ to $\mathcal{D}_1$ to produce the proof of $C[w]$:

$$\frac{\dfrac{\begin{array}{c}\mathcal{D}_1\\ \forall w'.\, w \prec w' \longrightarrow \Gamma \vdash A[w']\end{array}}{\Gamma \vdash \Box A[w]}\ \Box I \qquad \dfrac{\begin{array}{c}\mathcal{D}_2\\ (\forall w'.\, w \prec w' \longrightarrow \Gamma \vdash A[w']) \longrightarrow \Gamma \vdash C[w]\end{array}}{\Gamma \vdash C[w]}\ \Box E}{\Gamma \vdash C[w]} \quad \Longrightarrow_R \quad \begin{array}{c}\mathcal{D}_2\ \mathcal{D}_1\\ \Gamma \vdash C[w]\end{array}$$

The reason our definition of $\Box E$ is strong enough is that it is precisely a mapping of proofs of $w \prec w'$ to proofs of $A[w']$ that is needed to introduce $\Box A[w]$ to begin with. Local completeness thus holds since the second premise to $\Box E$ exactly mirrors the structure of $\Box I$, making us able to expand a proof of $\Box A[w]$ by applying $\Box E$ and using $\Box I$ as its second premise. This new local expansion mirrors the local expansion for modal possibility.

$$\begin{array}{c}\mathcal{D}\\ \Gamma \vdash \Box A[w]\end{array} \quad \Longrightarrow_E \quad \frac{\begin{array}{c}\mathcal{D}\\ \Gamma \vdash \Box A[w]\end{array} \quad \Box I}{\Gamma \vdash \Box A[w]}\ \Box E$$

3.4 Not-possibility and not-necessity

In "Negation in the light of modal logic," Došen gives a classical Kripke semantics for negation; he writes "not A" as $\not\Diamond A$ and says "not A holds at w if and only if A doesn't hold at any world accessible from w"[2]. In Došen's setting, $\not\Diamond$ corresponds to regular intuitionistic negation.

Just as we rely on reflection over the accessibility relation and over provability to give meaning to $\Box$ and $\Diamond$, we can reflect over *non-provability* to give meaning to Došen's modal negation in constructive provability logic. Doing so allows us to simplify the discussion in Section 2.3. In that discussion, we reflected the fact that $Q_1[\beta] \vdash Q_2[\beta]$ is not the case by proving $Q_1[\beta] \vdash \Diamond Q_2 \supset C[\alpha]$ for any C. Using the natural interpretation of Došen's modal negation in constructive provability logic, we can instead prove $Q_1[\beta] \vdash \not\Diamond Q_2[\alpha]$ – we say that under the assumption $Q_1[\beta]$, Q_2 is not possible at α.

We use $\neg(\Gamma \vdash A[w])$ ("it is not the case that $\Gamma \vdash A[w]$") as shorthand for $\Gamma \vdash A[w] \longrightarrow 0$, where 0 is meta-level contradiction. This means that there is a mapping from proofs of $\Gamma \vdash A[w]$ to a proof of contradiction, which indicates that $\Gamma \vdash A[w]$ is contradictory. Given this notation, it is simple to define $\not\Diamond$: we are thus justified in concluding $\not\Diamond A[w]$ if we can prove that, for any w' accessible from w, it is not the case that $A[w']$. The way we use proofs of $\not\Diamond A[w]$ is similar to the way we used proofs of $\Box A[w]$, except we require that $A[w']$ be false instead of true (for all w' accessible from w).

$$\frac{\forall w'.\, w \prec w' \longrightarrow \neg(\Gamma \vdash A[w'])}{\Gamma \vdash \not\Diamond A[w]}\ \not\Diamond I$$

$$\frac{\Gamma \vdash \not\Diamond A[w] \quad (\forall w'.\, w \prec w' \longrightarrow \neg(\Gamma \vdash A[w'])) \longrightarrow \Gamma \vdash C[w]}{\Gamma \vdash C[w]}\ \not\Diamond E$$

The local reduction is quite similar to the reduction for modal necessity, but we now reflect over non-provability at all accessible worlds.

$$\frac{\dfrac{\begin{array}{c}\mathcal{D}_1\\ \forall w'.\, w \prec w' \longrightarrow \neg(\Gamma \vdash A[w'])\end{array}}{\Gamma \vdash \not\Diamond A[w]}\ \not\Diamond I \qquad \begin{array}{c}\mathcal{D}_2\\ (\forall w'.\, w \prec w' \longrightarrow \neg(\Gamma \vdash A[w'])) \longrightarrow \Gamma \vdash C[w]\end{array}}{\Gamma \vdash C[w]}\ \not\Diamond E$$

$$\Longrightarrow_R \quad \begin{array}{c}\mathcal{D}_2\ \mathcal{D}_1\\ \Gamma \vdash C[w]\end{array}$$

The local expansion for $\not\Diamond$ is also unsurprising given the local reduction for possibility and necessity:

$$\begin{array}{c}\mathcal{D}\\ \Gamma \vdash \not\Diamond A[w]\end{array} \quad \Longrightarrow_E \quad \frac{\begin{array}{c}\mathcal{D}\\ \Gamma \vdash \not\Diamond A[w]\end{array} \quad \not\Diamond I}{\Gamma \vdash \not\Diamond A[w]}\ \not\Diamond E$$

Došen also considered a modal negation that was dual to not-possibility; we follow Došen in calling this operator $\not\Box$, and just as Došen relates $\not\Diamond$ to intuitionistic negation he relates $\not\Box$ to its dual, called *Brouwerian negation* in the literature. We are justified in concluding $\not\Box A[w]$ if we can show that $A[w']$ is not provable for some w' accessible from w. We use proofs of $\not\Box A[w]$ to prove $C[w]$ if we can produce a higher-order mapping that, given a proof that A is contradictory at w' for some w' accessible from w, produces a proof of $C[w]$.

$$\frac{w \prec w' \quad \neg(\Gamma \vdash A[w'])}{\Gamma \vdash \not\Box A[w]}\ \not\Box I \qquad \frac{\Gamma \vdash \not\Box A[w] \quad \forall w'.\, w \prec w' \longrightarrow \neg(\Gamma \vdash A[w']) \longrightarrow \Gamma \vdash C[w]}{\Gamma \vdash C[w]}\ \not\Box E$$

The local reduction and expansion are completely analogous to those of $\Diamond$, with the appropriate changes to reflection over non-provability:

$$\frac{\dfrac{\begin{array}{c}\mathcal{D}_w\\ w \prec w'\end{array} \quad \begin{array}{c}\mathcal{D}_1\\ \neg(\Gamma \vdash A[w'])\end{array}}{\Gamma \vdash \not\Box A[w]}\ \not\Box I \qquad \begin{array}{c}\mathcal{D}_2\\ \forall w'.\, w \prec w' \longrightarrow \neg(\Gamma \vdash A[w']) \longrightarrow \Gamma \vdash C[w]\end{array}}{\Gamma \vdash C[w]}\ \not\Box E$$

$$\Longrightarrow_R \quad \begin{array}{c}(\mathcal{D}_2\ \mathcal{D}_w)\ \mathcal{D}_1\\ \Gamma \vdash C[w]\end{array}$$

$$\overset{\mathcal{D}}{\Gamma \vdash \not\square A[w]} \quad \Longrightarrow_E \quad \frac{\Gamma \vdash \not\square A[w] \quad \not\square I}{\Gamma \vdash \not\square A[w]}\ \not\square E$$

The definitions of $\square$ and $\not\Diamond$ (resp. $\Diamond$ and $\not\square$) are similar in having a universal (resp. existential) character, but the primary logical tension is between $\Diamond$ and $\not\Diamond$ (resp. $\square$ and $\not\square$). Assuming both $\Diamond A$ and $\not\Diamond A$ (resp. $\square A$ and $\not\square A$) at the same world is contradictory in the sense that they allow us to prove any other proposition. In other words, both $\not\Diamond A \supset \Diamond A \supset C$ and $\not\square A \supset \square A \supset C$ are axioms of minimal **CPL** (see `MinimalCPL/Axioms.agda`).

