Adequacy with Later Credits in the Iris Logic

Student	Freja Marott Crawford
Student Number	201908608
Advisor	Amin Timany

2/1/2026 – Department of Computer Science, Aarhus University – 10 ECTS

Abstract

In this project, we look into the proof of the Iris adequacy theorem with and without later credits.

The addition of later credits to the Iris logic has caused complications in the proof of the adequacy theorem. This is because the fancy update modality is defined using a *later eliminating* update modality instead of a *basic* update modality, when we have later credits in the logic. The basic update modality has useful properties when interacting with plain propositions, which all depend on the rule: $\models\!\!\Rrightarrow \blacksquare P \vdash P$. Consequently, without later credits in the logic, we can keep some resources used to prove a plain proposition under a fancy update modality; this does not work with later credits in the logic.

The work-around in the current proof of the Iris adequacy theorem with later credits in the Rocq formalisation of Iris is to "duplicate the instantiation of the Iris proof". Concretely, they instantiate the proof twice get the resources twice, using the resources from the second instantiation to prove a plain proposition under a fancy update.

Therefore, in this project, we simplify and improve the proof of the Iris adequacy theorem to avoid instantiating the proof twice.

Our initial attempt is to adapt the current adequacy proof *without* later credits to work *with* later credits in the logic. To do this, we first come up with analogous later credit versions of lemmas used in the proof of the adequacy theorem without later credits, specifically the lemmas that allow us to keep resources and eliminating fancy update modalities when the goal is plain. This approach turns out to be complicated and even unfeasible.

Instead, we introduce a new structure of the adequacy proof that builds on a new modality, the half fancy update modality. This modality has desirable properties, and allows us to prove useful lemmas and ultimately, we solve the problem of "running the proof twice" for the strong adequacy theorem with later credits in the logic.

All proofs mentioned in this project can be found in my GitHub project.

Contents

1 Introduction

This report covers a project on the adequacy theorem of the Iris logic. We study how the addition of later credits to the logic has affected the proof of the Iris adequacy theorem, with the goal of improving the proof of the adequacy theorem.

First, in section 2, we explain adequacy of a logic, and consider a weak and a strong adequacy theorem.

In section 3, we look into the soundness of the Iris logic, and we state and prove some soundness lemmas.

We introduce later credits and the later eliminating update modality in section 4, as well as the two different definitions of the fancy update modality; one using the basic update modality, and the other using the later eliminating update modality.

In section 5, we introduce the weakest precondition and a weak adequacy theorem in a simple setting. We define the weakest precondition for the simply typed lambda calculus (STLC), where we do not need state (i.e. a heap), and where we do not have later credits in the logic. We state and prove the weak adequacy theorem, and introduce the lemmas needed for the proof.

The next step is to consider a language with expressions that can modify the heap. In section 6, we add state to the language we are considering (λ_{ref}). We discuss the modifications and additions this causes in the weakest precondition and the adequacy theorem. In particular, we introduce a state interpretation and fancy update modalities.
In section 6.1, we state and prove some of the lemmas needed for the proof of the adequacy theorem, which we prove in section 6.2. Some additional lemmas are needed for manipulating (fancy) update modalities, which all ultimately depend on the lemma $\Rightarrow\!\!\!\!\blacksquare P \vdash P$. We prove these in section 6.3.

In section 7 we zoom in on proving an adequacy theorem with later credits in the logic and identify the challenges that arise from using the later eliminating update modality.
First, in section 7.1, we go through the proof of the weak adequacy theorem with later credits in the logic following the current Iris proof structure. This approach does not translate to the proof of the strong adequacy theorem, so we explore alternative proof strategies.
Next, in section 7.2, we attempt to reuse the proof structure of the adequacy theorem without later credits by adapting the lemmas from the previous section to use the later eliminating update modality – This turns out to be difficult. Therefore, in section 7.3, we attempt an alternative direction, where we introduce a new modality, the half fancy update modality. This modality has some desirable properties; among other things, it facilitates the elimination of fancy update modalities, and it commutes in one direction with introducible modalities.[1]
We prove two versions of the weak adequacy theorem with later credits: In section 7.4 we do a proof in a setting where the weakesst precondition does not include later credits. Here, we spend all the later credits in the proof and leaving no later credits to the user proving the weakest precondition. This corresponds to having no later credits in the logic.
Then, in section 7.5, we prove the weak adequacy theorem in a setting where the weakest precondition does include later credits. This means that the user can actually use the later credits.

Finally, in section 8 we prove the strong adequacy theorem in a setting with and without later credits. These proofs also use the half update modality. Notably, we avoid "running the WP proof twice", which is currently necessary in the proof of the strong adequacy theorem in Iris.

[1] By an *introducible* modality, we mean a modality $\heartsuit$ satisfying $P \vdash \heartsuit P$. *Commutativity in one direction* of two modalities $\heartsuit$ and $\heartsuit$ means satisfaction of $\heartsuit\heartsuit P \vdash \heartsuit\heartsuit P$, but not (necessarily) $\heartsuit\heartsuit P \vdash \heartsuit\heartsuit P$.

2 Adequacy

In this section, we look into the adequacy of the weakest precondition[2] in the Iris program logic. The high-level intuition of "adequacy" is that proving the weakest precondition of an expression in the logic implies statements about the actual execution of the program, expressed in the meta logic. Here, we describe the adequacy statements in a setting with state, which we will introduce in full detail later (section 5.2).

We consider two different adequacy statements – weak and strong – in sections 2.1 and 2.2. We consider the weak adequacy theorem to get an understanding of the relevant lemmas and ideas in the proof. We will later look at the proof in different settings, both with and without later credits in the logic, to get an understanding of the differences and the challenges that arise when we have later credits in the logic. The strong adequacy theorem is analogous to the Iris adequacy theorem in the Rocq formalisation of Iris, and we will study this theorem in various settings as well.

2.1 Weak Adequacy

We define what it means for an expression e to be *adequate* with respect to a pure predicate[3] φ and a state σ.
The expression e is *adequate* if for every configuration (e', σ') that e can step to in the state σ, e' is either reducible, or e' is a value satisfying φ in the meta logic.

Definition 2.1. For any expression e, state σ, and pure predicate φ,

$$\mathsf{adequate}_{\varphi}(e, \sigma) \triangleq \forall e', \sigma', n.\ (e, \sigma) \to^n (e', \sigma') \implies (\mathsf{val}(e') \land \varphi(e')) \lor \mathsf{red}(e', \sigma').$$

Where $\mathsf{red}(e, \sigma) \triangleq \exists e', \sigma'.\ (e, \sigma) \to (e', \sigma')$.

The weak adequacy theorem, which we define below, states if we own the state interpretation S of σ, and we can prove the weakest precondition for expression e with postcondition φ, then e is adequate with respect to φ and σ.
This statement captures what we expect from a proof of the weakest precondition, namely that e is reducible (in the state σ for which we have the state interpretation S), and if the program terminates with some value e', then e' satisfies the postcondition.

Theorem 2.2. (Weak Adequacy Theorem) For any expression e, pure predicate φ and state σ,

$$(\vdash \Rrightarrow_{\top} \exists\, S : State \to iProp.\ S(\sigma) * \mathsf{wp}_{\top}\, e\, \{\varphi\}) \implies \mathsf{adequate}_{\varphi}(e, \sigma).$$

2.2 Strong Adequacy

We now state the stronger adequacy theorem, which is the version that is proved for the Iris logic.[4]

Theorem 2.3. (Strong Adequacy Theorem) For any expressions e and e', states σ and σ', natural number n, Iris predicate Φ and proposition φ,

$$\Big(\Big(\vdash \Rrightarrow_{\top} \exists\, S.\ S(\sigma) * \mathsf{wp}_{\top}\, e\, \{\Phi\} * \big(\ulcorner \mathsf{notStuck}\ (e', \sigma')\urcorner * S(\sigma') * (\mathsf{if}\ \mathsf{val}(e')\ \mathsf{then}\ \Phi(e')) \mathrel{-\!\!*}\ {}_{\top}\Rrightarrow_{\emptyset}\ \ulcorner\varphi\urcorner\big)\Big)$$
$$\land\ (e, \sigma) \to^n (e', \sigma')\Big) \implies \varphi.$$

Where $\mathsf{notStuck}\ (e', \sigma') \triangleq \mathsf{val}(e') \lor \mathsf{red}(e', \sigma')$.

To prove this, we essentially have to prove that if we have the weakest precondition of e and the state interpretation S of σ, and (e, σ) reduces to some configuration (e', σ'), then we have the state interpretation S for σ', e' is not stuck in state σ', and if e' is a value, it satisfies Φ.
The stronger adequacy theorem implies the weaker one, if we choose $\varphi = (\mathsf{val}(e') \land \Phi(e')) \lor \mathsf{red}(e', \sigma')$.

[2] In this section, we have not yet defined the weakest precondition. We will define it in different versions in sections 5 and 6.4.
[3] A *pure predicate* is a predicate of type $Val \to Prop$.
[4] In the Iris logic, the adequacy theorem proved in iris/program_logic/adequacy.v is the strong adequacy theorem in a concurrent setting.

3 Soundness of the Logic

In the proofs of the adequacy theorems, we will have to prove entailments in the Iris logic. The soundness lemmas, which we will study in this section, are statements about entailment in the logic, stated in the meta logic, e.g. that to prove $\vdash P$ (i.e. prove P in the logic) it suffices to prove $\vdash \triangleright P$, and how proving a pure proposition in the logic implies the proposition in the meta logic.

We consider the definition of entailment.

Definition 3.1. We define entailment using semantic interpretations of propositions, $[\![P]\!], [\![Q]\!] \in \mathsf{UPred}(M)$, where M of type $\mathsf{iResUR}\ \Sigma$ describes the resources inside the Iris model.

$$P \vdash Q \triangleq \forall n, a.\ \big(n \in \mathcal{V}(a) \land n \in [\![P]\!](a)\big) \implies n \in [\![Q]\!](a).$$

By definition, the semantic interpretation of propositions is monotone. Specifically, it is upwards closed in resources, and downwards closed in steps, as formalised in the following axiom:

Axiom 3.2. For any $A \in \mathsf{UPred}(M)$, any natural numbers n and m, and any resources a and b,

$$n \in A(a) \implies a \overset{n}{\preceq} b \implies m \leq n \implies m \in A(b).$$

The semantic interpretation of the Iris base logic is defined in [JKJ+18] p. 35. We state the ones we will use below.

Definition 3.3. Semantic interpretations of a selection of propositions.

For any resource a,

$$[\![\ulcorner P \urcorner]\!](a) \triangleq \begin{cases} \mathbb{N} & \text{if } P \\ \emptyset & \text{otherwise} \end{cases}$$
$$[\![\triangleright P]\!](a) \triangleq \{n \mid n = 0 \ \lor\ n - 1 \in [\![P]\!](a)\}$$
$$[\![\blacksquare P]\!](a) \triangleq [\![P]\!](\varepsilon)$$
$$[\![\Rightarrow\!\!\!\triangleright P]\!](a) \triangleq \{n \mid \forall m \leq n, c.\ m \in \mathcal{V}(a \cdot c) \implies \exists b.\ m \in \mathcal{V}(b \cdot c) \land m \in [\![P]\!](b)\}$$

Here, ε is the empty resource; it is the unit element of the unital camera M, and therefore the least element w.r.t. the extension order.
These semantic interpretations of propositions all satisfy monotonicity as stated in axiom 3.2.

3.1 Soundness Lemmas

We state and prove the soundness lemmas needed for the proofs of the adequacy theorems.

Lemma 3.4. For any pure proposition φ,

$$(\vdash \ulcorner \varphi \urcorner) \implies \varphi.$$

Proof. We assume $\vdash \ulcorner \varphi \urcorner$, i.e. $\mathsf{True} \vdash \ulcorner \varphi \urcorner$. By definition, this means that for any natural number n and any resource a, if $n \in \mathcal{V}(a) \land n \in [\![\mathsf{True}]\!](a)$, then $n \in [\![\varphi]\!](a)$.
By definition, $n \in [\![\mathsf{True}]\!](a)$ for all n and all a, hence we conclude $[\![\ulcorner \varphi \urcorner]\!](a) = \mathbb{N}$ for all a. From this, it follows that φ must hold in the meta logic. □

Auxiliary Lemma 3.5. For any Iris proposition P,

$$(\vdash \triangleright P) \implies \vdash P.$$

Proof. From the assumption and the soundness of semantic entailment, we can assume $\forall n, a.\ n \in \mathcal{V}(a) \land n \in [\![\mathsf{True}]\!](a) \implies n \in [\![\triangleright P]\!](a)$.
We instantiate the hypothesis with $n := n + 1$ and $a := \varepsilon$, so we get $n + 1 \in \mathcal{V}(\varepsilon) \land n + 1 \in [\![\mathsf{True}]\!](\varepsilon) \implies n + 1 \in [\![\triangleright P]\!](\varepsilon)$.
The empty resource is valid for all n, and by definition, $[\![\mathsf{True}]\!](\varepsilon)$ holds. Therefore, we can assume $n + 1 \in [\![\triangleright P]\!](\varepsilon)$, which we can unfold to get $n \in [\![P]\!](\varepsilon)$.
Now all we need to prove is $n \in [\![P]\!](a)$, which follows from upwards closedness of resources (axiom 3.2). □

Lemma 3.6. For any Iris propisition P and any natural number n,

$$(\vdash \triangleright^n P) \implies \vdash P.$$

Proof. We prove this lemma by induction on n.

The base case $n = 0$ is immediate.

Assume we have the following induction hypothesis: $\forall P, n.\ (\vdash \triangleright^n P) \implies \vdash P$.
We will prove $\forall P, n.\ (\vdash \triangleright^{n+1} P) \implies \vdash P$.
First, we assume $\vdash \triangleright^{n+1} P$, for some n and some P. We can rewrite this to $\vdash \triangleright \triangleright^n P$. By lemma 3.5, this implies $\vdash \triangleright^n P$. Now we can use the induction hypothesis with the above assumption, which gives us $\vdash P$, which is what we wanted to prove. □

As mentioned, the lemma $\models\!\!\Rrightarrow \blacksquare P \vdash P$ is a very important building block in the adequacy theorem without later credits. Fundamentally, $\blacksquare P$ is a strong assumption; it tells us that P holds for the empty resource, hence, by monotonicity (upwards closedness), for *all* resources. This property is used in the proof of lemma 3.7, where we assume $\blacksquare P$ after an update – we get to assume $[\![\blacksquare P]\!](b)$ for some b, but by definition, the resource b does not matter, and we get $[\![P]\!](\epsilon)$.

Lemma 3.7. For any Iris proposition P,

$$\models\!\!\Rrightarrow \blacksquare P \vdash P.$$

Proof. We unfold the definition of semantic entailment (def. 3.1):

$$\forall n, a.\ n \in \mathcal{V}(a) \land n \in [\![\models\!\!\Rrightarrow \blacksquare P]\!](a) \implies n \in [\![P]\!](a).$$

To prove this, we first assume $n \in \mathcal{V}(a)$ for some natural number n and resource a. Additionally, we assume $n \in [\![\models\!\!\Rrightarrow \blacksquare P]\!](a)$, which means that $\forall m \leq n, c.\ m \in \mathcal{V}(a \cdot c) \implies \exists b.\ m \in \mathcal{V}(b \cdot c) \land m \in [\![P]\!](\varepsilon)$ by definition 3.3.
We instantiate the above assumption with $m = n$ and $c = \varepsilon$, and get the following assumption:

$$n \in \mathcal{V}(a \cdot \varepsilon) \implies \exists b.\ n \in \mathcal{V}(b \cdot \varepsilon) \land n \in [\![P]\!](\varepsilon).$$

We have assumed $n \in \mathcal{V}(a)$ and we know $\mathcal{V}(a \cdot \varepsilon) = \mathcal{V}(a)$. We instantiate the above implication with this assumption, which gives us, among other things, $n \in [\![P]\!](\varepsilon)$.
Since $\varepsilon \overset{n}{\preceq} a$ for any resource a and any n, we can apply the monotonicity axiom (axiom 3.2) with $n \in [\![P]\!](\varepsilon)$, and get $n \in [\![P]\!](a)$, which is what we wanted to show. □

3.2 Soundness Lemmas That Allocate Ghost Names

Some of the soundness lemmas that we will encounter later need to allocate ghost names to initialise the fancy update modalities and later credits (see defs. 4.2 and 4.1). We mark these soundness lemmas with a ghost symbol: 👻.
Concretely, the soundness lemmas marked by "👻" allocate the needed ghost names, either directly (e.g. lemmas 4.3 and 8.4) or indirectly by applying such an allocation lemma.

4 Later Credits in the Iris Logic

Later credits are introduced to the Iris logic in the paper *Later Credits: Resourceful Reasoning for the Later Modality* [SGT+22]. The motivation is to make elimination of later modalities in proofs easier. Concretely, if we have an assumption $\triangleright P$, it can be challenging to "eliminate the later" to be able to use P. This can easily happen in a proof, for instance if we open invariants or do Löb induction. In the paper, they show how the addition of later credits to the logic can simplify proofs, and that we can prove statements that are not immediately provable without later credits.

A later credit is an ownable resource that allows the user to eliminate a later modality. This means that the elimination of later modalities is now an amortized elimination instead of corresponding one-to-one

to program reduction steps represented by guarding later modality in the definition of the weakest precondition, which we state later, in definitions 5.2 and 6.2.

The authors accomplish the amortized elimination of later modalities in the Iris logic by adding a new resource $£n$ (n later credits) and a later eliminating update modality, $\Rightarrow^{£} P$. In practice, a user can update a proposition $\triangleright P$ to $\Rightarrow^{£} P$ for the cost of a later credit, i.e. by giving up ownership of $£1$.
The following rules showcase this interaction between later credits and the later eliminating update modality, and how a later credit is obtained by taking a pure step:

$$\textsc{LEUpdLater}\quad £1 * \triangleright P \vdash \Rightarrow^{£} P \qquad\qquad \textsc{PureStep}\quad \frac{\{P * £1\}\, e'\, \{v.\ Q\} \qquad e \to_{pure} e'}{\{P\}\, e\, \{v.\ Q\}}$$

4.1 The Later Eliminating Update Modality

The later eliminating update modality can be seen as a replacement of the basic update modality, and it indeed satisfies almost all the same rules as the basic update modality (see e.g. [JKJ+18] p. 37, Fig. 11.). However, the later eliminating update modality does *not* satisfy the rule $\Rightarrow^{£} \blacksquare P \vdash P$. As we will soon discover, this makes it challenging to prove the adequacy theorems.

The later eliminating update modality is defined recursively:

Definition 4.1.

$$\Rightarrow^{£} P \triangleq \forall n.\ £_{\bullet} n \twoheadrightarrow \Rightarrow (£_{\bullet} n * P) \vee (\exists m. \ulcorner m < n \urcorner * £_{\bullet} m * \triangleright \Rightarrow^{£} P)$$

Where $£_{\bullet} n \triangleq \boxed{\bullet n}^{\gamma_{lc}}$ and $£n \triangleq \boxed{\circ n}^{\gamma_{lc}}$ in the resource algebra $Auth(\mathbb{N}, +)$.

