Abstract Local Reasoning for Concurrent Libraries

Azalea Raad Adam Wright
Mark Wheelhouse Philippa Gardner

{azalea, adw07, mjw03, pg}@doc.ic.ac.uk

March 24, 2014

Contents

1. Structural Separation Logic

We introduce the technical details of *generalised SSL* and formalise various ingredients necessary for building an abstract library. Abstract libraries allow programs that manipulate abstract structures without concern for the implementation. This is achieved through a set of atomic commands associated with the library.

Definition 1 (Atomic Commands)**.** For an abstract library $\mathbb{A}$, the set of *abstract atomic commands* is denoted $\textsc{Atom}_{\mathbb{A}}$.

The commands of an abstract library operate on *abstract heaps* mapping *addresses* to *abstract data*. We proceed with the definition of addresses.

Definition 2. (Addresses) Given an abstract library $\mathbb{A}$, a set of program variables PVars, a countably infinite set of abstract addresses SAdd ranged over by $\mathbf{x}, \mathbf{y}, \mathbf{z}$, and a library-specific set of machine addresses $\textsc{MAdd}_{\mathbb{A}}$ ranged over by $\mathcal{R}$, $\mathcal{R}_1$, $\mathcal{R}_2$, such that the domains of PVars, SAdd and $\textsc{MAdd}_{\mathbb{A}}$ are pairwise disjoint, the set of *addresses of abstract library* $\mathbb{A}$ ranged over by a, a_1, a_2, is defined as:

$$\textsc{Add}_{\mathbb{A}} \triangleq \textsc{MAdd}_{\mathbb{A}} \uplus \textsc{SAdd}$$

Definition 3 (Addressing Algebra)**.** Given an abstract library $\mathbb{A}$ and an arbitrary countable set of values $\textsc{Values}_{\mathbb{A}}$, a *structural addressing algebra* on $\textsc{Values}_{\mathbb{A}}$ consists of a countably infinite set of structural addresses SAdd, a countable set of addressable data $\textsc{Data}_{\mathbb{A}}$, an *addresses* function $\mathit{addrs}(.)$ and a *compression* function $\mathit{comp}(.)$:

$$\mathcal{A}_{\mathbb{A}} \triangleq \left(\begin{array}{c} \textsc{SAdd}, \textsc{Data}_{\mathbb{A}}, \\ \mathit{addrs}(.) : \textsc{Data}_{\mathbb{A}} \to \wp(\textsc{SAdd}), \\ \mathit{comp}(.) : \textsc{SAdd} \overset{\text{fin}}{\to} \textsc{Data}_{\mathbb{A}} \to \textsc{Data}_{\mathbb{A}} \to \textsc{Data}_{\mathbb{A}} \end{array} \right)$$

where $\textsc{Data}_{\mathbb{A}}$is ranged over by $d, d_1, \cdots, d_n$ and the instance $\mathit{comp}(\mathbf{x}, d_1, d_2)$ is written $d_1 \circ_{\mathbf{x}} d_2$. The following properties must hold for a structural addressing algebra:

1. *Value containment*: Values are data, $\textsc{Values}_{\mathbb{A}} \subseteq \textsc{Data}_{\mathbb{A}}$
2. *Unaddressed values*: For all $v \in \textsc{Values}_{\mathbb{A}}$. $\mathit{addrs}(v) = \varnothing$

3. *Address properties*: For all $d_1, d_2 \in \textsc{Data}_{\mathbb{A}}$, $\mathbf{x} \in \textsc{SAdd}$, if $d_1 \circ_{\mathbf{x}} d_2$ is defined then:
   (a) *Containment*: $\mathbf{x} \in \mathit{addrs}(d_1)$
   (b) *Non-overlap*: $\mathit{addrs}(d_1) \cap \mathit{addrs}(d_2) \subseteq \{\mathbf{x}\}$
   (c) *Preservation*: $(\mathit{addrs}(d_1) \setminus \{\mathbf{x}\}) \cup \mathit{addrs}(d_2) = \mathit{addrs}(d_1 \circ_{\mathbf{x}} d_2)$
4. *Identity*: For all $d \in \textsc{Data}_{\mathbb{A}}$ and $\mathbf{x} \in \textsc{SAdd}$, $\mathbf{x} \circ_{\mathbf{x}} d = d$.
5. *Arbitrary addresses*: For all $d_1, d_2 \in \textsc{Data}_{\mathbb{A}}$ and $\mathbf{x}, \mathbf{y} \in \textsc{SAdd}$, if $\mathbf{x} \in \mathit{addrs}(d_1)$ and either $\mathbf{y} \notin \mathit{addrs}(d_1)$ or $\mathbf{y} = \mathbf{x}$, then $d_1 \circ_{\mathbf{x}} \mathbf{y}$ is defined. Also, $d_1 \circ_{\mathbf{x}} \mathbf{x} = d_1$.
6. *Compression left-cancellativity*: For all $d_1, d_2, d_3 \in \textsc{Data}_{\mathbb{A}}$ and $\mathbf{x} \in \textsc{SAdd}$, if $d_1 \circ_{\mathbf{x}} d_2 = d_1 \circ_{\mathbf{x}} d_3$, then $d_2 = d_3$.
7. *Compression quasi-associativity*: For all $d_1, d_2, d_3 \in \textsc{Data}_{\mathbb{A}}$ and $\mathbf{x}, \mathbf{y} \in \textsc{SAdd}$ where $\mathbf{y} \in \mathit{addrs}(d_2)$ and either $\mathbf{y} \notin \mathit{addrs}(d_1)$ or $\mathbf{x} = \mathbf{y}$, $(d_1 \circ_{\mathbf{x}} d_2) \circ_{\mathbf{y}} d_3 = d_1 \circ_{\mathbf{x}} (d_2 \circ_{\mathbf{y}} d_3)$.
8. *Compression quasi-commutativity*: For all $d_1, d_2, d_3 \in \textsc{Data}_{\mathbb{A}}$ and $\mathbf{x}, \mathbf{y} \in \textsc{SAdd}$ where $\mathbf{x} \notin \mathit{addrs}(d_3)$ and $\mathbf{y} \notin \mathit{addrs}(d_2)$, $(d_1 \circ_{\mathbf{x}} d_2) \circ_{\mathbf{y}} d_3 = (d_1 \circ_{\mathbf{y}} d_3) \circ_{\mathbf{x}} d_2$.

where undefined terms are considered equal.

Abstract data is stored in *abstract heaps*, which are similar to standard heaps. Given an abstract library $\mathbb{A}$, an abstract heap is a mapping from addresses to abstract data. When a heap cell is addressed with an abstract address, we call it an *abstract heap cell*.

Definition 4 (Abstract Heaps)**.** Given an abstract library $\mathbb{A}$, its associated set of addresses $\textsc{Add}_{\mathbb{A}}$ and abstract data $\textsc{Data}_{\mathbb{A}}$, the set of *abstract heaps* $\mathcal{H}_{\mathbb{A}}$, ranged over by $h, h_1, \cdots, h_n$, are functions of the type:

$$h : \textsc{Add}_{\mathbb{A}} \xrightarrow{\text{fin}} \textsc{Data}_{\mathbb{A}}$$

subject to the following restrictions:

$$\forall a_1, a_2 \in \textsc{Add}_{\mathbb{A}}.\ a_1 = a_2 \vee \mathit{addrs}(h(a_1)) \cap \mathit{addrs}(h(a_2)) = \varnothing$$
$$\nexists\, \mathbf{x} \in \textsc{SAdd}.\ \mathbf{x}\ D_h^+\ \mathbf{x}$$
$$\forall \mathbf{x} \in \mathrm{dom}(h) \cap \textsc{SAdd}.\ \exists \mathcal{R} \in \textsc{MAdd}_{\mathbb{A}}.\ \mathcal{R}\ D_h^+\ \mathbf{x}$$

where the descendent relation D for heap h is defined as $a\ D_h\ \mathbf{y} \iff \mathbf{y} \in \mathit{addrs}(h(a))$ and D_h^+ is its transitive closure.

By design, abstract heaps are similar to standard heaps and the construction of a separation algebra over them is thus straightforward.

Definition 5 (Abstract Heap Separation Algebra)**.** The *separation algebra of abstract heaps* for an abstract library $\mathbb{A}$ is defined as $(\mathcal{H}_\mathbb{A}, \bullet_\mathbb{A}, \mathbf{0}_\mathbb{A})$, where $\bullet_\mathbb{A}$ is disjoint function union if the result is a consistent abstract heap, and undefined in all other cases; $\mathbf{0}_\mathbb{A}$ is a partial function with an empty domain and co-domain.

To use our libraries in a standard programming language, we pair the abstract heaps with the standard *variables as resource* model [2].

Definition 6 (Abstract Machine Separation Algebra)**.** The *separation algebra of abstract machines* $\mathcal{SA}_\mathbb{A} \triangleq (\Sigma \times \mathcal{H}_\mathbb{A}, (\bullet_\sigma, \bullet_\mathbb{A}), (\mathbf{0}_\sigma, \mathbf{0}_\mathbb{A}))$, is defined as the Cartesian product of the separation algebra of variables $(\Sigma, \bullet_\sigma, \mathbf{0}_\sigma)$ and the algebra of abstract heaps (definition 5).

In order to reason about our programs, we use the program logic of the *Views* framework as described in [1]. We instantiate the framework with the separation algebra of abstract machines (def. 6) as the view monoid and the tree library commands (def. 1) as the atomic commands. We describe the axioms associated with the tree library commands in definition 7.

For an abstract library $\mathbb{A}$, our views are sets of abstract machine states in $\wp(\Sigma \times \mathcal{H}_\mathbb{A})$. We define the *set of complete abstract data* as the set of abstract data with no abstract body addresses: $\textsc{CompData}_\mathbb{A} = \{d \in \mathcal{H}_\mathbb{A} \mid \mathit{addrs}(d) = \varnothing\}$.

Definition 7 (Axioms)**.** Given an abstract library $\mathbb{A}$, the axiomatisation of atomic commands is denoted $\textsc{Axiom}_\mathbb{A} : \textsc{Atom}_\mathbb{A} \to (\Sigma \times \mathcal{H}_\mathbb{A}) \times (\Sigma \times \mathcal{H}_\mathbb{A})$.

The operational semantics of the views framework is described by a labelled transition system. Transitions are between states, and are labelled by atomic commands or *id* where *id* labels computation steps in which the state is not changed. We extend the *id* transitions of the views framework with two additional relations corresponding to abstract allocation and deallocation (definition 8). In other words, abstract allocation and deallocation do not change the underlying program states and can be seen as *id* transitions.

Definition 8 (Abstract Allocation)**.** Given an abstract library $\mathbb{A}$, for all $\mathbf{x} \in \textsc{SAdd}$, $a \in \textsc{Add}_\mathbb{A}$ and $d_1, d_2 \in \textsc{Data}_\mathbb{A}$, the *abstract allocation and deallocation relations* are defined as follows where $\{p\}\ id\ \{q\}$ denotes $(p, q) \in id$.

$$\{a \to d_1 \circ_\mathbf{x} d_2\} \quad id \quad \{\exists \mathbf{y} \in \textsc{SAdd}.\, a \to d_1 \circ_\mathbf{x} \mathbf{y} * \mathbf{y} \to d_2\}$$
$$\{\exists \mathbf{y} \in \textsc{SAdd}.\, a \to d_1 \circ_\mathbf{x} \mathbf{y} * \mathbf{y} \to d_2\} \quad id \quad \{a \to d_1 \circ_\mathbf{x} d_2\}$$

The existential quantification of the abstract address $\mathbf{y}$ is analogous to the existential quantification used for heap allocation in separation logic.

We have now defined all the ingredients necessary for building an abstract library.

Definition 9 (Abstract Library)**.** Given a set of abstract heaps $\mathcal{H}_{\mathbb{A}}$ (def. 4), the set of associated atomic commands $\textsc{Atom}_{\mathbb{A}}$ (def. 1) and their axiomatisation $\textsc{Axiom}_{\mathbb{A}}$ (def. 7), the *abstract library* $\mathbb{A}$ is defined as:

$$\mathbb{A} \triangleq (\mathcal{H}_{\mathbb{A}}, \textsc{Atom}_{\mathbb{A}}, \textsc{Axiom}_{\mathbb{A}})$$

2. Module Translation

Definition 10 (Stable Interfaces)**.** Given the set of inner interfaces $\textsc{In}_\tau$ and the set of outer interfaces $\textsc{Out}_\tau$ associated with a translation, the *set of inner interface functions* $\mathcal{I}_\tau^{\mathsf{in}} : \wp(\textsc{SAdd} \rightharpoonup \textsc{In}_\tau)$, and the *set of outer interface functions* $\mathcal{I}_\tau^{\mathsf{out}} : \wp(\textsc{SAdd} \rightharpoonup \textsc{Out}_\tau)$, consist of interface functions mapping abstract addresses to their inner and outer interfaces, respectively. The Cartesian product of the two, constitutes the *set of interface function pairs* $\mathcal{I}_\tau = \mathcal{I}_\tau^{\mathsf{in}} \times \mathcal{I}_\tau^{\mathsf{out}}$. Given an interface function $I \in \mathcal{I}_\tau$, we write I^{in} and I^{out} for the first and the second projections, respectively.

Similarly, the *set of stable inner-interface functions* ${\mathcal{SI}_\tau}^{\mathsf{in}} : \wp(\textsc{SAdd} \rightharpoonup \wp(\textsc{In}_\tau))$, and the *set of stable outer-interface functions* ${\mathcal{SI}_\tau}^{\mathsf{out}} : \wp(\textsc{SAdd} \rightharpoonup \wp(\textsc{Out}_\tau))$ consist of interface functions mapping abstract addresses to a set of possible inner and outer interfaces, respectively. The Cartesian product of the two forms the *set of stable interface function pairs* $\mathcal{SI}_\tau \triangleq {\mathcal{SI}_\tau}^{\mathsf{in}} \times {\mathcal{SI}_\tau}^{\mathsf{out}}$. We follow the above convention and given a stable interface function pair SI, we write SI^{in} and SI^{out} for the first and second projections. The *set of inner interfaces* $\textsc{In}_\tau$

Definition 11 (Heap Translation Function)**.** Given an abstract library $\mathbb{A} \triangleq (\wp(\Sigma \times \mathcal{H}_\mathbb{A}), \textsc{Atom}_\mathbb{A}, \textsc{Axiom}_\mathbb{A})$, a concrete library $\mathbb{B} \triangleq (\wp(\Sigma \times \mathcal{M}_\mathbb{B}), \textsc{Atom}_\mathbb{B}, \textsc{Axiom}_\mathbb{B})$ where $(\mathcal{M}_\mathbb{B}, \bullet_\mathbb{B}, \mathbf{0}_\mathbb{B})$ denotes the separation algebra of the concrete module, an *abstract heap translation function*

$$\langle . \rangle^{(\cdot)} : \mathcal{H}_\mathbb{A} \to \mathcal{I}_\tau \to \wp(\mathcal{M}_\mathbb{B})$$

provides a transformation from heaps of library $\mathbb{A}$ into states of library $\mathbb{B}$.

Definition 12 (Implementation Function)**.** An implementation function

$$[\![.]\!]_\tau : \textsc{Atom}_\mathbb{A} \to \textsc{Prog}_\mathbb{B}$$

provides an implementation for each atomic command of the abstract module $\textsc{Atom}_\mathbb{A}$ in the language of the concrete module $\textsc{Prog}_\mathbb{B}$ as a correspondingly named procedure. The translation of high-level programs written in $\textsc{Prog}_\mathbb{A}$ is then achieved by replacing each atomic command of library $\mathbb{A}$ with a call to the associated procedure while other constructs of the program remain unchanged.

Definition 13 (Library Translation)**.** Given an abstract library

$$\mathbb{A} \triangleq (\wp(\Sigma \times \mathcal{H}_{\mathbb{A}}), \textsc{Atom}_{\mathbb{A}}, \textsc{Axiom}_{\mathbb{A}})$$

and a concrete library

$$\mathbb{B} \triangleq (\wp(\Sigma \times \mathcal{M}_{\mathbb{B}}), \textsc{Atom}_{\mathbb{B}}, \textsc{Axiom}_{\mathbb{B}})$$

a *library translation* $\tau : \mathbb{A} \to \mathbb{B}$ from abstract library $\mathbb{A}$ to concrete library $\mathbb{B}$, is a 4-tuple of the set of interfaces, the set of stable interface function pairs, the heap translation function and the implementation function $\left(\left(\mathcal{I}_\tau^{\mathsf{in}} \times \mathcal{I}_\tau^{\mathsf{out}}\right), \mathcal{SI}_\tau, \langle . \rangle^{(\cdot)}, [\![.]\!]_\tau\right)$. In the context of a library translation $\tau : \mathbb{A} \to \mathbb{B}$, we refer to $\mathbb{A}$ as the abstract or high-level library and $\mathbb{B}$ as the concrete or low-level library.

Definition 14 (Abstract Machine Translation Function)**.** Given a library translation $\tau : \mathbb{A} \to \mathbb{B} \triangleq \left(\left(\mathcal{I}_\tau^{\mathsf{in}} \times \mathcal{I}_\tau^{\mathsf{out}}\right), \mathcal{SI}_\tau, \langle . \rangle^{(\cdot)}, [\![.]\!]_\tau\right)$, the *abstract machine translation function*:

$$[\![.]\!]_{(\cdot)} : (\Sigma \times \mathcal{H}_{\mathbb{A}}) \to \mathcal{SI}_\tau \to (\Sigma \times \mathcal{M}_{\mathbb{B}})$$

is defined as:

$$[\![p]\!]_{SI} \triangleq \left\{ (\sigma, m) \;\middle|\; \begin{array}{l} (\sigma, h) \in p \;\wedge \\ m \in \bigcup\limits_{I \in SI\downarrow} \left\{ \langle h \rangle^{I \uplus I'} \;\middle|\; \mathrm{dom}(I'^{\mathsf{in}}) = h^{\mathsf{in}} \;\wedge\; \mathrm{dom}(I'^{\mathsf{out}}) = h^{\mathsf{out}} \right\} \end{array} \right\}$$

where

$$\begin{array}{ll} h^{\mathsf{in}} & \triangleq \{\mathbf{x} \mid \mathbf{x} \in (\textsc{Sadd} \cap \mathrm{dom}(h))\} \\ h^{\mathsf{out}} & \triangleq \{\mathbf{x} \mid \mathbf{x} \in (\textsc{Sadd} \cap \text{co-dom}(h))\} \\ SI\downarrow & \triangleq SI^{\mathsf{in}}\downarrow \times SI^{\mathsf{out}}\downarrow \\ SI^{\mathsf{in}}\downarrow & \triangleq \left\{ I \in \mathcal{I}_\tau^{\mathsf{in}} \;\middle|\; \begin{array}{l} \mathrm{dom}(I) = \mathrm{dom}(SI^{\mathsf{in}}) \wedge \\ \forall \mathbf{x} \in \mathrm{dom}(I).\; I(\mathbf{x}) \in SI^{\mathsf{in}}(\mathbf{x}) \end{array} \right\} \\ SI^{\mathsf{out}}\downarrow & \triangleq \left\{ I \in \mathcal{I}_\tau^{\mathsf{out}} \;\middle|\; \begin{array}{l} \mathrm{dom}(I) = \mathrm{dom}(SI^{\mathsf{out}}) \wedge \\ \forall \mathbf{x} \in \mathrm{dom}(I).\; I(\mathbf{x}) \in SI^{\mathsf{out}}(\mathbf{x}) \end{array} \right\} \end{array}$$

The composition of interface functions is given as:

$$I_1 \uplus I_2 = \left(I_1{}^{\mathsf{in}} \uplus I_2{}^{\mathsf{in}},\; I_1{}^{\mathsf{out}} \uplus I_2{}^{\mathsf{out}}\right)$$

$$\left(I_1{}^{\mathsf{in}} \uplus I_2{}^{\mathsf{in}}\right)(\mathbf{x}) \triangleq \begin{cases} I_1{}^{\mathsf{in}}(\mathbf{x}) & \text{if } \mathbf{x} \in \mathrm{dom}(I_1{}^{\mathsf{in}}) \;\wedge\; \mathbf{x} \notin \mathrm{dom}(I_2{}^{\mathsf{in}}) \\ I_2{}^{\mathsf{in}}(\mathbf{x}) & \text{if } \mathbf{x} \in \mathrm{dom}(I_2{}^{\mathsf{in}}) \;\wedge\; \mathbf{x} \notin \mathrm{dom}(I_1{}^{\mathsf{in}}) \\ \text{undefined} & \text{otherwise} \end{cases}$$

and the composition of outer interfaces is defined analogously.