3.5 Verifying the defining principles

The previous sections introduced the full natural deduction presentation of minimal CPL and discussed the local soundness and completeness of the introduction and elimination rules for implication $A \supset B$, modal possibility $\Diamond A$, modal necessity $\square A$, modal not-possibility $\not\Diamond A$, and modal not-necessity $\not\square A$. The local soundness and completeness of the modal connectives relied on meta-level theorem application, but local soundness for implication, and therefore for the logic as a whole, relied on the defining principles of constructive provability logic. To recall:

Definition of hypothetical judgment for constructive provability logic:
- *Hypothesis rule*: If $A_i[w_i] \in \Gamma$, then $\Gamma \vdash A_i[w_i]$.
- *Weakening principle*: If $\Gamma \subseteq_w \Gamma'$ and $\Gamma \vdash A[w]$, then $\Gamma' \vdash A[w]$.
- *Strengthening principle*: If $\Gamma =_w \Gamma'$ and $\Gamma \vdash A[w]$, then $\Gamma' \vdash A[w]$.
- *Substitution principle*: If $\Gamma \vdash A[w]$ and $\Gamma, A[w] \vdash C[w]$, then $\Gamma \vdash C[w]$.

We did not directly rely on the strengthening principle, but it was necessary to ensure that our higher-order formulations made sense in the first place. In this section, we will circle back around and ensure that our definitions respect the logic's defining principles. The Agda formalization of the proofs in this section can be found in `MinimalCPL/NatDeduction.agda`.

We prove both the weakening principle and strengthening principles by proving a stronger statement that uses a third relation on contexts $\Gamma \subseteqq_w \Gamma'$. We say that $\Gamma \subseteqq_w \Gamma'$ if:

- $A[w] \in \Gamma$ implies $A[w] \in \Gamma'$, and if
- For any w' accessible in one or more steps from w, $A[w'] \in \Gamma$ if and only if $A[w'] \in \Gamma'$.[8]

It is straightforward to show that both $\Gamma \subseteq_w \Gamma'$ and $\Gamma =_w \Gamma'$ imply $\Gamma \subseteqq_w \Gamma'$, so Theorem 3 below verifies both the weakening and strengthening principles.

Theorem 3 (Weakening)**.** *If $\Gamma \subseteqq_w \Gamma'$ and $\Gamma \vdash A[w]$, then $\Gamma' \vdash A[w]$, and the resulting proof has the same shape.*

Proof. By induction on the accessibility relation and on the proof of $\Gamma \vdash A[w]$. □

[8]For technical reasons – namely, that it is simpler to avoid proving decidability of the accessibility relation – we use a slightly stronger version of $\Gamma \subseteqq_w \Gamma'$ in the Agda development. We show that this relation implies the definition above in `AltPartialOrder.agda`.

This is the first time we have explicitly discussed induction on the accessibility relation. We have said that the definition of constructive provability logic is parametrized over an arbitrary converse well-founded accessibility relation, and informally described a converse well-founded accessibility relation as one with no infinite ascending chains $(w_0 \prec w_1 \prec \ldots)$. Another definition of a converse well-founded accessibility relation, and the one that we use in the Agda formalization (see `Accessibility/Inductive.agda`), is that an accessibility relation is converse well-founded if it *admits an induction principle*. In other words, a binary relation $w \prec w'$ over an arbitrary set W is converse-well founded if, for any property $P(w)$, we know $P(w)$ holds for every w if we know that, for every w, $P(w)$ holds under the assumption of $P(w')$ for every $w \prec w'$.

We actually prove Theorem 3 as two separate theorems in the Agda development. The first proof is by induction over the accessibility relation, but it does not establish that the resulting proof has the same shape. A second theorem, which relies on the first one, establishes that the resulting proof has the same shape, but only the part of the proof that is at world w – this is what we need to get induction for the substitution principle to work, and the proof does not require induction over the accessibility relation. The details of the "totally nameless representation" we use to capture the shape of the proof are outside the scope of this report, but are discussed elsewhere [10].

Theorem 4 (Substitution)**.** *If* $\Gamma \vdash A[w]$ *and* $\Gamma, A[w] \vdash C[w]$*, then* $\Gamma \vdash C[w]$.

Proof. We refer to the proof of the first premise, $\Gamma \vdash A[w]$, as $\mathcal{D}$ and proceed by induction on the shape of $\Gamma, A[w] \vdash C[w]$. We present only the cases for implication and $\Diamond$. The remaining cases follow similar reasoning principles and are included in our Agda development.

Case:

$$\dfrac{\begin{array}{c}\mathcal{D}_1 \\ \Gamma, A[w], C_1[w] \vdash C_2[w]\end{array}}{\Gamma, A[w] \vdash C_1 \supset C_2[w]} \supset I$$

$\mathcal{D}_1' :: \Gamma, C_1[w], A[w] \vdash C_2[w]$ by weakening principle on $\mathcal{D}_1$
$\mathcal{F}_1 :: \Gamma, C_1[w] \vdash C_2[w]$ by i.h. on $\mathcal{D}$ and $\mathcal{D}_1'$
$\mathcal{F} :: \Gamma \vdash C_1 \supset C_2[w]$ by $\supset I$ on $\mathcal{F}_1$

Case:

$$\dfrac{\begin{array}{cc}\mathcal{D}_1 & \mathcal{D}_2 \\ \Gamma, A[w] \vdash C_1 \supset C_2[w] & \Gamma, A[w] \vdash C_1[w]\end{array}}{\Gamma, A[w] \vdash C_2[w]} \supset E$$

$\mathcal{F}_1 :: \Gamma \vdash C_1 \supset C_2[w]$ by i.h. on $\mathcal{D}$ and $\mathcal{D}_1$
$\mathcal{F}_2 :: \Gamma \vdash C_1[w]$ by i.h. on $\mathcal{D}$ and $\mathcal{D}_2$
$\mathcal{F} :: \Gamma \vdash C_2[w]$ by $\supset E$ on $\mathcal{F}_1$ and $\mathcal{F}_2$

Case:

$$\dfrac{\begin{array}{cc}\mathcal{D}_w & \mathcal{D}_1 \\ w \prec w' & \Gamma, A[w] \vdash C[w']\end{array}}{\Gamma, A[w] \vdash \Diamond C[w]} \Diamond I$$

$\mathcal{F}_1 :: \Gamma \vdash C[w']$ by strengthening principle on $\mathcal{D}_1$
$\mathcal{F} :: \Gamma \vdash \Diamond C[w]$ by $\Diamond I$ on $\mathcal{D}_w$ and $\mathcal{F}_1$

Case:

$$\dfrac{\begin{array}{cc}\mathcal{D}_1 & \mathcal{D}_2 \\ \Gamma, A[w] \vdash \Diamond B[w] & \forall w'.\, w \prec w' \longrightarrow \Gamma, A[w] \vdash B[w'] \longrightarrow \Gamma, A[w] \vdash C[w]\end{array}}{\Gamma, A[w] \vdash C[w]}\ \Diamond E$$

$\mathcal{F}_1 :: \Gamma \vdash \Diamond B[w]$ by i.h. on $\mathcal{D}_1$
$\mathcal{F}_2 :: \forall w'.\, w \prec w' \longrightarrow \Gamma \vdash B[w'] \longrightarrow \Gamma \vdash C[w]$
by the following hypothetical reasoning:
Assume that for an arbitrary w' we have $\mathcal{D}_w :: w \prec w'$ and $\mathcal{D}_0 :: \Gamma \vdash B[w']$
$\mathcal{D}_0' :: \Gamma, A[w] \vdash B[w]$ by strengthening principle on $\mathcal{D}_0$
$\mathcal{D}_2' :: \Gamma, A[w] \vdash C[w]$ by $\mathcal{D}_2$ on $\mathcal{D}_w$ and $\mathcal{D}_0'$
$\mathcal{F}_2' :: \Gamma \vdash C[w]$ by i.h. on $\mathcal{D}_2'$
$\mathcal{F} :: \Gamma \vdash C[w]$ by $\Diamond E$ on $\mathcal{F}_1$ and $\mathcal{F}_2$

As we previously stated, the remaining cases can be found in the Agda development (see `MinimalCPL/NatDeduction.agda`). □

There are two things to note about the substitution theorem before we turn to the sequent calculus for constructive provability logic. First, we rely critically on the fact that our induction is on the *shape* of the derivation in $\supset I$ when we use the weakening principle to exchange the premises $A[w]$ and $C_1[w]$ and call the induction hypothesis on the resulting derivation. Second, substitution at a given world w is *totally independent* of whether the substitution principle holds at any of the worlds accessible from w – when we consider proofs about truth at worlds w' accessible from w we turn to the weakening and strengthening principles, not the induction hypothesis (the $\Diamond I$ case is a particularly good example of this).