The resource $£_{\bullet} n$ is the later credit supply, and describes an upper bound of the credits available in the logic. We have the following rules for the later credit supply. The rule for giving up credits (SupplyDecr) is used in the proof of the rule LEUpdLater.

$$\textsc{SupplyBound}\quad £_{\bullet} n * £m \vdash \ulcorner n \geq m \urcorner \qquad\qquad \textsc{SupplyDecr}\quad £_{\bullet}(n+m) * £n \vdash \Rightarrow £_{\bullet} m$$

We can understand the definition of the later eliminating update modality the following way: When we have the proposition $\Rightarrow^{£} P$, then, for any supply of later credits, we either don't spend any later credits and get $\Rightarrow P$, or we spend some later credits and get $\Rightarrow^{£} P$ under a later modality.
The disjunction underlines the choice we get to make with the introduction of later credits to the logic; we get to decide whether to eliminate a later modality or to save "the right to eliminate a later", i.e. a later credit.

4.2 The Fancy Update Modality

Ownership of a proposition under a fancy update modality, ${}_{\mathcal{E}_1}\Rightarrow_{\mathcal{E}_2} P$, means that we can do an update (either a basic or a later eliminating update) when additionally opening invariants with names in $\mathcal{E}_1$, and after the update, the invariants with names in $\mathcal{E}_2$ are enabled. Fancy update modalities appear in the definition of the weakest precondition, and thus manipulating these modalities becomes an important consideration in the proof of the adequacy theorems, as we will see in later sections.

The definition of the fancy update modality ${}_{\mathcal{E}_1}\Rightarrow_{\mathcal{E}_2}$ depends on whether we have later credits available in the logic. When we do not have later credits, we define the fancy update modality using the basic update modality, and when we do have later credits, we instead use the later eliminating update modality. We distinguish the two different versions with a superscript b for the basic version and $£$ for the later eliminating version.[5]

Definition 4.2.

$$ {}_{\mathcal{E}_1}\Rightarrow^{\mathrm{b}}_{\mathcal{E}_2} P \triangleq\ W * \boxed{\mathcal{E}_1}^{\gamma En} \twoheadrightarrow \Rightarrow \diamond (W * \boxed{\mathcal{E}_2}^{\gamma En} * P) \qquad \text{(Without Later Credits)}$$

$$ {}_{\mathcal{E}_1}\Rightarrow^{£}_{\mathcal{E}_2} P \triangleq\ W * \boxed{\mathcal{E}_1}^{\gamma En} \twoheadrightarrow \Rightarrow^{£} \diamond (W * \boxed{\mathcal{E}_2}^{\gamma En} * P) \qquad \text{(With Later Credits)}$$

[5] In the later sections, I will almost always omit the b in the basic version.

W is world satisfaction, and the ghost resources with ghost name γEn describe which invariants are available.

To prove ${}_{\mathcal{E}_1}\Rrightarrow_{\mathcal{E}_2} P$ (regardless of whether we have later credits), we get to assume W and that invariants with names in $\mathcal{E}_1$ are enabled, and we must reestablish W, ensure that invariants in $\mathcal{E}_2$ are available (i.e. get ownership of $\boxed{\mathcal{E}_2}^{\gamma En}$) and finally prove P, all under an update modality (basic or later-eliminating) and an except-0 modality.

The following allocation lemma allows us to initialise the world satisfaction and ghost names to enable invariants:

Lemma 4.3. 👻

$$\vdash \Rrightarrow \exists \gamma_{En}, W * \boxed{\top}^{\gamma En}.$$

5 Adequacy for STLC

We start by defining the weakest precondition and stating the *weak* adequacy theorem (see definition 2.2) for a simple language, STLC, and investigate the proof of the adequacy theorem in this setting. We strip most of the complexity regarding (fancy) update modalities and thereby expose the basic structure of the proof of the weak adequacy theorem.

Definition 5.1. We define the language STLC as follows:

$$\begin{aligned} e ::= {} & () \mid (e, e) \mid \mathrm{fst}\ e \mid \mathrm{snd}\ e \\ & \mid \mathrm{inj}_1\ e \mid \mathrm{inj}_2\ e \mid \mathrm{case}\ e\ \mathrm{with}\ \mathrm{inj}_1 \Rightarrow e \mid \mathrm{inj}_2 \Rightarrow e\ \mathrm{end} \\ & \mid \lambda x.e \mid e\ e. \end{aligned}$$

We will write $e \to e'$ to represent an expression e reducing to expression e' in this language.[6]

The weakest precondition $\mathsf{wp}\, e\, \{\Phi\}$ of an expression e in the language is meant to ensure that e is either a value and $\Phi(e)$ holds, or e can reduce to an expression e', for which $\mathsf{wp}\, e'\, \{\Phi\}$ holds recursively.
In this simple language we do not have a state and therefore we do not need any update modalities to update the state. This makes the definition of the weakest precondition relatively straightforward.

Definition 5.2. (Weakest Precondition)
We define the weakest precondition for an expression e in the language and a predicate Φ of type $\mathit{Val} \to \mathit{iProp}$.

$$\mathsf{wp}\, e\, \{\Phi\} \triangleq \Big(\ulcorner \mathsf{val}(e) \urcorner \wedge \Phi(e)\Big) \vee \Big(\ulcorner \mathsf{red}(e) \urcorner \wedge (\forall e',\ \ulcorner e \to e' \urcorner \mathrel{-\!\!*} \triangleright \mathsf{wp}\, e'\, \{\Phi\}\Big).$$

Where $\mathsf{red}(e) \triangleq \exists e'.e \to e'$.

We define what it means for an expression to be *adequate* with respect to a pure predicate φ in this setting. This holds if for every expression e' that e can step to, e' is either reducible, or it is a value satisfying $\varphi(e)$ in the meta logic.

Definition 5.3. For any expression e, and any pure predicate Φ,

$$\mathsf{adequate}_{\varphi}(e) \triangleq \forall e', n.\ e \to^n e' \implies \big(\mathsf{val}(e') \wedge \varphi(e')\big) \vee \mathsf{red}(e').$$

The weak adequacy theorem, which we define below, states that the weakest precondition means something in the meta logic, namely that if we can prove the weakest precondition for some expression e and pure proposition φ, then e is adequate with respect to φ.

Theorem 5.4. (Weak Adequacy Theorem) For any expression e and any pure predicate φ,

$$(\vdash \mathsf{wp}\, e\, \{\varphi\}) \implies \mathsf{adequate}_{\varphi}(e).$$

5.1 Lemmas for the Proof of the Adequacy Theorem

Before proving the weak adequacy theorem (section 5.2), we state and prove some necessary auxiliary lemmas, both about the weakest precondition and taking reduction steps, as well as soundness lemmas for proving propositions in the logic.

Lemma 5.5. For any expression e and any predicate Φ,

$$\forall e'.\ e \to e' \implies \mathsf{wp}\, e\, \{\Phi\} \vdash \triangleright \mathsf{wp}\, e'\, \{\Phi\}.$$

Proof. Assume $e \to e'$ for some expression e', and assume $\mathsf{wp}\, e\, \{\Phi\}$, which, by unfolding the definition, gives us $\Big(\ulcorner \mathsf{val}(e) \urcorner \wedge \Phi(e)\Big) \vee \Big(\ulcorner \mathsf{red}(e) \urcorner \wedge (\forall e',\ \ulcorner e \to e' \urcorner \mathrel{-\!\!*} \triangleright \mathsf{wp}\, e'\, \{\Phi\}\Big)$. The goal is to prove $\triangleright \mathsf{wp}\, e'\, \{\Phi\}$.

First, we assume that the left-hand side of the weakest precondition disjunction holds. This is a contradiction: we have assumed that $\mathsf{val}(e)$ and that e can step to e', but values are irreducible.

Second, we assume that the right-hand side holds, i.e. $\ulcorner \mathsf{red}(e) \urcorner \wedge (\forall e',\ \ulcorner e \to e' \urcorner \mathrel{-\!\!*} \triangleright \mathsf{wp}\, e'\, \{\Phi\})$.
We instantiate the right side of the conjunction with e', and use the assumption $e \to e'$. This gives us $\triangleright \mathsf{wp}\, e'\, \{\Phi\}$, which is what we wanted to prove. □

[6] We do not give the reduction rules here. See the pure reduction rules in e.g. [BB23] p. 5.

The above lemma can be generalised to an expression taking n steps:

Lemma 5.6. For any predicate Φ and any $n \in \mathbb{N}$,

$$\forall e, e'.\ e \to^n e' \implies \mathsf{wp}\, e\, \{\Phi\} \vdash \triangleright^n \mathsf{wp}\, e'\, \{\Phi\}.$$

Proof. The proof goes by induction on the number of steps, n. In the induction step, we apply lemma 5.5, transitivity of entailment, as well as monotonicity of the later modality. □

Lemma 5.7. For any expression e and any pure proposition φ,

$$\mathsf{wp}\, e\, \{\varphi\} \vdash \ulcorner \mathsf{val}(e) \land \varphi(e) \lor \mathsf{red}(e) \urcorner.$$

Proof. We assume $\mathsf{wp}\, e\, \{\varphi\}$, which, by unfolding the definition, gives us $\Big(\ulcorner \mathsf{val}(e) \urcorner \land \varphi(e)\Big) \lor \Big(\ulcorner \mathsf{red}(e) \urcorner \land (\forall e',\ \ulcorner e \to e' \urcorner \mathrel{-\!\!*} \triangleright \mathsf{wp}\, e'\, \{\varphi\}\Big)$. First, we assume that the left-hand side of the disjunction holds. This immediately gives us the right disjunction of our goal. Second, we assume that the right-hand side holds, i.e. $\ulcorner \mathsf{red}(e) \urcorner \land (\forall e',\ \ulcorner e \to e' \urcorner \mathrel{-\!\!*} \triangleright \mathsf{wp}\, e'\, \{\varphi\})$. From this, we can immediately prove the right-hand side of the goal, $\mathsf{red}(e)$. □

Finally, we need the soundness lemmas, lemma 3.4 and lemma 3.6, which we proved in section 3.

5.2 Proving the Adequacy Theorem

Now, we can prove the adequacy theorem.

Proof. (Proof of theorem 5.4),
We assume $\vdash \mathsf{wp}\, e\, \{\varphi\}$, and that $e \to^n e'$ for some expression e' and natural number n. We have to show $(\mathsf{val}(e') \land \varphi(e')) \lor \mathsf{red}(e')$.
First, we apply lemmas 3.4 and 3.6 with n, the number of steps of $e \to^n e'$. This turns the goal into a proof of an Iris proposition,

$$\vdash \triangleright^n \ulcorner (\mathsf{val}(e') \land \varphi(e')) \lor \mathsf{red}(e') \urcorner.$$

By lemma 5.7 and monotonicity of the later modality, it suffices to show the weakest precondition of e' under n later modalities, i.e.

$$\vdash \triangleright^n \mathsf{wp}\, e'\, \{\varphi\}.$$

This follows immediately from lemma 5.6 with the assumption $\vdash \mathsf{wp}\, e\, \{\varphi\}$. □

6 Adequacy for λ_{ref}

We now consider a language, λ_{ref}, with expressions that can manipulate the heap, such as heap allocation and heap reads and writes. This makes the definition of the weakest precondition more complicated, and consequently, the proof of the adequacy theorem becomes significantly more involved. In particular, we add fancy update modalities to the definition of the weakest precondition.

Furthermore, we assume that we do not have later credits in the logic.[7]

Definition 6.1. We define the new language λ_{ref} as an extension of STLC (section 5):

$$\begin{aligned} e ::= {} & () \mid (e, e) \mid \text{fst } e \mid \text{snd } e \\ & \mid \text{inj}_1\ e \mid \text{inj}_2\ e \mid \text{case } e \text{ with } \text{inj}_1 \Rightarrow e \mid \text{inj}_2 \Rightarrow e \text{ end} \\ & \mid \lambda x.e \mid e\ e \\ & \mid \ell \mid \text{ref } e \mid !e \mid e \leftarrow e. \end{aligned}$$

Since the new expressions (load, store and allocate) use a heap, we now describe reductions of expressions with respect to a state that represents the heap.
The state is a map from locations to the values they store. Formally, we use the resource algebra $Auth(Loc \xrightarrow{fin} Ex(Val))$, and define the state, σ, and points-to predicates $\ell \mapsto v$, as elements of the resource algebra for some fixed ghost name γ_{Heap}:

$$\begin{aligned} \ell \mapsto v &\triangleq \boxed{\circ[\ell \mapsto v]}^{\gamma_{Heap}} \\ \sigma &\triangleq \boxed{\bullet\sigma}^{\gamma_{Heap}} \end{aligned}$$

The weakest precondition manages the authoritative part of the heap, $\boxed{\bullet\sigma}^{\gamma_{Heap}}$. It must ensure that the state is updated for programs that modify the heap, e.g. allocate or store values. This is how the ghost heap is tied to the physical heap.

Below, we write the reduction rules for the new alloc, load and store operations, which depend on (and modify) the state:[8]

$$\begin{aligned} (\text{ref } v, \sigma) &\to (\ell, \sigma[\ell \mapsto v]) && \text{If } \sigma(\ell) = \bot. \\ (!\ell, \sigma) &\to (v, \sigma) && \text{If } \sigma(\ell) = v. \\ (\ell \leftarrow v, \sigma) &\to ((), \sigma[\ell \mapsto v]) && \text{If } \sigma(\ell) = v'. \end{aligned}$$

We must ensure that we define the weakest precondition so that we can prove the following rules for the state-manipulating expressions, which we expect from the above reduction rules:

$$\begin{aligned} \triangleright(\forall \ell.\ \ell \mapsto v \mathrel{-\!\!*} \Phi(\ell)) &\vdash \mathsf{wp}\ \text{ref } v\ \{\Phi\} \\ \triangleright(\ell \mapsto v * (\ell \mapsto v \mathrel{-\!\!*} \Phi(v))) &\vdash \mathsf{wp}\ !\ell\ \{\Phi\} \\ \triangleright(\ell \mapsto v' * (\ell \mapsto v \mathrel{-\!\!*} \Phi(\ ))) &\vdash \mathsf{wp}\ \ell \leftarrow v\ \{\Phi\} \end{aligned}$$

Definition 6.2. (Weakest Precondition)
We define the weakest precondition for an expression e, mask $\mathcal{E}$ and a predicate Φ of type $Val \to iProp$.

$$\begin{aligned} \mathsf{wp}_{\mathcal{E}}\ e\ \{\Phi\} \triangleq {} & \Big(\mathsf{val}(e) \wedge \Rrightarrow_{\mathcal{E}} \Phi(e)\Big) \\ & \vee \Big(\forall \sigma.\ S(\sigma) \mathrel{-\!\!*} {}_{\mathcal{E}}\Rrightarrow_{\emptyset} \\ & \quad \big(\ulcorner \mathsf{red}(e, \sigma) \urcorner \wedge \ \triangleright\ (\forall e', \sigma'.\ \ulcorner (e, \sigma) \to (e', \sigma') \urcorner \mathrel{-\!\!*} {}_{\emptyset}\Rrightarrow_{\mathcal{E}} \\ & \quad (S(\sigma') * \mathsf{wp}_{\mathcal{E}}\ e'\ \{\Phi\}))\big)\Big). \end{aligned}$$

Where $\mathsf{red}(e, \sigma) \triangleq \exists e', \sigma'.(e, \sigma) \to (e', \sigma')$, and $S(\sigma) \triangleq \boxed{\bullet\sigma}^{\gamma_{Heap}}$.

[7] Whenever we write the fancy update modality ${}_{\mathcal{E}_1}\Rrightarrow_{\mathcal{E}_2}$ in this section, we mean the basic version, ${}_{\mathcal{E}_1}\Rrightarrow^{\mathrm{b}}_{\mathcal{E}_2}$.
[8] The reduction rules for the pure reductions remain the same as in STLC.

This definition of the weakest precondition is intuitively very similar to the one for STLC (definition 5.2). Again, either e is a value and the proposition $\Phi(e)$ holds (albeit after an update), or, in any state σ for which we have the state interpretation (S), e is reducible to e' (and state σ'), and the weakest precondition holds recursively for e'.
Additionally, we add the state interpretation and fancy update modalities to enable updating the state for programs that modify the heap, and thus tie the ghost heap to the physical heap.

We repeat the definitions of $\mathsf{adequate}$ and the adequacy theorem from section 2. Notably, they are analogous to how we defined them for STLC.

Definition 6.3. For any expression e, state σ and pure predicate φ,

$$\mathsf{adequate}_{\varphi}(e,\sigma) \triangleq \forall e', \sigma', n.\ (e,\sigma) \to^n (e',\sigma') \implies (\mathsf{val}(e') \wedge \varphi(e')) \vee \mathsf{red}(e',\sigma').$$

Theorem 6.4. (Weak Adequacy Theorem) For any expression e and pure predicate φ,

$$(\vdash \Rrightarrow_{\top} \exists\, S : \mathit{State} \to \mathit{iProp}.\ S(\sigma) * \mathsf{wp}_{\top}\, e\, \{\varphi\}) \implies \mathsf{adequate}_{\varphi}(e,\sigma).$$

In this definition, we existentially quantify over the state interpretation, because we will allocate the ghost name γ_{Heap} in the proof using allocation lemma 4.3.[9]

6.1 Lemmas for the Proof of the Adequacy Theorem

We state and prove lemmas needed in the proof of the adequacy theorem (section 6.2).

The lemmas involving the weakest precondition are analogous to the lemmas needed for the previous simpler adequacy theorem (section 5.2). However, in these proofs, we will additionally use rules for the fancy update modality stated in appendix A.

Furthermore, the added fancy update modalities in the definition of the weakest precondition necessitate additional soundness lemmas for handling iterated update and later modalities and for manipulating masks.

First, we prove lemmas about the weakest precondition.

Lemma 6.5. For any expression e, state σ, mask $\mathcal{E}$, and predicate Φ of type $\mathit{Var} \to \mathit{iProp}$,

$$\forall e', \sigma'.\ (e,\sigma) \to (e',\sigma') \implies \mathsf{wp}_{\mathcal{E}}\, e\, \{\Phi\} * S(\sigma) \vdash {}_{\mathcal{E}}\Rrightarrow_{\emptyset} \triangleright\, {}_{\emptyset}\Rrightarrow_{\mathcal{E}} (\mathsf{wp}_{\mathcal{E}}\, e'\, \{\Phi\} * S(\sigma'))\,.$$

Proof. Assume $(e,\sigma) \to (e',\sigma')$ for some e' and σ', and assume $\mathsf{wp}_{\mathcal{E}}\, e\, \{\Phi\}$ and $S(\sigma)$.
We will show that ${}_{\mathcal{E}}\Rrightarrow_{\emptyset} \triangleright\, {}_{\emptyset}\Rrightarrow_{\mathcal{E}} (\mathsf{wp}_{\mathcal{E}}\, e'\, \{\Phi\} * S(\sigma'))$.
We unfold the definition of the weakest precondition, and consider the two cases.
Either, $\mathsf{val}(e) \wedge \Rrightarrow_{\mathcal{E}} \Phi(e)$. However, e cannot be a value, since we have assumed e can take a step.
Therefore, we must be in the case where e is not a value, i.e.:

$$\forall \sigma.\ S(\sigma) \mathrel{-\!\!*} {}_{\mathcal{E}}\Rrightarrow_{\emptyset} \left(\ulcorner \mathsf{red}(e,\sigma) \urcorner \wedge \triangleright\, (\forall e', \sigma'.\ \ulcorner (e,\sigma) \to (e',\sigma') \urcorner \mathrel{-\!\!*} {}_{\emptyset}\Rrightarrow_{\mathcal{E}} (S(\sigma') * \mathsf{wp}_{\mathcal{E}}\, e'\, \{\Phi\}))\right)$$

We instantiate the above assumption with $S(\sigma)$, and eliminate the fancy update modality ${}_{\mathcal{E}}\Rrightarrow_{\emptyset}$ with FupdChangeMask, and introduce the fancy update modality $\Rrightarrow_{\emptyset}$ and cancel the later modality in the assumption and goal.
Now, we have to prove:

$${}_{\emptyset}\Rrightarrow_{\mathcal{E}} (\mathsf{wp}_{\mathcal{E}}\, e'\, \{\Phi\} * S(\sigma'))$$

And we have the assumption

$$\ulcorner \mathsf{red}(e,\sigma) \urcorner \wedge (\forall e', \sigma'.\ \ulcorner (e,\sigma) \to (e',\sigma') \urcorner \mathrel{-\!\!*} {}_{\emptyset}\Rrightarrow_{\mathcal{E}} (S(\sigma') * \mathsf{wp}_{\mathcal{E}}\, e'\, \{\Phi\}))$$

We can now instantiate the step with the assumed step, $(e,\sigma) \to (e',\sigma')$, which gives us the following assumption:

$${}_{\emptyset}\Rrightarrow_{\mathcal{E}} (S(\sigma') * \mathsf{wp}_{\mathcal{E}}\, e'\, \{\Phi\}))$$

We eliminate the fancy update modality in the assumption with FupdChangeMask, which turns the goal into $\Rrightarrow_{\mathcal{E}} S(\sigma') * \mathsf{wp}_{\mathcal{E}}\, e'\, \{\Phi\}$. After introducing the fancy update modality, this corresponds exactly to the assumption. □

[9] Technically, we also quantify over the the ghost names for world satisfaction used for fancy update modalities.