Definition 15 (Translated Triple)**.** Given a library translation $\tau : \mathbb{A} \to \mathbb{B}$, $p, q \in (\Sigma \times \mathcal{H}_{\mathbb{A}})$ and $\mathbb{C} \in \textsc{Prog}_{\mathbb{A}}$, the *translated triple* is defined as:

$$\Omega \vDash_{\mathbb{A}} \tau.\{p\}\ \mathbb{C}\ \{q\} \triangleq \forall SI \in \mathcal{SI}_{\tau}.\ \ [\![\Omega]\!]_{\tau} \vDash_{\mathbb{B}} \{[\![p]\!]_{SI}\}\ [\![\mathbb{C}]\!]_{\tau}\ \{[\![q]\!]_{SI}\}$$

with $$[\![\Omega]\!]_{\tau} \triangleq \{\mathtt{f} : [\![p]\!]_{SI} \rightarrowtail [\![q]\!]_{SI} \mid (\mathtt{f} : p \rightarrowtail q) \in \Omega\ \wedge\ SI \in \mathcal{SI}_{\tau}\}$$

Definition 16 (Sound Library Translation)**.** A library translation $\tau : \mathbb{A} \to \mathbb{B}$ is a *sound library translation* if for all $\Omega \in \textsc{PEnv}$, $p, q \in (\Sigma \times \mathcal{H}_{\mathbb{A}})$ and $\mathbb{C} \in \textsc{Prog}_{\mathbb{A}}$,

$$\Omega \vDash_{\mathbb{A}} \{p\}\ \mathbb{C}\ \{q\} \implies \Omega \vDash_{\mathbb{A}} \tau.\ \{p\}\ \mathbb{C}\ \{q\}$$

Theorem 1 (Sound library translation)**.** A library translation $\tau : \mathbb{A} \to \mathbb{B}$ is sound if it has the following three properties.

Property 1 (Axiom Correctness)**.** For all $\Omega \in \textsc{PEnv}$, $p, q \in (\Sigma \times \mathcal{H}_{\mathbb{A}})$ and $\mathrm{C} \in \textsc{Atom}_{\mathbb{A}}$,

$$\Omega \vDash_{\mathbb{A}} \{p\}\ C\ \{q\} \implies \Omega \vDash_{\mathbb{A}} \tau.\{p\}\ C\ \{q\}$$

This property ensures that the translated library correctly implements the high-level atomic commands and satisfies the same specification.

Property 2 (Monotonicity of *id* Relation)**.** For all $h_1, h_2 \in \mathcal{H}_{\mathbb{A}}$: and $I \in \mathcal{I}_{\tau}$:

$$\left\{\ \{h_1\}\ \right\}\ id\ \left\{\ \{h_2\}\ \right\} \implies \left\{\ \langle h_1 \rangle^I\ \right\}\ id\ \left\{\ \langle h_2 \rangle^I\ \right\}$$

Property 3 (Separation Preservation)**.** For all $h_1, h_2 \in \mathcal{H}_{\mathbb{A}}$ and $I, I' \in \mathcal{I}_{\tau}$

$$\langle h_1 \bullet_{\mathbb{A}} h_2 \rangle^I \equiv \exists I_1, I_2.\ I_1 \cup I_2 = I\ \wedge\ \langle h_1 \rangle^{I_1} \bullet_{\mathbb{B}} \langle h_2 \rangle^{I_2}$$

This property is necessary to establish the correctness of translated *concurrent* programs. At the abstract level two threads can operate on two disjoint (decomposable) states concurrently. We need to allow for similar behaviour at the implementation level and we achieve this by requiring that the translation of a state can be decomposed analogously.

Proof. The proof is by induction over the structure of the proof $\Omega \vDash_{\mathbb{A}} \{p\}\ \mathbb{C}\ \{q\}$. In each case we consider the last rule applied in the proof. We assume, as the inductive hypothesis, that the translated premises of each rule have proofs in $\mathbb{B}$. We show how to derive a proof of translated conclusions from these translated premises. Note that when translating abstract machines (definition 14), the variable store remains unchanged and is not affected by the translation function. Hence, in the proofs below the

$\mathsf{vsafe}\,(e)\,, \mathsf{vtrue}\,(e)\,, \mathsf{vfalse}\,(e)$ predicates are also unaffected under the translation. We make use of this in several of the proof cases.

Axiom case:
This follows immediately from property 1.

Sequencing case:

$$\dfrac{\dfrac{\dfrac{\dfrac{\Omega \vDash_{\mathbb{A}} \tau.\ \{p\}\mathbb{C}_1\{q\} \quad \Omega \vDash_{\mathbb{A}} \tau.\ \{q\}\mathbb{C}_2\{r\}}{\begin{array}{c}\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p]\!]_{SI}\}\ [\![\mathbb{C}_1]\!]_\tau\ \{[\![q]\!]_{SI}\} \\ \forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![q]\!]_{SI}\}\ [\![\mathbb{C}_2]\!]_\tau\ \{[\![r]\!]_{SI}\}\end{array}}\ \text{Def.}}{\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p]\!]_{SI}\}\ [\![\mathbb{C}_1]\!]_\tau ; [\![\mathbb{C}_2]\!]_\tau\ \{[\![r]\!]_{SI}\}}\ \textsc{Sequencing}}{\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p]\!]_{SI}\}\ [\![\mathbb{C}_1;\mathbb{C}_2]\!]_\tau\ \{[\![r]\!]_{SI}\}}\ \text{Def.}}{\Omega \vDash_{\mathbb{A}} \tau.\ \{p\}\mathbb{C}_1;\mathbb{C}_2\{r\}}$$

If case:

$$\dfrac{\dfrac{\dfrac{\dfrac{\begin{array}{c}\Omega \vDash_{\mathbb{A}} \tau.\ \{p \wedge \mathsf{vtrue}\,(e)\}\ \mathbb{C}_1\ \{q\} \\ \Omega \vDash_{\mathbb{A}} \tau.\ \{p \wedge \mathsf{vfalse}\,(e)\}\ \mathbb{C}_2\ \{q\}\end{array}}{\begin{array}{c}\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p \wedge \mathsf{vtrue}\,(e)]\!]_{SI}\}\ [\![\mathbb{C}_1]\!]_\tau\ \{[\![q]\!]_{SI}\} \\ \forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p \wedge \mathsf{vfalse}\,(e)]\!]_{SI}\}\ [\![\mathbb{C}_2]\!]_\tau\ \{[\![q]\!]_{SI}\}\end{array}}\ \text{Def.}}{\begin{array}{c}\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p]\!]_{SI} \wedge \mathsf{vtrue}\,(e)\}\ [\![\mathbb{C}_1]\!]_\tau\ \{[\![q]\!]_{SI}\} \\ \forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p]\!]_{SI} \wedge \mathsf{vfalse}\,(e)\}\ [\![\mathbb{C}_2]\!]_\tau\ \{[\![q]\!]_{SI}\}\end{array}} \qquad \dfrac{p \subseteq \mathsf{vsafe}\,(e)}{[\![p]\!]_{SI} \subseteq \mathsf{vsafe}\,(e)}}{\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p]\!]_{SI}\}\ \texttt{if}\ e\ \texttt{then}\ [\![\mathbb{C}_1]\!]_\tau\ \texttt{else}\ [\![\mathbb{C}_2]\!]_\tau\ \{[\![q]\!]_{SI}\}}\ \textsc{If}}{\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p]\!]_{SI}\}\ [\![\texttt{if}\ e\ \texttt{then}\ \mathbb{C}_1\ \texttt{else}\ \mathbb{C}_2]\!]_\tau\ \{[\![q]\!]_{SI}\}}\ \text{Def.}}{\Omega \vDash_{\mathbb{A}} \tau.\ \{p\}\ \texttt{if}\ e\ \texttt{then}\ \mathbb{C}_1\ \texttt{else}\ \mathbb{C}_2\ \{q\}}$$

While case:

$$\dfrac{\dfrac{\dfrac{\dfrac{\Omega \vDash_{\mathbb{A}} \tau.\ \{p \wedge \mathsf{vtrue}\,(e)\}\,\mathbb{C}\,\{p\}}{\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p \wedge \mathsf{vtrue}\,(e)]\!]_{SI}\}\ [\![\mathbb{C}]\!]_\tau\ \{[\![p]\!]_{SI}\}}\ \text{Def.}}{\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p]\!]_{SI} \wedge \mathsf{vtrue}\,(e)\}\ [\![\mathbb{C}]\!]_\tau\ \{[\![p]\!]_{SI}\}} \qquad \dfrac{p \subseteq \mathsf{vsafe}\,(e)}{[\![p]\!]_{SI} \subseteq \mathsf{vsafe}\,(e)}}{\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p]\!]_{SI}\}\ \texttt{while}\ e\ \texttt{do}\ [\![\mathbb{C}]\!]_\tau\ \{[\![q \wedge \mathsf{vfalse}\,(e)]\!]_{SI}\}}\ \textsc{While}}{\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p]\!]_{SI}\}\ [\![\texttt{while}\ e\ \texttt{do}\ \mathbb{C}]\!]_\tau\ \{[\![q \wedge \mathsf{vfalse}\,(e)]\!]_{SI}\}}\ \text{Def.}}{\Omega \vDash_{\mathbb{A}} \tau.\ \{p\}\ \texttt{while}\ e\ \texttt{do}\ \mathbb{C}\ \{q \wedge \mathsf{vfalse}\,(e)\}}$$

PARALLEL case:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Omega \vDash_{\mathbb{A}} \tau.\ \{p_1\}\ \mathbb{C}_1\ \{q_1\} \quad \Omega \vDash_{\mathbb{A}} \tau.\ \{p_2\}\ \mathbb{C}_2\ \{q_2\}}{\begin{array}{c}\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p_1]\!]_{SI}\}\ [\![\mathbb{C}_1]\!]_\tau\ \{[\![q_1]\!]_{SI}\} \\ \forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p_2]\!]_{SI}\}\ [\![\mathbb{C}_2]\!]_\tau\ \{[\![q_2]\!]_{SI}\}\end{array}}\ \text{Def.}}{\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p_1]\!]_{SI} * [\![p_2]\!]_{SI}\}\ [\![\mathbb{C}_1]\!]_\tau \parallel [\![\mathbb{C}_2]\!]_\tau\ \{[\![q_1]\!]_{SI} * [\![q_2]\!]_{SI}\}}\ \textsc{Parallel}}{\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p_1 * p_2]\!]_{SI}\}\ [\![\mathbb{C}_1 \parallel \mathbb{C}_2]\!]_\tau\ \{[\![q_1 * q_2]\!]_{SI}\}}\ \textit{Lemma2}}{\Omega \vDash_{\mathbb{A}} \tau.\ \{p_1 * p_2\}\ \mathbb{C}_1 \parallel \mathbb{C}_2\ \{q_1 * q_2\}}\ \text{Def.}$$

FRAME case:

$$\dfrac{\dfrac{\dfrac{\dfrac{\Omega \vDash_{\mathbb{A}} \tau.\ \{p\}\ \mathbb{C}\ \{q\}}{\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p]\!]_{SI}\}\ [\![\mathbb{C}]\!]_\tau\ \{[\![q]\!]_{SI}\}}\ \textsc{Frame}}{\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p]\!]_{SI} * [\![r]\!]_{SI}\}\ [\![\mathbb{C}]\!]_\tau\ \{[\![q]\!]_{SI} * [\![r]\!]_{SI}\}}\ \textit{Lemma2}}{\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p * r]\!]_{SI}\}\ [\![\mathbb{C}]\!]_\tau\ \{[\![q * r]\!]_{SI}\}}\ \text{Def.}}{\Omega \vDash_{\mathbb{A}} \tau.\ \{p * r\}\ \mathbb{C}\ \{q * r\}}$$

DISJUNCTION case:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Omega \vDash_{\mathbb{A}} \tau.\ \{p_1\}\ \mathbb{C}\ \{q_1\} \quad \Omega \vDash_{\mathbb{A}} \tau.\ \{p_2\}\ \mathbb{C}\ \{q_2\}}{\begin{array}{c}\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p_1]\!]_{SI}\}\ [\![\mathbb{C}]\!]_\tau\ \{[\![q_1]\!]_{SI}\} \\ \forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p_2]\!]_{SI}\}\ [\![\mathbb{C}]\!]_\tau\ \{[\![q_2]\!]_{SI}\}\end{array}}\ \text{Def.}}{\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p_1]\!]_{SI} \vee [\![p_2]\!]_{SI}\}\ [\![\mathbb{C}]\!]_\tau\ \{[\![q_1]\!]_{SI} \vee [\![q_2]\!]_{SI}\}}\ \textsc{Disjunction}}{\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p_1 \vee p_2]\!]_{SI}\}\ [\![\mathbb{C}]\!]_\tau\ \{[\![q_1 \vee q_2]\!]_{SI}\}}\ \text{Def.}}{\Omega \vDash_{\mathbb{A}} \tau.\ \{p_1 \vee p_2\}\ \mathbb{C}\ \{q_1 \vee q_2\}}$$

CONSEQUENCE case:

$$\dfrac{\dfrac{\dfrac{(p, p') \in id}{\forall SI \in \mathcal{SI}_\tau.\ ([\![p]\!]_{SI}, [\![p']\!]_{SI}) \in id}\ \mathbf{P}2 \quad (\star) \quad \dfrac{(q', q) \in id}{\forall SI \in \mathcal{SI}_\tau.\ ([\![q']\!]_{SI}, [\![q]\!]_{SI}) \in id}\ \mathbf{P}2}{\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p]\!]_{SI}\}\ [\![\mathbb{C}]\!]_\tau\ \{[\![q]\!]_{SI}\}}\ \text{Def.}}{\Omega \vDash_{\mathbb{A}} \tau.\ \{p\}\mathbb{C}\ \{q\}}\ \textsc{Consequence}$$

$$(\star) = \dfrac{\Omega \vDash_{\mathbb{A}} \tau.\ \{p'\}\ \mathbb{C}\ \{q'\}}{\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p']\!]_{SI}\}\ [\![\mathbb{C}]\!]_\tau\ \{[\![q']\!]_{SI}\}}\ \text{Def.}$$

where $\mathbf{P}2$ denotes Property 2.

Existential case:

$$\dfrac{\dfrac{\dfrac{\dfrac{\Omega \vDash_{\mathbb{A}} \tau.\ \{p\}\ \mathbb{C}\ \{q\}}{\forall SI \in \mathcal{SI}_\tau.\ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p]\!]_{SI}\}\ [\![\mathbb{C}]\!]_\tau\ \{[\![q]\!]_{SI}\}}\ \text{Def.}}{\forall SI \in \mathcal{SI}_\tau.\ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{\exists X.\, [\![p]\!]_{SI}\}\ [\![\mathbb{C}]\!]_\tau\ \{\exists X.\, [\![q]\!]_{SI}\}}\ \textsc{Existential}}{\forall SI \in \mathcal{SI}_\tau.\ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![\exists X.\, p]\!]_{SI}\}\ [\![\mathbb{C}]\!]_\tau\ \{[\![\exists X.\, q]\!]_{SI}\}}\ \text{Def.}}{\Omega \vDash_{\mathbb{A}} \tau.\ \{\exists X.\, p\}\ \mathbb{C}\ \{\exists X.\, q\}}\ \text{Def.}$$

Assign case:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{(s, \mathbf{0}_{\mathbb{A}}) \subseteq \mathsf{vsafe}\,(e)}{(s, \mathbf{0}_{\mathbb{B}}) \subseteq \mathsf{vsafe}\,(e)}}{\forall SI \in \mathcal{SI}_\tau.\ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \quad \left\{\ (s, \mathbf{0}_{\mathbb{B}}) \;\middle|\; (s, \mathbf{0}_{\mathbb{A}}) \in \{(\mathsf{var}\,(\mathtt{x}, v) * \sigma) \times \mathbf{0}_{\mathbb{A}}\}\ \right\}}\ \textsc{Assign}}{\mathtt{x} := e}}{\left\{\ (s, \mathbf{0}_{\mathbb{B}}) \;\middle|\; (s, \mathbf{0}_{\mathbb{A}}) \in \{\left(\mathsf{var}\left(\mathtt{x}, \mathcal{E}\,(e)^{\mathsf{var}(\mathtt{x}, v) * \sigma}\right) * \sigma\right) \times \mathbf{0}_{\mathbb{A}}\}\ \right\}}}{\forall SI \in \mathcal{SI}_\tau.\ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \quad \left\{\ (s, m) \;\middle|\; \begin{array}{l} (s, \mathbf{0}_{\mathbb{A}}) \in \{(\mathsf{var}\,(\mathtt{x}, v) * \sigma) \times \mathbf{0}_{\mathbb{A}}\} \wedge \\ m \in \left(\bigvee\limits_{I \in SI\downarrow} \left(\langle \mathbf{0}_{\mathbb{A}} \rangle^I\right)\right) \end{array}\ \right\}}\ \textit{Lemma1}$$

$$\dfrac{\dfrac{\mathtt{x} := e}{\left\{\ (s, m) \;\middle|\; \begin{array}{l} (s, \mathbf{0}_{\mathbb{A}}) \in \{\left(\mathsf{var}\left(\mathtt{x}, \mathcal{E}\,(e)^{\mathsf{var}(\mathtt{x}, v) * \sigma}\right) * \sigma\right) \times \mathbf{0}_{\mathbb{A}}\} \wedge \\ m \in \left(\bigvee\limits_{I \in SI\downarrow} \left(\langle \mathbf{0}_{\mathbb{A}} \rangle^I\right)\right) \end{array}\ \right\}}}{\forall SI \in \mathcal{SI}_\tau.\ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \quad \begin{array}{c} \{[\![(\mathsf{var}\,(\mathtt{x}, v) * \sigma) \times \mathbf{0}_{\mathbb{A}}]\!]_{SI}\} \\ [\![\mathtt{x} := e]\!]_\tau \\ \left\{[\![\left(\mathsf{var}\left(\mathtt{x}, \mathcal{E}\,(e)^{\mathsf{var}(\mathtt{x}, v) * \sigma}\right) * \sigma\right) \times \mathbf{0}_{\mathbb{A}}]\!]_{SI}\right\} \end{array}}\ \text{Def.}$$

$$\Omega \vDash_{\mathbb{A}} \tau.\ \{(\mathsf{var}\,(\mathtt{x}, v) * \sigma) \times \mathbf{0}_{\mathbb{A}}\}\ \mathtt{x} := e\ \left\{\left(\mathsf{var}\left(\mathtt{x}, \mathcal{E}\,(e)^{\mathsf{var}(\mathtt{x}, v) * \sigma}\right) * \sigma\right) \times \mathbf{0}_{\mathbb{A}}\right\}$$