In the next section, we will see that the *global soundness* of the logic at any given world is similarly independent of the soundness of the logic at any accessible world. While this is not a particularly useful property in the totally uniform presentation of constructive provability logic that we have given here, it introduces the interesting possibility that **CPL** can be used non-uniformly to reason about *families* of logics connected by an accessibility relation. Even if some of the logics are poorly-behaved or even inconsistent, we can reason consistently about the (potentially inconsistent) logics as long as the reasoning is being done at a world where we can prove consistency; inconsistency at some world does not threaten the consistency of worlds that can access (and therefore reason about) that world.

4 Sequent calculus

So far we have presented the defining principles of a natural deduction system for constructive provability logic, introduced the connectives of minimal **CPL**, and shown by the sanity checks of

local soundness and local completeness that minimal **CPL** is defined in a reasonable way. However, the local checks in the previous section are insufficient to establish the *global* soundness of the logic. One statement of global soundness is that we want $\cdot \vdash A[w]$ to *not* be true for an arbitrary A – logics that can prove anything aren't especially useful outside of politics.

We have already discussed one theorem that touches on global soundness: in Section 2.3 we presented Theorem 2, which states that for distinct propositions Q_1 and Q_2 it is not the case that $\cdot \vdash Q_1 \supset Q_2[\beta]$. However, we said at the time that it is difficult to prove this sort of statement in a natural deduction system. If we try to prove that $\cdot \vdash Q_1 \supset Q_2[\beta]$ is not the case by assuming that we have a proof of it and proving a contradiction, essentially all we can do is case analysis on the structure of the assumed proof. If the last rule is $\supset I$, then we have a smaller proof of $Q_1[\beta] \vdash Q_2[\beta]$, which somehow feels like progress. However, we also have to deal with the case where the last rule is $\supset I$ and we have two subproofs, one a proof of $\cdot \vdash A[\beta]$ and the other a proof of $\cdot \vdash A \supset (Q_1 \supset Q_2)[\beta]$. That new formula A can be anything, which effectively prevents us from simply case analyzing our rules in this bottom-up fashion. A sequent calculus system, on the other hand, obeys the *sub-formula property*: if we have a sequent proof of $\cdot \Rightarrow A[\beta]$, we know that all the subproofs of that proof will only mention sub-formulas of A.

A sequent calculus is a proof system composed of so-called right and left rules. Right rules show us how to prove a proposition, and are usually quite similar to the natural deduction introduction rules (which, in general, obey the sub-formula property already in a natural deduction system). The right rule for implication, for instance, is identical to the implication introduction rule except that we use $\Rightarrow$ instead of $\vdash$ to represent the hypothetical judgment of the sequent calculus.

$$\frac{\Gamma, A[w] \Rightarrow B[w]}{\Gamma \Rightarrow A \supset B[w]} \supset R$$

Left rules, on the other hand, show us how to use antecedents. The left rule for implication looks quite different than modus ponens, but it expresses roughly the same thing: if we have $A \supset B$ (as an antecedent) and if we can prove A, then we can use B (by adding it as an antecedent in the right sub-proof).

$$\frac{\Gamma, A \supset B[w] \Rightarrow A[w] \quad \Gamma, A \supset B[w], B[w] \Rightarrow C[w]}{\Gamma, A \supset B[w] \Rightarrow C[w]} \supset L$$

Note that all the symbols appearing free in the premise (Γ, A, B, C, and w) are present in the conclusion, so this rule obeys the sub-formula property. This rule, and the others we present in Figure 1, follows the usual convention in sequent calculus presentations of playing fast and loose with the ordering of antecedents – in the natural deduction presentation we were careful to treat the antecedents of the hypothetical judgment as just a sequence. If we wanted to be pedantic about the $\supset L$ rule, we could either write the conclusion of $\supset L$ as $\Gamma, A \supset B[w], \Gamma' \Rightarrow C[w]$ to clarify that the implication can appear anywhere in the context (and alter the premises to the rule accordingly) or else we could write the conclusion as $\Gamma \Rightarrow C[w]$ and add an additional premise $A \supset B[w] \in \Gamma$. In the Agda development, where playing fast and loose is forbidden, we take the latter of these two options.

$$\frac{}{\Gamma, Q[w] \Rightarrow Q[w]}\ \mathit{init}\quad (Q \text{ is an atomic proposition})$$

$$\frac{\Gamma, A[w] \Rightarrow B[w]}{\Gamma \Rightarrow A \supset B[w]}\ \supset R \qquad \frac{\Gamma, A \supset B[w] \Rightarrow A[w] \quad \Gamma, A \supset B[w], B[w] \Rightarrow C[w]}{\Gamma, A \supset B[w] \Rightarrow C[w]}\ \supset L$$

$$\frac{w \prec w' \quad \Gamma \Rightarrow A[w']}{\Gamma \Rightarrow \Diamond A[w]}\ \Diamond R \qquad \frac{\forall w'.\, w \prec w' \longrightarrow \Gamma \Rightarrow A[w'] \longrightarrow \Gamma, \Diamond A[w] \Rightarrow C[w]}{\Gamma, \Diamond A[w] \Rightarrow C[w]}\ \Diamond L$$

$$\frac{\forall w'.\, w \prec w' \longrightarrow \Gamma \Rightarrow A[w']}{\Gamma \Rightarrow \Box A[w]}\ \Box R$$

$$\frac{(\forall w'.\, w \prec w' \longrightarrow \Gamma \Rightarrow A[w']) \longrightarrow \Gamma, \Box A[w] \Rightarrow C[w]}{\Gamma, \Box A[w] \Rightarrow C[w]}\ \Box L$$

$$\frac{\forall w'.\, w \prec w' \longrightarrow \neg(\Gamma \Rightarrow A[w'])}{\Gamma \Rightarrow \not\Diamond A[w]}\ \not\Diamond R$$

$$\frac{(\forall w'.\, w \prec w' \longrightarrow \neg(\Gamma \Rightarrow A[w'])) \longrightarrow \Gamma, \not\Diamond A[w] \Rightarrow C[w]}{\Gamma, \not\Diamond A[w] \Rightarrow C[w]}\ \not\Diamond L$$

$$\frac{w \prec w' \quad \neg(\Gamma \Rightarrow A[w'])}{\Gamma \Rightarrow \not\Box A[w]}\ \not\Box R \qquad \frac{\forall w'.\, w \prec w' \longrightarrow \neg(\Gamma \Rightarrow A[w']) \longrightarrow \Gamma, \not\Box A[w] \Rightarrow C[w]}{\Gamma, \not\Box A[w] \Rightarrow C[w]}\ \not\Box L$$

Figure 1: Sequent Calculus for minimal **CPL**

Because the rules of the sequent calculus manipulate assumptions directly, we can restrict the hypothesis rule to atomic propositions only; the previous hypothesis rule becomes a defining principle of the logic, the *identity principle*. Other than that change, the defining principles of the sequent calculus judgment $\Gamma \Rightarrow A[w]$ for constructive provability logic are quite similar to the defining principles of the hypothetical judgment $\Gamma \vdash A[w]$:

Definition of the sequent calculus judgment for constructive provability logic:
- *Hypothesis rule*: If $Q[w_i] \in \Gamma$, where Q is an atomic proposition, then $\Gamma \Rightarrow Q[w_i]$.
- *Identity principle*: If $A[w_i] \in \Gamma$, then $\Gamma \Rightarrow A[w_i]$.
- *Weakening principle*: If $\Gamma \subseteq_w \Gamma'$ and $\Gamma \Rightarrow A[w]$, then $\Gamma' \Rightarrow A[w]$.
- *Strengthening principle*: If $\Gamma =_w \Gamma'$ and $\Gamma \Rightarrow A[w]$, then $\Gamma' \Rightarrow A[w]$.
- *Cut principle*: If $\Gamma \Rightarrow A[w]$ and $\Gamma, A[w] \Rightarrow C[w]$, then $\Gamma \Rightarrow C[w]$.