Lemma 6.6. For any expression e, state σ, mask $\mathcal{E}$, any $n \in \mathbb{N}$, and any Iris proposition Φ,

$$\forall e', \sigma'.\ (e, \sigma) \to^n (e', \sigma') \implies \mathsf{wp}_{\mathcal{E}}\, e\, \{\Phi\} * S(\sigma) \vdash ({}_{\mathcal{E}}\Rightarrow_{\emptyset} \triangleright\, {}_{\emptyset}\Rightarrow_{\mathcal{E}})^n\, (\mathsf{wp}_{\mathcal{E}}\, e'\, \{\Phi\} * S(\sigma'))\,.$$

Proof. The proof goes by induction on the number of steps, n. In the induction step, we apply lemma 6.5. □

Lemma 6.7. For any expression e, any state σ, any mask $\mathcal{E}$ and any pure predicate φ,

$$\mathsf{wp}_{\mathcal{E}}\, e\, \{\varphi\} * S(\sigma) \vdash (\Rightarrow_{\mathcal{E}} \ulcorner \mathsf{val}(e) \land \varphi(e) \urcorner) \lor {}_{\mathcal{E}}\Rightarrow_{\emptyset} \ulcorner \mathsf{red}(e) \urcorner\,.$$

Proof. Assume $\mathsf{wp}_{\mathcal{E}}\, e\, \{\varphi\}$ and $S(\sigma)$. We will prove $(\Rightarrow_{\mathcal{E}} \ulcorner \mathsf{val}(e) \land \varphi(e) \urcorner) \lor {}_{\mathcal{E}}\Rightarrow_{\emptyset} \ulcorner \mathsf{red}(e) \urcorner$.

We unfold the definition of the weakest precondition and consider the two disjunctions.

First, we consider the case where $\mathsf{val}(e) \land \Rightarrow_{\mathcal{E}} \varphi(e)$, from which we can easily prove the left-hand side of our goal.

Next, we consider the case where e is not a value:

$$\forall \sigma.\ S(\sigma) \mathrel{-\!\!*} {}_{\mathcal{E}}\Rightarrow_{\emptyset} \left(\ulcorner \mathsf{red}(e, \sigma) \urcorner \land \triangleright\, (\forall e', \sigma'.\ \ulcorner (e, \sigma) \to (e', \sigma') \urcorner \mathrel{-\!\!*} {}_{\emptyset}\Rightarrow_{\mathcal{E}} (S(\sigma') * \mathsf{wp}_{\mathcal{E}}\, e'\, \{\varphi\}))\right)$$

We instantiate the assumption with the state interpretation $S(\sigma)$, which gives us

$${}_{\mathcal{E}}\Rightarrow_{\emptyset} \left(\ulcorner \mathsf{red}(e, \sigma) \urcorner \land \triangleright\, (\forall e', \sigma'.\ \ulcorner (e, \sigma) \to (e', \sigma') \urcorner \mathrel{-\!\!*} {}_{\emptyset}\Rightarrow_{\mathcal{E}} (S(\sigma') * \mathsf{wp}_{\mathcal{E}}\, e'\, \{\varphi\}))\right).$$

In particular, we conclude ${}_{\mathcal{E}}\Rightarrow_{\emptyset} \ulcorner \mathsf{red}(e, \sigma) \urcorner$, which corresponds exactly to the right-hand side of the goal. □

Next, we state and prove other lemmas used in the proof of the adequacy theorem.

We need the lemma for soundness of pure propositions (lemma 3.4) in order to go from the Iris logic to the meta logic, as in the previous adequacy theorem proof for STLC.

Additionally, we will use several lemmas that include fancy update modalities.

First, we need lemmas concerning fancy update modalities that do not depend on whether or not we have later credits in the logic. We will prove these in appendix B:

Lemma 6.8.

$$\forall P, n, \mathcal{E}.\ ({}_{\mathcal{E}}\Rightarrow_{\emptyset} \triangleright\, {}_{\emptyset}\Rightarrow_{\mathcal{E}})^{n+1} \Rightarrow_{\mathcal{E}} P \vdash ({}_{\mathcal{E}}\Rightarrow_{\emptyset} \triangleright\, {}_{\emptyset}\Rightarrow_{\mathcal{E}})^{n+1} P.$$

Lemma 6.9.

$$\forall P, Q, n, \mathcal{E}_1, \mathcal{E}_2.\ (P \vdash Q) \implies ({}_{\mathcal{E}_1}\Rightarrow_{\mathcal{E}_2} \triangleright\, {}_{\mathcal{E}_2}\Rightarrow_{\mathcal{E}_1})^n\, P \vdash ({}_{\mathcal{E}_1}\Rightarrow_{\mathcal{E}_2} \triangleright\, {}_{\mathcal{E}_2}\Rightarrow_{\mathcal{E}_1})^n\, Q.$$

Finally, we need two lemmas that only work for the fancy update modality defined using the basic update modality. Their proofs depend on lemma 3.7, i.e. $\Rightarrow \blacksquare P \vdash P$. We will prove these lemmas in section 6.3.

Lemma 6.10.

$$\forall P, \mathcal{E}_1, \mathcal{E}_2.\ {}_{\mathcal{E}_1}\Rightarrow_{\mathcal{E}_2} \blacksquare P \vdash \Rightarrow_{\mathcal{E}_1} P.$$

Lemma 6.11. 👻

$$\forall P, \mathcal{E}, n.\ \vdash ({}_{\mathcal{E}}\Rightarrow_{\emptyset} \triangleright\, {}_{\emptyset}\Rightarrow_{\mathcal{E}})^n\, P \implies \vdash P.$$

6.2 Proving the Adequacy Theorem

We prove the adequacy theorem.

Proof. (Proof of theorem 6.4.) Assume $\vdash \Rrightarrow_\top \exists\, S : State \to iProp.\ S(\sigma) * \mathsf{wp}_\top\ e\ \{\Phi\})$, and that $(e, \sigma) \to^n (e', \sigma')$ for some expression e', state σ' and $n \in \mathbb{N}$.
We will prove:

$$(\mathsf{val}(e') \land \Phi(e')) \lor \mathsf{red}(e', \sigma').$$

This is a pure proposition, so by lemmas 3.4 and 6.11 with $n+1$, it suffices to show:

$$\vdash ({}_\top\Rrightarrow_\emptyset \triangleright {}_\emptyset\Rrightarrow_\top)^{n+1}\ \ulcorner(\mathsf{val}(e') \land \Phi(e')) \lor \mathsf{red}(e', \sigma')\urcorner,$$

Now we eliminate the fancy update modality in our assumption, and we thus assume the existence of S, such that $S(\sigma)$ and $\mathsf{wp}_\top\ e\ \{\Phi\}$.
We rewrite the goal using lemma 6.8, and eliminate modalities using FupdChangeMask, FupdIntro and the introducibility of the later modality. We get the following goal:

$$\vdash ({}_\top\Rrightarrow_\emptyset \triangleright {}_\emptyset\Rrightarrow_\top)^n\ \Rrightarrow_\top\ \ulcorner(\mathsf{val}(e') \land \Phi(e')) \lor \mathsf{red}(e', \sigma')\urcorner$$

Now, if we use lemma 6.6 with the assumptions $S(\sigma)$ and $\mathsf{wp}_\top\ e\ \{\Phi\}$, as well as the n steps $(e, \sigma) \to^n (e', \sigma')$, it gives us the following assumption:

$$\vdash ({}_\top\Rrightarrow_\emptyset \triangleright {}_\emptyset\Rrightarrow_\top)^n\ (\mathsf{wp}_\top\ e'\ \{\Phi\} * S(\sigma'))$$

By lemma 6.9 (monotonicity) and the above assumption, it suffices to show the following:

$$\mathsf{wp}_\top\ e'\ \{\Phi\} * S(\sigma') \vdash\ \Rrightarrow_\top \ulcorner(\mathsf{val}(e') \land \Phi(e')) \lor \mathsf{red}(e', \sigma')\urcorner.$$

We apply lemma 6.7 with $\mathsf{wp}_\top\ e'\ \{\Phi\}$ and $S(\sigma')$, which gives us the assumption:

$$(\Rrightarrow_\top \ulcorner\mathsf{val}(e') \land \Phi(e')\urcorner) \lor {}_\top\Rrightarrow_\emptyset \ulcorner\mathsf{red}(e')\urcorner.$$

We have the goal:

$$\Rrightarrow_\top \ulcorner(\mathsf{val}(e') \land \Phi(e')) \lor \mathsf{red}(e', \sigma')\urcorner.$$

If we are in the case $\Rrightarrow_\top \ulcorner\mathsf{val}(e') \land \Phi(e')\urcorner$, then we eliminate the fancy update modality in the assumption and goal, and prove the left-hand side of the goal, $\ulcorner(\mathsf{val}(e') \land \Phi(e'))\urcorner$, immediately with the assumption.

If we are in the other case, ${}_\top\Rrightarrow_\emptyset \ulcorner\mathsf{red}(e')\urcorner$ of the disjunction, then we first use lemma 6.10 with $\mathcal{E}_1 = \top$ and $\mathcal{E}_2 = \emptyset$. This turns the goal (a plain proposition) into ${}_\top\Rrightarrow_\emptyset \ulcorner(\mathsf{val}(e') \land \Phi(e')) \lor \mathsf{red}(e', \sigma')\urcorner$.
We then eliminate the fancy update modality ${}_\top\Rrightarrow_\emptyset$ in the assumption ${}_\top\Rrightarrow_\emptyset \ulcorner\mathsf{red}(e')\urcorner$ using FupdChangeMask, which turns the goal into $\Rrightarrow_\emptyset \ulcorner\mathsf{red}(e')\urcorner$. Finally, we introduce the fancy update modality with FupdIntro, and prove $\ulcorner\mathsf{red}(e')\urcorner$ with the assumption. □

6.3 Fancy Update Modality Lemmas

In this section, we prove the following two lemmas used in the proof of the adequacy theorem, which depend on lemma 3.7, $\Rrightarrow \blacksquare P \vdash P$.

Lemma 6.10 (fupd_plainly_mask):

$$\forall P, \mathcal{E}_1, \mathcal{E}_2.\ {}_{\mathcal{E}_1}\Rrightarrow_{\mathcal{E}_2} \blacksquare P \vdash \Rrightarrow_{\mathcal{E}_1} P,$$

and 👻-soundness lemma 6.11 (later_fupd_N_soundness_no_lc'):

$$\forall P, \mathcal{E}, n.\ \vdash ({}_{\mathcal{E}}\Rrightarrow_\emptyset \triangleright {}_\emptyset\Rrightarrow_{\mathcal{E}})^n\ P \implies \vdash P.$$

Since we assume we do not have later credits in the logic, the fancy update modalities are defined using the basic update modality.

The diagram below shows how the proofs of these lemmas (later_fupd_N_soundness_no_lc' and fupd_plainly_mask) ultimately depend on lemma 3.7 (bupd_plainly).

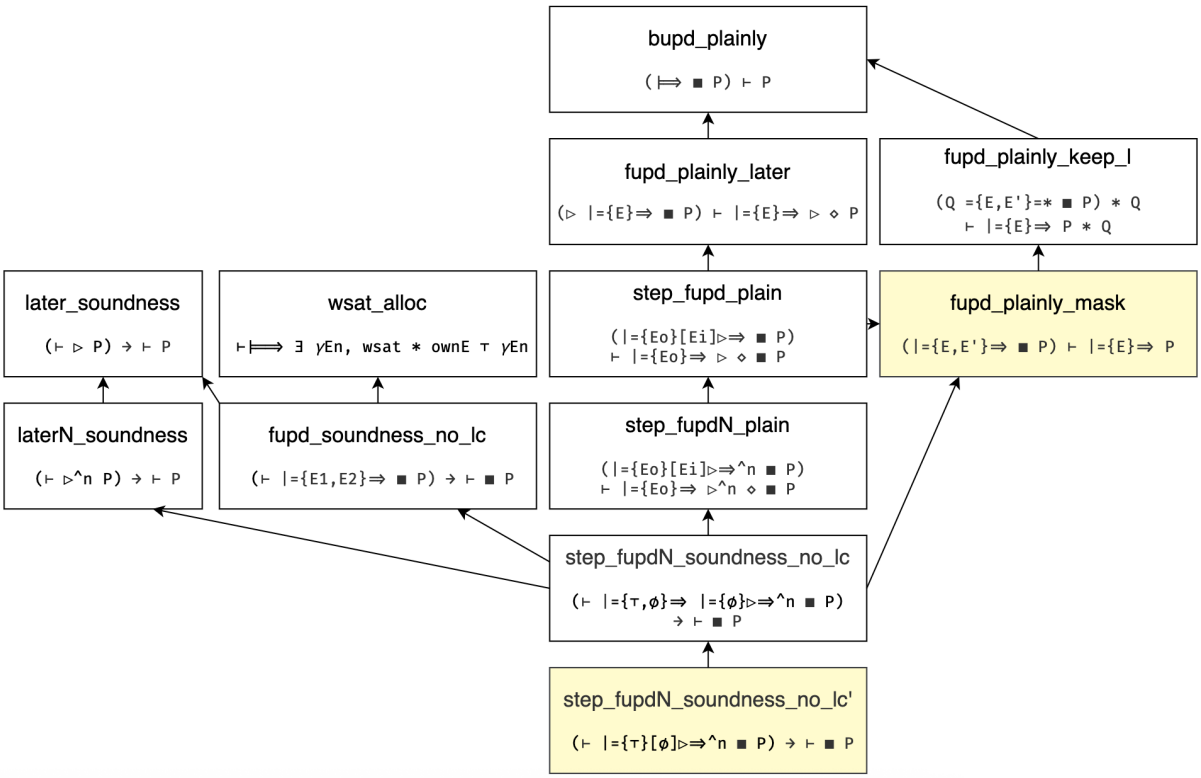

Figure 1: This figure shows dependencies between lemmas. An arrow from lemma X to lemma Y means that lemma Y is used in the proof of lemma X. The yellow lemmas (lemmas 6.17 and 6.10) are used in the proof of the adequacy theorem.

Auxiliary Lemma 6.12. (fupd_plainly_keep_l)

$$\forall P, Q, \mathcal{E}_1, \mathcal{E}_2.\ (Q \mathrel{-\!\!*}\ {}_{\mathcal{E}_1}\Rightarrow\!\!\!\blacksquare_{\mathcal{E}_2} P) * Q \vdash \Rightarrow\!\!\!\blacksquare_{\mathcal{E}_1} P * Q.$$

Proof. We simply unfold the definition of the fancy update modality. The proof then follows from lemma 3.7 and the rule A.1, which lets us keep propositions used to prove a plain proposition. □

We can finally prove the lemma used in the proof of the adequacy theorem, lemma 6.10. With logic rules trans and $\top$-introduction, and laws of (affine) bunched implications, we can derive the entailment from lemma 6.12.

Proof. (Proof of lemma 6.10, fupd_plainly_mask)

We want to show

$$ {}_{\mathcal{E}_1}\Rightarrow\!\!\!\blacksquare_{\mathcal{E}_2} P \vdash \Rightarrow\!\!\!\blacksquare_{\mathcal{E}_1} P$$

By transitivity, it suffices to show

$$ {}_{\mathcal{E}_1}\Rightarrow\!\!\!\blacksquare_{\mathcal{E}_2} P \vdash \Rightarrow\!\!\!\blacksquare_{\mathcal{E}_1} P * \mathsf{True}$$

and

$$\Rightarrow\!\!\!\blacksquare_{\mathcal{E}_1} P * \mathsf{True} \vdash \Rightarrow\!\!\!\blacksquare_{\mathcal{E}_1} P$$

The latter follows from $*$-weak.
We now use lemma 6.12. This gives us the following:

$$ {}_{\mathcal{E}_1}\Rightarrow\!\!\!\blacksquare_{\mathcal{E}_2} P \vdash (\mathsf{True} \mathrel{-\!\!*}\ {}_{\mathcal{E}_1}\Rightarrow\!\!\!\blacksquare_{\mathcal{E}_2} P) * \mathsf{True}$$

By True-I and $-\!\!*$-E it suffices to prove

$$ {}_{\mathcal{E}_1}\Rightarrow\!\!\!\blacksquare_{\mathcal{E}_2} P \vdash {}_{\mathcal{E}_1}\Rightarrow\!\!\!\blacksquare_{\mathcal{E}_2} P,$$

which is immediate. □

We now state and prove the auxiliary lemmas needed in the proof of lemma 6.11.

Auxiliary Lemma 6.13. (fupd_plain_later) For any plain Iris proposition P, and for any mask $\mathcal{E}$,

$$\triangleright \Rightarrow_{\mathcal{E}} P \vdash \Rightarrow_{\mathcal{E}} \triangleright \diamond P.$$

Proof. We assume $\triangleright \Rightarrow_{\mathcal{E}} P$ and we want to show $\Rightarrow_{\mathcal{E}} \triangleright \diamond P$ for some proposition P and mask $\mathcal{E}$.
First, we unfold the definition of the (basic) fancy update modality in the assumption $\triangleright \Rightarrow_{\mathcal{E}} P$:

$$\triangleright (W * \boxed{\mathcal{E}}^{\gamma_{En}} \twoheadrightarrow \Rightarrow \diamond (W * \boxed{\mathcal{E}}^{\gamma_{En}} * P)).$$

And in the goal, $\Rightarrow_{\mathcal{E}} \triangleright \diamond P$:

$$W * \boxed{\mathcal{E}}^{\gamma_{En}} \twoheadrightarrow \Rightarrow \diamond (W * \boxed{\mathcal{E}}^{\gamma_{En}} * \triangleright \diamond P).$$

We assume $W * \boxed{\mathcal{E}}^{\gamma_{En}}$, and the goal becomes:

$$\Rightarrow \diamond (W * \boxed{\mathcal{E}}^{\gamma_{En}} * \triangleright \diamond P).$$

Now, we prove $\triangleright \diamond P$ from the assumptions. We note that since $\triangleright \diamond P$ is a plain proposition, we keep the resources used to prove it.
By monotonicity of the later modality, it suffices to prove $\diamond P$ with the assumption:

$$W * \boxed{\mathcal{E}}^{\gamma_{En}} \twoheadrightarrow \Rightarrow \diamond (W * \boxed{\mathcal{E}}^{\gamma_{En}} * P).$$

We now specialize the assumption with $W * \boxed{\mathcal{E}}^{\gamma_{En}}$, which gives us the following assumption:

$$\Rightarrow \diamond (W * \boxed{\mathcal{E}}^{\gamma_{En}} * P).$$

We use lemma 3.7 to eliminate the update modality in the assumption:

$$\diamond (W * \boxed{\mathcal{E}}^{\gamma_{En}} * P).$$

We can cancel the except-0 modality in the assumption with the goal $\diamond P$, and use P from the assumption to prove the goal, P.