LOCAL case:

$$\dfrac{\dfrac{\dfrac{\Omega \vDash_{\mathbb{A}} \tau.\ \{p * \{\{\mathtt{x} \to -\} \times \mathbf{1}_{\mathbb{A}}\}\}\ \mathbb{C}\ \{q * \{\{\mathtt{x} \to -\} \times \mathbf{1}_{\mathbb{A}}\}\}}{\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \begin{array}{c}\{[\![p * \{\{\mathtt{x} \to -\} \times \mathbf{1}_{\mathbb{A}}\}]\!]_{SI}\} \\ [\![\mathbb{C}]\!]_\tau \\ \{[\![q * \{\{\mathtt{x} \to -\} \times \mathbf{1}_{\mathbb{A}}\}]\!]_{SI}\}\end{array}}\ \text{Def.}}{\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \begin{array}{c}\{[\![p]\!]_{SI} * \{\{\mathtt{x} \to -\} \times \mathbf{1}_{\mathbb{B}}\}\} \\ [\![\mathbb{C}]\!]_\tau \\ \{[\![q]\!]_{SI} * \{\{\mathtt{x} \to -\} \times \mathbf{1}_{\mathbb{B}}\}\}\end{array}}\ (\star)}{\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p]\!]_{SI}\}\ \mathtt{local\ x\ in}\ [\![\mathbb{C}]\!]_\tau\ \{[\![q]\!]_{SI}\}}\ \textsc{Local}}{\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega]\!]_\tau\, \tau \vDash_{\mathbb{B}} \{[\![p]\!]_{SI}\}\ [\![\mathtt{local\ x\ in}\ \mathbb{C}]\!]_\tau\ \{[\![q]\!]_{SI}\}}\ \text{Def.}}{\Omega \vDash_{\mathbb{A}} \tau.\ \{p\}\ \mathtt{local\ x\ in}\ \mathbb{C}\ \{q\}}\ \text{Def.}$$

$$(\star) = \dfrac{p \cap \mathsf{vsafe}\,(\mathtt{x}) = \varnothing}{[\![p]\!]_{SI} \cap \mathsf{vsafe}\,(\mathtt{x}) = \varnothing}$$

CALL case:

$$\dfrac{\dfrac{\dfrac{r' \subseteq \mathsf{vsafe}\,(\vec{e})}{\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega; \mathtt{f} : p \rightarrowtail q]\!]_\tau\, \tau \vDash_{\mathbb{B}} \begin{array}{c}\left\{[\![p\left(\mathcal{E}\,(e)^{r'}\right)]\!]_{SI} * r'\right\} \\ [\![\mathtt{call}\ \vec{\mathtt{r}} := \mathtt{f}(\vec{e})]\!]_\tau \\ \{[\![\exists \vec{w}.\ q\,(\vec{w})]\!]_{SI} * s'\}\end{array}}\ \textsc{Call}}{\forall SI \in \mathcal{SI}_\tau.\ \ [\![\Omega; \mathtt{f} : p \rightarrowtail q]\!]_\tau\, \tau \vDash_{\mathbb{B}} \begin{array}{c}\{[\![p\,(\mathcal{E}\,(e)^{r}) * r]\!]_{SI}\} \\ [\![\mathtt{call}\ \vec{\mathtt{r}} := \mathtt{f}(\vec{e})]\!]_\tau \\ \{[\![q\,(\vec{w}) * s]\!]_{SI}\}\end{array}}\ \text{Def.}}{\Omega; \mathtt{f} : p \rightarrowtail q\ \ \vDash_{\mathbb{A}} \tau.\ \ \{p\,(\mathcal{E}\,(e)^{r}) * r\}\ \mathtt{call}\ \vec{\mathtt{r}} := \mathtt{f}(\vec{e})\ \{q\,(\vec{w}) * s\}}\ \text{Def.}$$

where

$$r = \{\{\vec{\mathtt{r}} \to \vec{v} \bullet_\sigma \sigma\} \times \mathbf{1}_{\mathbb{A}}\}$$
$$s = \{\{\vec{\mathtt{r}} \to \vec{w} \bullet_\sigma \sigma\} \times \mathbf{1}_{\mathbb{A}}\}$$

$$r' = \{\{\vec{\mathtt{r}} \to \vec{v} \bullet_\sigma \sigma\} \times \mathbf{1}_{\mathbb{B}}\}$$
$$s' = \{\{\vec{\mathtt{r}} \to \vec{w} \bullet_\sigma \sigma\} \times \mathbf{1}_{\mathbb{B}}\}$$

□

Lemma 1 (Corollary of Property 3)**.**

$$\forall I \in \mathcal{I}_\tau.\ \ \langle \mathbf{0}_{\mathbb{A}} \rangle^I = \mathbf{0}_{\mathbb{B}}$$

Proof. Pick an arbitrary $I \in \mathcal{I}_\tau$ and let $h \in \mathcal{H}_\mathbb{A}$ be an arbitrary heap. Then we have:

$$\begin{aligned} \langle h \bullet_\mathbb{A} \mathbf{0}_\mathbb{A} \rangle^I &= \langle h \rangle^I && \text{(By properties of } \mathbf{0}_\mathbb{A}\text{)} \\ &= \langle h \rangle^I \bullet_\mathbb{B} \mathbf{0}_\mathbb{B} && \text{(By properties of } \mathbf{0}_\mathbb{B}\text{)} \quad (1) \end{aligned}$$

On the other hand,

$$\langle h \bullet_\mathbb{A} \mathbf{0}_\mathbb{A} \rangle^I = \langle h \rangle^I \bullet_\mathbb{B} \langle \mathbf{0}_\mathbb{A} \rangle^I \quad \text{(By Property 3)} \quad (2)$$

From (1), (2) and the cancellation property of separation algebras, we can deduce:

$$\langle \mathbf{0}_\mathbb{A} \rangle^I = \mathbf{0}_\mathbb{B}$$

as required. □

Lemma 2 (Separation Preservation)**.** Given a module translation $\tau : \mathbb{A} \to \mathbb{B}$, the composition * is preserved by the abstract machine translation function (def. 14). That is, for all $p, q \in \mathcal{V}_\mathbb{A}$ and $SI \in \mathcal{SI}_\tau$

$$[\![p * q]\!]_{SI} = [\![p]\!]_{SI} * [\![q]\!]_{SI}$$

Proof. Take arbitrary $p, q \in \wp(\Sigma \times \mathcal{H}_{\mathbb{A}})$ and $SI \in \mathcal{SI}_{\tau}$, then:

$$
\begin{aligned}
[\![p]\!]_{SI} * [\![q]\!]_{SI} &= \left\{ (\sigma_1 \bullet_{\sigma} \sigma_2, m^1_{\mathbb{B}} \bullet_{\mathbb{B}} m^2_{\mathbb{B}}) \;\middle|\; \begin{array}{l} (\sigma_1, h^1_{\mathbb{A}}) \in p \;\wedge\; (\sigma_2, h^2_{\mathbb{A}}) \in q \\ \mathrm{dom}({I_1}^{\mathsf{in}}) = {h^1_{\mathbb{A}}}^{\mathsf{in}} \\ \mathrm{dom}({I_1}^{\mathsf{out}}) = {h^1_{\mathbb{A}}}^{\mathsf{out}} \\ m^1_{\mathbb{B}} \in \bigcup\limits_{I \in SI_{\downarrow}} \left(\left\langle h^1_{\mathbb{A}} \right\rangle^{I \uplus I_1} \right) \\ \mathrm{dom}({I_2}^{\mathsf{in}}) = {h^2_{\mathbb{A}}}^{\mathsf{in}} \\ \mathrm{dom}({I_2}^{\mathsf{out}}) = {h^2_{\mathbb{A}}}^{\mathsf{out}} \\ m^2_{\mathbb{B}} \in \bigcup\limits_{I \in SI_{\downarrow}} \left(\left\langle h^2_{\mathbb{A}} \right\rangle^{I \uplus I_2} \right) \end{array} \right\} \\
&= \left\{ (\sigma_1 \bullet_{\sigma} \sigma_2, m_{\mathbb{B}}) \;\middle|\; \begin{array}{l} (\sigma_1, h^1_{\mathbb{A}}) \in p \;\wedge\; (\sigma_2, h^2_{\mathbb{A}}) \in q \\ \mathrm{dom}({I_1}^{\mathsf{in}}) = {h^1_{\mathbb{A}}}^{\mathsf{in}} \\ \mathrm{dom}({I_1}^{\mathsf{out}}) = {h^1_{\mathbb{A}}}^{\mathsf{out}} \\ \mathrm{dom}({I_2}^{\mathsf{in}}) = {h^2_{\mathbb{A}}}^{\mathsf{in}} \\ \mathrm{dom}({I_2}^{\mathsf{out}}) = {h^2_{\mathbb{A}}}^{\mathsf{out}} \\ m_{\mathbb{B}} \in \bigcup\limits_{I \in SI_{\downarrow}} \left(\left\langle h^1_{\mathbb{A}} \right\rangle^{I \uplus I_1} \bullet_{\mathbb{B}} \left\langle h^2_{\mathbb{A}} \right\rangle^{I \uplus I_2} \right) \end{array} \right\} \\
\text{(By Property 3)} &= \left\{ (\sigma_1 \bullet_{\sigma} \sigma_2, m_{\mathbb{B}}) \;\middle|\; \begin{array}{l} (\sigma_1, h^1_{\mathbb{A}}) \in p \;\wedge\; (\sigma_2, h^2_{\mathbb{A}}) \in q \\ \mathrm{dom}({I_1}^{\mathsf{in}}) = {h^1_{\mathbb{A}}}^{\mathsf{in}} \\ \mathrm{dom}({I_1}^{\mathsf{out}}) = {h^1_{\mathbb{A}}}^{\mathsf{out}} \\ \mathrm{dom}({I_2}^{\mathsf{in}}) = {h^2_{\mathbb{A}}}^{\mathsf{in}} \\ \mathrm{dom}({I_2}^{\mathsf{out}}) = {h^2_{\mathbb{A}}}^{\mathsf{out}} \\ m_{\mathbb{B}} \in \bigcup\limits_{I \in SI_{\downarrow}} \left(\left\langle h^1_{\mathbb{A}} \bullet_{\mathbb{B}} h^2_{\mathbb{A}} \right\rangle^{I \uplus (I_1 \cup I_2)} \right) \end{array} \right\} \\
&= \left\{ (\sigma, m_{\mathbb{B}}) \;\middle|\; \begin{array}{l} (\sigma, h_{\mathbb{A}}) \in p * q \\ \mathrm{dom}({I'}^{\mathsf{in}}) = {h_{\mathbb{A}}}^{\mathsf{in}} \\ \mathrm{dom}({I'}^{\mathsf{out}}) = {h_{\mathbb{A}}}^{\mathsf{out}} \\ m_{\mathbb{B}} \in \bigcup\limits_{I \in SI_{\downarrow}} \left(\left\langle h_{\mathbb{A}} \right\rangle^{I \uplus I'} \right) \end{array} \right\} \\
&= [\![p * q]\!]_{SI}
\end{aligned}
$$

□

3. Tree Translation $\tau : \mathbb{T} \to \mathbb{C}$

Definition 17 (Tree heap translation function)**.** The tree heap representation function:

$$\langle (\cdot) \rangle^I : \mathcal{H}_{\mathbb{T}} \to \mathcal{I}_\tau \to \wp(\mathcal{M}_{\mathbb{C}})$$

is defined by induction over the structure of tree heaps as:

$$\begin{aligned}
\langle \mathbf{0}_{\mathbb{T}} \rangle^I &\triangleq \text{emp} \\
\langle \mathsf{tree}\,(\mathcal{R}, t) \rangle^I &\triangleq \mathsf{tree}\,(I, \mathcal{R}, t) \\
\langle \mathsf{tree}\,(\mathbf{x}, t) \rangle^I &\triangleq \mathsf{tree}\,(I, \mathbf{x}, t) \\
\langle h_1 \bullet_{\mathbb{T}} h_2 \rangle^I &\triangleq \exists I_1, I_2.\, I_1 \cup I_2 = I \ \wedge\ \langle h_1 \rangle^{I_1} \bullet_{\mathbb{C}} \langle h_2 \rangle^{I_2}
\end{aligned}$$

with

$$\begin{aligned}
\mathsf{tree}\,(I, \mathcal{R}, t) &\triangleq \exists i, j.\, \mathsf{treeFrag}\,(I, t)\,(i, j)\,(\mathsf{null}, \mathsf{null}, \mathsf{null}) \\
\mathsf{tree}\,(I, \mathbf{x}, t) &\triangleq \mathsf{treeFrag}\,(I, t)\,(i^x, j^x)\,(l^x, u^x, r^x)\ * \\
&\quad I^{\mathsf{in}}(\mathbf{x}) \doteq (i^x, j^x)\ *\ I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x) \\
\\
\mathsf{treeFrag}\,(I, \varnothing)\,(i, j)\,(l, u, r) &\triangleq (i \doteq r) * (j \doteq l) \\
\mathsf{treeFrag}\,(I, \mathbf{x})\,(i, j)\,(l, u, r) &\triangleq I^{\mathsf{in}}(\mathbf{x}) \doteq (i, j)\ *\ I^{\mathsf{out}}(\mathbf{x}) \doteq (l, u, r) \\
\mathsf{treeFrag}\,(I, t_1 \otimes t_2)\,(i, j)\,(l, u, r) &\triangleq \exists p, q.\ \mathsf{treeFrag}\,(I, t_1)\,(i, p)\,(l, u, q) \\
&\quad *\ \mathsf{treeFrag}\,(I, t_2)\,(q, j)\,(p, u, r) \\
\mathsf{treeFrag}\,(I, n[t])\,(i, j)\,(l, u, r) &\triangleq i \doteq j \doteq n * n.u \to u \\
&\quad * \mathsf{Left}\,(n, l, u) * \mathsf{First}\,(n, d) \\
&\quad * \mathsf{Last}\,(n, e) * \mathsf{Right}\,(n, r, u) \\
&\quad * \exists d, e.\, \mathsf{treeFrag}\,(I, t)\,(d, e)\,(\mathsf{null}, n, \mathsf{null})
\end{aligned}$$

For readability we use the the following shorthands in the definitions above:

$$
\begin{array}{rcll}
n.l & \triangleq & n & \text{//the left sibling} \\
n.u & \triangleq & n+1 & \text{//the parent of the node} \\
n.d & \triangleq & n+2 & \text{//the first child} \\
n.e & \triangleq & n+3 & \text{//the last child} \\
n.r & \triangleq & n+4 & \text{//the right sibling} \\
n.lL & \triangleq & n+5 & \text{//the left sibling lock} \\
n.dL & \triangleq & n+6 & \text{//the first child lock} \\
n.eL & \triangleq & n+7 & \text{//the last child lock} \\
n.rL & \triangleq & n+8 & \text{//the right sibling lock}
\end{array}
$$

The predicates used in the above translation are defined as:

$$
\begin{aligned}
\mathsf{Left}\,(n,l,u) &\triangleq \mathsf{ownsR}\,(l,n,u,1) * \mathsf{isLLock}\left(n,u,\tfrac{1}{2}\right)\\
\mathsf{isLLock}\,(n,u,\pi) &\triangleq \exists \mathsf{R}, l.\, [\mathcal{L}]^{\mathsf{R}}_{\pi} *\\
&\qquad \boxed{\mathsf{LUnlocked}\,(\mathsf{R},n,l,u) \vee \mathsf{LLocked}\,(\mathsf{R},n,l,u)}^{\mathsf{R}}_{\mathsf{LC}(\mathsf{R},n,u)}\\
\mathsf{LUnlocked}\,(\mathsf{R},n,l,u) &\triangleq n.lL \to 0 * [\mathcal{U}]^{\mathsf{R}}_{1} * \in^{\mathsf{R},n,l,u}\\
\mathsf{LLocked}\,(\mathsf{R},n,l,u) &\triangleq n.lL \to 1 * \mathsf{LWit}\,(l,n,u)\\
\mathsf{ownsR}\,(l,n,u,\pi) &\triangleq \exists \mathsf{R}.\, [\mathcal{W}]^{\mathsf{R}}_{\pi} *\\
&\qquad \boxed{\mathsf{LUnlocked}\,(\mathsf{R},n,l,u) \vee \mathsf{LLocked}\,(\mathsf{R},n,l,u)}^{\mathsf{R}}_{\mathsf{LC}(\mathsf{R},n,u)}\\
\mathsf{LWit}\,(l,n,u) &\triangleq \mathsf{ownsR}\left(l,n,u,\tfrac{1}{2}\right) \vee\\
&\qquad \begin{pmatrix} (l \neq \mathsf{null} \wedge \mathsf{ownsL}\left(l,n,u,\tfrac{1}{2}\right))\\ \vee (l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{ownsD}\left(u,n,\tfrac{1}{2}\right)) \end{pmatrix}\\
\mathsf{LInit}\,(n,l,u) &\triangleq n.lL \to - * n.u \overset{\frac{1}{4}}{\mapsto} -\\
&\qquad * \begin{pmatrix} n.l \to l\\ \vee (l \neq \mathsf{null} \wedge l.u \overset{\frac{1}{4}}{\mapsto} -)\\ \vee (l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.u \overset{\frac{1}{4}}{\mapsto} -) \end{pmatrix}\\
\mathsf{LC}(\mathsf{R},n,u) &\triangleq \begin{cases} [\mathcal{L}]: & \mathsf{LUnlocked}\,(\mathsf{R},n,l,u) \rightsquigarrow \mathsf{LLocked}\,(\mathsf{R},n,l,u)\\ [\mathcal{U}]: & \mathsf{LLocked}\,(\mathsf{R},n,l,u) \rightsquigarrow \mathsf{LUnlocked}\,(\mathsf{R},n,l',u)\\ [\mathcal{W}]: & \begin{array}{l} \mathsf{LInit}\,(n,l,u) \rightsquigarrow\\ \quad \mathsf{LUnlocked}\,(\mathsf{R},n,l,u) \vee \mathsf{LLocked}\,(\mathsf{R},n,l,u)\\ \mathsf{LUnlocked}\,(\mathsf{R},n,l,u) \vee \mathsf{LLocked}\,(\mathsf{R},n,l,u)\\ \quad \rightsquigarrow \mathsf{LInit}\,(n,l,u) \end{array} \end{cases}\\
\in^{\mathsf{R},n,l,u} &\triangleq n.l \overset{\frac{1}{2}}{\mapsto} l *\\
&\qquad \begin{pmatrix} \left(\begin{array}{l} l \neq \mathsf{null} \wedge l.r \overset{\frac{1}{2}}{\mapsto} n * \mathsf{isRLock}\left(l,u,\tfrac{1}{2}\right) \end{array} \right)\\ \vee \left(\begin{array}{l} l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge\\ u.d \overset{\frac{1}{2}}{\mapsto} n * \mathsf{isDLock}\left(u,\tfrac{1}{2}\right) \end{array} \right)\\ \vee \left(l \doteq u \doteq \mathsf{null} * n.l \overset{\frac{1}{2}}{\mapsto} l * \mathsf{isLLock}\left(n,u,\tfrac{1}{2}\right) \right) \end{pmatrix}
\end{aligned}
$$