The sequent calculus formulation of minimal **CPL** is shown in Figure 1. Our habit of playing fast and loose with the ordering of antecedents does create a gap between our on-paper presentation and the Agda formalization in `MinimalCPL/Core.agda`. For the sake of a simple presentation, the on-paper presentation omits irrelevant premises from rules where applicable. For instance, the premise of $\Diamond L$ is $\forall w'.\, w \prec w' \longrightarrow \Gamma \Rightarrow A[w'] \longrightarrow \Gamma, \Diamond A[w] \Rightarrow C[w]$, but if we were going to accurately capture the Agda representation, we would need to leave the irrelevant hypothesis in the context, and the premise would be $\forall w'.\, w \prec w' \longrightarrow \Gamma, \Diamond A[w] \Rightarrow A[w'] \longrightarrow \Gamma, \Diamond A[w] \Rightarrow C[w]$. The strengthening principle ensures that this is a distinction that does not make a difference.

Now that we have defined the sequent calculus, we can see how it is useful for proving that certain logical statements are not the case by giving an analogue to Theorem 2:

Theorem 5. *For distinct atomic propositions Q_1 and Q_2, it is not the case that $\cdot \Rightarrow Q_1 \supset Q_2[\beta]$.*

Proof. We are given a proof $\mathcal{D} :: \cdot \Rightarrow Q_1 \supset Q_2[\beta]$, and we must proof a contradiction. By case analysis on $\mathcal{D}$, we see that no left rule is possible (because the context is empty) and the only possible right rule is $\supset R$. Therefore, we now have a proof $\mathcal{D}' :: Q_1 \Rightarrow Q_2[\beta]$. By case analysis on $\mathcal{D}'$, we see that no left rule applies (because none of the left rules work on atomic propositions), no right rule applies, and the initial rule does not apply because the antecedent and the consequent are distinct, so we are done. □

4.1 Verifying the defining principles

The rules in Figure 1 are close enough to the rules of our natural deduction presentation that we will omit a detailed explanation of each rule as well as the verification of the strengthening and weakening principles, which closely follow the discussion in the previous section. We will, however, work through the verification of the defining principles of cut and identity.

Despite the superficial similarity of the definition of the hypothetical judgment for **CPL** and the definition of the sequent calculus judgment for **CPL** that we just discussed, the defining principles of a sequent calculus judgment say quite a bit more about the logic. In particular, the new identity principle is a *global completeness* property, the global version of local completeness, and the *cut principle* (which we called a substitution principle in the natural deduction presentation) is a *global soundness* property. We will not discuss the implications of this; for our current purposes, the sequent calculus is primarily important because it allows us to easily prove that certain sequent calculus judgments are not the case, and the identity and cut principles are primarily important because they allow us, in Section 5, to establish the equivalence of the natural deduction and sequent calculus presentations of **CPL**.

Because some sequent calculus presentations include the cut principle as an explicit rule (like the hypothesis rule), the verification of the cut principle, which shows that such a rule is admissible, is traditionally called *cut admissibility*. The admissibility of cut shows that if we have a proof of a proposition, we are justified in using it as an assumption in another proof. It is therefore analogous to the substitution theorem in natural deduction systems, though the proof is more involved.

Theorem 6 (Cut admissibility)**.** *If $\Gamma \Rightarrow A[w]$ and $\Gamma, A[w] \Rightarrow C[w]$, then $\Gamma \Rightarrow C[w]$.*

Proof. We refer to the proof of the first premise, $\Gamma \Rightarrow A[w]$, as $\mathcal{D}$ and refer to the proof of the second premise, $\Gamma, A[w] \Rightarrow C[w]$, as $\mathcal{E}$. We proceed by lexicographic induction, first on the principal formula A, and then on the shapes of the two derivations $\mathcal{D}$ and $\mathcal{E}$ (either one or both gets smaller if the principal formula remains the same). The cases of cut admissibility are classified as *principal* cuts, *left commutative* cuts, and *right commutative* cuts. We illustrate the proof technique by presenting the cases corresponding to $\supset$ and $\Diamond$.

Case: $A = A \supset B$ – Principal cut

$$\mathcal{D} = \dfrac{\begin{array}{c}\mathcal{D}_1 \\ \Gamma, A[w] \Rightarrow B[w]\end{array}}{\Gamma \Rightarrow A \supset B[w]}\ \supset R$$

$$\mathcal{E} = \dfrac{\begin{array}{cc}\mathcal{E}_1 & \mathcal{E}_2 \\ \Gamma, A \supset B[w] \Rightarrow A[w] & \Gamma, A \supset B[w], B[w] \Rightarrow C[w]\end{array}}{\Gamma, A \supset B[w] \Rightarrow C[w]}\ \supset L$$

$\mathcal{D}' :: \Gamma, B[w] \Rightarrow A \supset B[w]$ by weakening principle on $\mathcal{D}$
$\mathcal{E}'_1 :: \Gamma \Rightarrow A[w]$ by i.h. on $A \supset B$, $\mathcal{D}$ and $\mathcal{E}_1$
$\mathcal{E}'_2 :: \Gamma, B[w] \Rightarrow C[w]$ by i.h. on $A \supset B$, $\mathcal{D}'$ and $\mathcal{E}_2$
$\mathcal{F} :: \Gamma \Rightarrow B[w]$ by i.h. on A, $\mathcal{E}'_1$ and $\mathcal{D}_1$
$\mathcal{F}' :: \Gamma \Rightarrow C[w]$ by i.h. on B, $\mathcal{F}$ and $\mathcal{E}'_2$

Case: $(\Gamma = \Gamma', B_1 \supset B_2[w])$ – Left commutative cut

$$\mathcal{D} = \dfrac{\begin{array}{cc}\mathcal{D}_1 & \mathcal{D}_2 \\ \Gamma', B_1 \supset B_2[w] \Rightarrow B_1[w] & \Gamma', B_1 \supset B_2[w], B_2[w] \Rightarrow A[w]\end{array}}{\Gamma', B_1 \supset B_2[w] \Rightarrow A[w]}\ \supset L$$

$$\dfrac{\begin{array}{c}\mathcal{E} \\ \Gamma', B_1 \supset B_2[w], A[w] \Rightarrow C[w]\end{array}}{}$$

$\mathcal{E}' :: \Gamma', B_1 \supset B_2[w], B_2[w], A[w] \Rightarrow C[w]$ by weakening principle on $\mathcal{E}$
$\mathcal{F}_2 :: \Gamma', B_1 \supset B_2[w], B_2[w] \Rightarrow C[w]$ by i.h. on A, $\mathcal{D}_2$ and $\mathcal{E}'$
$\mathcal{F} :: \Gamma', B_1 \supset B_2[w] \Rightarrow C[w]$ by $\supset L$ on $\mathcal{D}_1$ and $\mathcal{F}_2$

Case: Right commutative cut, right rule

$$\dfrac{\begin{array}{c}\mathcal{D} \\ \Gamma \Rightarrow A[w]\end{array}}{}$$

$$\mathcal{E} = \dfrac{\begin{array}{c}\mathcal{E}_1 \\ \Gamma, A[w], C_1[w] \Rightarrow C_2[w]\end{array}}{\Gamma, A[w] \Rightarrow C_1 \supset C_2[w]}\ \supset R$$

$\mathcal{E}'_1 :: \Gamma, C_1[w], A[w] \Rightarrow C_2[w]$ by weakening principle on $\mathcal{E}_1$
$\mathcal{F}_1 :: \Gamma, C_1[w] \Rightarrow C_2[w]$ by i.h. on A , $\mathcal{D}$ and $\mathcal{E}'_1$
$\mathcal{F} :: \Gamma \Rightarrow C_1 \supset C_2[w]$ by $\supset R$ on $\mathcal{F}_1$