Finally, we want to prove $\Rightarrow \diamond (W * \boxed{\mathcal{E}}^{\gamma_{En}} * \triangleright \diamond P)$ with the following assumptions:

$$\triangleright \diamond P * W * \boxed{\mathcal{E}}^{\gamma_{En}}$$

This follows immediately by the introducibility of the update and except-0 modalities. □

Auxiliary Lemma 6.14. (fupd_soundness_no_lc)
For any plain Iris proposition P, and any masks $\mathcal{E}_1$ and $\mathcal{E}_2$,

$$\vdash {}_{\mathcal{E}_1}\Rightarrow_{\mathcal{E}_2} P \implies \vdash P.$$

Proof. Assume $\vdash {}_{\mathcal{E}_1}\Rightarrow_{\mathcal{E}_2} P$. We want to prove $\vdash P$.
By lemma 3.5, it suffices to prove

$$\vdash \triangleright P.$$

We allocate world satisfaction and enable all invariants under an update modality (lemma 4.3). This gives us the following assumption:

$$\Rightarrow \exists \gamma_{En}, W * \boxed{\top}^{\gamma_{En}}.$$

Since the goal is plain, we apply lemma 3.7 to eliminate the update modality in the assumption. This gives us the assumption (for some ghost name γ_{En}):

$$W * \boxed{\top}^{\gamma_{En}}$$

And goal:

$$\Rightarrow \triangleright P.$$

We now prove ${}_{\top}\Rrightarrow_{\mathcal{E}_2} P$, by using the assumption ${}_{\mathcal{E}_1}\Rrightarrow_{\mathcal{E}_2} P$, the rule FupdIntroMask and the fact that $\mathcal{E} \subseteq \top$ for all masks $\mathcal{E}$.
We unfold the definition of the fancy update modality, and specialize it with W and $\boxed{\top}^{\gamma En}$. This gives us the assumption:

$$\Rrightarrow \diamond (W * \boxed{\mathcal{E}_2}^{\gamma En} * P).$$

We use monotonicity of the update modality to eliminate the update modality in the assumption. Furthermore, we can eliminate the except-0 modality in the assumption, since we have a later modality in the goal. Now the goal P follows immediately from the assumption.

□

Auxiliary Lemma 6.15. (step_fupd_plain) For any plain Iris proposition P, and any masks $\mathcal{E}_1$ and $\mathcal{E}_2$,

$${}_{\mathcal{E}_1}\Rrightarrow_{\mathcal{E}_2} \triangleright {}_{\mathcal{E}_2}\Rrightarrow_{\mathcal{E}_1} P \vdash \Rrightarrow_{\mathcal{E}_1} \triangleright \diamond P.$$

Proof. The proof follows from lemmas 6.10 and 6.13, as well as the rule FupdChangeMask. □

Auxiliary Lemma 6.16. (step_fupdN_plain) For any plain proposition P, any masks $\mathcal{E}_1$ and $\mathcal{E}_2$, and any natural number n,

$$({}_{\mathcal{E}_1}\Rrightarrow_{\mathcal{E}_2} \triangleright {}_{\mathcal{E}_2}\Rrightarrow_{\mathcal{E}_1})^n P \vdash \Rrightarrow_{\mathcal{E}_1} \triangleright^n \diamond P.$$

Proof. The proof goes by induction on n. In the inductive step, we apply lemma 6.15. □

Auxiliary Lemma 6.17. 👻 (step_fupdN_soundness_no_lc)
For any plain Iris proposition P and any natural number n,

$$\vdash {}_{\top}\Rrightarrow_{\emptyset} (\Rrightarrow_{\emptyset} \triangleright \Rrightarrow_{\emptyset})^n\ P \implies \vdash P.$$

Proof. Assume $\vdash {}_{\top}\Rrightarrow_{\emptyset} (\Rrightarrow_{\emptyset} \triangleright \Rrightarrow_{\emptyset})^n\ P$ for some P and n. We want to prove $\vdash P$. By lemmas 3.6 with $n+1$ and 6.14, it suffices to show the following proposition:

$$\vdash \Rrightarrow_{\top} \triangleright \triangleright^n P.$$

Next, we use lemma 6.10 with $\mathcal{E}_1 = \top$ and $\mathcal{E}_2 = \emptyset$, to get the following goal:

$${}_{\top}\Rrightarrow_{\emptyset} \triangleright \triangleright^n P.$$

Now we use FupdChangeMask with the assumption ${}_{\top}\Rrightarrow_{\emptyset} (\Rrightarrow_{\emptyset} \triangleright \Rrightarrow_{\emptyset})^n\ P$. We now have show the following goal:

$$\vdash \Rrightarrow_{\emptyset} \triangleright \triangleright^n P.$$

And we have the following assumption:

$$(\Rrightarrow_{\emptyset} \triangleright \Rrightarrow_{\emptyset})^n\ P$$

We use lemma 6.16 to get the following assumption:

$$\Rrightarrow_{\emptyset} \triangleright^n \diamond P$$

We can use the monotonicity of the fancy update modality to cancel $\Rrightarrow_{\emptyset}$ in the goal and assumption. This turns the goal into $\triangleright \triangleright^n P$, and the assumption becomes $\triangleright^n \diamond P$.
Next, we use the monotonicity of the later modality to eliminate n laters.
The goal $\triangleright P$ now follows from the assumption $\diamond P$. □

Proof. (Proof of 👻-soundness lemma 6.11, later_fupd_N_soundness_no_lc')

We first apply lemma 6.17, such that it suffices to prove the following entailment:

$$\vdash {}_{\top}\Rrightarrow_{\emptyset} (\Rrightarrow_{\emptyset} \triangleright \Rrightarrow_{\emptyset})^n\ P.$$

The proof proceeds by induction on n, and uses rules about fancy update modalities (appendix A). □

7 Weak Adequacy With Later Credits

In this section, we prove the *weak* adequacy theorem with later credits in the logic.

We distinguish between two settings. In the first setting, we do *not* modify the definition of the weakest precondition to include later credits. In this setting, the proof of the adequacy theorem does not need to "give the later credits to the weakest precondition", and the outcome is that a user *cannot* use the later credits. Therefore, this setting, which we will refer to as "weakest precondition *without* later credits", corresponds to the setting without later credits in the logic from the user's point of view. In the second setting, we do modify the weakest precondition to include a later credit per step. This means that in the proof of the adequacy theorem, we will have to give all later credits to the weakest precondition. We will refer to this setting as "weakest precondition *with* later credits".

In section 7.1, we show how we can prove the weak adequacy theorem with existing lemmas using a proof structure that differs from the no-later-credits version. We note that although we can prove the weak adequacy theorem this way, it gets problematic to use the same ideas in the proof of the strong adequacy theorem. We will see why in section 8.2.

In section 7.2, we attempt an analogous proof to the one without later credits (section 6), by adapting the auxiliary lemmas to use the later eliminating update modality instead of the basic update modality. As we will see, this approach requires ownership of the later credit supply and later credits which will be "passed around" in the lemmas.

This passing around of later credits and later credit supply complicates the proofs significantly, especially when the proof requires us to eliminate multiple fancy update modalities. Therefore, we introduce the half fancy update modality in section 7.3, and use this to prove different and more easily applicable lemmas that are useful for proving the weak adequacy theorem. We now prove the weak adequacy theorem using the half fancy update modality lemmas in the two settings. In the first version – weakest precondition without later credits (section 7.4) – we allow the adequacy proof to "spend" all later credits. That is, this is analogous to not having later credits in the logic.

Finally, in section 7.5, we do proof in the second version – weakest precondition with later credits – that allows the user to actually use later credits in the logic. Specifically, the adequacy proof spends zero later credits, and the weakest precondition requires one later credit per reduction step.

7.1 Adequacy Proof With Existing Lemmas

It is possible to prove the weak adequacy theorem with existing lemmas by adapting the proof of the (strong) adequacy theorem in the Iris logic with later credits.[10]
We first give a different definition of the weakest precondition which includes later credits. With this definition, we not only get a later modality for each reduction step, we also get one later credit.[11]

Definition 7.1. (Weakest Precondition With Later Credits)
We define the weakest precondition for an expression e, a mask $\mathcal{E}$, and a predicate Φ of type $\mathsf{val} \to \mathit{iProp}$.

$$\begin{aligned}\mathsf{wp}_{\mathcal{E}}\, e\, \{\Phi\} \triangleq \Big(\mathsf{val}(e) \wand \pvs[\mathcal{E}]^{\pounds} \Phi(e)\Big) \lor \\ \Bigg(\forall \sigma.\ S(\sigma) \wand \pvs[\mathcal{E}][\emptyset]^{\pounds}\Big(\ulcorner \mathsf{red}(e,\sigma)\urcorner * \\ \big(\pounds 1 \wand \pvs[\emptyset]^{\pounds} \triangleright \pvs[\emptyset]^{\pounds}\ (\forall e', \sigma'.\ \ulcorner(e,\sigma) \to (e',\sigma')\urcorner \wand \\ \pvs[\emptyset][\mathcal{E}]^{\pounds} S(\sigma') * \mathsf{wp}_{\mathcal{E}}\, e'\, \{\Phi\}\big)\Big)\Bigg).\end{aligned}$$

Where $\mathsf{red}(e,\sigma) \triangleq \exists e', \sigma'. (e,\sigma) \to (e',\sigma')$ and $S(\sigma) \triangleq \boxed{\bullet \sigma}^{\gamma_{Heap}}$.

[10] See iris/program_logic/adequacy.v.
[11] We use the definition from the Rocq implementation, iris/program_logic/weakestpre.v.

First, we state the lemmas concerning the weakest precondition for the proof of the adequacy theorem.

The proof requires slightly different lemmas for the weakest precondition concerning reduction steps. The difference is the fancy update modalities.

Lemma 7.2. (Compare with 6.6)
For any expression e, state σ, mask $\mathcal{E}$, any $n \in \mathbb{N}$, and any Iris proposition Φ,

$$\forall e', \sigma'.\ (e, \sigma) \to^n (e', \sigma') \implies \pounds n * \mathsf{wp}_{\mathcal{E}}\, e\, \{\Phi\} * S(\sigma) \vdash {}_{\mathcal{E}}\Rrightarrow^{\pounds}_{\emptyset} (\Rrightarrow^{\pounds}_{\emptyset} \triangleright \Rrightarrow^{\pounds}_{\emptyset})^n {}_{\emptyset}\Rrightarrow^{\pounds}_{\mathcal{E}} (\mathsf{wp}_{\mathcal{E}}\, e'\, \{\Phi\} * S(\sigma'))\,.$$

In this version of lemma 6.6, the masks of the *iterated* fancy update modality is the empty set. The proof of this lemma is very similar to the earlier version, so I will not repeat it here.

Many of the lemmas and auxiliary lemmas needed for the proof are similar to (or even the same as) the ones used in the proof without later credits.
The below lemma is similar to lemma 6.17.

Lemma 7.3. 👻
For any plain Iris proposition P and any natural numbers n and m.

$$\pounds m \twoheadrightarrow {}_{\top}\Rrightarrow^{\pounds}_{\emptyset} (\Rrightarrow^{\pounds}_{\emptyset} \triangleright \Rrightarrow^{\pounds}_{\emptyset})^n P \vdash P.$$

As shown in the diagram (fig. 2) in the appendix, the proof of the crucial soundness lemma for introducing iterated fancy update and later modalities rely on the rule LEUpdLater. This rule only holds for the fancy update modality defined using the later eliminating update modality.

The auxiliary lemmas used in this proof can be found in the Rocq implementation; most of them in iris/base_logic/lib/fancy_updates.v and iris/base_logic/lib/later_credits.v.

7.1.1 Proof of the Weak Adequacy Theorem

Theorem 7.4. (Weak Adequacy Theorem With Later Credits)
For any expression e and pure predicate φ,

$$(\vdash \Rrightarrow^{\pounds}_{\top} \exists\, S : \mathit{State} \to \mathit{iProp}.\ S(\sigma) * \mathsf{wp}_{\top}\, e\, \{\varphi\}) \implies \mathsf{adequate}_{\varphi}(e, \sigma).$$

Proof. Assume $\vdash \Rrightarrow^{\pounds}_{\top} \exists\, S : \mathit{State} \to \mathit{iProp}.\ S(\sigma) * \mathsf{wp}_{\top}\, e\, \{\varphi\}$. We want to prove $\mathsf{adequate}_{\varphi}(e, \sigma)$, meaning:

$$\forall e', \sigma', n.\ (e, \sigma) \to^n (e', \sigma') \implies (\mathsf{val}(e') \wedge \varphi(e')) \vee \mathsf{red}(e', \sigma').$$

By lemmas 3.4 and 7.16, it suffices to show:

$${}_{\top}\Rrightarrow^{\pounds}_{\emptyset} (\Rrightarrow^{\pounds}_{\emptyset} \triangleright \Rrightarrow^{\pounds}_{\emptyset})^{n+1} \ulcorner (\mathsf{val}(e') \wedge \varphi(e')) \vee \mathsf{red}(e', \sigma') \urcorner$$

With ownership of $\pounds n$.

We apply lemma 6.8, and we eliminate the fancy update modality in the assumption using FupdChangeMask. This gives us the following assumption for some S:

$$S(\sigma) * \mathsf{wp}_{\top}\, e\, \{\varphi\}.$$

The goal is now:

$${}_{\top}\Rrightarrow^{\pounds}_{\emptyset} \triangleright \Rrightarrow^{\pounds}_{\emptyset} (\Rrightarrow^{\pounds}_{\emptyset} \triangleright \Rrightarrow^{\pounds}_{\emptyset})^n \Rrightarrow^{\pounds}_{\emptyset} \ulcorner (\mathsf{val}(e') \wedge \varphi(e')) \vee \mathsf{red}(e', \sigma') \urcorner.$$

After applying lemma 7.2 with the assumptions, and lemma 6.9 to cancel the iterated fancy update modalities, we have the following goal:

$${}_{\top}\Rrightarrow^{\pounds}_{\emptyset} \ulcorner (\mathsf{val}(e') \wedge \varphi(e')) \vee \mathsf{red}(e', \sigma') \urcorner.$$

And the following assumptions:

$$S(\sigma') * \mathsf{wp}_{\top}\, e'\, \{\varphi\}).$$

Now we apply lemma 5.7 with the above assumptions. This gives us the assumption that e' is either a value satisfying φ, or e' is reducible in σ'. The goal follows immediately in both cases. □

As we will see later in section 8.2, we cannot generalise this proof to also work for the strong adequacy theorem; we are missing a way to prove a plain proposition under a fancy update modality while keeping the resources used to prove it.

7.2 An Analogous Proof Structure

In this section, we attempt to state and prove lemmas with later credits in the logic analogous to the lemmas used in the proof of the weak adequacy theorem without later credits that we proved in section 6. The idea is to use the same proof structure as in the version without later credits (section 6.3) and to be able to prove the weak adequacy theorem in this way.

As explained in section 6.3, the lemma stating that $\Rightarrow \blacksquare P \vdash P$, lemma 3.7, is a crucial component of the proof of the adequacy theorem; Both lemmas 6.11 and 6.10 rely on it.

The analogous version for the later eliminating update modality, $\Rightarrow^{£} \blacksquare P \vdash P$, does not hold. This is clear from the definition of the later eliminating update, which requires ownership of the later credit supply. Instead, we will prove a similar, but weaker rule (lemma 7.5), where we assume ownership of all n later credits. The goal is to use it to prove analogous later-credit version of the auxiliary lemmas for the adequacy proof, 6.11 and 6.10 (as in section 6.3), which we then would use in the proof of the weak adequacy theorem with later credits.
However, it turns out to be difficult to prove these lemmas with our current techniques. The main challenge is to "carry around" the later credits and the later credit supply in the proofs, which is necessary in the fundamental lemmas for eliminating update modalities.

In this section, we will illustrate some of the difficulties we run into when trying to prove analogous lemmas to prove the adequacy with a proof of the same structure as the version without later credits.

7.2.1 Proving Analogous Lemmas

First, we formulate an analogous lemma to lemma 3.7, $\Rightarrow \blacksquare P \vdash P$.

We begin by illustrating why $\Rightarrow^{£} \blacksquare P \vdash P$ does not hold:
We assume $\Rightarrow^{£} \blacksquare P$, which gives us the following assumption by unfolding the definition of the later eliminating update (def. 4.1):

$$\forall n, £_\bullet\, n \mathrel{-\!\!*} \Rightarrow (£_\bullet\, n * \blacksquare P) \lor (\exists m,\ \ulcorner m < n \urcorner * £_\bullet\, m * \triangleright \Rightarrow^{£} \blacksquare P).$$

Since we have not assumed ownership of $£_\bullet\, n$, we get stuck; we cannot instantiate the assumption to get P, which is what we want to prove.

A natural next approach is to assume ownership of $£_\bullet\, n$ for some n. Then we can prove the following statement:[12]

$$£_\bullet\, n * \Rightarrow^{£} \blacksquare P \vdash \triangleright^n P.$$

We can assume ownership of m later credits as well, to get rid of the $n - m$ later modalities in the goal.[13]

$$£_\bullet\, n * £m * \Rightarrow^{£} \blacksquare P \vdash \triangleright^{n-m} P.$$

There is one immediate problem: We lose the later credit supply and the later credits in the "continuation"![14]
In practice, this means that we can only eliminate a later eliminating update modality *once*.
We therefore come up with the following lemma, that lets us prove $\blacksquare P$ under a later eliminating update modality in the continuation *with* the later credits and the later credit supply:[15]

Lemma 7.5.

$$\forall P, n.\ \ £_\bullet\, n * £n * \Rightarrow^{£}(£_\bullet\, n * £n \mathrel{-\!\!*} \blacksquare P) \vdash P.$$

Proof. We assume ownership of $£_\bullet\, n$ and $£n$, and we assume the hypothesis $\Rightarrow^{£}(£_\bullet\, n * £n \mathrel{-\!\!*} \blacksquare P)$. The goal is to prove P.

[12] We omit the proof. It goes by Löb induction and case distinction of n.
[13] We omit the proof. It goes by Löb induction and case distinction of $n - m$, and uses the rule SupplyBound.
[14] By continuation, I mean the proof obligation after applying the lemma. E.g. in this case, it is $\Rightarrow^{£} \blacksquare P$.
[15] In the following, we will assume ownership of all later credits, i.e. $£_\bullet\, n$ and $£n$, because it makes the lemmas simpler. Since we will not succeed in this undertaking regardless, it does not really matter that we do not consider the more general versions of the lemmas here.