$$
\begin{aligned}
\mathsf{Right}\,(n,r,u) &\triangleq \mathsf{isRLock}\left(n,u,\tfrac{1}{2}\right) * \mathsf{ownsL}\,(n,r,u,1)\\
\mathsf{isRLock}\,(n,u,\pi) &\triangleq \exists \mathsf{R}, r.\, [\mathcal{L}]^{\mathsf{R}}_{\pi} *\\
&\qquad \boxed{\mathsf{RUnlocked}\,(n,r,u) \vee \mathsf{RLocked}\,(n,r,u)}^{\mathsf{R}}_{\mathsf{LC}(\mathsf{R},n,u)}\\
\mathsf{RUnlocked}\,(n,r,u) &\triangleq n.rL \to 0 * [\mathcal{U}]^{\mathsf{R}}_{1} * \ni^{n,r,u}\\
\mathsf{RLocked}\,(n,r,u) &\triangleq n.rL \to 1 * \mathsf{RWit}\,(n,r,u)\\
\mathsf{ownsL}\,(n,r,u,\pi) &\triangleq \exists \mathsf{R}.\, [\mathcal{W}]^{\mathsf{R}}_{\pi} *\\
&\qquad \boxed{\mathsf{RUnlocked}\,(n,r,u) \vee \mathsf{RLocked}\,(n,r,u)}^{\mathsf{R}}_{\mathsf{LC}(\mathsf{R},n,u)}\\
\mathsf{RWit}\,(n,r,u) &\triangleq \mathsf{ownsL}\left(n,r,u,\tfrac{1}{2}\right) \vee\\
&\qquad \left(\begin{array}{l}(r \neq \mathsf{null} \wedge \mathsf{ownsR}\left(n,r,u,\tfrac{1}{2}\right))\\ \vee (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{ownsE}\left(u,n,\tfrac{1}{2}\right))\end{array}\right)\\
\mathsf{RInit}\,(n,r,u) &\triangleq n.rL \to - * n.u \overset{\frac{1}{4}}{\mapsto} -\\
&\qquad * \begin{pmatrix} n.r \to r\\ \vee (r \neq \mathsf{null} \wedge r.u \overset{\frac{1}{4}}{\mapsto} -)\\ (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.u \overset{\frac{1}{4}}{\mapsto} -)\end{pmatrix}\\
\mathsf{RC}(\mathsf{R},n,u) &\triangleq \begin{cases}
[\mathcal{L}]: & \mathsf{RUnlocked}\,(n,r,u) \rightsquigarrow \mathsf{RLocked}\,(n,r,u)\\
[\mathcal{U}]: & \mathsf{RUnlocked}\,(n,r,u) \rightsquigarrow \mathsf{RLocked}\,(n,r',u)\\
[\mathcal{W}]: & \begin{array}{l}\mathsf{RInit}\,(n,r,u) \rightsquigarrow\\ \quad \mathsf{RUnlocked}\,(n,r,u) \vee \mathsf{RLocked}\,(n,r,u)\\ \mathsf{RUnlocked}\,(n,r,u) \vee \mathsf{RLocked}\,(n,r,u)\\ \quad \rightsquigarrow \mathsf{RInit}\,(n,r,u)\end{array}
\end{cases}\\
\ni^{n,r,u} &\triangleq n.r \overset{\frac{1}{2}}{\mapsto} r *\\
&\qquad \left(\begin{array}{l}\left(\begin{array}{l} r \neq \mathsf{null} \wedge\\ r.l \overset{\frac{1}{2}}{\mapsto} n * \mathsf{isLLock}\left(r,u,\tfrac{1}{2}\right)\end{array}\right)\\ \vee \left(\begin{array}{l} r = \mathsf{null} \wedge\\ u.e \overset{\frac{1}{2}}{\mapsto} n * \mathsf{isELock}\left(u,\tfrac{1}{2}\right)\end{array}\right)\\ \vee \left(\begin{array}{l} r \doteq u \doteq \mathsf{null} * n.r \overset{\frac{1}{2}}{\mapsto} r * \mathsf{isRLock}\left(n,u,\tfrac{1}{2}\right)\end{array}\right)\end{array}\right)
\end{aligned}
$$

$$
\begin{array}{rcl}
\mathsf{First}\,(n,d) & \triangleq & \mathsf{isDLock}\left(n,\frac{1}{2}\right) * \ \mathsf{ownsD}\,(n,d,1) \\
\mathsf{isDLock}\,(n,\pi) & \triangleq & \exists \mathsf{R}, d.\,[\mathcal{A}]^{\mathsf{R}}_{\pi} * \\
 & & \boxed{\mathsf{DUnlocked}\,(n,d) \vee \mathsf{DLocked}\,(n,d)}^{\mathsf{R}}_{\mathsf{DC}(\mathsf{R},n)} \\
 & & \\
\mathsf{DUnlocked}\,(n,d) & \triangleq & n.dL \to 0 * [\mathcal{U}]^{\mathsf{R}}_{1} * \lll^{n,d} \\
\mathsf{DLocked}\,(n,d) & \triangleq & n.dL \to 1 * \mathsf{DWit}\,(n,d) \\
\mathsf{DWit}\,(n,d) & \triangleq & \mathsf{ownsD}\left(n,d,\frac{1}{2}\right) \vee (d \neq \mathsf{null} \wedge \mathsf{ownsR}\left(\mathsf{null},d,n,\frac{1}{2}\right)) \\
\mathsf{ownsD}\,(n,d,\pi) & \triangleq & \exists \mathsf{R}.\,[\mathcal{W}]^{\mathsf{R}}_{\pi} * \\
 & & \boxed{\mathsf{DUnlocked}\,(n,d) \vee \mathsf{DLocked}\,(n,d)}^{\mathsf{R}}_{\mathsf{DC}(\mathsf{R},n)} \\
 & & \\
\mathsf{DC}(\mathsf{R},n) & \triangleq & \left\{ \begin{array}{ll}
[\mathcal{L}]: & \mathsf{DUnlocked}\,(n,d) \rightsquigarrow \mathsf{DLocked}\,(n,d) \\
[\mathcal{U}]: & \mathsf{DLocked}\,(n,d) \rightsquigarrow \mathsf{DUnlocked}\,(n,d') \\
[\mathcal{W}]: & \begin{array}{l} \mathsf{DInit}\,(n,d) \rightsquigarrow \\ \quad \mathsf{DUnlocked}\,(n,d) \vee \mathsf{DLocked}\,(n,d) \\ \mathsf{DUnlocked}\,(n,d) \vee \mathsf{DLocked}\,(n,d) \\ \quad \rightsquigarrow \mathsf{DInit}\,(n,d) \end{array}
\end{array} \right. \\
 & & \\
\mathsf{DInit}\,(n,d) & \triangleq & n.dL \to - * n.u \overset{\frac{1}{4}}{\mapsto} - \\
 & & * \left(\begin{array}{l} n.d \to d \\ \vee (d \neq \mathsf{null} \wedge d.u \overset{\frac{1}{4}}{\mapsto} -) \end{array} \right) \\
\lll^{n,d} & \triangleq & n \overset{\frac{1}{2}}{\mapsto} d * \\
 & & \left(\begin{array}{l} \left(\begin{array}{l} d \neq \mathsf{null} \wedge \\ d.l \overset{\frac{1}{2}}{\mapsto} \mathsf{null} * \ \mathsf{isLLock}\left(d,n,\frac{1}{2}\right) \end{array} \right) \\ \vee \left(\ d \doteq \mathsf{null} \ * n.d \overset{\frac{1}{2}}{\mapsto} d * \ \mathsf{isDLock}\left(n,\frac{1}{2}\right) \ \right) \end{array} \right)
\end{array}
$$

$$
\begin{aligned}
\mathsf{Last}\,(n,e) &\triangleq \mathsf{isELock}\left(n,\tfrac{1}{2}\right) * \mathsf{ownsE}\,(n,e,1)\\
\mathsf{isELock}\,(n,\pi) &\triangleq \exists \mathsf{R}, e.\, [\mathcal{A}]^{\mathsf{R}}_{\pi} * \\
&\qquad \boxed{\mathsf{EUnlocked}\,(n,e) \vee \mathsf{ELocked}\,(n,e)}^{\mathsf{R}}_{\mathsf{EC}(\mathsf{R},n)}\\
\\
\mathsf{EUnlocked}\,(n,e) &\triangleq \quad n.eL \to 0 * [\mathcal{U}]^{\mathsf{R}}_{1} * \circledcirc^{n,e}\\
\mathsf{ELocked}\,(n,e) &\triangleq n.eL \to 1 * \mathsf{EWit}\,(n,e)\\
\mathsf{ownsE}\,(n,e,\pi) &\triangleq \exists \mathsf{R}.\, [\mathcal{W}]^{\mathsf{R}}_{\pi} * \\
&\qquad \boxed{\mathsf{EUnlocked}\,(n,e) \vee \mathsf{ELocked}\,(n,e)}^{\mathsf{R}}_{\mathsf{EC}(\mathsf{R},n)}\\
\mathsf{EWit}\,(n,e) &\triangleq \mathsf{ownsE}\left(n,e,\tfrac{1}{2}\right) \vee \left(e \neq \mathsf{null} \wedge \mathsf{ownsL}\left(e,\mathsf{null},n,\tfrac{1}{2}\right)\right)\\
\mathsf{EInit}\,(n,e) &\triangleq n.eL \to - * n.u \overset{\frac{1}{4}}{\mapsto} -\\
&\qquad * \left(\begin{array}{l} n.e \to e \\ \\ \vee (e \neq \mathsf{null} \wedge e.u \overset{\frac{1}{4}}{\mapsto} -) \end{array} \right)\\
\mathsf{EC}(\mathsf{R},n) &\triangleq \left\{ \begin{array}{ll} [\mathcal{L}]: & \mathsf{EUnlocked}\,(n,e) \rightsquigarrow \mathsf{ELocked}\,(n,e) \\ \\ [\mathcal{U}]: & \mathsf{ELocked}\,(n,e) \rightsquigarrow \mathsf{EUnlocked}\,(n,e') \\ \\ [\mathcal{W}]: & \begin{array}{l} \mathsf{EInit}\,(n,e) \rightsquigarrow \\ \quad \mathsf{EUnlocked}\,(n,e) \vee \mathsf{ELocked}\,(n,e) \\ \mathsf{EUnlocked}\,(n,e) \vee \mathsf{ELocked}\,(n,e) \\ \quad \rightsquigarrow \mathsf{EInit}\,(n,e) \end{array} \end{array} \right.\\
\circledcirc^{n,e} &\triangleq n \overset{\frac{1}{2}}{\mapsto} e * \\
&\qquad \left(\begin{array}{l} \left(\begin{array}{l} e \neq \mathsf{null} \wedge \\ e.r \overset{\frac{1}{2}}{\mapsto} \mathsf{null} * \mathsf{isRLock}\left(e,n,\frac{1}{2}\right) \end{array} \right) \\ \vee \left(e \doteq \mathsf{null} * n.e \overset{\frac{1}{2}}{\mapsto} e * \mathsf{isELock}\left(n,\tfrac{1}{2}\right) \right) \end{array} \right)
\end{aligned}
$$

Definition 18 (Interfaces)**.** The sets of *inner* and *outer interfaces* associated with abstract addresses of tree heaps are defined as:

$$\textsc{In}_{\tau} \triangleq \left(\mathbb{N}^{+} \uplus \{\mathsf{null}\}\right)^{2} \qquad\qquad \textsc{Out}_{\tau} \triangleq \left(\mathbb{N}^{+} \uplus \{\mathsf{null}\}\right)^{3}$$

while the set of *inner* and *outer interface functions* are defined as $\mathcal{I}^{\mathsf{in}}_{\tau} : \wp(\textsc{SAdd} \rightharpoonup \textsc{In}_{\tau})$, and $\mathcal{I}^{\mathsf{out}}_{\tau} : \wp(\textsc{SAdd} \rightharpoonup \textsc{Out}_{\tau})$, respectively. The set of interface function pairs is then given as the Cartesian product of the two: $\mathcal{I}_{\tau} : \mathcal{I}^{\mathsf{in}}_{\tau} \times \mathcal{I}^{\mathsf{out}}_{\tau}$.

Definition 19 (Stable Interface Functions)**.** Given the sets of inner and outer interfaces IN_τ, OUT_τ (def. 18), the *set of stable inner-interface functions* $\mathcal{SI}_\tau{}^{\mathsf{in}} : \wp(\text{SADD} \rightharpoonup \wp(\text{IN}_\tau))$, and the *set of stable outer-interface functions* $\mathcal{SI}_\tau{}^{\mathsf{out}} : \wp(\text{SADD} \rightharpoonup \wp(\text{OUT}_\tau))$ consist of interface functions mapping abstract addresses to a set of possible inner and outer interfaces, respectively. The Cartesian product of the two forms the set of stable interface function pairs $\mathcal{SI}_\tau \triangleq \mathcal{SI}_\tau{}^{\mathsf{in}} \times \mathcal{SI}_\tau{}^{\mathsf{out}}$. Given a stable interface function pair SI, we write SI^{in} and SI^{out} for the first and second projections.

Definition 20 (Implementation Function)**.** The implementation function

$$[\![.]\!]_\tau : \text{ATOM}_\mathbb{T} \to \text{PROG}_\mathbb{C}$$

provides an implementation for each atomic command of tree library $\mathbb{T}$ as a correspondingly named procedure given in Figures 3.1, 3.2 and 3.3 with:

```
  x.left ≜ x
    x.up ≜ x + 1
 x.first ≜ x + 2
  x.last ≜ x + 3
 x.right ≜ x + 4
 x.leftL ≜ x + 5
x.firstL ≜ x + 6
 x.lastL ≜ x + 7
x.rightL ≜ x + 8
```

We have now defined all necessary components for formalising the translation.

Definition 21 (Translation)**.** The translation $\tau : \mathbb{T} \to \mathbb{C}$ is a 4-tuple of the set of interfaces, the set of stable interface function pairs, the tree heap translation function and the implementation function: $\Big((\text{IN}_\tau \times \text{OUT}_\tau), \mathcal{SI}_\tau, \langle . \rangle^{(.)}, [\![.]\!]_\tau\Big)$.

```
proc n := getUp(m){
  n := [m.up]
}
proc n := getLeft(m){
  n:= [m.left]
}
proc n := getRight(m){
  n:= [m.right]
}

proc n := getFirst(m){
  n:= [m.first]
}
proc n := getLast(m){
  n:= [m.last]
}
proc n := newNode(){
  n:= alloc(9) ;
  n.leftL := 1 ;
  n.rightL := 1 ;
  n.firstL := 1 ;
  n.lastL := 1 ;
}
proc disposeNode(n){
  dealloc(n, 9)
}
proc lock(a){
  while(!<CAS(a, 0, 1)>)
    skip ;
}
```

```
proc newNodeAfter(n){
  local x,r,u in
    u:= [n.up] ;
    x := newNode() ;
    [x.up]:= u ;
    [x.left]:= n ;
    unlock(x.leftL) ;
    [x.first]:= null ;
    unlock(x.firstL) ;
    [x.last]:= null ;
    unlock(x.lastL) ;
    lock(n.rightL) ;
    r:= [n.right] ;
    if r ≠ null then
      lock(r.leftL)
    else if u ≠ null then
      lock(u.lastL)
    [x.right]:= r ;
    unlock(x.rightL) ;
    if r ≠ null then
      [r.left]:= x ;
      unlock(r.leftL) ;
    else if u ≠ null then
      [u.last]:= x ;
      unlock(u.lastL) ;
    [n.right]:= x ;
    unlock(n.rightL)
}
proc unlock(a){
  <[a:= 0]> ;
}
```

Figure 3.1: Procedures for the heap-based implementation of the tree module.

```
proc deleteTree(n){
  local l, u, d, r in
    u := [n.up] ;
    //Acquiring the necessary locks.
    lock(n.leftL) ; l:= [n.left] ;
    if l ≠ null then lock(l.rightL)
    else if u ≠ null then lock(u.firstL) ;
    lock(n.rightL) ; r:= [n.right] ;
    if r ≠ null then lock(r.leftL) ;
    else if u ≠ null then lock(u.lastL) ;
    //Pointer Swinging.
    if l ≠ null then [l.right] := r ;
    else if u ≠ null then [u.first] := r ;
    if r ≠ null then [r.left] := l ;
    else if u ≠ null then [u.last] := l ;
    //Unlocking the acquired locks.
    if l ≠ null then unlock(l.rightL) ;
    else if u ≠ null then unlock(u.firstL) ;
    if r ≠ null then unlock(r.leftL) ;
    else if u ≠ null then unlock(u.lastL) ;
    d := [n.first] ; call disposeForest(d) ;
    disposeNode(n) ;
}

proc disposeForest(n){
  local r, d in
    if n ≠ null then
      r := [n.right] ;
      call disposeForest (r) ;
      d := [n.first] ;
      call disposeForest (d) ;
      disposeNode(n)
}
```

Figure 3.2: Procedures for the heap-based implementation of the tree module (continued).

```
proc appendChild(m,n){
  local l,u,e,r in
    u := [n.up] ;
    //Acquiring the necessary locks.
    lock(n.leftL) ; l:= [n.left] ;
    if l ≠ null then lock(l.rightL)
    else if u ≠ null then lock(u.firstL) ;
    lock(n.rightL) ; r:= [n.right] ;
    if r ≠ null then lock(r.leftL) ;
    else if u ≠ null then lock(u.lastL) ;
    //Pointer Swinging.
    if l ≠ null then [l.right] := r ;
    else if u ≠ null then [u.first] := r ;
    if r ≠ null then [r.left] := l ;
    else if u ≠ null then [u.last] := l ;
    //Unlocking the acquired locks.
    if l ≠ null then unlock(l.rightL) ;
    else if u ≠ null then unlock(u.firstL) ;
    if r ≠ null then unlock(r.leftL) ;
    else if u ≠ null then unlock(u.lastL) ;
    [n.up]:= m ; [n.right]:= null ;
    lock(m.lastL) ;
    e:= [m.last] ; [n.left]:= e ;
    if e ≠ null then lock(e.rightL) ;
    else lock(m.firstL) ;
    if e ≠ null then [e.right]:= n ; unlock(e.rightL) ;
    else [m.first]:= n ; unlock(m.firstL) ;
    unlock(n.leftL) ;
    [m.last]:= n ; unlock(m.lastL) ; unlock(n.rightL) ;
}
```

Figure 3.3: Procedures for the heap-based implementation of the tree module (continued).

3.1 Soundness of Translation $\tau : \mathbb{T} \to \mathbb{C}$

Theorem 2 (Sound Transformation)**.** The module translation $\tau : \mathbb{T} \to \mathbb{C}$ is a sound translation.

Proof. In lemmata 3 to 5 we show that the translation $\tau : \mathbb{T} \to \mathbb{C}$ satisfies the three properties stated in theorem 1. The soundness of translation $\tau : \mathbb{T} \to \mathbb{C}$ then follows directly from theorem 1.

Lemma 3 (Monotonicity of *id* Relation)**.** Given the translation $\tau : \mathbb{T} \to \mathbb{C}$, for all $h_1, h_2 \in \mathcal{H}_{\mathbb{T}}$ and $I \in \mathcal{I}_\tau$:

$$\left\{\{h_1\}\right\} id \left\{\{h_2\}\right\} \implies \left\{ \langle h_1 \rangle^I \right\} id \left\{ \langle h_2 \rangle^I \right\}$$

Proof. Recall that the only *id* transitions between abstract trees pertain to abstract allocation and deallocation. Hence, it suffices to show that for all $t_1, t_2 \in \textsc{Data}_{\mathbb{T}}$, $I \in \mathcal{I}_\tau$, $\mathbf{a} \in \textsc{SAdd} \cup \{\mathcal{R}\}$ and $\mathbf{x}, \mathbf{y} \in \textsc{SAdd}$

$$\langle \mathsf{tree}\,(\mathbf{a}, t_1 \circ_{\mathbf{x}} t_2) \rangle^I \equiv \exists \mathbf{y} \in \textsc{SAdd}, in, out. \langle \mathsf{tree}\,(\mathbf{a}, t_1 \circ_{\mathbf{x}} \mathbf{y}) \rangle^{I'} \bullet_{\mathbb{C}} \langle \mathsf{tree}\,(\mathbf{y}, t_2) \rangle^{I'}$$

with $I' \triangleq \left(I^{\mathsf{in}}[\mathbf{y} \mapsto in], \mathbf{y} \mapsto out^{\mathsf{out}}\right)$. The proof of the above statement is provided in Appendix A.