Case: $(\Gamma = \Gamma', B_1 \supset B_2[w])$ – Right commutative cut, left rule

$$\dfrac{\begin{array}{c}\mathcal{D} \\ \Gamma', B_1 \supset B_2[w] \Rightarrow A[w]\end{array}}{}$$

$$\mathcal{E} = \dfrac{\begin{array}{cc}\mathcal{E}_1 & \mathcal{E}_2 \\ \Gamma', B_1 \supset B_2[w], A[w] \Rightarrow B_1[w] & \Gamma', B_1 \supset B_2[w], A[w], B_2[w] \Rightarrow C[w]\end{array}}{\Gamma', B_1 \supset B_2[w], A[w] \Rightarrow C[w]}\ \supset L$$

$\mathcal{E}_2' :: \Gamma', B_1 \supset B_2[w], B_2[w], A[w] \Rightarrow C[w]$ by weakening principle on $\mathcal{E}_2$
$\mathcal{F}_1 :: \Gamma', B_1 \supset B_2[w] \Rightarrow B_1[w]$ by i.h. on A , $\mathcal{D}$ and $\mathcal{E}_1$
$\mathcal{F}_2 :: \Gamma', B_1 \supset B_2[w], B_2[w] \Rightarrow C[w]$ by i.h. on A , $\mathcal{D}$ and $\mathcal{E}_2'$
$\mathcal{F} :: \Gamma', B_1 \supset B_2[w] \Rightarrow C[w]$ by $\supset L$ on $\mathcal{F}_1$ and $\mathcal{F}_2$

Case: ($A = \Diamond A$) – Principal cut

$$\mathcal{D} = \dfrac{\begin{array}{cc}\mathcal{D}_w & \mathcal{D}_1 \\ w \prec w' & \Gamma \Rightarrow A[w']\end{array}}{\Gamma \Rightarrow \Diamond A[w]}\ \Diamond R$$

$$\mathcal{E} = \dfrac{\begin{array}{c}\mathcal{E}_1 \\ \forall w'.\, w \prec w' \longrightarrow \Gamma \Rightarrow A[w'] \longrightarrow \Gamma, \Diamond A[w] \Rightarrow C[w]\end{array}}{\Gamma, \Diamond A[w] \Rightarrow C[w]}\ \Diamond L$$

$\mathcal{E}_1' :: \Gamma, \Diamond A[w] \Rightarrow C[w]$ by $\mathcal{E}_1$ on $\mathcal{D}_w$ and $\mathcal{D}_1$
$\mathcal{F} :: \Gamma \Rightarrow C[w]$ by i.h. on $\Diamond A$, $\mathcal{D}$ and $\mathcal{E}_1'$

Case: ($\Gamma = \Gamma', \Diamond B[w]$) – Left commutative cut

$$\mathcal{D} = \dfrac{\begin{array}{c}\mathcal{D}_1 \\ \forall w'.\, w \prec w' \longrightarrow \Gamma' \Rightarrow B[w'] \longrightarrow \Gamma', \Diamond B[w] \Rightarrow A[w]\end{array}}{\Gamma', \Diamond B[w] \Rightarrow A[w]}\ \Diamond L$$

$$\begin{array}{c}\mathcal{E} \\ \Gamma', \Diamond B[w], A[w] \Rightarrow C[w]\end{array}$$

$\mathcal{F}_1 :: \forall w'.\, w \prec w' \longrightarrow \Gamma' \Rightarrow B[w'] \longrightarrow \Gamma', \Diamond B[w] \Rightarrow C[w]$
by the following hypothetical reasoning:
Assume that for an arbitrary w' we have $\mathcal{D}_w :: w \prec w'$ and $\mathcal{D}_0 :: \Gamma' \Rightarrow B[w']$
$\mathcal{D}_1' :: \Gamma', \Diamond B[w] \Rightarrow A[w]$ by $\mathcal{D}_1$ on $\mathcal{D}_w$ and $\mathcal{D}_0$
$\mathcal{F}_1' :: \Gamma', \Diamond B[w] \Rightarrow C[w]$ by i.h. on A, $\mathcal{D}_1'$ and $\mathcal{E}$
$\mathcal{F} :: \Gamma', \Diamond B[w] \Rightarrow C[w]$ by $\Diamond L$ on $\mathcal{F}_1$

Case: Right commutative cut, right rule

$$\begin{array}{c}\mathcal{D} \\ \Gamma \Rightarrow A[w]\end{array}$$

$$\mathcal{E} = \dfrac{\begin{array}{cc}\mathcal{E}_w & \mathcal{E}_1 \\ w \prec w' & \Gamma, A[w] \Rightarrow C[w']\end{array}}{\Gamma, A[w] \Rightarrow \Diamond C[w]}\ \Diamond R$$

$\mathcal{F}_1 :: \Gamma \Rightarrow C[w']$ by strengthening principle on $\mathcal{E}_1$
$\mathcal{F} :: \Gamma \Rightarrow \Diamond C[w]$ by $\Diamond R$ on $\mathcal{E}_w$ and $\mathcal{F}_1$

Case: ($\Gamma = \Gamma', \Diamond B[w]$) – Right commutative cut, left rule

$$\overset{\mathcal{D}}{\Gamma', \Diamond B[w] \Rightarrow A[w]}$$

$$\mathcal{E} = \frac{\overset{\mathcal{E}_1}{\forall w'.\, w \prec w' \longrightarrow \Gamma', A[w] \Rightarrow B[w'] \longrightarrow \Gamma', \Diamond B[w], A[w] \Rightarrow C[w]}}{\Gamma', \Diamond B[w], A[w] \Rightarrow C[w]}\ \Diamond L$$

$\mathcal{F}_1 :: \forall w'.\, w \prec w' \longrightarrow \Gamma' \Rightarrow B[w'] \longrightarrow \Gamma', \Diamond B[w] \Rightarrow C[w]$
by the following hypothetical reasoning:
Assume that for an arbitrary w' we have $\mathcal{D}_w :: w \prec w'$ and $\mathcal{D}_0 :: \Gamma' \Rightarrow B[w']$
$\mathcal{D}_0' :: \Gamma', A[w] \Rightarrow B[w']$ by strengthening principle on $\mathcal{D}_0$
$\mathcal{E}_1' :: \Gamma', \Diamond B[w], A[w] \Rightarrow C[w]$ by $\mathcal{E}_1$ on $\mathcal{D}_w$ and $\mathcal{D}_0'$
$\mathcal{F}_1' :: \Gamma', \Diamond B[w] \Rightarrow C[w]$ by i.h. on A, $\mathcal{D}$ and $\mathcal{E}_1'$
$\mathcal{F} :: \Gamma', \Diamond B[w] \Rightarrow C[w]$ by $\Diamond L$ on $\mathcal{F}_1$

The other cases are similar (see `MinimalCPL/Sequent.agda`). □

The identity theorem is the global analogue of local completeness. Identity shows us that the left rules of the sequent calculus are strong enough to decompose a complex proposition down to its atomic constituents (which can then be proved by the *init* rule).

Theorem 7 (Identity)**.** *For all A, it is the case that* $\Gamma, A[w] \Rightarrow A[w]$.

Proof. By structural induction on A. We present here some illustrative cases:

Case: ($A = Q$, where Q is atomic)

$\mathcal{F} :: \Gamma, Q[w] \Rightarrow Q[w]$ By rule *init*

Case: ($A = A \supset B$)

$\mathcal{F}_1 :: \Gamma, A[w] \Rightarrow A[w]$ by i.h. on A
$\mathcal{F}_1' :: \Gamma, A \supset B[w], A[w] \Rightarrow A[w]$ by weakening principle on $\mathcal{F}_1$
$\mathcal{F}_2 :: \Gamma, B[w] \Rightarrow B[w]$ by i.h. on B
$\mathcal{F}_2' :: \Gamma, A \supset B[w], A[w], B[w] \Rightarrow B[w]$ by weakening principle on $\mathcal{F}_2$
$\mathcal{F}' :: \Gamma, A \supset B[w], A[w] \Rightarrow B[w]$ by $\supset L$ on $\mathcal{F}_1'$ and $\mathcal{F}_2'$
$\mathcal{F} :: \Gamma, A \supset B[w] \Rightarrow A \supset B[w]$ by $\supset R$ on $\mathcal{F}'$

Case: ($A = \Diamond A$)