We first use lemma 3.7, which turns the goal into $\Rightarrow \blacksquare P$.
Then, we unfold the definition of the later eliminating update modality in the hypothesis:

$$\forall n'.\ £_\bullet n' \twoheadrightarrow \Rightarrow(£_\bullet n' * (£_\bullet n * £n \twoheadrightarrow \blacksquare P)) \lor (\exists m. \ulcorner m < n' \urcorner * £_\bullet m * \triangleright \Rightarrow^{£}(£_\bullet n * £n \twoheadrightarrow \blacksquare P))$$

We instantiate the hypothesis with n and with $£_\bullet n$. We now have the following assumption:

$$\Rightarrow(£_\bullet n * (£_\bullet n * £n \twoheadrightarrow \blacksquare P)) \lor (\exists m. \ulcorner m < n \urcorner * £_\bullet m * \triangleright \Rightarrow^{£}(£_\bullet n * £n \twoheadrightarrow \blacksquare P).$$

Next, we eliminate the basic update modality in our hypothesis, and introduce it in our goal.
The assumption is a disjunction, and we consider both sides.

First, we consider the case where the hypothesis is the left-hand side of the disjunction,

$$£_\bullet n * (£_\bullet n * £n \twoheadrightarrow \blacksquare P).$$

We already own $£n$, so we can specialize the assumption $£_\bullet n * £n \twoheadrightarrow \blacksquare P$ with $£_\bullet n$ and $£n$ to get $\blacksquare P$, which is exactly what we had to show.

In the other case, we assume $\exists m. \ulcorner m < n \urcorner * £_\bullet m * \triangleright \Rightarrow^{£}(£_\bullet n * £n \twoheadrightarrow \blacksquare P)$.
This leads to a contradiction; we own $£n$, and this assumption gives us $£_\bullet m$ for some $m < n$. However, $£_\bullet m * £n \twoheadrightarrow n \leq m$, by the definition of later credits and later credit supply. □

The idea now is to use the above lemma to prove analogous versions of lemmas 6.10 and 6.17 that work in a setting with later credits. That is, we attempt to follow the lemma dependency structure illustrated in section 6.3 (fig. 1).

With this lemma, we first prove a version of 6.12 that works in a setting with later credits.

Auxiliary Lemma 7.6. (Analogous to lemma 6.12, fupd_plainly_keep_l)

$$\forall P, n, \mathcal{E}, \mathcal{E}'.\ \left(£_\bullet n * £n * Q * (Q \twoheadrightarrow {}_{\mathcal{E}}\Rightarrow^{£}_{\mathcal{E}'} \blacksquare(£_\bullet n * £n \twoheadrightarrow P))\right) \vdash {}\Rightarrow^{£}_{\mathcal{E}} P * Q.$$

Proof. This lemma follows a similar pattern as the proof of lemma 6.12; we unfold the definition of the fancy update modality. The proof follows from lemma 7.5 (instead of lemma 3.7) and the rule A.1, which lets us keep propositions used to prove a plain proposition. □

The fact that we could prove the above lemma in a very similar manner to the version of the lemma without later credits seems to be a good sign. However, we had to make small adjustments because of the later credits and the later credit supply. For example, we will get the later credits and the later credit supply in the continuation *under a plainly modality*, in order to apply the previous lemma – That makes this lemma useless in practice.

The same thing happens in the next lemma:

Lemma 7.7. (Analogous to lemma 6.10, fupd_plainly_mask)

$$\forall P, n, \mathcal{E}, \mathcal{E}'.\ \left(£_\bullet n * £n * {}_{\mathcal{E}}\Rightarrow^{£}_{\mathcal{E}'} \blacksquare(£_\bullet n * £n \twoheadrightarrow P)\right) \vdash {}\Rightarrow^{£}_{\mathcal{E}} P.$$

Proof. We assume $£_\bullet n * £n * {}_{\mathcal{E}}\Rightarrow^{£}_{\mathcal{E}'} \blacksquare(£_\bullet n * £n \twoheadrightarrow P)$, and we want to prove $\Rightarrow^{£}_{\mathcal{E}} P$.
It suffices to prove $\Rightarrow^{£}_{\mathcal{E}} P * \mathsf{True}$.
We apply lemma 7.6 with the assumptions (where Q is True). This gives us the following assumptions:

$$£_\bullet n * £n * \Rightarrow^{£}_{\mathcal{E}}(£_\bullet n * £n \twoheadrightarrow P).$$

We can eliminate the fancy update modality by monotonicity, and use $£_\bullet n * £n$ to instantiate the wand. This gives us the assumption P, which is exactly what we wanted to show. □

Now, we prove the analogous later-credit versions of the auxiliary lemmas used in the proof of lemma 6.17. First, we prove a lemma that is analogous to lemma 6.13. Note that the proof follows the proof of lemma 6.13 very closely! The only notable differences is the use of lemma 7.5 instead of lemma 3.7, and the fact that we need to assume ownership of later credits and the later credit supply, and to keep these around throughout the proof.

Auxiliary Lemma 7.8. (Analogous to lemma 6.13, fupd_plainly_later)

$$\forall P, n, \mathcal{E}.\ \left(£_\bullet n * £n * \triangleright \Rightarrow^{£}_{\mathcal{E}} (£_\bullet n * £n \mathrel{-\!\!*} \blacksquare P)\right) \vdash \Rightarrow^{£}_{\mathcal{E}} \triangleright \diamond P * £_\bullet n * £n.$$

Proof. In the proof, we unfold the definition of the fancy update modality and use lemma A.1 to prove the plain proposition $\triangleright \diamond \blacksquare P$ and keep the resources used to prove it. □

In the dependency diagram (fig. 1) for the lemmas used in the proof of the adequacy theorem without later credits, the lemma 6.13, fupd_plainly_later, and lemma 6.10, fupd_plainly_mask, are used to prove lemma 6.15, step_fupd_plain.
However, as hinted earlier, lemma 7.7 (Analogous to lemma 6.10) is not useful, and the shape of the lemmas with the later credits and later credit supply in the continuation, is not compatible with the earlier proofs without later credits. If we try to do an analogous proof to the proof of lemma 6.15, we end up with the following assumption:

$$\triangleright\, {}_{\mathcal{E}'}\Rightarrow^{£}_{\mathcal{E}} \blacksquare P,$$

And the goal

$${}_{\mathcal{E}'}\Rightarrow^{£}_{\mathcal{E}} \blacksquare(£_\bullet n * £n \mathrel{-\!\!*} \blacksquare(\blacksquare \triangleright \diamond P)).$$

Now, this is where we would apply lemma 7.8 to move the later modality outside of the fancy update modality. However, we do not assume ownership of the later credits and the later credit supply, which the lemma requires, and the goal does not have the correct shape, because of the later credits and the later credit supply – and the later credits and later credit supply are certainly not plain.

We can actually prove the lemma 7.9 more directly, by unfolding the definition of the fancy update modality, and by applying lemma 7.5 multiple times. Therefore, it seems that this approach of proving analogous lemmas and reusing the proof structure from the version of the proof of the adequacy theorem without later credits is not the right approach.

Auxiliary Lemma 7.9. (Analogous to 6.15, step_fupd_plain)

$$\forall P, \mathcal{E}, \mathcal{E}', n.\ \ £_\bullet n * £n * {}_{\mathcal{E}}\Rightarrow^{£}_{\mathcal{E}'} \triangleright\, {}_{\mathcal{E}'}\Rightarrow^{£}_{\mathcal{E}} (£_\bullet n * £n \mathrel{-\!\!*} \blacksquare P) \ \vdash\ \Rightarrow^{£}_{\mathcal{E}} \triangleright \diamond P.$$

Proof. We assume

$$£_\bullet n * £n * {}_{\mathcal{E}}\Rightarrow^{£}_{\mathcal{E}'} \triangleright\, {}_{\mathcal{E}'}\Rightarrow^{£}_{\mathcal{E}} (£_\bullet n * £n \mathrel{-\!\!*} \blacksquare P),$$

And we want to prove:

$$\Rightarrow^{£}_{\mathcal{E}} \triangleright \diamond P.$$

We unfold the definition of the fancy update modality in the goal:

$$W * \boxed{\mathcal{E}}^{\gamma En} \mathrel{-\!\!*} \Rightarrow^{£} \diamond (W * \boxed{\mathcal{E}}^{\gamma En} * \triangleright \diamond P).$$

And we introduce $W * \boxed{\mathcal{E}}^{\gamma En}$ to the context.
We assert the plain proposition $\triangleright \diamond \blacksquare P$ – that is, we get to keep the resources used to keep it.
To prove $\triangleright \diamond \blacksquare P$, we first specialize the assumption

$${}_{\mathcal{E}}\Rightarrow^{£}_{\mathcal{E}'} \triangleright\, {}_{\mathcal{E}'}\Rightarrow^{£}_{\mathcal{E}} (£_\bullet n * £n \mathrel{-\!\!*} \blacksquare P)$$

with the world satisfaction and mask, to get:

$$\Rightarrow^{£} \diamond (W * \boxed{\mathcal{E}'}^{\gamma En} * (\triangleright\, {}_{\mathcal{E}'}\Rightarrow^{£}_{\mathcal{E}} (£_\bullet n * £n \mathrel{-\!\!*} \blacksquare P)).$$

We use lemma 7.5 with the later credits and later credit supply to eliminate the later eliminating credit update in the assumption.
We now have the assumption (as well as later credits and later credit supply):

$$\diamond (W * \boxed{\mathcal{E}'}^{\gamma En} * (\triangleright\, {}_{\mathcal{E}'}\Rightarrow^{£}_{\mathcal{E}} (£_\bullet n * £n \mathrel{-\!\!*} \blacksquare P))$$

And the goal:

$$\triangleright \diamond \blacksquare P.$$

We eliminate the except-0 modality and the later modality in the assumption:

$$W * \boxed{\mathcal{E}'}^{\gamma En} * ({}_{\mathcal{E}'}\Rightarrow^{\pounds}_{\mathcal{E}}(\pounds_\bullet n * \pounds n \mathrel{-\!\!*} \blacksquare P))$$

And we have the goal:

$$\diamond \blacksquare P.$$

We can instantiate the wand with the world satisfaction and mask in the assumption:

$$\Rightarrow^{\pounds} \diamond (W * \boxed{\mathcal{E}}^{\gamma En} * (\pounds_\bullet n * \pounds n \mathrel{-\!\!*} \blacksquare P)).$$

Again, we use lemma 7.5 with the later credits and later credit supply to eliminate the later eliminating credit update in the assumption. We also eliminate the except-0 modality in the assumption, and introduce it in the goal.
We now have the following assumption:

$$W * \boxed{\mathcal{E}}^{\gamma En} * (\pounds_\bullet n * \pounds n \mathrel{-\!\!*} \blacksquare P).$$

We can instantiate the wand with the later credits and later credit supply to get $\blacksquare P$, which is exactly the goal.

Now it suffices to prove:

$$\Rightarrow^{\pounds} \diamond (W * \boxed{\mathcal{E}}^{\gamma En} * \triangleright \diamond P).$$

With the following assumptions:

$$\begin{aligned}
&\triangleright \diamond \blacksquare P,\\
&\pounds_\bullet n * \pounds n,\\
&{}_{\mathcal{E}}\Rightarrow^{\pounds}_{\mathcal{E}'} \triangleright {}_{\mathcal{E}'}\Rightarrow^{\pounds}_{\mathcal{E}} (\pounds_\bullet n * \pounds n \mathrel{-\!\!*} \blacksquare P),\\
&W * \boxed{\mathcal{E}}^{\gamma En}.
\end{aligned}$$

The goal follows by introducing the later eliminating update and except-0 modality, framing, and from the eliminability of the plainly modality. □

Finally, we will try to prove a later-credit version of lemma 6.16. Again, we would like to follow the proof described in section 6.3, i.e. do induction on m and apply lemma 7.9 (Analogous to 6.15, step_fupd_plain). This does not work, as we need the later credits and later credit supply *both* for applying the lemma *and* for using the induction hypothesis.
We will state the lemma and try (and fail) to prove it:

Lemma 7.10.

$$\forall P, \mathcal{E}, \mathcal{E}', n, m.\ \ \pounds_\bullet n * \pounds n * ({}_{\mathcal{E}}\Rightarrow^{\pounds}_{\mathcal{E}'} \triangleright {}_{\mathcal{E}'}\Rightarrow^{\pounds}_{\mathcal{E}})^m (\pounds_\bullet n * \pounds n \mathrel{-\!\!*} \blacksquare P) \ \vdash\ \Rightarrow^{\pounds}_{\mathcal{E}} \triangleright^m \diamond \blacksquare P.$$

(Attempted proof.) We do induction on m. In the base case, we have to show

$$\Rightarrow^{\pounds}_{\mathcal{E}} \diamond \blacksquare P$$

with the assumption:

$$\pounds_\bullet n * \pounds n * (\pounds_\bullet n * \pounds n \mathrel{-\!\!*} \blacksquare P)$$

We instantiate the wand with the later credits and later credit supply in the assumption, which gives us $\blacksquare P$. From this, the goal follows by introducing modalities.

Next, we assume the entailment holds for m, i.e. we have the following induction hypothesis:

$$\pounds_\bullet n * \pounds n * ({}_{\mathcal{E}}\Rightarrow^{\pounds}_{\mathcal{E}'} \triangleright {}_{\mathcal{E}'}\Rightarrow^{\pounds}_{\mathcal{E}})^m (\pounds_\bullet n * \pounds n \mathrel{-\!\!*} \blacksquare P) \ \vdash\ \Rightarrow^{\pounds}_{\mathcal{E}} \triangleright^m \diamond \blacksquare P.$$

We want to prove:

$$\Rightarrow^{\pounds}_{\mathcal{E}} \triangleright^{m+1} \diamond \blacksquare P.$$

With the assumption:

$$£_\bullet\, n * £ n * ({}_{\mathcal{E}}\Rightarrow^{£}_{\mathcal{E}'} \triangleright {}_{\mathcal{E}'}\Rightarrow^{£}_{\mathcal{E}})^{m+1}(£_\bullet\, n * £ n \mathrel{-\!\!*} \blacksquare P).$$

We can use the previous lemma (lemma 7.9) with the later credits and later credit supply (after rewriting the modalities in the goal to match). We then get the following goal:

$${}_{\mathcal{E}}\Rightarrow^{£}_{\mathcal{E}'} \triangleright {}_{\mathcal{E}'}\Rightarrow^{£}_{\mathcal{E}} (£_\bullet\, n * £ n \mathrel{-\!\!*} \blacksquare \triangleright^m P).$$

We then eliminate one iteration of the fancy update modality and the later modality in the assumption – this gives us the following assumption:

$$({}_{\mathcal{E}}\Rightarrow^{£}_{\mathcal{E}'} \triangleright {}_{\mathcal{E}'}\Rightarrow^{£}_{\mathcal{E}})^{m}(£_\bullet\, n * £ n \mathrel{-\!\!*} \blacksquare P),$$

And the following goal:

$$\Rightarrow^{£}_{\mathcal{E}} (£_\bullet\, n * £ n \mathrel{-\!\!*} \blacksquare \triangleright^m P).$$

To proceed, we need the later credits. That is, we need ownership of the later credits and the later credit supply in order to apply the induction hypothesis with the above assumption. But then we have to introduce the fancy update modality in the goal. This leaves us with the following goal:

$$\blacksquare \triangleright^m P,$$

After we instantiate the induction hypothesis with the later credits and the assumption

$$({}_{\mathcal{E}}\Rightarrow^{£}_{\mathcal{E}'} \triangleright {}_{\mathcal{E}'}\Rightarrow^{£}_{\mathcal{E}})^{m}(£_\bullet\, n * £ n \mathrel{-\!\!*} \blacksquare P),$$

we get the following assumption:

$$\Rightarrow^{£}_{\mathcal{E}} \triangleright^m \diamond \blacksquare P.$$

We cannot use this to prove the goal, as we have a fancy update modality in the assumption, and no later credits we can use to eliminate it. We abort the proof.

Of course one can think of many variants of this proof – we can do the induction later, or we can try to do the proof by unfolding the definition of the fancy update modality and use lemma 7.5, as we saw in the proof of lemma 7.9. However, we keep running into problems with "losing" the later credits and supply along the way (which are necessary to eliminate fancy update modalities in the assumptions), or having to introduce modalities earlier than desired, to get to the later credits (as we saw in the above attempted proof, right before applying the induction hypothesis).

Even if this lemma is provable, it is not intuitive to come up with a (good) proof. Therefore, we go in a different direction, and define a modality that makes it easier to work with proofs where we have later credits and the later credit supply.

7.3 Different Approach: Half Fancy Update Modality

To prove the lemmas necessary for the proof of the adequacy theorem, we use an "auxiliary" modality; a half fancy update modality, $\Rightarrow^{\mathrm{h}}_{\mathcal{E}}$. It is defined as the "first half" of the fancy update modality (def. 4.2):

Definition 7.11.

$$\Rightarrow^{\mathrm{h}}_{\mathcal{E}} P \triangleq W * \boxed{\mathcal{E}}^{\gamma En} \mathrel{-\!\!*} P.$$

Intuitively, this is like a fancy update modality, except we do not care about updating, re-establishing world satisfaction or enabling invariants after the update.

This modality is the main component of the new structure of the proof of the adequacy theorem – both the weak and strong versions.

With this modality, we can actually prove all of the "analogous lemmas" that we attempted to prove in section 7.2.1.[16] We do not prove these here, but they can be found in the Rocq code.

[16] The lemmas in diagram 1.

Interestingly, however, it is no longer necessary or even useful to attempt to prove the adequacy theorem with a similar proof as in the setting without later credits. As we will see, the lemmas that we can prove using the half fancy update modality warrant a slightly different proof structure.

In the following sections, we will show lemmas for eliminating fancy update modalities using the half fancy update modality, later credits and the later credit supply.

This modality satisfies some helpful rules such as commuting in one direction with both the basic and the later eliminating update modalities, as well as the later and except-0 modalities. We show an excerpt of the rules below.

HfupdIntro
$$P \vdash \Rightarrow^{\mathrm{h}}_{\mathcal{E}} P$$

HfupdMono
$$\frac{P \vdash Q}{\Rightarrow^{\mathrm{h}}_{\mathcal{E}} P \vdash \Rightarrow^{\mathrm{h}}_{\mathcal{E}} Q}$$

HfupdLater
$$\triangleright \Rightarrow^{\mathrm{h}}_{\mathcal{E}} P \vdash \Rightarrow^{\mathrm{h}}_{\mathcal{E}} \triangleright P$$

HfupdExcept0
$$\diamond \Rightarrow^{\mathrm{h}}_{\mathcal{E}} P \vdash \Rightarrow^{\mathrm{h}}_{\mathcal{E}} \diamond P$$

HfupdBupd
$$\Rightarrow \Rightarrow^{\mathrm{h}}_{\mathcal{E}} P \vdash \Rightarrow^{\mathrm{h}}_{\mathcal{E}} \Rightarrow P$$

HfupdLeUpd
$$\Rightarrow^{£} \Rightarrow^{\mathrm{h}}_{\mathcal{E}} P \vdash \Rightarrow^{\mathrm{h}}_{\mathcal{E}} \Rightarrow^{£} P$$

BupdPlainlyHfupd
$$\Rightarrow^{\mathrm{h}}_{\mathcal{E}} \Rightarrow \blacksquare P \vdash \Rightarrow^{\mathrm{h}}_{\mathcal{E}} P$$

7.3.1 An Auxiliary Lemma

We state a very useful lemma; it has a similar application as lemma 6.12.
If we have a goal Q under a half fancy update modality, and we have some resources R in the assumption, then this lemma lets us use R to prove some plain proposition P under a half fancy update modality (which can be used to eliminate a fancy update modality, as we will see later), as well as to use both R and P to prove our goal Q under a half fancy update modality.