Lemma 4 (Composition Preservation)**.** The composition operator is preserved by the translation $\tau : \mathbb{T} \to \mathbb{C}$. That is, for all $h_{\mathbb{T}}, h'_{\mathbb{T}} \in \mathcal{H}_{\mathbb{T}}$ and $I \in \mathcal{I}_\tau$:

$$\left\langle h_{\mathbb{T}} \bullet_{\mathbb{T}} h'_{\mathbb{T}} \right\rangle^I = \exists I_1, I_2. I_1 \cup I_2 \doteq I \ \wedge \ \langle h_{\mathbb{T}} \rangle^{I_1} \bullet_{\mathbb{C}} \left\langle h'_{\mathbb{T}} \right\rangle^{I_2}$$

Proof. This follows immediately from the definition of $\langle . \rangle^{(\cdot)}$. □

Lemma 5 (Axiom Correctness)**.** For all $\Omega \in \textsc{PEnv}$, $\mathbb{C} \in \textsc{Atom}_{\mathbb{T}}$, $(p, \mathbb{C}, q) \in \textsc{Axiom}_{\mathbb{T}}$ and $SI \in \mathcal{SI}_\tau$,

$$[\![\Omega]\!]_\tau \vDash_{\mathbb{B}} \{[\![p]\!]_{SI}\} \ \ [\![\mathbb{C}]\!]_\tau \ \ \{[\![q]\!]_{SI}\}$$

Proof. We do not give the proofs for all of the basic commands in the Tree library. We give a few examples to illustrate the techniques involved in the proof.

Axiom Correctness: `deleteTree`

Let $\mathcal{I}_D \triangleq \{I \in \mathcal{I}_\tau \mid \mathrm{dom}(I^{\mathsf{in}}) = \{\mathbf{x}\} \wedge \mathrm{dom}(I^{\mathsf{out}}) = \varnothing\}$.
Pick an arbitrary $SI \in \mathcal{SI}_\tau$. We then need to show:

$$\left\{ \left(\mathsf{var}\left(\mathtt{n}, n\right), m\right) \;\middle|\; m \in \left(\bigvee_{I \in SI\downarrow} \left(\exists I_1 \in \mathcal{I}_D . \left\langle \mathsf{tree}\left(\mathbf{x}, n[t]\right)\right\rangle^{I \uplus I_1} \right) \right) \right\}$$
$$[\![\mathtt{deleteTree(n)}]\!]_\tau$$
$$\left\{ \left(\mathsf{var}\left(\mathtt{n}, n\right), m\right) \;\middle|\; m \in \left(\bigvee_{I \in SI\downarrow} \left(\exists I_2 \in \mathcal{I}_D . \left\langle \mathsf{tree}\left(\mathbf{x}, \varnothing\right)\right\rangle^{I \uplus I_2} \right) \right) \right\}$$

Pick $I_1, I_2 \in \mathcal{I}_\tau$ such that ${I_1}^{\mathsf{in}}(\mathbf{x}) = (n, n)$ and ${I_2}^{\mathsf{in}}(\mathbf{x}) = (r^x, l^x)$. We give a proof outline below showing that the implementation of `deleteTree` satisfies its specification.

$$\left\{ \bigvee_{I \in SI\downarrow} \left(\langle \mathsf{tree}\,(\mathbf{x}, n[t]) \rangle^{I \uplus I_1} \ \wedge \ addrs\,(t) = \varnothing \right) \ \times \{\mathsf{var}\,(\mathtt{n}, n)\} \right\}$$

```
proc deleteTree(n){
```

$$\left\{ \bigvee_{I \in SI\downarrow} (\mathsf{tree}\,(I \uplus I_1, \mathbf{x}, n[t]) \wedge addrs\,(t) = \varnothing) \quad \times \{\mathsf{var}\,(\mathtt{n}, n)\} \right\}$$

```
  local l,u,d,r in
```

$$\left\{ \begin{array}{l} \bigvee_{I \in SI\downarrow} (\mathsf{tree}\,(I, \mathbf{x}, n[t]) \wedge addrs\,(t) = \varnothing) \\ \times \{\mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, -) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, -)\} \end{array} \right\}$$

$$\left\{ \begin{array}{l} \bigvee_{I \in SI\downarrow} \left\{ \ I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x) \ * \ n.u \to u^x * \mathsf{Left}\,(n, l^x, u^x) * \mathsf{Right}\,(n, r^x, u^x) \ \right\} \\ * \exists d, e.\, \mathsf{First}\,(n, d) * \mathsf{Last}\,(n, e) * \mathsf{treeFrag}\,(I, t)\,((d, e)\,(\mathsf{null}, n, \mathsf{null}) \\ \times \{\mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, -) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, -)\} \end{array} \right\}$$

//By lemma 12

$$\left\{ \begin{array}{l} \bigvee_{I \in SI\downarrow} \left\{ \ I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x) \ * \ n.u \to u * \mathsf{Left}\,(n, l^x, u^x) * \mathsf{Right}\,(n, r^x, u^x) \ \right\} \\ * \exists d, e.\, n.d \to d * n.dL \to 0 * n.e \to e * n.eL \to 0 * ||t||^{((d,e)(\mathsf{null}, n, \mathsf{null})} \\ \times \{\mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, -) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, -)\} \end{array} \right\}$$

```
  u:= [n.up] ; d:= [n.first] ;
```

$$\left\{ \begin{array}{l} \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l} I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x) \ * \ n.u \to u * \mathsf{Left}\,(n, l^x, u^x) * \mathsf{Right}\,(n, r^x, u^x) \\ * \mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, u^x) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, d) \end{array} \right\} \\ * \exists d, e.\, n.d \to d * n.dL \to 0 * n.e \to e * n.eL \to 0 * ||t||^{((d,e)(\mathsf{null}, n, \mathsf{null})} \end{array} \right\}$$

$$\left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l} I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x) \ * \ \mathsf{Left}\,(n, l^x, u^x) \\ * \mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, u^x) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, d) \end{array} \right\} \right\}$$

$$\left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l} I^{\mathsf{out}}(\mathbf{x}) = (l^x, u^x, r^x) * \ \mathsf{isLLock}\left(n, u^x, \frac{1}{2}\right) * \mathsf{ownsR}\,(n, l^x, u^x, 1) \\ * \mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, u^x) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, d) \end{array} \right\} \right\}$$

```
  lock(n.leftL) ;
```

$$\left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l} I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x) * \\ \exists \mathsf{R}_{n.l}.\, [\mathcal{L}]^{\mathsf{R}_{n.l}}_{\frac{1}{2}} * [\mathcal{U}]^{\mathsf{R}_{n.l}}_{1} * \mathsf{ownsR}\left(l^x, n, u^x, \frac{3}{4}\right) \\ * \Subset^{\mathsf{R}, n, l^x, u^x} * \boxed{n.lL \to 1 * \mathsf{ownsR}\left(l^x, n, u^x, \frac{1}{4}\right)}^{\mathsf{R}_{n.l}}_{\mathsf{LC}(\mathsf{R}_{n.l}, n, u^x)} \\ * \mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, u^x) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, d) \end{array} \right\} \right\}$$

$$\left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l} I^{\mathsf{out}}(\mathbf{x}) = (l^x, u^x, r^x) * \ \mathsf{ownsR}\left(n, l^x, u^x, \frac{3}{4}\right) * \Subset^{\mathsf{R}, n, l^x, u^x} \\ * \mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, u^x) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, d) \end{array} \right\} \right\}$$

```
  l:= [n.left] ;
```

$$\left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l} I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x) * \ \mathsf{ownsR}\left(n, l^x, u^x, \frac{3}{4}\right) * \Subset^{\mathsf{R}, n, l^x, u^x} \\ * \mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, l^x) * \mathsf{var}\,(\mathtt{u}, u^x) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, d) \end{array} \right\} \right\}$$

$$\left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l} I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x) * \mathsf{ownsR}\left(n, l^x, u^x, \frac{3}{4}\right) * n.l \overset{\frac{1}{2}}{\mapsto} l^x \\ * \left(\begin{array}{l} \left(\begin{array}{l} l^x \neq \mathsf{null} \ \wedge \ l^x.r \overset{\frac{1}{2}}{\mapsto} n * \ \mathsf{isRLock}\left(l^x, u^x, \frac{1}{2}\right) \end{array} \right) \\ \vee \left(\begin{array}{l} l^x = \mathsf{null} \wedge u^x \neq \mathsf{null} \wedge u^x.d \overset{\frac{1}{2}}{\mapsto} n * \ \mathsf{isDLock}\left(u^x, \frac{1}{2}\right) \end{array} \right) \\ \vee \left(\begin{array}{l} l^x = \mathsf{null} \wedge u^x = \mathsf{null} \wedge n.l \overset{\frac{1}{2}}{\mapsto} l^x * \mathsf{isLLock}\left(n, u^x, \frac{1}{2}\right) \end{array} \right) \end{array} \right) \\ * \mathsf{var}(\mathtt{n}, n) * \mathsf{var}(\mathtt{l}, l^x) * \mathsf{var}(\mathtt{u}, u^x) * \mathsf{var}(\mathtt{r}, -) * \mathsf{var}(\mathtt{d}, d) \end{array} \right\} \right\}$$

```
if l ≠ null then   lock(l.rightL)
else if u ≠ null then   lock(u.firstL) ;
```

$$\left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l} I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x) * \boxed{\mathsf{ownsR}\left(n, l^x, u^x, \frac{1}{2}\right)} * n.l \overset{\frac{1}{2}}{\mapsto} l^x \\ * \left(\begin{array}{l} \left(\begin{array}{l} l^x \neq \mathsf{null} \ \wedge \ l^x.r \overset{\frac{1}{2}}{\mapsto} n \\ * \exists \mathsf{R}_{l.r}. \left[\mathcal{L}\right]^{\mathsf{R}_{l.r}}_{\frac{1}{2}} * \boxed{\left[\mathcal{U}\right]^{\mathsf{R}_{l.r}}_{1} * \ni^{l^x, n, u^x}} \\ * \boxed{l^x.rL \to 1 * \mathsf{ownsR}\left(l^x, n, u^x, \frac{1}{4}\right)}^{\mathsf{R}_{l.r}}_{\mathsf{RC}(\mathsf{R}_{l.r}, l^x, u^x)} \end{array} \right) \\ \vee \left(\begin{array}{l} l^x = \mathsf{null} \wedge u^x \neq \mathsf{null} \wedge u^x.d \overset{\frac{1}{2}}{\mapsto} n \\ * \exists \mathsf{R}_{u.d}. \left[\mathcal{L}\right]^{\mathsf{R}_{u.d}}_{\frac{1}{2}} * \boxed{\left[\mathcal{U}\right]^{\mathsf{R}_{u.d}}_{1} * \lll^{u^x, n}} \\ * \boxed{u^x.dL \to 1 * \mathsf{ownsR}\left(\mathsf{null}, n, u^x, \frac{1}{4}\right)}^{\mathsf{R}_{u.d}}_{\mathsf{DC}(\mathsf{R}_{u.d}, u^x)} \end{array} \right) \\ \vee \left(\begin{array}{l} l^x = \mathsf{null} \wedge u^x = \mathsf{null} \wedge n.l \overset{\frac{1}{2}}{\mapsto} l^x \\ * \mathsf{isLLock}\left(n, u^x, \frac{1}{2}\right) * \mathsf{ownsR}\left(l^x, n, u^x, \frac{1}{4}\right) \end{array} \right) \end{array} \right) \\ * \mathsf{var}(\mathtt{n}, n) * \mathsf{var}(\mathtt{l}, l^x) * \mathsf{var}(\mathtt{u}, u^x) * \mathsf{var}(\mathtt{r}, -) * \mathsf{var}(\mathtt{d}, d) \end{array} \right\} \right\}$$

$$\left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l} I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x) * \ n.l \overset{1}{\mapsto} l^x * \exists \mathsf{R}_{n.l}. \left[\mathcal{W}\right]^{\mathsf{R}_{n.l}}_{\frac{1}{2}} * \left[\mathcal{L}\right]^{\mathsf{R}_{n.l}}_{1} * \left[\mathcal{U}\right]^{\mathsf{R}_{n.l}}_{1} \\ * \boxed{n.lL \to 1 * \left[\mathcal{W}\right]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{n.l}}_{\mathsf{LC}(\mathsf{R}_{n.l}, n, u^x)} * \mathsf{Right}(n, r^x, u^x) \\ * \left(\begin{array}{l} \left(\begin{array}{l} l^x \neq \mathsf{null} \ \wedge \ l^x.r \overset{1}{\mapsto} n * \exists \mathsf{R}_{l.r}. \\ \left[\mathcal{L}\right]^{\mathsf{R}_{l.r}}_{\frac{1}{2}} * \left[\mathcal{U}\right]^{\mathsf{R}_{l.r}}_{1} * \boxed{l^x.rL \to 1 * \left[\mathcal{W}\right]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{l.r}}_{\mathsf{RC}(\mathsf{R}_{l.r}, l^x, u^x)} \end{array} \right) \\ \vee \left(\begin{array}{l} l^x = \mathsf{null} \wedge u^x \neq \mathsf{null} \wedge u^x.d \overset{1}{\mapsto} n * \exists \mathsf{R}_{u.d}. \\ \left[\mathcal{L}\right]^{\mathsf{R}_{u.d}}_{\frac{1}{2}} * \left[\mathcal{U}\right]^{\mathsf{R}_{u.d}}_{1} * \boxed{u^x.dL \to 1 * \left[\mathcal{W}\right]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{u.d}}_{\mathsf{DC}(\mathsf{R}_{u.d}, u^x)} \end{array} \right) \\ \vee \left(l^x = \mathsf{null} \wedge u^x = \mathsf{null} \wedge \left[\mathcal{W}\right]^{\mathsf{R}_{n.l}}_{\frac{1}{4}} \right) \end{array} \right) \\ * \mathsf{var}(\mathtt{n}, n) * \mathsf{var}(\mathtt{l}, l^x) * \mathsf{var}(\mathtt{u}, u^x) * \mathsf{var}(\mathtt{r}, -) * \mathsf{var}(\mathtt{d}, d) \end{array} \right\} \right\}$$

//Do the same for the right hand side

`lock(n.rightL)` ; `r:= [n.right]` ;

`if r` $\neq$ null `then lock(r.leftL)  else if u` $\neq$ null `then lock(u.lastL)` ;

$$
\left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l}
I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x) * \ \exists \mathsf{R}_{n.l}. [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{2}} [\mathcal{L}]^{\mathsf{R}_{n.l}}_{1} * [\mathcal{U}]^{\mathsf{R}_{n.l}}_{1} \\
* n.l \overset{1}{\mapsto} l^x * n.r \overset{1}{\mapsto} r^x * \boxed{n.lL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{n.l}}_{\mathsf{LC}(\mathsf{R}_{n.l}, n, u^x)} \\
* \left(\begin{array}{l} l^x \neq \mathsf{null} \ \wedge \ l^x.r \overset{1}{\mapsto} n * \exists \mathsf{R}_{l.r}. \\ [\mathcal{L}]^{\mathsf{R}_{l.r}}_{\frac{1}{2}} * [\mathcal{U}]^{\mathsf{R}_{l.r}}_{1} * \boxed{l^x.rL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{l.r}}_{\mathsf{RC}(\mathsf{R}_{l.r}, l^x, u^x)} \end{array} \right) \\
\quad \vee \left(\begin{array}{l} l^x = \mathsf{null} \wedge u^x \neq \mathsf{null} \wedge u^x.d \overset{1}{\mapsto} n * \exists \mathsf{R}_{u.d}. \\ [\mathcal{L}]^{\mathsf{R}_{u.d}}_{\frac{1}{2}} * [\mathcal{U}]^{\mathsf{R}_{u.d}}_{1} * \boxed{u^x.dL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{u.d}}_{\mathsf{DC}(\mathsf{R}_{u.d}, u^x)} \end{array} \right) \\
\quad \vee \left(l^x = \mathsf{null} \wedge u^x = \mathsf{null} \wedge [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}} \right) \\
* \exists \mathsf{R}_{n.r}. [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{2}} * [\mathcal{L}]^{\mathsf{R}_{n.r}}_{1} * [\mathcal{U}]^{\mathsf{R}_{n.r}}_{1} * \boxed{n.rL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}}}^{\mathsf{R}_{n.r}}_{\mathsf{RC}(\mathsf{R}_{n.r}, n, u^x)} \\
* \left(\begin{array}{l} r^x \neq \mathsf{null} \ \wedge \ r^x.l \overset{1}{\mapsto} n * \exists \mathsf{R}_{r.l}. \\ [\mathcal{L}]^{\mathsf{R}_{r.l}}_{\frac{1}{2}} * [\mathcal{U}]^{\mathsf{R}_{r.l}}_{1} * \boxed{r^x.lL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}}}^{\mathsf{R}_{r.l}}_{\mathsf{LC}(\mathsf{R}_{r.l}, r^x, u^x)} \end{array} \right) \\
\quad \vee \left(\begin{array}{l} r^x = \mathsf{null} \wedge u^x \neq \mathsf{null} \wedge u^x.e \overset{1}{\mapsto} n * \exists \mathsf{R}_{u.e}. \\ [\mathcal{L}]^{\mathsf{R}_{u.e}}_{\frac{1}{2}} * [\mathcal{U}]^{\mathsf{R}_{u.e}}_{1} * \boxed{u^x.eL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}}}^{\mathsf{R}_{u.e}}_{\mathsf{EC}(\mathsf{R}_{u.e}, u^x)} \end{array} \right) \\
\quad \vee \left(r^x = \mathsf{null} \wedge u^x = \mathsf{null} \wedge [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}} \right) \\
* \mathsf{var}(\mathtt{n}, n) * \mathsf{var}(\mathtt{l}, l^x) * \mathsf{var}(\mathtt{u}, u^x) * \mathsf{var}(\mathtt{r}, r^x) * \mathsf{var}(\mathtt{d}, d)
\end{array} \right\} \right\}
$$

`if l` $\neq$ null `then  [l.right] := r else if u` $\neq$ null `then  [u.first] := r` ;