$\mathcal{F}_1 :: \forall w'.\, w \prec w' \longrightarrow \Gamma \Rightarrow A[w'] \longrightarrow \Gamma, \Diamond A[w] \Rightarrow \Diamond A[w]$
by the following hypothetical reasoning:
Assume that for an arbitrary w' we have $\mathcal{D}_w :: w \prec w'$ and $\mathcal{D}_0 :: \Gamma \Rightarrow A[w']$
$\mathcal{D}_1 :: \Gamma \Rightarrow \Diamond A[w]$ by $\Diamond R$ on $\mathcal{D}_0$
$\mathcal{D}_1' :: \Gamma, \Diamond A[w] \Rightarrow \Diamond A[w]$ by weakening principle on $\mathcal{D}_1$
$\mathcal{F} :: \Gamma, \Diamond A[w] \Rightarrow \Diamond A[w]$ by $\Diamond L$ on $\mathcal{F}_1$

Case: ($A = \Box A$)

$\mathcal{F}_1 :: (\forall w'.\, w \prec w' \longrightarrow \Gamma \Rightarrow A[w']) \longrightarrow \Gamma, \Box A[w] \Rightarrow \Box A[w]$
by the following hypothetical reasoning:
Assume $\mathcal{D}_0 :: \forall w'.\, w \prec w' \longrightarrow \Gamma \Rightarrow A[w']$
$\mathcal{D}_1 :: \Gamma \Rightarrow \Box A[w]$ by $\Box R$ on $\mathcal{D}_0$
$\mathcal{D}'_1 :: \Gamma, \Box A[w] \Rightarrow \Box A[w]$ by weakening principle on $\mathcal{D}_1$
$\mathcal{F} :: \Gamma, \Box A[w] \Rightarrow \Box A[w]$ by $\Box L$ on $\mathcal{F}_1$

The other cases are similar (see `MinimalCPL/Sequent.agda`). □

5 Equivalence of sequent calculus and natural deduction

In Section 3, we introduced constructive provability logic as a natural deduction system that allows us to reflect over provability at accessible worlds, and in Section 4 we introduced a sequent calculus formulation of **CPL** that allows us to more easily establish meaningful statements about provability at accessible worlds. In this section, we tie up loose ends by showing that the natural deduction and sequent calculus formulations of **CPL** are equivalent. Given the equivalence of these two presentations of minimal **CPL**, it is a simple matter to use Theorem 5 (it is not the case that $\cdot \Rightarrow Q_1 \supset Q_2[\beta]$) to prove Theorem 2 (it is not the case that $\cdot \vdash Q_1 \supset Q_2[\beta]$).

Proving soundness and completeness of sequent calculi is generally a fairly simple task once the defining principles of the natural deduction and sequent calculus systems have been verified. In our case there is one wrinkle: both directions of the proof have to be established simultaneously. If we call "soundness" the proof that $\Gamma \Rightarrow A[w]$ implies $\Gamma \vdash A[w]$ and call "completeness" the proof in the other direction,[9] then the soundness of $\Diamond R$ relies on soundness at accessible worlds, but the soundness of $\Diamond L$ relies on *completeness* at accessible worlds.

Theorem 8 (Equivalence of sequent calculus and natural deduction)**.**

(i) If $\Gamma \vdash A[w]$ *then* $\Gamma \Rightarrow A[w]$

(ii) If $\Gamma \Rightarrow A[w]$ *then* $\Gamma \vdash A[w]$

Proof. By lexicographic induction, first on the accessibility relation and second on the given derivation. We have to assume the induction hypothesis in both directions at accessible worlds, but we can prove the two directions independently at a given world under the assumption that both directions hold at accessible worlds. We prove (i) in Section 5.1 and (ii) in Section 5.2. In those sections, we write "by i.h." when we are calling the induction hypothesis on a smaller derivation at the same world, and we write "by i.h.(i)" or "by i.h.(ii)" when we are calling the induction hypothesis at an accessible world.

[9] This is therefore the view that privileges the natural deduction system, because "soundness" is the soundness of the sequent calculus with respect to natural deduction. It would be just as appropriate to call the "soundness" direction the completeness of natural deduction with respect to the sequent calculus!

We elide the cases for $\not\Diamond$ and $\not\Box$ since they are very similar to the cases for $\Box$ and $\Diamond$. The full proof is included in our Agda development (see `MinimalCPL/Equiv.agda`). $\square$

5.1 From natural deduction to sequent calculus

Case hyp**:**

$$\frac{}{\Gamma, A[w] \vdash A[w]}\ hyp$$

$\mathcal{F} :: \Gamma, A[w] \Rightarrow A[w]$ by identity principle

Case $\supset I$**:**

$$\frac{\begin{array}{c}\mathcal{D}_1\\ \Gamma, A[w] \vdash B[w]\end{array}}{\Gamma \vdash A \supset B[w]}\ \supset I$$

$\mathcal{E}_1 :: \Gamma, A[w] \Rightarrow B[w]$ by i.h. on $\mathcal{D}_1$
$\mathcal{F} :: \Gamma \Rightarrow A \supset B[w]$ by $\supset R$ on $\mathcal{E}_1$

Case $\supset E$**:**

$$\frac{\begin{array}{cc}\mathcal{D}_1 & \mathcal{D}_2\\ \Gamma \vdash A \supset B[w] & \Gamma \vdash A[w]\end{array}}{\Gamma \vdash B[w]}\ \supset E$$

$\mathcal{E}_1 :: \Gamma \Rightarrow A \supset B[w]$ by i.h. on $\mathcal{D}_1$
$\mathcal{E}_2 :: \Gamma \Rightarrow A[w]$ by i.h. on $\mathcal{D}_2$
$\mathcal{F}_1 :: \Gamma, A \supset B[w] \Rightarrow A[w]$ by weakening principle on $\mathcal{E}_2$
$\mathcal{F}_2 :: \Gamma, A \supset B[w], B[w] \Rightarrow B[w]$ by identity principle
$\mathcal{F} :: \Gamma, A \supset B[w] \Rightarrow B[w]$ by $\supset L$ on $\mathcal{F}_1$ and $\mathcal{F}_2$
$\mathcal{F}' :: \Gamma \Rightarrow B[w]$ by cut principle on $\mathcal{E}_1$ and $\mathcal{F}$

Case $\Diamond I$**:**

$$\frac{\begin{array}{cc}\mathcal{D}_w & \mathcal{D}_1\\ w \prec w' & \Gamma \vdash A[w']\end{array}}{\Gamma \vdash \Diamond A[w]}\ \Diamond I$$

$\mathcal{E}_1 :: \Gamma \Rightarrow A[w']$ by i.h.(i) on $\mathcal{D}_1$
$\mathcal{F} :: \Gamma \Rightarrow \Diamond A[w]$ by $\Diamond R$ on $\mathcal{D}_w$ and $\mathcal{E}_1$

Case $\Diamond E$**:**

$$\frac{\begin{array}{cc}\mathcal{D}_1 & \mathcal{D}_2\\ \Gamma \vdash \Diamond A[w] & \forall w'.\, w \prec w' \longrightarrow \Gamma \vdash A[w'] \longrightarrow \Gamma \vdash C[w]\end{array}}{\Gamma \vdash C[w]}\ \Diamond E$$

$\mathcal{E}_1 :: \Gamma \Rightarrow \Diamond A[w]$ by i.h. on $\mathcal{D}_1$
$\mathcal{E}_2 :: \forall w'.\, w \prec w' \longrightarrow \Gamma \Rightarrow A[w'] \longrightarrow \Gamma, \Diamond A[w] \Rightarrow C[w]$
by the following hypothetical reasoning:
Assume that for an arbitrary w' we have $\mathcal{D}_w :: w \prec w'$ and $\mathcal{E}_0 :: \Gamma \Rightarrow A[w']$
$\mathcal{D}_0 :: \Gamma \vdash A[w']$ by i.h.(ii) on $\mathcal{E}_0$
$\mathcal{D}_2' :: \Gamma \vdash C[w]$ by $\mathcal{D}_2$ on $\mathcal{D}_w$ and $\mathcal{D}_0$
$\mathcal{E}_2' :: \Gamma \Rightarrow C[w]$ by i.h. on $\mathcal{D}_2'$
$\mathcal{E}_2'' :: \Gamma, \Diamond A[w] \Rightarrow C[w]$ by weakening principle on $\mathcal{E}_2'$
$\mathcal{F} :: \Gamma, \Diamond A[w] \Rightarrow C[w]$ by $\Diamond L$ on $\mathcal{E}_2$
$\mathcal{F}' :: \Gamma \Rightarrow C[w]$ by cut principle on $\mathcal{E}_1$ and $\mathcal{F}$