Lemma 7.12. For any Iris propositions Q and R, for any plain Iris proposition P, and for any mask $\mathcal{E}$,

$$R * (R \mathrel{-\!\!*} \Rightarrow^{\mathrm{h}}_{\mathcal{E}} P) * (R \mathrel{-\!\!*} P \mathrel{-\!\!*} \Rightarrow^{\mathrm{h}}_{\mathcal{E}} Q) \vdash \Rightarrow^{\mathrm{h}}_{\mathcal{E}} Q.$$

Proof. This follows from unfolding the definition of the half fancy update modality (def. 7.11), as well as the rule for keeping resources when proving a plain proposition (lemma A.1). □

7.4 Weak Adequacy Theorem: Weakest Precondition Without Later Credits

In this section, we prove the adequacy theorem in a setting with later credits. However, we allow the proof to spend *all* later credits, and we keep the old definition of the weakest precondition (def. 6.2). This corresponds to having no later credits in the logic, since the user cannot spend them.

7.4.1 Lemmas for the Proof

First, we state a lemma for eliminating a later credit update modality in an assumption, using later credits and the later credit supply, if the goal is $\Rightarrow P$. This is similar to lemma 7.5 in that the goal can eliminate an update modality. In this version, however, we do not require the goal to be plain.

Lemma 7.13. For any Iris proposition P and any natural number n,

$$£_\bullet n * £n * \Rightarrow^{£}(£_\bullet n * £n \mathrel{-\!\!*} \Rightarrow P) \vdash \Rightarrow P.$$

Proof. We assume ownership of $£_\bullet n$ and $£n$, and we assume the hypothesis $\Rightarrow^{£}(£_\bullet n * £n \mathrel{-\!\!*} \Rightarrow P)$. The goal is to prove $\Rightarrow P$.

First, we unfold the definition of the later eliminating update modality in the hypothesis:

$$\forall n'.\ £_\bullet n' \mathrel{-\!\!*} \Rightarrow (£_\bullet n' * (£_\bullet n * £n \mathrel{-\!\!*} \Rightarrow P)) \vee (\exists m.\ulcorner m < n' \urcorner * £_\bullet m * \triangleright \Rightarrow^{£}(£_\bullet n * £n \mathrel{-\!\!*} \Rightarrow P))$$

We instantiate the hypothesis with n and with $£_\bullet n$. We now have the following assumption:

$$\Rightarrow (£_\bullet n * (£_\bullet n * £n \mathrel{-\!\!*} \Rightarrow P)) \vee (\exists m.\ulcorner m < n \urcorner * £_\bullet m * \triangleright \Rightarrow^{£}(£_\bullet n * £n \mathrel{-\!\!*} \Rightarrow P)$$

Next, we eliminate the basic update modality in our hypothesis, and introduce it in our goal, which becomes P.

The assumption is a disjunction, and we consider both sides.

First, we consider the case where the hypothesis is the left-hand side of the disjunction,

$$£_\bullet n * (£_\bullet n * £n \mathrel{-\!\!*} \Rightarrow P)$$

We own $£n$ as well as $£_\bullet n$, so we can specialize the wand $£_\bullet n * £n \mathrel{-\!\!*} \Rightarrow P$ to get $\Rightarrow P$, which is exactly what we had to show.

In the other case, we assume $\exists m. \ulcorner m < n \urcorner * £_\bullet m * \triangleright \Rightarrow^{£} (£_\bullet n * £n \mathrel{-\!\!*} \Rightarrow P)$.
This leads to a contradiction; we own $£n$, and this assumption gives us $£_\bullet m$ for some $m < n$. However, $£_\bullet m * £n \mathrel{-\!\!*} n \leq m$, by the definition of later credits and later credit supply.

□

In the following lemmas, the idea is to wrap the goal and the continuation in a half update.
We come up with the following lemma for eliminating a fancy update modality in an assumption using later credits and the later credit supply, when the goal is under a half update modality:

Lemma 7.14. For all Iris propositions Q, any Iris proposition P that can eliminate an except-0 and a basic update modality, any masks $\mathcal{E}$ and $\mathcal{E}'$, and any natural number n,

$$£_\bullet n * £n * ({}_{\mathcal{E}}\Rightarrow^{£}_{\mathcal{E}'} Q) * (£_\bullet n * £n * Q \mathrel{-\!\!*} \Rightarrow^{\mathrm{h}}_{\mathcal{E}'} P) \vdash \Rightarrow^{\mathrm{h}}_{\mathcal{E}} P.$$

Proof. We assume $£_\bullet n * £n * ({}_{\mathcal{E}}\Rightarrow^{£}_{\mathcal{E}'} Q) * (£_\bullet n * £n * Q \mathrel{-\!\!*} \Rightarrow^{\mathrm{h}}_{\mathcal{E}'} P)$, and unfold the definition of the fancy update modality (with the later eliminating update), and the half fancy update modality.
This turns the assumption ${}_{\mathcal{E}}\Rightarrow^{£}_{\mathcal{E}'} Q$ into the following:

$$W * \boxed{\mathcal{E}}^{\gamma En} \mathrel{-\!\!*} \Rightarrow^{£} \diamond (W * \boxed{\mathcal{E}'}^{\gamma En} * Q),$$

And the assumption $£_\bullet n * £n * Q \mathrel{-\!\!*} \Rightarrow^{\mathrm{h}}_{\mathcal{E}'} P$ becomes:

$$£_\bullet n * £n * Q \mathrel{-\!\!*} (W * \boxed{\mathcal{E}'}^{\gamma En} \mathrel{-\!\!*} P).$$

We unfold the definition of the half fancy update modality in the goal:

$$W * \boxed{\mathcal{E}}^{\gamma En} \mathrel{-\!\!*} P.$$

We eliminate the wand in the assumption with $W * \boxed{\mathcal{E}}^{\gamma En}$ to get the following assumption:

$$\Rightarrow^{£} \diamond (W * \boxed{\mathcal{E}'}^{\gamma En} * Q).$$

We apply lemma 7.13 with $£_\bullet n$ and $£n$ to eliminate the later eliminating update in the above assumption.
We can apply the lemma since P can eliminate a basic update modality.
Now we have the goal P, and the assumptions

$$\diamond (W * \boxed{\mathcal{E}'}^{\gamma En} * Q)$$

and

$$£_\bullet n * £n * Q \mathrel{-\!\!*} (W * \boxed{\mathcal{E}'}^{\gamma En} \mathrel{-\!\!*} P),$$

As well as the later credits and later credit supply.

We eliminate the except-0 modality in the assumption, and get assumptions Q and $W * \boxed{\mathcal{E}'}^{\gamma En}$.
The goal P now follows immediately from our assumed ownership of $£_\bullet n * £n * Q$ and $W * \boxed{\mathcal{E}'}^{\gamma En}$, as well as the assumption:

$$£_\bullet n * £n * Q \mathrel{-\!\!*} (W * \boxed{\mathcal{E}'}^{\gamma En} \mathrel{-\!\!*} P).$$

□

We also have a lemma for allocating later credits and fancy update modalities (like lemma 4.3):

Lemma 7.15. 👻
For any natural number n and mask $\mathcal{E}$,

$$\vdash \Rightarrow \pounds_\bullet\, n * \pounds n * (\forall P,\ \Rightarrow^{\mathrm{h}}{}_{\mathcal{E}}\, P \mathrel{-\!\!*} P).$$

Finally, we have a lemma for turning $n+1$ later modalities in the goal into n iterated fancy update and later modalities. The proof of this lemma showcases how easily we can eliminate fancy update modalities in assumptions with lemma 7.14, and how nicely the half fancy update modality behaves when interacting with other modalities (here, the later modality).

Lemma 7.16. For any plain Iris propositions P, and any natural numbers n and m,

$$\pounds_\bullet\, m * \pounds m * ((_\top\Rightarrow^{\pounds}_{\emptyset} \triangleright {}_\emptyset\Rightarrow^{\pounds}_{\top})^n \pounds_\bullet\, m * \pounds m \mathrel{-\!\!*} \Rightarrow^{\mathrm{h}}{}_{\top} P) \vdash \Rightarrow^{\mathrm{h}}{}_{\top} \triangleright^{n+1} P.$$

Proof. Assume $\pounds_\bullet\, m * \pounds m$ and

$$(_\top\Rightarrow^{\pounds}_{\emptyset} \triangleright {}_\emptyset\Rightarrow^{\pounds}_{\top})^n \pounds_\bullet\, m * \pounds m \mathrel{-\!\!*} \Rightarrow^{\mathrm{h}}{}_{\top} P.$$

We want to prove $\Rightarrow^{\mathrm{h}}{}_{\top} \triangleright^{n+1} P$. We do induction on n. In the base case, we have the assumptions $\pounds_\bullet\, m * \pounds m$, as well as $\pounds_\bullet\, m * \pounds m \mathrel{-\!\!*} \Rightarrow^{\mathrm{h}}{}_{\top} P$ and we want to prove $\Rightarrow^{\mathrm{h}}{}_{\top} \triangleright P$. This follows immediately from the assumptions as well as the introducibility of the later modality.

Next, we assume the entailment holds for n, i.e. we have the following induction hypothesis:

$$\pounds_\bullet\, m * \pounds m * ((_\top\Rightarrow^{\pounds}_{\emptyset} \triangleright {}_\emptyset\Rightarrow^{\pounds}_{\top})^n \pounds_\bullet\, m * \pounds m \mathrel{-\!\!*} \Rightarrow^{\mathrm{h}}{}_{\top} P) \vdash \Rightarrow^{\mathrm{h}}{}_{\top} \triangleright^{n+1} P.$$

And we want to prove the following goal:

$$\Rightarrow^{\mathrm{h}}{}_{\top} \triangleright^{n+2} P.$$

With assumptions $\pounds_\bullet\, m * \pounds m$ and

$$_\top\Rightarrow^{\pounds}_{\emptyset} \triangleright {}_\emptyset\Rightarrow^{\pounds}_{\top} (_\top\Rightarrow^{\pounds}_{\emptyset} \triangleright {}_\emptyset\Rightarrow^{\pounds}_{\top})^n \pounds_\bullet\, m * \pounds m \mathrel{-\!\!*} \Rightarrow^{\mathrm{h}}{}_{\top} P.$$

Since P is plain, so is $\triangleright^{n+2} P$. Therefore we can apply lemma 7.14, to eliminate a fancy update modality in the goal. Furthermore, we can cancel a later modality since the later modality commutes in one direction with the half fancy update modality.
Finally, we apply lemma 7.14 again to eliminate another fancy update modality.

Now we have the following goal:

$$\Rightarrow^{\mathrm{h}}{}_{\top} \triangleright^{n+1} P.$$

And the following assumption:

$$(_\top\Rightarrow^{\pounds}_{\emptyset} \triangleright {}_\emptyset\Rightarrow^{\pounds}_{\top})^n \pounds_\bullet\, m * \pounds m \mathrel{-\!\!*} \Rightarrow^{\mathrm{h}}{}_{\top} P.$$

As well as the later credits and the later credit supply.
The goal follows immediately by applying the induction hypothesis with the assumptions. □

7.4.2 Proof of the Weak Adequacy Theorem

We prove the weak adequacy theorem (thm. 2.2) with later credits.

Proof. Assume $\vdash \Rightarrow^{\pounds}_{\top} \exists\, S : State \to iProp.\ S(\sigma) * \mathsf{wp}_\top\, e\, \{\varphi\}$. We want to prove $\mathsf{adequate}_\varphi(e, \sigma)$, meaning:

$$\forall e', \sigma', n.\ (e, \sigma) \to^n (e', \sigma') \implies (\mathsf{val}(e') \wedge \varphi(e')) \vee \mathsf{red}(e', \sigma').$$

By lemmas 3.4 and 3.6 it suffices to show:

$$\triangleright^{n+2} \ulcorner (\mathsf{val}(e') \wedge \varphi(e')) \vee \mathsf{red}(e', \sigma') \urcorner.$$

By applying lemma 7.15, we get ownership of $\pounds_\bullet\, m$ and $\pounds m$ (for any m we choose), and we get to put the goal under a fancy update modality:

$$\Rightarrow^{\mathrm{h}}{}_{\top} \triangleright^{n+2} \ulcorner (\mathsf{val}(e') \wedge \varphi(e')) \vee \mathsf{red}(e', \sigma') \urcorner.$$

Now, we can apply lemma 7.14 with the later credits and later credit supply to eliminate the fancy update modality in the assumption; and we get the state interpretation and weakest precondition:

$$S(\sigma) * \mathsf{wp}_{\top}\, e\, \{\varphi\}.$$

With these, and the assumption that $(e, \sigma) \to^n (e', \sigma')$, we apply lemma 6.6. This gives us the following assumption:

$$({}_{\top}\Rightarrow^{\pounds}_{\emptyset} \triangleright {}_{\emptyset}\Rightarrow^{\pounds}_{\top})^n \left(\mathsf{wp}_{\top}\, e'\, \{\Phi\} * S(\sigma')\right).$$

Now, we apply lemma 7.16 with the later credits and later credit supply. This turns our goal into the following:

$$({}_{\top}\Rightarrow^{\pounds}_{\emptyset} \triangleright {}_{\emptyset}\Rightarrow^{\pounds}_{\top})^n \pounds_{\bullet}\, m * \pounds m \twoheadrightarrow \Rightarrow^{\mathrm{h}}_{\top} \triangleright \ulcorner \mathsf{val}(e') \wedge \varphi(e')) \vee \mathsf{red}(e', \sigma') \urcorner.$$

We cancel the n iterations of fancy update and later modalities in the goal and the assumption.
We now have the assumptions $\mathsf{wp}_{\top}\, e'\, \{\Phi\} * S(\sigma')$ as well as the later credits and the later credit supply. And we have the following goal:

$$\Rightarrow^{\mathrm{h}}_{\top} \triangleright \ulcorner \mathsf{val}(e') \wedge \varphi(e')) \vee \mathsf{red}(e', \sigma') \urcorner.$$

Next, we apply lemma 6.7 with the weakest precondition and state interpretation. This gives us two cases. Either, e' is a value:

$$\Rightarrow^{\pounds}_{\top} \ulcorner \mathsf{val}(e') \wedge \varphi(e') \urcorner$$

Or e' is reducible:

$${}_{\top}\Rightarrow^{\pounds}_{\emptyset} \ulcorner \mathsf{red}(e') \urcorner.$$

In both cases, we apply lemma 7.14 with the later credits and later credit supply to eliminate the fancy update modality in the assumption. The goal – which is a disjunction – follows from each assumption respectively, and from the introducibility of the half fancy update and later modalities. □

7.5 Weak Adequacy Theorem: Weakest Precondition With Later Credits

We now consider the proof of the weak adequacy theorem with later credits in the logic, and with later credits in the weakest precondition (def. 7.1). In this setting, the user can actually spend the later credits as intended.
This means that the lemmas used in the proof of the adequacy theorem can only require the later credit supply and 0 later credits. We generalise this to m later credits, where m is (necessarily) less than or equal to the supply.

7.5.1 Generalised Version of Lemmas: $m \leq n$ later credits

In this section, we generalise all lemmas from the previous section to have later credit supply n and m later credits for any $m \leq n$, i.e. $\pounds_{\bullet}\, n$ and $\pounds m$. In the proof of the adequacy theorem, m will be 0, signifying that no later credits are spent in the proof; all of them are used in the weakest precondition.

The difference and the challenge in this setting is that first of all, in the continuation, we do not know what the later credit supply is, only that it might be lower than when we started. Second, we get some iterated later and basic update modalities that we carry around in the goal and continuation.

Below we have a generalised version of lemma 7.13 for eliminating a later eliminating update modality:

Lemma 7.17.

$$\forall P, n, m.\ \ \pounds_{\bullet}\, n * \pounds m * \Rightarrow^{\pounds}(\forall k, \ulcorner k \leq n \urcorner * \pounds_{\bullet}\, k * \pounds m \twoheadrightarrow (\Rightarrow \triangleright)^{k-m} \Rightarrow P) \vdash (\Rightarrow \triangleright)^{n-m} \Rightarrow P.$$

The proof goes by induction on $n - m$. In the base case, when we have all later credits, we use lemma 7.13. In the induction step, the result follows from unfolding the later eliminating update modality, and applying the rule SupplyBound, as well as monotonicity of n iterations of basic update and later modalities.

Below we present the generalised version of lemma 7.14, for eliminating a fancy update modality, when the goal is under a half update modality.[17]

[17] We can prove a more general version where we do not assume than P is plain. In that version, we have iterated basic and later update modalities, instead of later modalities. However, the plain version suffices for the adequacy theorem and is conceptually simpler.

Lemma 7.18. For any Iris proposition Q, and any plain Iris proposition P which can eliminate an except-0 and a basic update modality, any masks $\mathcal{E}, \mathcal{E}'$ and any natural numbers n, m, r, and o, satisfying $n - m + r = o$,

$$\pounds_\bullet n * \pounds m * ({}_{\mathcal{E}}\Rrightarrow^{\pounds}_{\mathcal{E}'} Q) * (\forall k, \ulcorner k \leq n \urcorner * \pounds_\bullet k * \pounds m * Q \mathrel{-\!\!*} \Rrightarrow^{\mathrm{h}}_{\mathcal{E}'} \triangleright^{k-m+r} P) \\ \vdash \Rrightarrow^{\mathrm{h}}_{\mathcal{E}} \triangleright^{o} P.$$

The idea of o iterations of the later modality in the goal is the following: o is equal to $n - m$ (the current later credit supply minus the number of later credits we own) plus r extra iterations; that means we need at least $n - m$ later modalities, but if we have r more, then we keep those in the continuation. In the continuation, we thus have $k - m$ (the current later credit supply minus the number of later credits we own) plus the same extra number of later modalities r.

The essence of the proof is similar to the specialised proof (lemma 7.14). However, keeping track of the number of the later modalities, as well as the changing later credit supply makes the proof more verbose. The main idea in this proof is to do case distinction on r, and to use lemma 7.17,[18] as well as monotonicity of the later modality.

Below, we present a generalised version of lemma 7.16, where we can eliminate n iterations of a fancy update modality, a later modality, and a fancy update modality – i.e. $({}_{\top}\Rrightarrow^{\pounds}_{\emptyset} \triangleright {}_{\top}\Rrightarrow^{\pounds}_{\emptyset})^n$, – if the goal is under a half update modality, and we have $n + 1$ plus an additional $m - m'$ later modalities in the goal. The $m - m'$ is the difference between the current later credit supply and the number of later credits we own.[19]

Lemma 7.19. For any plain Iris proposition P and any natural numbers n, m and m',

$$\pounds_\bullet m * \pounds m' * ({}_{\top}\Rrightarrow^{\pounds}_{\emptyset} \triangleright {}_{\emptyset}\Rrightarrow^{\pounds}_{\top})^n (\forall k, \ulcorner k \leq m^{\urcorner} * \pounds_\bullet k * \pounds m' \mathrel{-\!\!*} \Rrightarrow^{\mathrm{h}}_{\top} \triangleright^{k-m'} P) \vdash \Rrightarrow^{\mathrm{h}}_{\top} \triangleright^{n+1+(m-m')} P.$$

The proof is similar to the proof of lemma 7.16. Again, since the later credit supply may change, and since we have later modalities involved, we have more things to bookkeep, which makes the proof more verbose. The idea, however, is similar: We do induction on n.
The base case follows immediately, with $k = m$.
The inductive step uses lemma 7.18 as well as the rule SupplyBound, and a lot of rewriting using facts about natural numbers.