`if r` $\neq$ null `then  [r.left] := l else if u` $\neq$ null `then  [u.last] := l` ;

$$
\left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l}
I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x) * \ \exists \mathsf{R}_{n.l}.\, [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{2}} [\mathcal{L}]^{\mathsf{R}_{n.l}}_{1} * [\mathcal{U}]^{\mathsf{R}_{n.l}}_{1} \\
* n.l \overset{1}{\mapsto} l^x * n.r \overset{1}{\mapsto} r^x * \boxed{n.lL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{n.l}}_{\mathsf{LC}(\mathsf{R}_{n.l}, n, u^x)} \\
* \left(\begin{array}{l}
\left(\begin{array}{l} l^x \neq \mathsf{null} \ \wedge \ l^x.r \overset{1}{\mapsto} r^x * \exists \mathsf{R}_{l.r}. \\ [\mathcal{L}]^{\mathsf{R}_{l.r}}_{\frac{1}{2}} * [\mathcal{U}]^{\mathsf{R}_{l.r}}_{1} * \boxed{l^x.rL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{l.r}}_{\mathsf{RC}(\mathsf{R}_{l.r}, l^x, u^x)} \end{array} \right) \\
\vee \left(\begin{array}{l} l^x = \mathsf{null} \wedge u^x \neq \mathsf{null} \wedge u^x.d \overset{1}{\mapsto} r^x * \exists \mathsf{R}_{u.d}. \\ [\mathcal{L}]^{\mathsf{R}_{u.d}}_{\frac{1}{2}} * [\mathcal{U}]^{\mathsf{R}_{u.d}}_{1} * \boxed{u^x.dL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{u.d}}_{\mathsf{DC}(\mathsf{R}_{u.d}, u^x)} \end{array} \right) \\
\vee \left(l^x = \mathsf{null} \wedge u^x = \mathsf{null} \wedge [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}} \right)
\end{array} \right) \\
* \exists \mathsf{R}_{n.r}.\, [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{2}} * [\mathcal{L}]^{\mathsf{R}_{n.r}}_{1} * [\mathcal{U}]^{\mathsf{R}_{n.r}}_{1} * \boxed{n.rL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}}}^{\mathsf{R}_{n.r}}_{\mathsf{RC}(\mathsf{R}_{n.r}, n, u^x)} \\
* \left(\begin{array}{l}
\left(\begin{array}{l} r^x \neq \mathsf{null} \ \wedge \ r^x.l \overset{1}{\mapsto} l^x * \exists \mathsf{R}_{r.l}. \\ [\mathcal{L}]^{\mathsf{R}_{r.l}}_{\frac{1}{2}} * [\mathcal{U}]^{\mathsf{R}_{r.l}}_{1} * \boxed{r^x.lL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}}}^{\mathsf{R}_{r.l}}_{\mathsf{LC}(\mathsf{R}_{r.l}, r^x, u^x)} \end{array} \right) \\
\vee \left(\begin{array}{l} r^x = \mathsf{null} \wedge u^x \neq \mathsf{null} \wedge u^x.e \overset{1}{\mapsto} l^x * \exists \mathsf{R}_{u.e}. \\ [\mathcal{L}]^{\mathsf{R}_{u.e}}_{\frac{1}{2}} * [\mathcal{U}]^{\mathsf{R}_{u.e}}_{1} * \boxed{u^x.eL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}}}^{\mathsf{R}_{u.e}}_{\mathsf{EC}(\mathsf{R}_{u.e}, u^x)} \end{array} \right) \\
\vee \left(r^x = \mathsf{null} \wedge u^x = \mathsf{null} \wedge [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}} \right)
\end{array} \right) \\
* \mathsf{var}(\mathtt{n}, n) * \mathsf{var}(\mathtt{l}, l^x) * \mathsf{var}(\mathtt{u}, u^x) * \mathsf{var}(\mathtt{r}, r^x) * \mathsf{var}(\mathtt{d}, d)
\end{array} \right\} \right\}
$$

$$
\left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l}
I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x) * \ n.l \to l^x * n.r \to r^x \\
* \ \mathsf{tree}(I \uplus I_2, \mathbf{x}, \varnothing) \ \wedge \ I_2 \in \mathcal{I}_D \wedge I_2^{\mathsf{in}}(\mathbf{x}) = (r^x, l^x) \\
* \exists \mathsf{R}_{n.l}, \mathsf{R}_{n.r}.\, [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{2}} * [\mathcal{L}]^{\mathsf{R}_{n.l}}_{1} * [\mathcal{U}]^{\mathsf{R}_{n.l}}_{1} * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{2}} * [\mathcal{L}]^{\mathsf{R}_{n.r}}_{1} * [\mathcal{U}]^{\mathsf{R}_{n.r}}_{1} \\
* \boxed{n.rL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}}}^{\mathsf{R}_{n.r}}_{\mathsf{RC}(\mathsf{R}_{n.r}, n, u^x)} * \boxed{n.lL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{n.l}}_{\mathsf{LC}(\mathsf{R}_{n.l}, n, u^x)} \\
* \left(\begin{array}{l}
\left(\begin{array}{l} l^x \neq \mathsf{null} \ \wedge \ l^x.r \overset{1}{\mapsto} r^x * \exists \mathsf{R}_{l.r}. \\ [\mathcal{L}]^{\mathsf{R}_{l.r}}_{\frac{1}{2}} * [\mathcal{U}]^{\mathsf{R}_{l.r}}_{1} * \boxed{l^x.rL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{l.r}}_{\mathsf{RC}(\mathsf{R}_{l.r}, l^x, u^x)} \end{array} \right) \\
\vee \left(\begin{array}{l} l^x = \mathsf{null} \wedge u^x \neq \mathsf{null} \wedge u^x.d \overset{1}{\mapsto} r^x * \exists \mathsf{R}_{u.d}. \\ [\mathcal{L}]^{\mathsf{R}_{u.d}}_{\frac{1}{2}} * [\mathcal{U}]^{\mathsf{R}_{u.d}}_{1} * \boxed{u^x.dL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{u.d}}_{\mathsf{DC}(\mathsf{R}_{u.d}, u^x)} \end{array} \right) \\
\vee \left(l^x = \mathsf{null} \wedge u^x = \mathsf{null} \wedge [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}} \right)
\end{array} \right) \\
* \left(\begin{array}{l}
\left(\begin{array}{l} r^x \neq \mathsf{null} \ \wedge \ r^x.l \overset{1}{\mapsto} l^x * \exists \mathsf{R}_{r.l}. \\ [\mathcal{L}]^{\mathsf{R}_{r.l}}_{\frac{1}{2}} * [\mathcal{U}]^{\mathsf{R}_{r.l}}_{1} * \boxed{r^x.lL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}}}^{\mathsf{R}_{r.l}}_{\mathsf{LC}(\mathsf{R}_{r.l}, r^x, u^x)} \end{array} \right) \\
\vee \left(\begin{array}{l} r^x = \mathsf{null} \wedge u^x \neq \mathsf{null} \wedge u^x.e \overset{1}{\mapsto} l^x * \exists \mathsf{R}_{u.e}. \\ [\mathcal{L}]^{\mathsf{R}_{u.e}}_{\frac{1}{2}} * [\mathcal{U}]^{\mathsf{R}_{u.e}}_{1} * \boxed{u^x.eL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}}}^{\mathsf{R}_{u.e}}_{\mathsf{EC}(\mathsf{R}_{u.e}, u^x)} \end{array} \right) \\
\vee \left(r^x = \mathsf{null} \wedge u^x = \mathsf{null} \wedge [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}} \right)
\end{array} \right) \\
* \mathsf{var}(\mathtt{n}, n) * \mathsf{var}(\mathtt{l}, l^x) * \mathsf{var}(\mathtt{u}, u^x) * \mathsf{var}(\mathtt{r}, r^x) * \mathsf{var}(\mathtt{d}, d)
\end{array} \right\} \right\}
$$

$$
\begin{array}{l}
\texttt{if l} \neq \mathsf{null}\ \texttt{then unlock(l.rightL) else if u} \neq \mathsf{null}\ \texttt{then unlock(u.firstL)}\,; \\
\texttt{if r} \neq \mathsf{null}\ \texttt{then unlock(r.leftL) else if u} \neq \mathsf{null}\ \texttt{then unlock(u.lastL)}\,; \\
\left\{
\begin{array}{l}
\bigvee_{I \in SI\downarrow} \left\{\ I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x)\ *\ \mathsf{tree}\,(I \uplus I_2, \mathbf{x}, \varnothing)\ \wedge\ I_2 \in \mathcal{I}_D * {I_2}^{\mathsf{in}}(\mathbf{x}) \doteq (r^x, l^x)\ \right\} \\
*n.l \to - * \exists \mathsf{R}_{n.l}.\ \boxed{[\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{3}{4}}}\ [\mathcal{L}]^{\mathsf{R}_{n.l}}_1 * [\mathcal{U}]^{\mathsf{R}_{n.l}}_1 * \boxed{n.lL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{LC}(\mathsf{R}_{n.l}, n, u^x)}}^{\mathsf{R}_{n.l}} \\
*n.r \to - * \exists \mathsf{R}_{n.r}.\ * \boxed{[\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{3}{4}}} * [\mathcal{L}]^{\mathsf{R}_{n.r}}_1 * [\mathcal{U}]^{\mathsf{R}_{n.r}}_1 * \boxed{n.rL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}}}^{\mathsf{RC}(\mathsf{R}_{n.r}, n, u^x)}}^{\mathsf{R}_{n.r}} \\
\times \{\mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, -) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, d)\}
\end{array}
\right\} \\
\left\{
\begin{array}{l}
\bigvee_{I \in SI\downarrow} \left\{\ \boxed{\langle \mathsf{tree}\,(\mathbf{x}, \varnothing)\rangle^{I \uplus I_2}}\ \wedge\ I_2 \in \mathcal{I}_D\ \right\} \\
*n.l \to - * \exists \mathsf{R}_{n.l}.\ [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{3}{4}} [\mathcal{L}]^{\mathsf{R}_{n.l}}_1 * [\mathcal{U}]^{\mathsf{R}_{n.l}}_1 * \boxed{n.lL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{LC}(\mathsf{R}_{n.l}, n, u^x)}}^{\mathsf{R}_{n.l}} \\
*n.r \to - * \exists \mathsf{R}_{n.r}.\ * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{3}{4}} * [\mathcal{L}]^{\mathsf{R}_{n.r}}_1 * [\mathcal{U}]^{\mathsf{R}_{n.r}}_1 * \boxed{n.rL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}}}^{\mathsf{RC}(\mathsf{R}_{n.r}, n, u^x)}}^{\mathsf{R}_{n.r}} \\
*\exists d, e.\ n.d \to d * n.dL \to 0 * n.e \to e * n.eL \to 0 * \|t\|^{(d,e)(\mathsf{null}, n, \mathsf{null})} * n.u \to - \\
\times \{\mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, -) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, d)\}
\end{array}
\right\} \\
\left\{\ \|t\|^{(d,e)(\mathsf{null}, n, \mathsf{null})} \times \{\mathsf{var}\,(\mathtt{d}, d)\}\ \right\}\ \ \texttt{disposeForest(d)}\ \ \left\{\ \mathrm{emp} \times \{\mathsf{var}\,(\mathtt{d}, -)\}\ \right\} \\
\left\{
\begin{array}{l}
\bigvee_{I \in SI\downarrow} \left\{\ \langle \mathsf{tree}\,(\mathbf{x}, \varnothing)\rangle^{I \uplus I_2}\ \wedge\ I_2 \in \mathcal{I}_D\ \right\} \\
*n.l \to - * \exists \mathsf{R}_{n.l}.\ [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{3}{4}} [\mathcal{L}]^{\mathsf{R}_{n.l}}_1 * [\mathcal{U}]^{\mathsf{R}_{n.l}}_1 * \boxed{n.lL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{LC}(\mathsf{R}_{n.l}, n, u^x)}}^{\mathsf{R}_{n.l}} \\
*n.r \to - * \exists \mathsf{R}_{n.r}.\ * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{3}{4}} * [\mathcal{L}]^{\mathsf{R}_{n.r}}_1 * [\mathcal{U}]^{\mathsf{R}_{n.r}}_1 * \boxed{n.rL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}}}^{\mathsf{RC}(\mathsf{R}_{n.r}, n, u^x)}}^{\mathsf{R}_{n.r}} \\
*n.d \to - * n.dL \to 0 * n.e \to - * n.eL \to 0 * n.u \to - \\
\times \{\mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, -) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, -)\}
\end{array}
\right\} \\
//\text{Use the } [\mathcal{W}] \text{ tokens on } \mathsf{R}_{n.lL} \text{ and } \mathsf{R}_{n.rL}. \\
\left\{
\begin{array}{l}
\bigvee_{I \in SI\downarrow} \left\{\ \langle \mathsf{tree}\,(\mathbf{x}, \varnothing)\rangle^{I \uplus I_2}\ \wedge\ I_2 \in \mathcal{I}_D\ \right\} \\
*n.l \to - * \exists \mathsf{R}_{n.l}.\ \boxed{[\mathcal{W}]^{\mathsf{R}_{n.l}}_1} * [\mathcal{L}]^{\mathsf{R}_{n.l}}_1 * [\mathcal{U}]^{\mathsf{R}_{n.l}}_1 * \boxed{n.lL \to 1 * \boxed{n.l \to l^x * n.u \overset{\frac{1}{4}}{\mapsto} u^x}}^{\mathsf{LC}(\mathsf{R}_{n.l}, n, u^x)}}^{\mathsf{R}_{n.l}} \\
*n.r \to - * \exists \mathsf{R}_{n.r}.\ \boxed{[\mathcal{W}]^{\mathsf{R}_{n.r}}_1} * [\mathcal{L}]^{\mathsf{R}_{n.r}}_1 * [\mathcal{U}]^{\mathsf{R}_{n.r}}_1 * \boxed{n.rL \to 1 * \boxed{n.r \to r^x * n.u \overset{\frac{1}{4}}{\mapsto} u^x}}^{\mathsf{RC}(\mathsf{R}_{n.r}, n, u^x)}}^{\mathsf{R}_{n.r}} \\
*n.d \to - * n.dL \to 0 * n.e \to - * n.eL \to 0 * n.u \to - \\
\times \{\mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, -) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, -)\}
\end{array}
\right\} \\
//\text{Destroy the } \mathsf{R}_{n.r} \text{ and } \mathsf{R}_{n.l} \text{ regions since we have all tokens on them.} \\
\left\{
\begin{array}{l}
\bigvee_{I \in SI\downarrow} \left\{\ \langle \mathsf{tree}\,(\mathbf{x}, \varnothing)\rangle^{I \uplus I_2}\ \wedge\ I_2 \in \mathcal{I}_D\ \right\} * \\
\boxed{n.lL \to 1 * n.l \to l^x * n.rL \to 1 * n.r \to r^x * n.u \overset{1}{\mapsto} -} * n.d \to - * n.dL \to 0 * n.e \to - * n.eL \to 0 \\
\times \{\mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, -) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, -)\}
\end{array}
\right\} \\
\texttt{disposeNode(n)} \\
\left\{\ \bigvee_{I \in SI\downarrow} \left\{\ \langle \mathsf{tree}\,(\mathbf{x}, \varnothing)\rangle^{I \uplus I_2}\ \wedge\ I_2 \in \mathcal{I}_D\ \right\} \times \{\mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, -) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, -)\}\ \right\} \\
\}
\end{array}
$$

$$
\left\{\ \bigvee_{I \in SI\downarrow} \left(\langle \mathsf{tree}\,(\mathbf{x}, \varnothing)\rangle^{I \uplus I_2}\ \wedge\ I_2 \in \mathcal{I}_D\right)\ \times \{\mathsf{var}\,(\mathtt{n}, n)\}\ \right\}
$$

4. Deadlock-Free Tree Translation $\theta : \mathbb{T} \to \mathbb{C}$

Definition 22 (Tree heap translation function)**.** The tree heap representation function:

$$\langle (\cdot) \rangle^I : \mathcal{H}_{\mathbb{T}} \to \mathcal{I}_\theta \to \wp(\mathcal{M}_{\mathbb{C}})$$

is defined by induction over the structure of tree segments as:

$$\begin{array}{rcl}
\langle \mathbf{0}_{\mathbb{T}} \rangle^I & \triangleq & \mathrm{emp} \\
\langle \mathsf{tree}\,(\mathcal{R}, t) \rangle^I & \triangleq & \mathsf{tree}\,(I, \mathcal{R}, t) \\
\langle \mathsf{tree}\,(\mathbf{x}, t) \rangle^I & \triangleq & \mathsf{tree}\,(I, \mathbf{x}, t) \\
\langle h_1 \bullet_{\mathbb{T}} h_2 \rangle^I & \triangleq & \exists I_1, I_2.\, I_1 \cup I_2 = I \ \wedge\ \langle h_1 \rangle^{I_1} \bullet_{\mathbb{C}} \langle h_2 \rangle^{I_2}
\end{array}$$

with

$$\begin{array}{rcl}
\mathsf{tree}\,(I, \mathcal{R}, t) & \triangleq & \exists i, j.\, \mathsf{treeFrag}\,(I, t)\,(i, j)\,(\mathsf{null}, \mathsf{null}, \mathsf{null})\,(1) \\
\mathsf{tree}\,(I, \mathbf{x}, t) & \triangleq & \mathsf{treeFrag}\,(I, t)\,(i^x, j^x)\,(l^x, u^x, r^x)\,(\pi^x)\ \wedge \\
 & & I^{\mathsf{in}}(\mathbf{x}) \doteq (i^x, j^x)\ \wedge\ I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x, \pi^x) \\
 & & \\
\mathsf{treeFrag}\,(I, \varnothing)\,(i, j)\,(l, u, r)\,(\pi) & \triangleq & (i = r) \wedge (j = l) \wedge \mathsf{isPLock}\,(u, \pi) * \\
 & & \big((l = u = r = \mathsf{null} \wedge \mathcal{R} \to i) \vee \mathrm{emp}\big) \\
\mathsf{treeFrag}\,(I, \mathbf{x})\,(i, j)\,(l, u, r)\,(\pi) & \triangleq & I^{\mathsf{in}}\mathbf{x} \doteq (i, j)\ \wedge\ I^{\mathsf{out}}(\mathbf{x}) \doteq (l, u, r, \pi) \\
\mathsf{treeFrag}\,(I, t_1 \otimes t_2)\,(i, j)\,(l, u, r)\,(\pi) & \triangleq & \exists p, q, \pi_1, \pi_2.\ \pi = \pi_1 + \pi_2 \wedge \\
 & & \mathsf{treeFrag}\,(I, t_1)\,(i, p)\,(l, u, q)\,(\pi_1) \\
 & & * \mathsf{treeFrag}\,(I, t_1)\,(q, j)\,(p, u, r)\,(\pi_2) \\
\mathsf{treeFrag}\,(I, n[t])\,(i, j)\,(l, u, r)\,(\pi) & \triangleq & i = j = n \wedge n.u \to u * \mathsf{isPLock}\,(u, \pi) \\
 & & * \begin{pmatrix} (u \neq \mathsf{null} \wedge n.uL \to u.nL) \\ \vee (u = \mathsf{null} \wedge n.uL \to \mathcal{R} + 1) \end{pmatrix} \\
 & & * \mathsf{Left}\,(n, l, u) * \mathsf{First}\,(n, d) \\
 & & * \mathsf{Last}\,(n, e) * \mathsf{Right}\,(n, r, u) \\
 & & * \exists d, e, \pi_1, \pi_2.\, \pi_1 + \pi_2 = 1 \wedge \\
 & & \mathsf{isPLock}\,(n, \pi_1) \\
 & & * \mathsf{treeFrag}\,(I, t)\,(d, e)\,(\mathsf{null}, n, \mathsf{null})\,(\pi_2)
\end{array}$$

For readability we use the the following shorthands in the definitions above:

$$\begin{array}{rcll} n.l & \triangleq & n & //\text{the left sibling} \\ n.u & \triangleq & n+1 & //\text{the parent of the node} \\ n.d & \triangleq & n+2 & //\text{the first child} \\ n.e & \triangleq & n+3 & //\text{the last child} \\ n.r & \triangleq & n+4 & //\text{the right sibling} \\ n.lL & \triangleq & n+5 & //\text{the left sibling lock} \\ n.uL & \triangleq & n+6 & //\text{the parent lock} \\ n.dL & \triangleq & n+7 & //\text{the first child lock} \\ n.eL & \triangleq & n+8 & //\text{the last child lock} \\ n.rL & \triangleq & n+9 & //\text{the right sibling lock} \\ n.nL & \triangleq & n+10 & //\text{the node lock} \end{array}$$