Case $\Box I$:

$$\frac{\begin{array}{c}\mathcal{D}_1\\ \forall w'.\, w \prec w' \longrightarrow \Gamma \vdash A[w']\end{array}}{\Gamma \vdash A[w]}\ \Box I$$

$\mathcal{E}_1 :: \forall w'.\, w \prec w' \longrightarrow \Gamma \Rightarrow A[w']$ by the following hypothetical reasoning:
Assume that for an arbitrary w' we have $\mathcal{D}_w :: w \prec w'$
$\mathcal{D}_1' :: \Gamma \vdash A[w']$ by $\mathcal{D}_1$ on $\mathcal{D}_w$
$\mathcal{E}_1' :: \Gamma \Rightarrow A[w']$ by i.h.(i) on $\mathcal{D}_1'$
$\mathcal{F} :: \Gamma \Rightarrow \Box A[w]$ by $\Box R$ on $\mathcal{E}_1$

Case $\Box E$:

$$\frac{\begin{array}{cc}\mathcal{D}_1 & \mathcal{D}_2\\ \Gamma \vdash \Box A[w] & (\forall w'.\, w \prec w' \longrightarrow \Gamma \vdash A[w']) \longrightarrow \Gamma \vdash C[w]\end{array}}{\Gamma \vdash C[w]}\ \Box E$$

$\mathcal{E}_1 :: \Gamma \Rightarrow \Box A[w]$ by i.h. on $\mathcal{D}_1$
$\mathcal{E}_2 :: (\forall w'.\, w \prec w' \longrightarrow \Gamma \Rightarrow A[w']) \longrightarrow \Gamma, \Box A[w] \Rightarrow C[w]$
by the following hypothetical reasoning:
Assume $\mathcal{E}_0 :: \forall w'.\, w \prec w' \longrightarrow \Gamma \Rightarrow A[w']$
$\mathcal{D}_0 :: \forall w'.\, w \prec w' \longrightarrow \Gamma \vdash A[w']$ by the following hypothetical reasoning:
Assume that for an arbitrary w' we have $\mathcal{D}_w :: w \prec w'$
$\mathcal{E}_0' :: \Gamma \Rightarrow A[w']$ by $\mathcal{E}_0$ on $\mathcal{D}_w$
$\mathcal{D}_0' :: \Gamma \vdash A[w']$ by i.h.(ii) on $\mathcal{E}_0'$
$\mathcal{D}_2' :: \Gamma \vdash C[w]$ by $\mathcal{D}_2$ on $\mathcal{D}_0$
$\mathcal{E}_2' :: \Gamma \Rightarrow C[w]$ by i.h. on $\mathcal{D}_2'$
$\mathcal{E}_2'' :: \Gamma, \Box A[w] \Rightarrow C[w]$ by weakening principle on $\mathcal{E}_2'$
$\mathcal{F} :: \Gamma, \Box A[w] \Rightarrow C[w]$ by $\Box L$ on $\mathcal{E}_2$
$\mathcal{F}' :: \Gamma \Rightarrow C[w]$ by cut principle on $\mathcal{E}_1$ and $\mathcal{F}$

5.2 From sequent calculus to natural deduction

Case $init$**:**

$$\frac{}{\Gamma, Q[w] \Rightarrow Q[w]}\ init$$

$\mathcal{F} :: \Gamma, Q[w] \vdash Q[w]$ by hyp

Case $\supset R$**:**

$$\frac{\begin{array}{c}\mathcal{D}_1\\ \Gamma, A[w] \Rightarrow B[w]\end{array}}{\Gamma \Rightarrow A \supset B[w]}\ \supset R$$

$\mathcal{E}_1 :: \Gamma, A[w] \vdash B[w]$ by i.h. on $\mathcal{D}_1$
$\mathcal{F} :: \Gamma \vdash A \supset B[w]$ by $\supset I$ on $\mathcal{E}_1$

Case $\supset L$**:**

$$\frac{\begin{array}{c}\mathcal{D}_1\\ \Gamma, A \supset B[w] \Rightarrow A[w]\end{array} \quad \begin{array}{c}\mathcal{D}_2\\ \Gamma, A \supset B[w], B[w] \Rightarrow C[w]\end{array}}{\Gamma, A \supset B[w] \Rightarrow C[w]}\ \supset L$$

$\mathcal{E}_1 :: \Gamma, A \supset B[w] \vdash A[w]$ by i.h. on $\mathcal{D}_1$
$\mathcal{E}_2 :: \Gamma, A \supset B[w], B[w] \vdash C[w]$ by i.h. on $\mathcal{D}_2$
$\mathcal{F}_2 :: \Gamma, A \supset B[w] \vdash A \supset B[w]$ by hyp
$\mathcal{F} :: \Gamma, A \supset B[w] \vdash B[w]$ by $\supset E$ on $\mathcal{E}_1$ and $\mathcal{F}_2$
$\mathcal{F}' :: \Gamma, A \supset B[w] \vdash C[w]$ by substitution principle on $\mathcal{F}$ and $\mathcal{E}_2$

Case $\Diamond R$**:**

$$\frac{\begin{array}{c}\mathcal{D}_w\\ w \prec w'\end{array} \quad \begin{array}{c}\mathcal{D}_1\\ \Gamma \Rightarrow A[w']\end{array}}{\Gamma \Rightarrow \Diamond A[w]}\ \Diamond R$$

$\mathcal{E}_1 :: \Gamma \vdash A[w']$ by i.h(ii) on $\mathcal{D}_1$
$\mathcal{F} :: \Gamma \vdash \Diamond A[w]$ by $\Diamond I$ on $\mathcal{D}_w$ and $\mathcal{E}_1$

Case $\Diamond L$**:**

$$\frac{\begin{array}{c}\mathcal{D}_1\\ \forall w'.\, w \prec w' \longrightarrow \Gamma \Rightarrow A[w'] \longrightarrow \Gamma, \Diamond A[w] \Rightarrow C[w]\end{array}}{\Gamma, \Diamond A[w] \Rightarrow C[w]}\ \Diamond L$$

$\mathcal{E}_1 :: \Gamma, \Diamond A[w] \Rightarrow \Diamond A[w]$ by *hyp*
$\mathcal{E}_2 :: \forall w'.\, w \prec w' \longrightarrow \Gamma, \Diamond A[w] \vdash A[w'] \longrightarrow \Gamma, \Diamond A[w] \vdash C[w]$
by the following hypothetical reasoning:
Assume that for an arbitrary w' we have $\mathcal{D}_w :: w \prec w'$ and $\mathcal{E}_0 :: \Gamma, \Diamond A[w] \vdash A[w']$
$\mathcal{D}_0 :: \Gamma, \Diamond A[w] \Rightarrow A[w']$ by i.h.(i) on $\mathcal{E}_0$
$\mathcal{D}'_0 :: \Gamma \Rightarrow A[w']$ by strengthening principle on $\mathcal{D}_0$
$\mathcal{D}'_1 :: \Gamma, \Diamond A[w] \Rightarrow C[w]$ by $\mathcal{D}_1$ on $\mathcal{D}_w$ and $\mathcal{D}'_0$
$\mathcal{E}'_1 :: \Gamma, \Diamond A[w] \vdash C[w]$ by i.h. on $\mathcal{D}'_1$
$\mathcal{F} :: \Gamma, \Diamond A[w] \Rightarrow C[w]$ by $\Diamond E$ on $\mathcal{E}_1$ and $\mathcal{E}_2$

Case $\Box R$:

$$\frac{\begin{array}{c}\mathcal{D}_1\\ \forall w'.\, w \prec w' \longrightarrow \Gamma \Rightarrow A[w']\end{array}}{\Gamma \Rightarrow \Box A[w]}\ \Box R$$