Finally, we will need the following two lemmas concerning the weakest precondition. First, we need lemma 6.7, and then we need a variant of 6.6 that additionally requires n later credits. Recall that in this setting, we use the definition of the weakest precondition with later credits (def. 7.1).

Lemma 7.20. For any expression e, state σ, mask $\mathcal{E}$, any $n \in \mathbb{N}$, and any Iris proposition Φ,

$$\forall e', \sigma'.\ (e, \sigma) \to^n (e', \sigma') \implies \pounds n * \mathsf{wp}_{\mathcal{E}}\, e\, \{\Phi\} * S(\sigma) \vdash ({}_{\mathcal{E}}\Rrightarrow_{\emptyset} \triangleright {}_{\emptyset}\Rrightarrow_{\mathcal{E}})^n\ \mathsf{wp}_{\mathcal{E}}\, e'\, \{\Phi\} * S(\sigma').$$

7.5.2 Proof of the Adequacy Theorem

The proof is very similar to the proof in the previous section (with later credits, but spending all of them). The main difference is that we cannot spend all later credits in the soundness lemmas we use, and thus we have some extra later modalities. Additionally, the later credit supply is not constant – every time we use lemma 7.18 with $\pounds_\bullet n$ to eliminate a fancy update in an assumption, we get back $\pounds_\bullet k$ for some $k \leq n$, instead of getting $\pounds_\bullet n$. The consequence of this is that we have to add n more later modalities to our goal in the beginning with lemma 3.6.

Proof. Assume $\vdash \Rrightarrow^{\pounds}_{\top} \exists\ S : State \to iProp.\ S(\sigma) * \mathsf{wp}_{\top}\, e\, \{\varphi\}$. We want to prove $\mathsf{adequate}_{\varphi}(e, \sigma)$, meaning:

$$\forall e', \sigma', n.\ (e, \sigma) \to^n (e', \sigma') \implies (\mathsf{val}(e') \wedge \varphi(e')) \vee \mathsf{red}(e', \sigma').$$

[18] In a plain version, i.e. assuming P is a plain proposition. Then we get iterated later modalities instead of iterated basic update and later modalities.
[19] Again, this lemma exists in a more general version where we do not assume P is plain, and instead have iterated basic update and later modalities instead of just later modalities.

By lemmas 3.4 and 3.6 with $2n+2$ it suffices to show:

$$\triangleright^{2n+2} \ulcorner (\mathsf{val}(e') \land \varphi(e')) \lor \mathsf{red}(e', \sigma') \urcorner .$$

By applying lemma 7.15, we get ownership of $\pounds_\bullet n$ and $\pounds n$ (where n is the number of steps), and we get to put the goal under a half fancy update modality:

$$\Rrightarrow^{\mathrm{h}}_{\top} \triangleright^{2n+2} \ulcorner (\mathsf{val}(e') \land \varphi(e')) \lor \mathsf{red}(e', \sigma') \urcorner .$$

Now, we can apply lemma 7.18 with 0 of the n later credits (by splitting $\pounds n$ into $\pounds n * \pounds 0$) and the later credit supply $\pounds_\bullet n$, to eliminate the fancy update modality in the assumption; and we get the state interpretation and weakest precondition:

$$S(\sigma) * \mathsf{wp}_{\top}\, e\, \{\varphi\}.$$

After applying this lemma, we have ownership of $\pounds n$ and $\pounds_\bullet k$ for some $k \leq n$. Additionally, we have the following goal:

$$\Rrightarrow^{\mathrm{h}}_{\top} \triangleright^{k+n+2} \ulcorner (\mathsf{val}(e') \land \varphi(e')) \lor \mathsf{red}(e', \sigma') \urcorner .$$

With the assumptions $S(\sigma)$, $\mathsf{wp}_{\top}\, e\, \{\varphi\}$ and $(e, \sigma) \to^n (e', \sigma')$ – and additionally $\pounds n$ – we apply lemma 7.20. This gives us the following assumption:

$$({}_{\top}\Rrightarrow^{\pounds}_{\emptyset} \triangleright_{\emptyset} \Rrightarrow^{\pounds}_{\top})^n \left(\mathsf{wp}_{\top}\, e'\, \{\Phi\} * S(\sigma')\right).$$

Now, we apply lemma 7.19 with 0 later credits and later credit supply $\pounds_\bullet k$. This turns our goal into the following:

$$({}_{\top}\Rrightarrow^{\pounds}_{\emptyset} \triangleright_{\emptyset} \Rrightarrow^{\pounds}_{\top})^n \forall k',\ \ulcorner k' \leq k \urcorner * \pounds_\bullet k' * \pounds 0 \mathrel{-\!\!*} \Rrightarrow^{\mathrm{h}}_{\top} \triangleright^{k'} \triangleright \ulcorner (\mathsf{val}(e') \land \varphi(e')) \lor \mathsf{red}(e', \sigma') \urcorner .$$

We cancel the n iterations of fancy update and later modalities in the goal and the assumption.
We now have the assumptions

$$\mathsf{wp}_{\top}\, e'\, \{\Phi\} * S(\sigma'),$$

As well as the later credit supply $\pounds_\bullet k'$ for some $k' \leq k$.
And we have the following goal:

$$\Rrightarrow^{\mathrm{h}}_{\top} \triangleright^{k'} \triangleright \ulcorner (\mathsf{val}(e') \land \varphi(e')) \lor \mathsf{red}(e', \sigma') \urcorner .$$

Next, we apply lemma 6.7 with the weakest precondition and state interpretation. This gives us two cases. Either, e' is a value,

$$\Rrightarrow^{\pounds}_{\top} \ulcorner \mathsf{val}(e') \land \varphi(e') \urcorner,$$

or e' is reducible,

$${}_{\top}\Rrightarrow^{\pounds}_{\emptyset} \ulcorner \mathsf{red}(e') \urcorner .$$

In both cases, we apply lemma 7.18 with 0 later credits and the later credit supply $\pounds_\bullet k'$ to eliminate the fancy update modality in the assumption. The goal – which is a disjunction – follows from each assumption respectively, and from the introducibility of the half fancy update and later modalities. □

8 Strong Adequacy Theorem

In this section, we prove the stronger adequacy theorem (as discussed in section 2.2). We prove the theorem without later credits in the logic (section 8), and with later credits, both for a definition of the weakest precondition *without* later credits (section 8.3) and for the weakest precondition *with* later credits (section 8.4).
Additionally, in section 8.2, we explain why the previous proof structure used in the proof of the weak adequacy theorem (section 7.1) does not generalise to the proof of the stronger adequacy theorem.

8.1 Without Later Credits

We prove the strong adequacy theorem in a setting without later credits.

It is worth mentioning that the stronger adequacy theorem without later credits can be proved in a different way than the one we are about to present. The Rocq proof can be found in an old commit from 2021. This proof crucially relies on lemma 6.12, which allows keeping resources used to prove a plain proposition (here: $\ulcorner \mathsf{notStuck}(e', \sigma') \urcorner$) under a fancy update modality, while keeping the resources used to prove it; the state interpretation of σ' and the weakest precondition of e'. We will not go through the old proof here (although we have proved it in Rocq).

The proof presented in this section uses the lemmas concerning the half fancy update modality.

As in the proof of the weaker adequacy theorem, we need lemmas concerning the weakest precondition. First of all, we need lemma 6.6. Second, we need a slightly different version of lemma 6.7.

Lemma 8.1. For any expression e, any state σ, any mask $\mathcal{E}$ and any Iris proposition Φ,

$$\mathsf{wp}_{\mathcal{E}}\, e\, \{\Phi\} * S(\sigma) \vdash \left(\Rightarrow_{\mathcal{E}} S(\sigma) * \ulcorner \mathsf{val}(e) \urcorner * \Phi(e)\right) \vee \left({}_{\mathcal{E}}\Rightarrow_{\emptyset} \ulcorner \mathsf{red}(e, \sigma) \urcorner\right).$$

The notable difference between this lemma and lemma 6.7 is that in this version, we keep the state interpretation in the case where e is a value.

Furthermore, we will need a lemma for turning $n+1$ laters into n iterations of fancy update and later modalities (like in lemma 6.16). In this version, we wrap the goal and the continuation in a half update modality. The proof is very similar to the proof of lemma 6.16.

Lemma 8.2. For any plain Iris proposition P and any natural number n,

$$({}_{\top}\Rightarrow_{\emptyset} \triangleright {}_{\emptyset}\Rightarrow_{\top})^n \Rightarrow^{\mathrm{h}}{}_{\top} P \vdash \Rightarrow^{\mathrm{h}}{}_{\top} \triangleright^{n+1} P.$$

Proof. The proof goes by induction on n, and additionally uses lemma 8.3 as well as the rules for the half update modality (section 7.3). □

Additionally, we will need a version of lemma 7.14 without later credits for eliminating a fancy update modality when the goal is under a half fancy update modality.

Lemma 8.3. For any Iris proposition P that can eliminate an except-0 and a basic update modality, and for any masks $\mathcal{E}$ and $\mathcal{E}'$,

$$({}_{\mathcal{E}}\Rightarrow_{\mathcal{E}'} Q) * (Q \mathrel{-\!\!*} \Rightarrow^{\mathrm{h}}{}_{\mathcal{E}'} P) \vdash \Rightarrow^{\mathrm{h}}{}_{\mathcal{E}} P.$$

Proof. We unfold the definition of the fancy update modality and the half fancy update modality. This gives us the following assumptions:

$$(W * \boxed{\mathcal{E}}^{\gamma En} \mathrel{-\!\!*} \Rightarrow \diamond(W * \boxed{\mathcal{E}'}^{\gamma En} * Q)) * (Q \mathrel{-\!\!*} (W * \boxed{\mathcal{E}'}^{\gamma En} \mathrel{-\!\!*} P)).$$

And the following goal:

$$(W * \boxed{\mathcal{E}}^{\gamma En} \mathrel{-\!\!*} P).$$

We assume $W * \boxed{\mathcal{E}}^{\gamma En}$ and instantiate the wand in the assumption. This gives us the following assumptions:

$$\Rightarrow \diamond(W * \boxed{\mathcal{E}'}^{\gamma En} * Q)) * (Q \mathrel{-\!\!*} (W * \boxed{\mathcal{E}'}^{\gamma En} \mathrel{-\!\!*} P)).$$

And goal:

$$P.$$

We eliminate the basic update and except-0 modalities in the assumption, and get:

$$W * \lfloor\lceil\overline{\mathcal{E}'}\rceil\rfloor^{\gamma En} * Q * (Q \mathrel{-\!\!*} (W * \lfloor\lceil\overline{\mathcal{E}'}\rceil\rfloor^{\gamma En} \mathrel{-\!\!*} P)).$$

The goal now follows from wand elimination. □

Finally, we need an allocation lemma for initialising the fancy update modalities:

Lemma 8.4.
For any mask $\mathcal{E}$,

$$\vdash \Rightarrow (\forall P,\ \Rightarrow^{\mathrm{h}}{}_{\mathcal{E}}\, P \mathrel{-\!\!*} P).$$

With these lemmas (and a few others from e.g. appendix A), we can prove the strong adequacy theorem.

8.1.1 Proof of the Strong Adequacy Theorem

Proof. We assume

$$\vdash \Rightarrow_{\top}\ \exists\ S.\ S(\sigma) * \mathsf{wp}_{\top}\, e\, \{\Phi\} * \left(\ulcorner \mathsf{notStuck}\ (e', \sigma')\urcorner \mathrel{-\!\!*} S(\sigma') \mathrel{-\!\!*} (\mathsf{if}\ \mathsf{val}(e')\ \mathsf{then}\ \Phi(e')) \mathrel{-\!\!*} {}_{\top}\Rightarrow_{\emptyset}\ \ulcorner\varphi\urcorner\right)$$

and

$$(e, \sigma) \to^n (e', \sigma').$$

The goal is to prove φ.
By lemmas 3.4 and 3.6, it suffices to prove:

$$\vdash \triangleright^{n+2} \ulcorner\varphi\urcorner.$$

We use lemma 8.4 to initialise the ghost names, and to put the goal under a half update modality:

$$\Rightarrow^{\mathrm{h}}{}_{\top}\, \triangleright^{n+2} \ulcorner\varphi\urcorner.$$

We can now use lemma 8.3 to get rid of the fancy update modality in the assumption:

$$\Rightarrow_{\top}\ \exists\ S.\ S(\sigma) * \mathsf{wp}_{\top}\, e\, \{\Phi\} * \left(\ulcorner \mathsf{notStuck}\ (e', \sigma')\urcorner \mathrel{-\!\!*} S(\sigma') \mathrel{-\!\!*} (\mathsf{if}\ \mathsf{val}(e')\ \mathsf{then}\ \Phi(e')) \mathrel{-\!\!*} {}_{\top}\Rightarrow_{\emptyset}\ \ulcorner\varphi\urcorner\right).$$

After applying the lemma, we have the following assumptions, for some state interpretation S:

$$S(\sigma) * \mathsf{wp}_{\top}\, e\, \{\Phi\} * \left(\ulcorner \mathsf{notStuck}\ (e', \sigma')\urcorner \mathrel{-\!\!*} S(\sigma') \mathrel{-\!\!*} (\mathsf{if}\ \mathsf{val}(e')\ \mathsf{then}\ \Phi(e')) \mathrel{-\!\!*} {}_{\top}\Rightarrow_{\emptyset}\ \ulcorner\varphi\urcorner\right).$$

We then apply lemma 8.2, which gives us the following goal:

$$({}_{\top}\Rightarrow_{\emptyset} \triangleright {}_{\emptyset}\Rightarrow_{\top})^n \Rightarrow^{\mathrm{h}}{}_{\top}\, \triangleright \ulcorner\varphi\urcorner.$$

Now we apply lemma 6.6 with the assumption $(e, \sigma) \to^n (e', \sigma')$, and the weakest precondition and state interpretation. This gives us the following assumption:

$$({}_{\top}\Rightarrow_{\emptyset} \triangleright {}_{\emptyset}\Rightarrow_{\top})^n \left(\mathsf{wp}_{\top}\, e'\, \{\Phi\} * S(\sigma')\right).$$

We apply lemma 6.9 to eliminate the n iterations of fancy update and later modalities in the assumption and in the goal.
This gives us the following goal:

$$\Rightarrow^{\mathrm{h}}{}_{\top}\, \triangleright \ulcorner\varphi\urcorner.$$

And the following assumptions:

$$S(\sigma') * \mathsf{wp}_{\top}\, e'\, \{\Phi\} * \left(\ulcorner \mathsf{notStuck}\ (e', \sigma')\urcorner \mathrel{-\!\!*} S(\sigma') \mathrel{-\!\!*} (\mathsf{if}\ \mathsf{val}(e')\ \mathsf{then}\ \Phi(e')) \mathrel{-\!\!*} {}_{\top}\Rightarrow_{\emptyset}\ \ulcorner\varphi\urcorner\right).$$

Next, we apply lemma 7.12 where the plain proposition (P) is $\diamond\ulcorner \mathsf{notStuck}\ (e', \sigma')\urcorner$, and the resources we want to use to prove P, and keep afterwards, are $S(\sigma') * \mathsf{wp}_{\top}\, e'\, \{\Phi\}$.

Applying this lemma gives us the subgoal of proving:

$$S(\sigma') * \mathsf{wp}_\top\, e' \{\Phi\} \twoheadrightarrow \Rrightarrow^{\mathrm{h}}{}_\top \diamond \ulcorner \mathsf{notStuck}\ (e', \sigma') \urcorner.$$

To prove this, we use lemma 8.1 with $S(\sigma') * \mathsf{wp}_\top\, e' \{\Phi\}$, which gives us a disjunction:

$$\left(\Rrightarrow_\top S(\sigma') * \ulcorner \mathsf{val}(e') \urcorner * \Phi(e')\right) \vee \left({}_\top\Rrightarrow_\emptyset \ulcorner \mathsf{red}(e', \sigma') \urcorner\right).$$

If we are in the first case (left), then we want to prove

$$\Rrightarrow^{\mathrm{h}}{}_\top \diamond \ulcorner \mathsf{notStuck}\ (e', \sigma') \urcorner$$

With assumption:

$$\Rrightarrow_\top S(\sigma') * \ulcorner \mathsf{val}(e') \urcorner * \Phi(e').$$

First, we use lemma 8.3 to eliminate the fancy update modality in the assumption. Then we can immediately prove that e' is not stuck, since it is a value.

If we are in the second case (right), then we want to prove

$$\Rrightarrow^{\mathrm{h}}{}_\top \diamond \ulcorner \mathsf{notStuck}\ (e', \sigma') \urcorner.$$

With the assumption:

$${}_\top\Rrightarrow_\emptyset \ulcorner \mathsf{red}(e', \sigma') \urcorner.$$

Again, we apply lemma 8.3 to eliminate the fancy update modality in the assumption. Then we use the assumption that $\ulcorner \mathsf{red}(e', \sigma') \urcorner$ to prove that e' is not stuck.

Now we can prove our main goal:

$$\Rrightarrow^{\mathrm{h}}{}_\top \triangleright \ulcorner \varphi \urcorner.$$

With assumptions:

$$\diamond \ulcorner \mathsf{notStuck}\ (e', \sigma') \urcorner * S(\sigma') * \mathsf{wp}_\top\, e' \{\Phi\} * \left(\ulcorner \mathsf{notStuck}\ (e', \sigma') \urcorner \twoheadrightarrow S(\sigma') \twoheadrightarrow (\mathsf{if}\ \mathsf{val}(e')\ \mathsf{then}\ \Phi(e')) \twoheadrightarrow {}_\top\Rrightarrow_\emptyset \ulcorner \varphi \urcorner\right).$$

We can eliminate the except-0 modality in the assumption $\diamond \ulcorner \mathsf{notStuck}\ (e', \sigma') \urcorner$. Then we specialise assumption $\ulcorner \mathsf{notStuck}\ (e', \sigma') \urcorner * S(\sigma') * (\mathsf{if}\ \mathsf{val}(e')\ \mathsf{then}\ \Phi(e')) \twoheadrightarrow {}_\top\Rrightarrow_\emptyset \ulcorner \varphi \urcorner$ with the assumption $\ulcorner \mathsf{notStuck}\ (e', \sigma') \urcorner$. This gives us the following assumptions:

$$S(\sigma') * \mathsf{wp}_\top\, e' \{\Phi\} * \left(S(\sigma') \twoheadrightarrow (\mathsf{if}\ \mathsf{val}(e')\ \mathsf{then}\ \Phi(e')) \twoheadrightarrow {}_\top\Rrightarrow_\emptyset \ulcorner \varphi \urcorner\right).$$

And we still have the following goal:

$$\Rrightarrow^{\mathrm{h}}{}_\top \triangleright \ulcorner \varphi \urcorner.$$

Now, we do case distinction on whether e' is a value.

If e' is a value, then we apply lemma 8.1. This gives us a disjunction:

$$\left(\Rrightarrow_\top S(\sigma') \twoheadrightarrow \ulcorner \mathsf{val}(e') \urcorner * \Phi(e')\right) \vee \left({}_\top\Rrightarrow_\emptyset \ulcorner \mathsf{red}(e', \sigma') \urcorner\right).$$

In the second case (right), we get a contradiction: e' is assumed to be a value, so it cannot be reducible.