The predicates used in the above translation are defined as:

$$\mathsf{isLock}\,(a,\pi) \triangleq \exists \mathsf{R}, \pi'.\, [\mathcal{L}]^{\mathsf{R}}_{\pi} * \boxed{\begin{array}{l} \left(a \to 0 * [\mathcal{U}]^{\mathsf{R}}_{1}\right) \\ \left(a \to 1 * [\mathcal{L}]^{\mathsf{R}}_{\pi'} * [\mathcal{U}]^{\mathsf{R}}_{1-\pi'}\right) \end{array}}^{\mathsf{R}}_{\mathsf{L}(\mathsf{R},a)}$$

$$\mathsf{isPLock}\,(u,\pi) \triangleq \begin{pmatrix} (u \neq \mathsf{null} \wedge \mathsf{isLock}\,(u.nL,\pi)) \\ \vee (u = \mathsf{null} \wedge \mathsf{isLock}\,(\mathcal{R}+1,\pi)) \end{pmatrix}$$

$$\mathsf{Locked}\,(a,\pi) \triangleq \exists \mathsf{R}.\, [\mathcal{U}]^{\mathsf{R}}_{\pi} * \boxed{a \to 1 * [\mathcal{L}]^{\mathsf{R}}_{\pi} * [\mathcal{U}]^{\mathsf{R}}_{1-\pi}}^{\mathsf{R}}_{\mathsf{L}(\mathsf{R},a)}$$

$$\mathsf{PLocked}\,(u,\pi) \triangleq \begin{pmatrix} (u \neq \mathsf{null} \wedge \mathsf{Locked}\,(u.nL,\pi)) \\ \vee (u = \mathsf{null} \wedge \mathsf{Locked}\,(\mathcal{R}+1,\pi)) \end{pmatrix}$$

$$\mathsf{L}(\mathsf{R},a) \triangleq \begin{cases} [\mathcal{L}]: & a \to 0 * [\mathcal{U}]^{\mathsf{R}}_{1} \rightsquigarrow \exists \pi.\, a \to 1 * [\mathcal{L}]^{\mathsf{R}}_{\pi} * [\mathcal{U}]^{\mathsf{R}}_{1-\pi} \\ & a \to 0 * [\mathcal{U}]^{\mathsf{R}}_{1} \rightsquigarrow [\mathcal{L}]^{\mathsf{R}}_{1} * [\mathcal{U}]^{\mathsf{R}}_{1} \\ [\mathcal{U}]: & a \to 1 * [\mathcal{L}]^{\mathsf{R}}_{\pi} * [\mathcal{U}]^{\mathsf{R}}_{1-\pi} \rightsquigarrow a \to 0 * [\mathcal{U}]^{\mathsf{R}}_{1} \\ & \mathsf{Init}\,(a) \rightsquigarrow a \to 0 * [\mathcal{U}]^{\mathsf{R}}_{1} \end{cases}$$

$$\mathsf{Init}\,(a) \triangleq \begin{pmatrix} (a \neq \mathcal{R}+1 \wedge \circledast^{a}_{l=a-10} l \to -) \\ \vee (a = \mathcal{R}+1 \wedge \circledast^{a}_{l=a-1} l \to -) \end{pmatrix}$$

$$
\begin{aligned}
\mathsf{Left}\,(n,l,u) &\triangleq \mathsf{ownsR}\,(l,n,u,1) * \mathsf{isLLock}\left(n,u,\tfrac{1}{2}\right)\\
\mathsf{isLLock}\,(n,u,\pi) &\triangleq \exists \mathsf{R}, l.\, [\mathcal{A}]^{\mathsf{R}}_{\pi} *\\
&\qquad \boxed{\begin{array}{l}\mathsf{LUnlocked}\,(\mathsf{R},n,l,u) \vee \mathsf{LAcquired}\,(\mathsf{R},n,l,u)\\ \vee \mathsf{LLocked}\,(\mathsf{R},n,l,u)\end{array}}^{\mathsf{R}}_{\mathsf{LC}(\mathsf{R},n,u)}\\
\mathsf{LUnlocked}\,(\mathsf{R},n,l,u) &\triangleq n.lL \to 0 * [\mathcal{U}]^{\mathsf{R}}_1 * \in^{\mathsf{R},n,l,u} * [\mathcal{L}]^{\mathsf{R}}_1\\
\mathsf{LAcquired}\,(\mathsf{R},n,l,u) &\triangleq n.lL \to 0 * [\mathcal{U}]^{\mathsf{R}}_1 * \in^{\mathsf{R},n,l,u} * \mathsf{PLocked}\,(u,-) * \mathsf{LWit}\,(l,n,u)\\
\mathsf{LLocked}\,(\mathsf{R},n,l,u) &\triangleq n.lL \to 1 * \mathsf{LWit}\,(l,n,u)\\
\mathsf{ownsR}\,(l,n,u,\pi) &\triangleq \exists \mathsf{R}.\, [\mathcal{W}]^{\mathsf{R}}_{\pi} *\\
&\qquad \boxed{\begin{array}{l}\mathsf{LUnlocked}\,(\mathsf{R},n,l,u) \vee \mathsf{LAcquired}\,(\mathsf{R},n,l,u)\\ \vee \mathsf{LLocked}\,(\mathsf{R},n,l,u)\end{array}}^{\mathsf{R}}_{\mathsf{LC}(\mathsf{R},n,u)}\\
\mathsf{LWit}\,(l,n,u) &\triangleq \mathsf{ownsR}\left(l,n,u,\tfrac{1}{2}\right) \vee\\
&\qquad \begin{pmatrix}(l \neq \mathsf{null} \wedge \mathsf{ownsL}\left(l,n,u,\frac{1}{2}\right))\\ \vee (l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{ownsD}\left(u,n,\frac{1}{2}\right))\end{pmatrix}\\
\mathsf{LInit}\,(n,l,u) &\triangleq n.lL \to - * n.u \overset{\frac{1}{4}}{\mapsto} -\\
&\qquad * \begin{pmatrix} n.l \to l\\ \vee (l \neq \mathsf{null} \wedge l.u \overset{\frac{1}{4}}{\mapsto} -)\\ \vee (l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.u \overset{\frac{1}{4}}{\mapsto} -)\end{pmatrix}\\
\mathsf{LC}(\mathsf{R},n,u) &\triangleq \begin{cases}
[\mathcal{L}]: & \mathsf{LAcquired}\,(\mathsf{R},n,l,u) \rightsquigarrow \mathsf{LLocked}\,(\mathsf{R},n,l,u)\\
[\mathcal{U}]: & \mathsf{LLocked}\,(\mathsf{R},n,l,u) \rightsquigarrow \mathsf{LUnlocked}\,(\mathsf{R},n,l,u)\\
[\mathcal{A}]: & \mathsf{LUnlocked}\,(\mathsf{R},n,l,u) \rightsquigarrow \mathsf{LAcquired}\,(\mathsf{R},n,l,u)\\
[\mathcal{W}]: & \begin{array}{l}\mathsf{LInit}\,(n,l,u) \rightsquigarrow\\ \quad \mathsf{LUnlocked}\,(\mathsf{R},n,l,u) \vee \mathsf{LLocked}\,(\mathsf{R},n,l,u)\\ \mathsf{LUnlocked}\,(\mathsf{R},n,l,u) \vee \mathsf{LLocked}\,(\mathsf{R},n,l,u)\\ \quad \rightsquigarrow \mathsf{LInit}\,(n,l,u)\end{array}
\end{cases}\\
\in^{\mathsf{R},n,l,u} &\triangleq n.l \overset{\frac{1}{2}}{\mapsto} l *\\
&\qquad \begin{pmatrix}
\begin{pmatrix} l \neq \mathsf{null} \wedge l.r \overset{\frac{1}{2}}{\mapsto} n * \mathsf{isRLock}\left(l,u,\frac{1}{2}\right)\end{pmatrix}\\
\vee \begin{pmatrix} l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge\\ u.d \overset{\frac{1}{2}}{\mapsto} n * \mathsf{isDLock}\left(u,\frac{1}{2}\right)\end{pmatrix}\\
\vee \begin{pmatrix} l = \mathsf{null} \wedge u = \mathsf{null} \wedge\\ \mathcal{R} \to n * n.l \overset{\frac{1}{2}}{\mapsto} l * \mathsf{isLLock}\left(n,u,\frac{1}{2}\right)\end{pmatrix}
\end{pmatrix}
\end{aligned}
$$

$$
\begin{aligned}
\mathsf{Right}\,(n,r,u) &\triangleq \mathsf{isRLock}\left(n,u,\tfrac{1}{2}\right) * \mathsf{ownsL}\,(n,r,u,1)\\
\mathsf{isRLock}\,(n,u,\pi) &\triangleq \exists \mathsf{R}, r.\, [\mathcal{A}]^{\mathsf{R}}_{\pi} *\\
&\quad \boxed{\begin{array}{l}\mathsf{RUnlocked}\,(n,r,u) \vee \mathsf{RLocked}\,(n,r,u)\\ \vee\ \mathsf{RInit}\,(n,r,u)\end{array}}^{\mathsf{R}}_{\mathsf{LC}(\mathsf{R},n,u)}\\
\mathsf{RUnlocked}\,(n,r,u) &\triangleq \begin{array}{l}\exists \pi.\, n.rL \to 0 * [\mathcal{U}]^{\mathsf{R}}_1 * \ni^{n,r,u}\\ * \left([\mathcal{L}]^{\mathsf{R}}_1 \vee (\mathsf{PLocked}\,(u,\pi) * \mathsf{RWit}\,(n,r,u))\right)\end{array}\\
\mathsf{RLocked}\,(n,r,u) &\triangleq n.rL \to 1 * \mathsf{RWit}\,(n,r,u)\\
\mathsf{ownsL}\,(n,r,u,\pi) &\triangleq \exists \mathsf{R}.\, [\mathcal{W}]^{\mathsf{R}}_{\pi} *\\
&\quad \boxed{\begin{array}{l}\mathsf{RUnlocked}\,(n,r,u) \vee \mathsf{RLocked}\,(n,r,u)\\ \vee\ \mathsf{RInit}\,(n,r,u)\end{array}}^{\mathsf{R}}_{\mathsf{LC}(\mathsf{R},n,u)}\\
\mathsf{RWit}\,(n,r,u) &\triangleq \mathsf{ownsL}\left(n,r,u,\tfrac{1}{2}\right) \vee\\
&\quad \left(\begin{array}{l}(r \neq \mathsf{null} \wedge \mathsf{ownsR}\left(n,r,u,\frac{1}{2}\right))\\ \vee(r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{ownsE}\left(u,n,\frac{1}{2}\right))\end{array}\right)\\
\mathsf{RInit}\,(n,r,u) &\triangleq n.rL \to - * n.u \overset{\frac{1}{4}}{\mapsto} -\\
&\quad * \begin{pmatrix} n.r \to r\\ \vee(r \neq \mathsf{null} \wedge r.u \overset{\frac{1}{4}}{\mapsto} -)\\ (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.u \overset{\frac{1}{4}}{\mapsto} -)\end{pmatrix}\\
\mathsf{RC}(\mathsf{R},n,u) &\triangleq \begin{cases}
[\mathcal{L}]: & n.rL \to 0 * [\mathcal{U}]^{\mathsf{R}}_1 * \ni^{n,r,u} * \mathsf{PLocked}\,(u,-)\\
& \quad \rightsquigarrow n.rL \to 1\\
[\mathcal{U}]: & n.rL \to 1 * \mathsf{RWit}\,(n,r,u) \rightsquigarrow\\
& \quad n.rL \to 0 * [\mathcal{U}]^{\mathsf{R}}_1 * \ni^{n,r',u} * [\mathcal{L}]^{\mathsf{R}}_1\\
[\mathcal{A}]: & [\mathcal{L}]^{\mathsf{R}}_1 \rightsquigarrow \mathsf{PLocked}\,(u,-) * \mathsf{RWit}\,(n,-,u)\\
[\mathcal{W}]: & \mathsf{RInit}\,(n,r,u) \rightsquigarrow\\
& \quad \mathsf{RUnlocked}\,(n,r,u) \vee \mathsf{RLocked}\,(n,r,u)\\
& \mathsf{RUnlocked}\,(n,r,u) \vee \mathsf{RLocked}\,(n,r,u)\\
& \quad \rightsquigarrow \mathsf{RInit}\,(n,r,u)
\end{cases}\\
\ni^{n,r,u} &\triangleq n.r \overset{\frac{1}{2}}{\mapsto} r *\\
&\quad \left(\begin{array}{l}\left(\begin{array}{l} r \neq \mathsf{null} \wedge\\ r.l \overset{\frac{1}{2}}{\mapsto} n * \mathsf{isLLock}\left(r,u,\frac{1}{2}\right)\end{array}\right)\\ \vee\left(\begin{array}{l} r = \mathsf{null} \wedge\\ u.e \overset{\frac{1}{2}}{\mapsto} n * \mathsf{isELock}\left(u,\frac{1}{2}\right)\end{array}\right)\\ \vee\left(\begin{array}{l} r = \mathsf{null} \wedge u = \mathsf{null} \wedge\\ n.r \overset{\frac{1}{2}}{\mapsto} r * \mathsf{isRLock}\left(n,u,\frac{1}{2}\right)\end{array}\right)\end{array}\right)
\end{aligned}
$$

$$
\begin{aligned}
\mathsf{First}\,(n,d) &\triangleq \mathsf{isDLock}\left(n,\tfrac{1}{2}\right) * \mathsf{ownsD}\,(n,d,1)\\
\mathsf{isDLock}\,(n,\pi) &\triangleq \exists \mathsf{R}, d.\,[\mathcal{A}]^{\mathsf{R}}_{\pi} *\\
&\qquad \boxed{\begin{array}{l}\mathsf{DUnlocked}\,(n,d) \vee \mathsf{DLocked}\,(n,d)\\ \vee\ \mathsf{DInit}\,(n,d)\end{array}}^{\mathsf{R}}_{\mathsf{DC}(\mathsf{R},n)}\\
\mathsf{DUnlocked}\,(n,d) &\triangleq \begin{array}{l}\exists \pi.\, n.dL \to 0 * [\mathcal{U}]^{\mathsf{R}}_1 * \Subset^{n,d}\\ * \left([\mathcal{L}]^{\mathsf{R}}_1 \vee (\mathsf{PLocked}\,(u,\pi) * \mathsf{DWit}\,(n,d))\right)\end{array}\\
\mathsf{DLocked}\,(n,d) &\triangleq n.dL \to 1 * \mathsf{DWit}\,(n,d)\\
\mathsf{DWit}\,(n,d) &\triangleq \mathsf{ownsD}\left(n,d,\tfrac{1}{2}\right) \vee (d \neq \mathsf{null} \wedge \mathsf{ownsR}\,(\mathsf{null},d,n,\mathsf{null})\ \tfrac{1}{2})\\
\mathsf{ownsD}\,(n,d,\pi) &\triangleq \exists \mathsf{R}.\,[\mathcal{W}]^{\mathsf{R}}_{\pi} *\\
&\qquad \boxed{\begin{array}{l}\mathsf{DUnlocked}\,(n,d) \vee \mathsf{DLocked}\,(n,d)\\ \vee\ \mathsf{DInit}\,(n,d)\end{array}}^{\mathsf{R}}_{\mathsf{DC}(\mathsf{R},n)}\\
\mathsf{DC}(\mathsf{R},n) &\triangleq \begin{cases}
[\mathcal{L}]: & n.dL \to 0 * [\mathcal{U}]^{\mathsf{R}}_1 * \Subset^{n,d} * \mathsf{PLocked}\,(u,-)\\ & \quad \rightsquigarrow n.dL \to 1\\
[\mathcal{U}]: & n.dL \to 1 * \mathsf{DWit}\,(n,d) \rightsquigarrow\\ & \quad n.dL \to 0 * [\mathcal{U}]^{\mathsf{R}}_1 * \Subset^{n,d'} * [\mathcal{L}]^{\mathsf{R}}_1\\
[\mathcal{A}]: & [\mathcal{L}]^{\mathsf{R}}_1 \rightsquigarrow \mathsf{PLocked}\,(n,\mathsf{null}) -\!\!* \mathsf{DWit}\,(n,-)\\
[\mathcal{W}]: & \mathsf{DInit}\,(n,d) \rightsquigarrow\\ & \quad \mathsf{DUnlocked}\,(n,d) \vee \mathsf{DLocked}\,(n,d)\\ & \mathsf{DUnlocked}\,(n,d) \vee \mathsf{DLocked}\,(n,d)\\ & \quad \rightsquigarrow \mathsf{DInit}\,(n,d)
\end{cases}\\
\mathsf{DInit}\,(n,d) &\triangleq n.dL \to - * n.u \overset{\frac{1}{4}}{\mapsto} -\\
&\qquad * \left(\begin{array}{l} n.d \to d\\ \\ \vee (d \neq \mathsf{null} \wedge d.u \overset{\frac{1}{4}}{\mapsto} -)\end{array}\right)\\
\Subset^{n,d} &\triangleq n \overset{\frac{1}{2}}{\mapsto} d *\\
&\qquad \left(\begin{array}{l}\left(\begin{array}{l} d \neq \mathsf{null} \wedge\\ \\ d.l \overset{\frac{1}{2}}{\mapsto} \mathsf{null} * \ \mathsf{isLLock}\left(d,n,\frac{1}{2}\right)\end{array}\right)\\ \vee \left(\begin{array}{l} d = \mathsf{null} \wedge\\ \\ n.d \overset{\frac{1}{2}}{\mapsto} d * \ \mathsf{isDLock}\left(n,\frac{1}{2}\right)\end{array}\right)\end{array}\right)
\end{aligned}
$$

$$
\begin{aligned}
\mathsf{Last}\,(n,e) &\triangleq \mathsf{isELock}\left(n,\tfrac{1}{2}\right) * \mathsf{ownsE}\,(n,e,1)\\
\mathsf{isELock}\,(n,\pi) &\triangleq \exists \mathsf{R}, e.\, [\mathcal{A}]^{\mathsf{R}}_{\pi} *\\
&\qquad \boxed{\begin{array}{l}\mathsf{EUnlocked}\,(n,e) \vee \mathsf{ELocked}\,(n,e)\\ \vee\ \mathsf{EInit}\,(n,e)\end{array}}^{\mathsf{R}}_{\mathsf{EC}(\mathsf{R},n)}\\
\mathsf{EUnlocked}\,(n,e) &\triangleq \begin{array}{l}\exists \pi.\, n.eL \to 0 * [\mathcal{U}]^{\mathsf{R}}_1 * \circledcirc^{n,e}\\ * \left([\mathcal{L}]^{\mathsf{R}}_1 \vee (\mathsf{PLocked}\,(u,\pi) * \mathsf{EWit}\,(n,e))\right)\end{array}\\
\mathsf{ELocked}\,(n,e) &\triangleq n.eL \to 1 * \mathsf{EWit}\,(n,e)\\
\mathsf{ownsE}\,(n,e,\pi) &\triangleq \exists \mathsf{R}.\, [\mathcal{W}]^{\mathsf{R}}_{\pi} *\\
&\qquad \boxed{\begin{array}{l}\mathsf{EUnlocked}\,(n,e) \vee \mathsf{ELocked}\,(n,e)\\ \vee\ \mathsf{EInit}\,(n,e)\end{array}}^{\mathsf{R}}_{\mathsf{EC}(\mathsf{R},n)}\\
\mathsf{EWit}\,(n,e) &\triangleq \mathsf{ownsE}\left(n,e,\tfrac{1}{2}\right) \vee (e \neq \mathsf{null} \wedge \vee \mathsf{ownsL}\,(e,\mathsf{null},n,\mathsf{null})\,\tfrac{1}{2})\\
\mathsf{EInit}\,(n,e) &\triangleq n.eL \to - * n.u \overset{\frac{1}{4}}{\mapsto} -\\
&\qquad * \left(\begin{array}{l} n.e \to e\\ \\ \vee (e \neq \mathsf{null} \wedge e.u \overset{\frac{1}{4}}{\mapsto} -)\end{array}\right)\\
\mathsf{EC}(\mathsf{R},n) &\triangleq \begin{cases}
[\mathcal{L}]: & n.eL \to 0 * [\mathcal{U}]^{\mathsf{R}}_1 * \circledcirc^{n,e} * \mathsf{PLocked}\,(u,-)\\
& \quad \rightsquigarrow n.eL \to 1\\
[\mathcal{U}]: & n.eL \to 1 * \mathsf{EWit}\,(n,e) \rightsquigarrow\\
& \quad n.eL \to 0 * [\mathcal{U}]^{\mathsf{R}}_1 * \circledcirc^{n,e'} * [\mathcal{L}]^{\mathsf{R}}_1\\
[\mathcal{A}]: & [\mathcal{L}]^{\mathsf{R}}_1 \rightsquigarrow \mathsf{PLocked}\,(n,\mathsf{null}) - * \mathsf{EWit}\,(n,-)\\
[\mathcal{W}]: & \begin{array}{l}\mathsf{EInit}\,(n,e) \rightsquigarrow\\ \quad \mathsf{EUnlocked}\,(n,e) \vee \mathsf{ELocked}\,(n,e)\\ \mathsf{EUnlocked}\,(n,e) \vee \mathsf{ELocked}\,(n,e)\\ \quad \rightsquigarrow \mathsf{EInit}\,(n,e)\end{array}
\end{cases}\\
\circledcirc^{n,e} &\triangleq n \overset{\frac{1}{2}}{\mapsto} e *\\
&\qquad \left(\begin{array}{l}\left(\begin{array}{l} e \neq \mathsf{null} \wedge\\ \\ e.r \overset{\frac{1}{2}}{\mapsto} \mathsf{null} * \mathsf{isRLock}\left(e,n,\frac{1}{2}\right)\end{array}\right)\\ \vee \left(\begin{array}{l} e = \mathsf{null} \wedge\\ \\ n.e \overset{\frac{1}{2}}{\mapsto} e * \mathsf{isELock}\left(n,\frac{1}{2}\right)\end{array}\right)\end{array}\right)
\end{aligned}
$$

Definition 23 (Interfaces)**.** The sets of *inner* and *outer interfaces* associ-

ated with abstract addresses of tree heaps are defined as:

$$\textsc{In}_\theta \triangleq (\mathbb{N}^+ \uplus \{\mathsf{null}\})^2 \qquad\qquad \textsc{Out}_\theta \triangleq (\mathbb{N}^+ \uplus \{\mathsf{null}\})^3 \times \{(0,1]\}$$

while the set of *inner* and *outer interface functions* are defined as $\mathcal{I}_\theta^{\mathsf{in}} : \wp(\textsc{SAdd} \rightharpoonup \textsc{In}_\theta)$, and $\mathcal{I}_\theta^{\mathsf{out}} : \wp(\textsc{SAdd} \rightharpoonup \textsc{Out}_\theta)$, respectively. The set of interface function pairs is then given as the Cartesian product of the two: $\mathcal{I}_\theta : \mathcal{I}_\theta^{\mathsf{in}} \times \mathcal{I}_\theta^{\mathsf{out}}$.