$\mathcal{E}_1 :: \forall w'.\, w \prec w' \longrightarrow \Gamma \vdash A[w']$ by the following hypothetical reasoning:
Assume that for an arbitrary w' we have $\mathcal{D}_w :: w \prec w'$
$\mathcal{D}'_1 :: \Gamma \Rightarrow A[w']$ by $\mathcal{D}_1$ on $\mathcal{D}_w$
$\mathcal{E}'_1 :: \Gamma \vdash A[w']$ by i.h.(ii) on $\mathcal{D}_1$
$\mathcal{F} :: \Gamma \vdash \Box A[w]$ by $\Box I$ on $\mathcal{E}_1$

Case $\Box L$:

$$\frac{\begin{array}{c}\mathcal{D}_1\\ (\forall w'.\, w \prec w' \longrightarrow \Gamma \Rightarrow A[w']) \longrightarrow \Gamma, \Box A[w] \Rightarrow C[w]\end{array}}{\Gamma, \Box A[w] \Rightarrow C[w]}\ \Box L$$

$\mathcal{E}_1 :: \Gamma, \Box A[w] \vdash \Box A[w]$ by *hyp*
$\mathcal{E}_2 :: (\forall w'.\, w \prec w' \longrightarrow \Gamma, \Box A[w] \vdash A[w']) \longrightarrow \Gamma, \Box A[w] \vdash C[w]$
by the following hypothetical reasoning:
Assume $\mathcal{E}_0 :: \forall w'.\, w \prec w' \longrightarrow \Gamma, \Box A[w] \vdash A[w']$
$\mathcal{D}_0 :: \forall w'.\, w \prec w' \longrightarrow \Gamma \Rightarrow A[w']$ by the following hypothetical reasoning:
Assume that for an arbitrary w' we have $\mathcal{D}_w :: w \prec w'$
$\mathcal{E}'_0 :: \Gamma, \Box A[w] \vdash A[w']$ by $\mathcal{E}_0$ on $\mathcal{D}_w$
$\mathcal{D}'_0 :: \Gamma, \Box A[w] \Rightarrow A[w']$ by i.h.(i) on $\mathcal{E}'_0$
$\mathcal{D}''_0 :: \Gamma \Rightarrow A[w']$ by strengthening principle on $\mathcal{D}'_0$
$\mathcal{D}'_1 :: \Gamma, \Box A[w] \Rightarrow C[w]$ by $\mathcal{D}_1$ on $\mathcal{D}_0$
$\mathcal{E}'_1 :: \Gamma, \Box A[w] \vdash C[w]$ by i.h. on $\mathcal{D}'_1$
$\mathcal{F} :: \Gamma, \Box A[w] \vdash C[w]$ by $\Box E$ on $\mathcal{E}_1$ and $\mathcal{E}_2$

This completes the discussion of the equivalence of the sequent calculus and natural deduction presentations of minimal **CPL**.

6 Conclusion

In this report, we have discussed the judgmental principles of constructive provability logic and given equivalent natural deduction and sequent calculus presentation for the minimal, modal fragment of this logic. We will conclude by elaborating a bit on the connections between our presentation of minimal **CPL**, minimal modal logic, and classical provability logic.

The word "minimal" used throughout this report was used in the sense of *minimal logic*, the subsystem of intuitionistic logic without a proper contradiction $\bot$. The lack of a proper contradiction was why we had to prove things like $Q_1[\beta] \vdash \Diamond Q_2 \supset C[\alpha]$ for an arbitrary C. If we had formalized an intuitionistic logic instead of a minimal logic, we could have simply proved that $Q_1[\beta] \vdash \Diamond Q_2 \supset \bot[\alpha]$ and relied on the fact that $\Gamma \vdash \bot \supset C[w]$ is universally true in intuitionistic logic. Our formalization of minimal logic was one reason why the $\not\Diamond$ and $\not\Box$ connectives were motivated – proving $\Gamma \vdash \not\Diamond A[w]$ does, in fact, imply that $\Gamma \vdash \Diamond A \supset C[w]$ for any C (this is a consequence of the axiom $N\Diamond$ in `MinimalCPL/Axioms.agda`).

We refer to this logic as constructive provability logic to both connect and distinguish from previous work on modal provability logics [1, 12]. The Gödel-Löb logic of provability, which is known variously as **G**, **L**, **GL**, **Pr**, **PrL**, **KW**, and **K4W**, has mostly only been given Hilbert-style and/or classical presentations. Both **CPL** and **GL** are motivated by a desire to reflect logical provability within logic, and both **CPL** and the Kripke semantics for **GL** require a converse well-founded accessibility relation, though **GL** additionally requires that the accessibility relation be transitive. The axiomatic presentation of **GL** is characterized by the following axioms:

- $K\Box$: $\Box(A \supset B) \supset \Box A \supset \Box B$,
- $4\Box$: $\Box A \supset \Box\Box A$,
- and GW: $\Box(\Box A \supset A) \supset \Box A$.

If we stipulate that **CPL**'s accessibility relation is transitive as well as converse well founded (and thus matches the Kripke accessibility relation for **GL**), these axioms are all universally true in minimal **CPL** (see `MinimalCPL/Axioms.agda`). We do not have a completeness result.

Acknowledgments. The help of Dan Licata and Jamie Morgenstern was invaluable for helping both of the authors learn Agda. Christopher Richards, Vivek Nigam, Henry de Young, David Baelde, and William Lovas gave us a number of important insights into this logic and related work surrounding it, and Christopher Richards, in particular, gave very helpful comments on an earlier draft. Frank Pfenning and André Platzer must be acknowledged for teaching us nearly everything we know about modal logic, and André Platzer's chance inclusion of the axiom **GL** on a course midterm, in particular, could not have been more auspicious.

References

[1] Artemov, S.N., Beklemishev, L.D.: Provability logic. In: Handbook of Philosophical Logic, 2nd ed. pp. 229–403. Kluwer (2004)

[2] Došen, K.: Negation in the light of modal logic. In: Gabbay, D.M. (ed.) What is negation?, pp. 77–86. Kluwer Academic Publishers (1999)

[3] Dummett, M.: The Logical Basis of Metaphysics. Harvard University Press, Cambridge, Massachusetts (1991)

[4] Harper, R.: Practical foundations for programming languages (2010), working draft, available online: `http://www.cs.cmu.edu/~rwh/plbook/book.pdf`

[5] Licata, D.R., Zeilberger, N., Harper, R.: Focusing on binding and computation. In: IEEE Symposium on Logic in Computer Science (2008)

[6] Martin-Löf, P.: *Hauptsatz* for the intuitionistic theory of iterated inductive definitions. In: Fenstad, J.E. (ed.) Proceedings of the Second Scandinavian Logic Symposium. pp. 179–216. North Holland, Amsterdam (1971)

[7] Martin-Löf, P.: On the meanings of the logical constants and the justifications of the logical laws. Nordic Journal of Philosophical Logic 1(1), 11–60 (1996)

[8] Norell, U.: Towards a practical programming language based on dependent type theory. Ph.D. thesis, Chalmers University of Technology (2007)

[9] Pfenning, F., Davies, R.: A judgmental reconstruction of modal logic. Mathematical Structures in Computer Science 11, 511–540 (2001), notes to an invited talk at the *Workshop on Intuitionistic Modal Logics and Applications (IMLA'99)*, Trento, Italy, July 1999

[10] Simmons, R.J.: Totally nameless representation, `http://requestforlogic.blogspot.com/2010/11/totally-nameless-representation.html`

[11] Simpson, A.K.: The Proof Theory and Semantics of Intuitionistic Modal Logic. Ph.D. thesis, University of Edinburgh (1994)

[12] Verbrugge, R.L.: Provability logic. In: Zalta, E.N. (ed.) The Stanford Encyclopedia of Philosophy. Winter 2010 edn. (2010)

[13] Whaley, J., Avots, D., Carbin, M., Lam, M.S.: Using datalog with binary decision diagrams for program analysis. In: Yi, K. (ed.) Proceedings of the 3nd Asian Symposium on Programming Languages and Systems (APLAS'05). pp. 97–118. Springer-Verlag LNCS 3780 (2005)

[14] Zeilberger, N.: Focusing and higher-order abstract syntax. In: Proceedings of the 35th Annual Symposium on Principles of Programming Languages (POPL'08). pp. 359–369. ACM, New York, NY, USA (2008)