In the first case (left), we apply lemma 8.3 to eliminate the update modality in the assumption. This gives us the assumptions:

$$S(\sigma') * \ulcorner \mathsf{val}(e') \urcorner * \Phi(e').$$

With these assumptions, we eliminate the wand in the below assumption:

$$S(\sigma') \twoheadrightarrow (\mathsf{if}\ \mathsf{val}(e')\ \mathsf{then}\ \Phi(e')) \twoheadrightarrow {}_\top\Rrightarrow_\emptyset \ulcorner \varphi \urcorner.$$

This gives us the assumption:

$${}_\top\Rrightarrow_\emptyset \ulcorner \varphi \urcorner.$$

Finally, since the goal is a half fancy update, we can use lemma 8.3 to eliminate the update modality in the assumption. This gives us the assumption $\ulcorner \varphi \urcorner$, which is what we wanted to prove (after introducing

the half fancy update and later modalities in the goal).

In the other case, where e' is not a value, we specialise the assumption

$$S(\sigma') \twoheadrightarrow (\mathsf{if}\ \mathsf{val}(e')\ \mathsf{then}\ \Phi(e')) \twoheadrightarrow {}_{\top}\Rightarrow_{\emptyset} \ulcorner\varphi\urcorner$$

with $S(\sigma')$ and True (since e' is not a value), and we again apply lemma 8.3 to eliminate the update modality in the assumption. This gives us the assumption $\ulcorner\varphi\urcorner$, from which we can prove the goal $\Rightarrow^{\mathrm{h}}{}_{\top} \triangleright \ulcorner\varphi\urcorner$ by introducing the half fancy update and later modality.
This completes the proof. □

To make the next sections more intuitive, we will try to spell out the proof structure of the above proof more clearly:

The idea is that we can apply our soundness lemmas on our pure goal, such that it suffices to prove the pure goal under n iterations of fancy update modalities with a later modality in between, and – importantly – under a half fancy update with mask $\top$.
This half fancy update modality is then used – by lemma 8.3 – to eliminate the fancy update modalities that we inevitably get in the assumptions from the lemmas concerning weakest precondition and taking steps.
Another crucial part is the use of lemma 7.12, that lets us prove $\ulcorner\mathsf{notStuck}\ (e', \sigma')\urcorner$ under a fancy update modality, while letting us keep the resources used to prove it, including the state interpretation of σ'.
The rest of the proof is basically applying lemma 5.7 that unfolds the weakest precondition, and considering the case where e' is a value and the one where e' is reducible, and using lemma 8.3 in both cases to eliminate the fancy update modalities in the assumptions.

The proof of the strong adequacy theorem with later credits, which we will see in later sections, share a similar structure.

8.2 With Later Credits – Why the Current Proof Fails

Currently, in the Rocq implementation of the Iris, the proof of the strong adequacy theorem applies a trick to work in a setting with later credits. The trick is to instantiate the Iris proof (allocate world satisfaction, later credits, fancy updates) twice, such that we get the resources, such as the state interpretation, twice.

We sketch why this trick is needed in the current the proof in the Rocq implementation of the Iris. Consider the strong adequacy statement:

For any expressions e and e', states σ and σ', natural number n, Iris predicate Φ and proposition φ,

$$\Big(\big(\vdash \Rightarrow^{£}{}_{\top}\ \exists\, S.\ S(\sigma) * \mathsf{wp}_{\top}\, e\, \{\Phi\} * \big(\ulcorner\mathsf{notStuck}\ (e', \sigma')\urcorner * S(\sigma') * (\mathsf{if}\ \mathsf{val}(e')\ \mathsf{then}\ \Phi(e')) \twoheadrightarrow {}_{\top}\Rightarrow^{£}{}_{\emptyset}\ \ulcorner\varphi\urcorner\big)\big)$$
$$\wedge\ (e, \sigma) \to^{n} (e', \sigma')\Big) \implies \varphi.$$

Intuitively, we assume that we have the weakest precondition, the state interpretation, and that e steps in n steps to e'. Then, to prove ${}_{\top}\Rightarrow^{£}{}_{\emptyset}\ \ulcorner\varphi\urcorner$, we will have to prove that e' is not stuck in state σ', and also we have to give up ownership of the state interpretation, and we have to prove that if e' is a value, then it satisfies the postcondition Φ.
With the lemmas for taking n steps, and with $S(\sigma)$ and the weakest precondition, we get $S(\sigma')$ and the weakest precondition of e' (under some updates and later modalities). With these resources, we can prove that e' is either a value satisfying Φ, or it is reducible (under fancy update modalities) – i.e. it is not stuck. However, to get this information, we have to give up the state interpretation $S(\sigma')$.
As hinted earlier, the problem is that we actually need to give up ownership of $S(\sigma')$ to prove the plain proposition $\ulcorner\mathsf{notStuck}\ (e', \sigma')\urcorner$ under a fancy update modality. The fact that it is under a fancy update modality is crucial, as we have to eliminate the update modalities we get from lemma 5.7.
In the setting where we do not have later credits, this problem is solved by lemma 6.12 that lets us keep $S(\sigma')$, since $\ulcorner\mathsf{notStuck}\ (e', \sigma')\urcorner$ is a plain proposition.
In this setting, we do not have such a lemma, and, as discussed in section 7.2.1, such a lemma would require ownership of later credits and the later credit supply. Thus, we get stuck.

8.3 Strong Adequacy: Weakest Precondition Without Later Credits

This is the same setting as the one in which we proved the weaker adequacy theorem in section 7.4: We have later credits in the logic, and we spend all later credits in the adequacy proof. That means we do not include later credits in the weakest precondition, and consequently this setting corresponds (from a user's perspective) to not having later credits in the logic. The proof can be found in the Rocq code.

The proof follows the same structure as the proof in a setting without later credits in the logic (section 8.1.1). We explain some of the key differences.

We use exactly the same lemmas concerning the weakest precondition and taking steps (lemmas 6.6 and 8.1), since the weakest precondition in this setting does not have later credits.
Instead of applying lemma 8.3 to eliminate fancy update modalities when the goal is under a half fancy update modality, we apply the later-credit version, lemma 7.14. This means that we actually have to own the later credit supply and all later credits.
Therefore, we use lemma 7.15 to not only get the goal under a half fancy update modality, but also to allocate the later credits and later credits supply.

Finally, instead of applying lemma 6.17 to turn $n+1$ later modalities into n iterations of fancy update modalities with a later modality in between, we apply the later-credit version, lemma 7.16.

8.4 Strong Adequacy: Weakest Precondition With Later Credits

In this setting, we have later credits in the logic, and we do not spend any later credits in the adequacy proof. This allows us to give the later credits to the weakest precondition, such that a user can actually spend them. We are in the same setting as in section 7.5.

The proof structure is similar to the proof in a setting without later credits in the logic (section 8.1.1), and of course to the proof in a setting with later credits but where we spend all of them (section 8.3). We sketch the main ideas and the main differences from the previous proofs of the strong adequacy theorem. The proof can be found in the Rocq code.

In this setting, the weakest precondition includes later credits (def. 7.1). This means that we will use lemma 7.20 instead of lemma 6.6. Additionally, we will need lemma 8.1.
A key difference is that the later credit supply potentially gets smaller every time we apply lemma 7.18 (for eliminating a fancy update modality when the goal is under a half fancy update modality) and therefore so does the number of later modalities in the continuation. Therefore, we need to apply lemma 3.6 with $3n+2$, in order to ensure that we have n later modalities in the goal for each fancy update modality we want to eliminate.

As in the proof of the weak adequacy theorem (section 7.5), we split the n later credits into $£n * £0$, and use the n later credits for the weakest precondition (lemma 7.20) and the 0 later credits for the soundness and fancy update elimination lemmas 7.18 and 7.19.

9 Conclusion

In this project, we have come up with a different proof of the strong adequacy theorem with later credits, that avoids the "trick" of initialising the proof twice to get the resources twice used in the current proof in the Rocq formalisation of Iris.
The proof presented in this project uses a new modality; the half fancy update modality. The half update modality together with ownership of later credit and the later credit supply is useful for eliminating fancy update modalities in assumptions.
Concretely, lemma 7.12 allows us to keep resources used to prove plain propositions when the goal is under a half fancy update modality. Furthermore, with lemma 7.14, we can eliminate a fancy update modality with later credits and the later credit supply when the goal is under a half fancy update modality (and the more general version, lemma 7.18).
These lemmas – along with the rules stating that e.g. the half fancy update commutes in one direction with indtroducible modalities – allow us to prove the strong adequacy theorem with later credits.

The ideas presented in this project report can be used to improve the adequacy proof in the Rocq formalisation of Iris. In this project, we have not concerned ourselves with concurrency, so we cannot immediately use the proof presented here in the Rocq formalisation of Iris.
However, Amin Timany has implemented (a variant of) the half fancy update modality in the Rocq formalisation of Iris and improved the proof of the adequacy theorem. His work is available in this MR.

References

[BB23] Lars Birkedal and Aleš Bizjak. Lecture notes on iris: Higher-order concurrent separation logic, 2023.

[JKJ+18] Ralf Jung, Robbert Krebbers, Jacques-Henri Jourdan, Aleš Bizjak, Lars Birkedal, and Derek Dreyer. Iris from the ground up: A modular foundation for higher-order concurrent separation logic. *Journal of Functional Programming*, 28:e20, 2018.

[SGT+22] Simon Spies, Lennard Gäher, Joseph Tassarotti, Ralf Jung, Robbert Krebbers, Lars Birkedal, and Derek Dreyer. Later credits: resourceful reasoning for the later modality. *Proc. ACM Program. Lang.*, 6(ICFP), August 2022.

A Rules: Fancy Update Modality and Plainly Modality

We will need some of the rules for the fancy update modality ([JKJ+18] p. 57)

$$\textsc{FupdIntro}\quad P \vdash \Rightarrow_{\mathcal{E}} P \qquad \textsc{FupdIntroMask}\quad \frac{\mathcal{E}_1 \subseteq \mathcal{E}_2}{\mathsf{True} \vdash {}_{\mathcal{E}_1}\Rightarrow_{\mathcal{E}_2} {}_{\mathcal{E}_2}\Rightarrow_{\mathcal{E}_1} \mathsf{True}} \qquad \textsc{FupdTrans}\quad {}_{\mathcal{E}_1}\Rightarrow_{\mathcal{E}_2} {}_{\mathcal{E}_2}\Rightarrow_{\mathcal{E}_3} P \vdash {}_{\mathcal{E}_1}\Rightarrow_{\mathcal{E}_3} P \qquad \textsc{FupdChangeMask}\quad \frac{R * P \vdash {}_{\mathcal{E}_2}\Rightarrow_{\mathcal{E}_3} Q}{R * {}_{\mathcal{E}_1}\Rightarrow_{\mathcal{E}_2} P \vdash {}_{\mathcal{E}_1}\Rightarrow_{\mathcal{E}_3} Q}$$

$$\textsc{FupdMono}\quad \frac{P \vdash Q}{{}_{\mathcal{E}_1}\Rightarrow_{\mathcal{E}_2} P \vdash {}_{\mathcal{E}_1}\Rightarrow_{\mathcal{E}_2} Q}$$

Lemma A.1.

$$\frac{Q \vdash \blacksquare P}{Q \vdash \blacksquare P * Q}$$

Proof. This proof follows from the rules for the plainly modality:

$$\textsc{Plainly-Sep}\ \frac{\wedge\text{-I}\ \dfrac{\textsc{Assumption}\ \dfrac{}{Q \vdash \blacksquare P} \qquad \textsc{Asm}\ \dfrac{}{Q \vdash Q}}{Q \vdash \blacksquare P \wedge Q}}{Q \vdash \blacksquare P * Q}$$

□

B Fancy Update Modality Lemmas for the Adequacy Theorem

Lemma 6.8.

$$\forall P, n, \mathcal{E}.\ ({}_{\mathcal{E}}\Rightarrow_{\emptyset} \triangleright {}_{\emptyset}\Rightarrow_{\mathcal{E}})^{n+1} \Rightarrow_{\mathcal{E}} P \vdash ({}_{\mathcal{E}}\Rightarrow_{\emptyset} \triangleright {}_{\emptyset}\Rightarrow_{\mathcal{E}})^{n+1} P.$$

Proof. We assume $({}_{\mathcal{E}}\Rightarrow_{\emptyset} \triangleright {}_{\emptyset}\Rightarrow_{\mathcal{E}})^{n+1} \Rightarrow_{\mathcal{E}} P$ for some P, n and $\mathcal{E}$, and we want to show $({}_{\mathcal{E}}\Rightarrow_{\emptyset} \triangleright {}_{\emptyset}\Rightarrow_{\mathcal{E}})^{n+1} P$.
First, we rewrite our goal to $({}_{\mathcal{E}}\Rightarrow_{\emptyset} \triangleright {}_{\emptyset}\Rightarrow_{\mathcal{E}})^{n}({}_{\mathcal{E}}\Rightarrow_{\emptyset} \triangleright {}_{\emptyset}\Rightarrow_{\mathcal{E}})\ P$.
We can now apply lemma 6.9 to eliminate $({}_{\mathcal{E}}\Rightarrow_{\emptyset} \triangleright {}_{\emptyset}\Rightarrow_{\mathcal{E}})^{n}$. Now we have to show

$$({}_{\mathcal{E}}\Rightarrow_{\emptyset} \triangleright {}_{\emptyset}\Rightarrow_{\mathcal{E}})\ \Rightarrow_{\mathcal{E}} P \vdash ({}_{\mathcal{E}}\Rightarrow_{\emptyset} \triangleright {}_{\emptyset}\Rightarrow_{\mathcal{E}})\ P.$$

This follows immediately by rewriting the hypothesis with FupdTrans. □

Lemma 6.9.

$$\forall P, Q, n, \mathcal{E}_1, \mathcal{E}_2.\ (P \vdash Q) \implies ({}_{\mathcal{E}_1}\Rightarrow_{\mathcal{E}_2} \triangleright {}_{\mathcal{E}_2}\Rightarrow_{\mathcal{E}_1})^{n} P \vdash ({}_{\mathcal{E}_2}\Rightarrow_{\mathcal{E}_1} \triangleright {}_{\mathcal{E}_2}\Rightarrow_{\mathcal{E}_1})^{n} Q$$

Proof. Assume $P \vdash Q$. We do induction on n.

Consider the case $n = 0$. We now have to prove $P \vdash Q$, which follows immediately from the assumption.

Next, we assume the claim holds for n, i.e. $({}_{\mathcal{E}_1}\Rightarrow_{\mathcal{E}_2} \triangleright {}_{\mathcal{E}_2}\Rightarrow_{\mathcal{E}_1})^{n} P \vdash ({}_{\mathcal{E}_1}\Rightarrow_{\mathcal{E}_2} \triangleright {}_{\mathcal{E}_2}\Rightarrow_{\mathcal{E}_1})^{n} Q$. This is our induction hypothesis.
We want to show that the following entailment holds:

$$({}_{\mathcal{E}_1}\Rightarrow_{\mathcal{E}_2} \triangleright {}_{\mathcal{E}_2}\Rightarrow_{\mathcal{E}_1})({}_{\mathcal{E}_1}\Rightarrow_{\mathcal{E}_2} \triangleright {}_{\mathcal{E}_2}\Rightarrow_{\mathcal{E}_1})^{n} P \vdash ({}_{\mathcal{E}_1}\Rightarrow_{\mathcal{E}_2} \triangleright {}_{\mathcal{E}_2}\Rightarrow_{\mathcal{E}_1})({}_{\mathcal{E}_1}\Rightarrow_{\mathcal{E}_2} \triangleright {}_{\mathcal{E}_2}\Rightarrow_{\mathcal{E}_1})^{n} Q.$$

This follows from the induction hypothesis after applying FupdMono, monotonicity of the later modality, and FupdMono again. □

C Diagram: Weak Adequacy Theorem With Later Credits

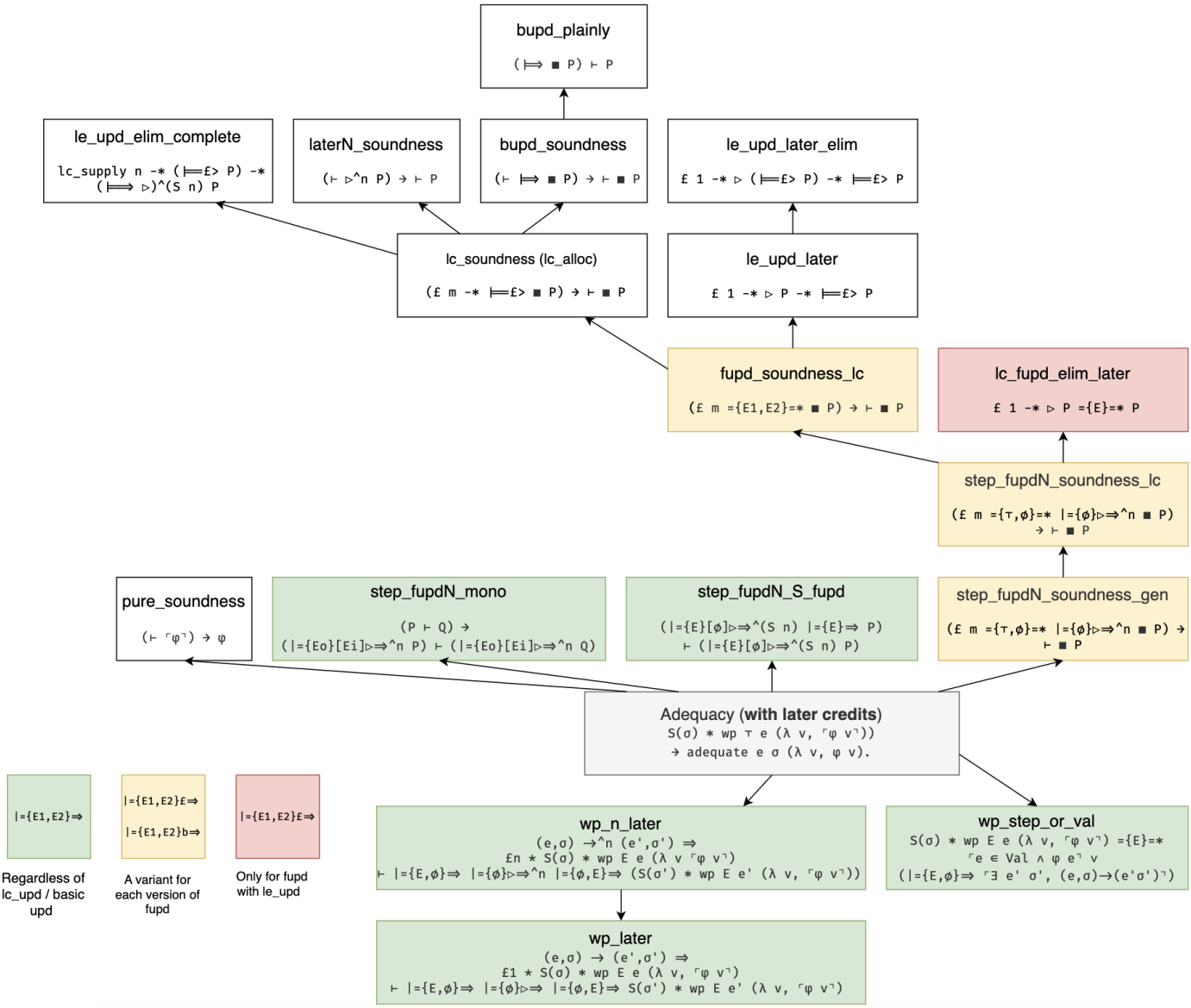

Figure 2: Overview of the lemmas used in the proof of the adequacy theorem. An arrow from lemma X to lemma Y means that lemma X uses lemma Y in its proof.