Definition 24 (Stable Interface Functions)**.** Given the sets of inner and outer interfaces $\textsc{In}_\theta$, $\textsc{Out}_\theta$ (def. 23), the *set of stable inner-interface functions* $\mathcal{SI}_\theta{}^{\mathsf{in}} : \wp(\textsc{SAdd} \rightharpoonup \wp(\textsc{In}_\theta))$, and the *set of stable outer-interface functions* $\mathcal{SI}_\theta{}^{\mathsf{out}} : \wp(\textsc{SAdd} \rightharpoonup \wp(\textsc{Out}_\theta))$ consist of interface functions mapping abstract addresses to a set of possible inner and outer interfaces, respectively. The Cartesian product of the two forms the set of stable interface function pairs $\mathcal{SI}_\theta \triangleq \mathcal{SI}_\theta{}^{\mathsf{in}} \times \mathcal{SI}_\theta{}^{\mathsf{out}}$. Given a stable interface function pair SI, we write SI^{in} and SI^{out} for the first and second projections.

Definition 25 (Implementation Function)**.** The implementation function

$$[\![.]\!]_\theta : \textsc{Atom}_{\mathbb{T}} \to \textsc{Prog}_{\mathbb{C}}$$

provides an implementation for each atomic command of tree library $\mathbb{T}$ as a correspondingly named procedure given in Figures 4.1, 4.2 and 4.3 with:

```
  x.left  ≜  x
    x.up  ≜  x + 1
 x.first  ≜  x + 2
  x.last  ≜  x + 3
 x.right  ≜  x + 4
 x.leftL  ≜  x + 6
   x.upL  ≜  x + 7
x.firstL  ≜  x + 8
 x.lastL  ≜  x + 9
x.rightL  ≜  x + 10
 x.nodeL  ≜  x + 11
```

We have now defined all necessary components for formalising the translation.

Definition 26 (Translation)**.** The translation $\theta : \mathbb{T} \to \mathbb{C}$ is a 4-tuple of the set of interfaces, the set of stable interface function pairs, the tree heap translation function and the implementation function: $\Big((\textsc{In}_\theta \times \textsc{Out}_\theta), \mathcal{SI}_\theta, \langle . \rangle^{(\cdot)}, [\![.]\!]_\theta\Big)$.

```
proc n := getUp(m){
  n := [m.up]
}
proc n := getLeft(m){
  n:= [m.left]
}
proc n := getRight(m){
  n:= [m.right]
}

proc n := getFirst(m){
  n:= [m.first]
}
proc n := getLast(m){
  n:= [m.last]
}
proc n := newNode(){
  n:= alloc(11) ;
  n.leftL := 1 ;
  n.rightL := 1 ;
  n.firstL := 1 ;
  n.lastL := 1 ;
  n.nodeL := 1 ;
}
proc disposeNode(n)(){
  dispose(n, 11)
}
proc lock(a){
  while(!<CAS(a, 0, 1)>)
    skip ;
}
proc unlock(a){
  <[a:= 0]> ;
}
```

```
proc newNodeAfter(n){
  local x,r,u,ul in
    u:= [n.up] ;
    ul:= [n.upL] ;
    x := newNode() ;
    [x.up]:= u ;
    [x.upL]:= ul ;
    [x.left]:= n ;
    unlock(x.leftL) ;
    [x.first]:= null ;
    unlock(x.firstL) ;
    [x.last]:= null ;
    unlock(x.lastL) ;
    unlock(x.nodeL) ;
    lock(ul) ;
    lock(n.rightL) ;
    r:= [n.right] ;
    if r ≠ null then
      lock(r.leftL)
    else if u ≠ null then
      lock(u.lastL)
    unlock(ul) ;
    [x.right]:= r ;
    unlock(x.rightL) ;
    if r ≠ null then
      [r.left]:= x ;
      unlock(r.leftL) ;
    else if u ≠ null then
      [u.last]:= x ;
      unlock(u.lastL) ;
    [n.right]:= x ;
    unlock(n.rightL)
}
```

Figure 4.1: Procedures for the translation $\theta : \mathbb{T} \to \mathbb{C}$.

```
proc deleteTree(n){
  local l,u,d,r,ul in
    u := [n.up] ; ul:= [n.upL] ;
    if u = null then t:= ul - 1 ;
    //Acquiring the necessary locks.
    lock(ul) ; lock(n.leftL) ; l:= [n.left] ;
    if l ≠ null then lock(l.rightL)
    else if u ≠ null then lock(u.firstL) ;
    lock(n.rightL) ; r:= [n.right] ;
    if r ≠ null then lock(r.leftL) ;
    else if u ≠ null then lock(u.lastL) ;
    unlock(ul) ;
    //Pointer Swinging.
    if l ≠ null then [l.right] := r ;
    else if u ≠ null then [u.first] := r ;
    else [ul-1]:= r
    if r ≠ null then [r.left] := l ;
    else if u ≠ null then [u.last] := l ;
    //Unlocking the acquired locks.
    if l ≠ null then unlock(l.rightL) ;
    else if u ≠ null then unlock(u.firstL) ;
    if r ≠ null then unlock(r.leftL) ;
    else if u ≠ null then unlock(u.lastL) ;
    d := [n.first] ; call disposeForest(d) ;
    disposeNode(n) ;
}

proc disposeForest(n){
  local r,d in
    if n ≠ null then
      r := [n.right] ;
      call disposeForest (r) ;
      d := [n.first] ;
      call disposeForest (d) ;
      disposeNode(n)
}
```

Figure 4.2: Procedures for the translation $\theta : \mathbb{T} \to \mathbb{C}$ (continued).

```
proc appendChild(m,n){
  local l,u,e,r,t,ul in
    u := [n.up] ; ul:= [n.upL] ;
    if u = null then t:= ul - 1 ;
    //Acquiring the necessary locks.
    lock(ul) ; lock(n.leftL) ; l:= [n.left] ;
    if l ≠ null then lock(l.rightL)
    else if u ≠ null then lock(u.firstL) ;
    lock(n.rightL) ; r:= [n.right] ;
    if r ≠ null then lock(r.leftL) ;
    else if u ≠ null then lock(u.lastL) ;
    unlock(ul) ;
    //Pointer Swinging.
    if l ≠ null then [l.right] := r ;
    else if u ≠ null then [u.first] := r ;
    else [t]:= r
    if r ≠ null then [r.left] := l ;
    else if u ≠ null then [u.last] := l ;
    //Unlocking the acquired locks.
    if l ≠ null then unlock(l.rightL) ;
    else if u ≠ null then unlock(u.firstL) ;
    if r ≠ null then unlock(r.leftL) ;
    else if u ≠ null then unlock(u.lastL) ;
    [n.up]:= m ; [n.upL] := m.nodeL ; [n.right]:= null ;
    lock(m.nodeL) ; lock(m.lastL) ;
    e:= [m.last] ; [n.left]:= e ;
    if e ≠ null then lock(e.rightL) ;
    else lock(m.firstL) ;
    unlock(m.nodeL) ;
    if e ≠ null then [e.right]:= n ; unlock(e.rightL) ;
    else [m.first]:= n ; unlock(m.firstL) ;
    unlock(n.leftL) ;
    [m.last]:= n ; unlock(m.lastL) ; unlock(n.rightL) ;
}
```

Figure 4.3: Procedures for the translation $\theta : \mathbb{T} \to \mathbb{C}$ (continued).

4.1 Soundness of Translation $\theta : \mathbb{T} \to \mathbb{C}$

Theorem 3 (Sound Transformation)**.** The module translation $\theta : \mathbb{T} \to \mathbb{C}$ is a sound translation.

Proof. In lemmata 6 to 8 we show that the translation $\theta : \mathbb{T} \to \mathbb{C}$ satisfies the three properties stated in theorem 1. The soundness of translation $\theta : \mathbb{T} \to \mathbb{C}$ then follows directly from theorem 1.

Lemma 6 (Monotonicity of id Relation)**.** Given the translation $\theta : \mathbb{T} \to \mathbb{C}$, for all $h_1, h_2 \in \mathcal{H}_{\mathbb{T}}$ and $I \in \mathcal{I}_\theta$:

$$\left\{\{h_1\}\right\}\ id\ \left\{\{h_2\}\right\} \implies \left\{\ \langle h_1 \rangle^I\ \right\}\ id\ \left\{\ \langle h_2 \rangle^I\ \right\}$$

Proof. Recall that the only id transitions between abstract trees pertain to abstract allocation and deallocation. Hence, it suffices to show that for all $t_1, t_2 \in \textsc{Data}_{\mathbb{T}}$, $I \in \mathcal{I}_\theta$, $\mathbf{a} \in \textsc{SAdd} \cup \{\mathcal{R}\}$ and $\mathbf{x}, \mathbf{y} \in \textsc{SAdd}$

$$\langle \mathsf{tree}\,(\mathbf{a}, t_1 \circ_{\mathbf{x}} t_2) \rangle^I \equiv \exists \mathbf{y} \in \textsc{SAdd}, in, out.\, \langle \mathsf{tree}\,(\mathbf{a}, t_1 \circ_{\mathbf{x}} \mathbf{y}) \rangle^{I'} \bullet_{\mathbb{C}} \langle \mathsf{tree}\,(\mathbf{y}, t_2) \rangle^{I'}$$

with $I' \triangleq \left(I^{\mathsf{in}}[\mathbf{y} \mapsto in], \mathbf{y} \mapsto out^{\mathsf{out}}\right)$. The proof of the above statement is provided in Appendix C.

Lemma 7 (Composition Preservation)**.** The composition operator is preserved by the translation $\theta : \mathbb{T} \to \mathbb{C}$. That is, for all $h_{\mathbb{T}}, h'_{\mathbb{T}} \in \mathcal{H}_{\mathbb{T}}$ and $I \in \mathcal{I}_\theta$:

$$\left\langle h_{\mathbb{T}} \bullet_{\mathbb{T}} h'_{\mathbb{T}} \right\rangle^I = \exists I_1, I_2.\, I_1 \cup I_2 \doteq I\ \wedge\ \langle h_{\mathbb{T}} \rangle^{I_1} \bullet_{\mathbb{C}} \left\langle h'_{\mathbb{T}} \right\rangle^{I_2}$$

Proof. This follows immediately from the definition of $\langle . \rangle^{(\cdot)}$. □

Lemma 8 (Axiom Correctness)**.** For all $\Omega \in \textsc{PEnv}$, $\mathbb{C} \in \textsc{Atom}_{\mathbb{T}}$, $(p, \mathbb{C}, q) \in \textsc{Axiom}_{\mathbb{T}}$ and $SI \in \mathcal{SI}_\theta$,

$$[\![\Omega]\!]_\theta \vDash_{\mathbb{B}} \{[\![p]\!]_{SI}\}\ \ [\![\mathbb{C}]\!]_\theta\ \ \{[\![q]\!]_{SI}\}$$

Proof. We do not give the proofs for all of the basic commands in the Tree library. We give a few examples to illustrate the techniques involved in the proof.

Axiom Correctness: `deleteTree`

Let $\mathcal{I}_D \triangleq \{I \in \mathcal{I}_\theta \mid \mathrm{dom}(I^{\mathsf{in}}) = \{\mathbf{x}\} \wedge \mathrm{dom}(I^{\mathsf{out}}) = \varnothing\}$.
Pick an arbitrary $SI \in \mathcal{SI}_\theta$. We then need to show:

$$\left\{ \left(\mathsf{var}\left(\mathtt{n}, n\right), m\right) \;\middle|\; m \in \left(\bigvee_{I \in SI\downarrow} \left(\exists I_1 \in \mathcal{I}_D . \left\langle \mathsf{tree}\left(\mathbf{x}, n[t]\right)\right\rangle^{I \uplus I_1} \right) \right) \right\}$$
$$[\![\mathtt{deleteTree(n)}]\!]_\theta$$
$$\left\{ \left(\mathsf{var}\left(\mathtt{n}, n\right), m\right) \;\middle|\; m \in \left(\bigvee_{I \in SI\downarrow} \left(\exists I_2 \in \mathcal{I}_D . \left\langle \mathsf{tree}\left(\mathbf{x}, \varnothing\right)\right\rangle^{I \uplus I_2} \right) \right) \right\}$$

Pick $I_1, I_2 \in \mathcal{I}_\tau$ such that ${I_1}^{\mathsf{in}}(\mathbf{x}) = (n, n)$ and ${I_2}^{\mathsf{in}}(\mathbf{x}) = (r^x, l^x)$. We give a proof outline below showing that the implementation of `deleteTree` satisfies its specification.

$$\left\{ \bigvee_{I \in SI\downarrow} \left(\langle \mathsf{tree}\,(\mathbf{x}, n[t]) \rangle^{I \uplus I_1} \ \wedge \ addrs\,(t) = \varnothing \right) \ \times \{\mathsf{var}\,(\mathtt{n}, n)\} \ \right\}$$

```
proc deleteTree(n){
```

$$\left\{ \bigvee_{I \in SI\downarrow} (\mathsf{tree}\,(I \uplus I_1, \mathbf{x}, n[t]) \wedge addrs\,(t) = \varnothing) \quad \times \{\mathsf{var}\,(\mathtt{n}, n)\} \ \right\}$$

```
  local l,u,d,r,ul in
```

$$\left\{ \begin{array}{l} \bigvee_{I \in SI\downarrow} (\mathsf{tree}\,(I, \mathbf{x}, n[t]) \wedge addrs\,(t) = \varnothing) \\ \times \{\mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, -) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, -) * \mathsf{var}\,(\mathtt{ul}, -) * \mathsf{var}\,(\mathtt{t}, -)\} \end{array} \right\}$$

$$\left\{ \begin{array}{l} \left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l} I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x, \pi^x) \ * \ n.u \to u^x * \mathsf{Left}\,(n, l^x, u^x) * \mathsf{Right}\,(n, r^x, u^x) \\ * \exists pl. \left((u^x \neq \mathsf{null} \wedge pl = u^x.nL) \vee (u^x = \mathsf{null} \wedge pl = \mathcal{R} + 1) \right) * n.uL \to pl * \mathsf{isLock}\,(pl, \pi^x) \end{array} \right. \right\} \\ \exists d, e, \pi_1, \pi_2. \ \ \pi_1, \pi_2 > 0 \wedge \pi_1 + \pi_2 = 1 \wedge \mathsf{isLock}\,(n.nL, \pi_1) \\ * \mathsf{First}\,(n, d) * \mathsf{Last}\,(n, e) * \mathsf{treeFrag}\,(I, t)\,((d, e)\,(\mathsf{null}, n, \mathsf{null})\,(\pi_2)) \\ \times \{\mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, -) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, -) * \mathsf{var}\,(\mathtt{ul}, -)\} \end{array} \right\}$$

```
  //By lemma 18
```

$$\left\{ \begin{array}{l} \left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l} I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x, \pi^x) \ * \ n.u \to u^x * \mathsf{Left}\,(n, l^x, u^x) * \mathsf{Right}\,(n, r^x, u^x) \\ * \exists pl. \left((u^x \neq \mathsf{null} \wedge pl = u^x.nL) \vee (u^x = \mathsf{null} \wedge pl = \mathcal{R} + 1) \right) * n.uL \to pl * \mathsf{isLock}\,(pl, \pi^x) \end{array} \right. \right\} \\ * \exists d, e.\, n.d \to d * n.dL \to 0 * n.e \to e * n.eL \to 0 * n.nL \to 0 * ||t||^{((d,e)(\mathsf{null}, n, \mathsf{null})} \\ \times \{\mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, -) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, -) * \mathsf{var}\,(\mathtt{ul}, -)\} \end{array} \right\}$$

```
  u:= [n.up] ; d:= [n.first] ; ul:= [n.upL] ;
```

$$\left\{ \begin{array}{l} \left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l} I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x, \pi^x) \ * \ n.u \to u^x * \mathsf{Left}\,(n, l^x, u^x) * \mathsf{Right}\,(n, r^x, u^x) \\ * \exists pl. \left((u^x \neq \mathsf{null} \wedge pl = u^x.nL) \vee (u^x = \mathsf{null} \wedge pl = \mathcal{R} + 1) \right) * n.uL \to pl * \mathsf{isLock}\,(pl, \pi^x) \\ * \mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, u^x) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, d) * \mathsf{var}\,(\mathtt{ul}, pl) \end{array} \right. \right\} \\ * \exists d, e.\, n.d \to d * n.dL \to 0 * n.e \to e * n.eL \to 0 * n.nL \to 0 * ||t||^{((d,e)(\mathsf{null}, n, \mathsf{null})} \end{array} \right\}$$

$$\left\{ \ \mathsf{isLock}\,(pl, \pi^x) * \mathsf{var}\,(\mathtt{ul}, pl) \ \right\}$$

```
  lock(ul)
```

$$\left\{ \ \mathsf{Locked}\,(pl, \pi^x) * \mathsf{var}\,(\mathtt{ul}, pl) \ \right\}$$

$$\left\{ \begin{array}{l} \left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l} I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x, \pi^x) \ * \ n.u \to u^x * \mathsf{Left}\,(n, l^x, u^x) * \mathsf{Right}\,(n, r^x, u^x) \\ * \exists pl. \left((u^x \neq \mathsf{null} \wedge pl = u^x.nL) \vee (u^x = \mathsf{null} \wedge pl = \mathcal{R} + 1) \right) * n.uL \to pl * \mathsf{Locked}\,(pl, \pi^x) \\ * \mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, u^x) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, d) * \mathsf{var}\,(\mathtt{ul}, pl) \end{array} \right. \right\} \\ * \exists d, e.\, n.d \to d * n.dL \to 0 * n.e \to e * n.eL \to 0 * n.nL \to 0 * ||t||^{((d,e)(\mathsf{null}, n, \mathsf{null})} \end{array} \right\}$$

$$\left\{ \begin{array}{l} \left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l} I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x, \pi^x) \ * \ * \mathsf{Left}\,(n, l^x, u^x) \\ * \exists pl. \left((u^x \neq \mathsf{null} \wedge pl = u^x.nL) \vee (u^x = \mathsf{null} \wedge pl = \mathcal{R} + 1) \right) * \mathsf{Locked}\,(pl, \pi^x) \\ * \mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, u^x) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, d) * \mathsf{var}\,(\mathtt{ul}, pl) \end{array} \right. \right\} \end{array} \right\}$$

$$\left\{ \begin{array}{l} \left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l} I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x, \pi^x) \ * \ * \ \mathsf{isLLock}\left(n, u^x, \frac{1}{2}\right) * \mathsf{ownsR}\,(n, l^x, u^x, 1) \\ * \exists pl. \left((u^x \neq \mathsf{null} \wedge pl = u^x.nL) \vee (u^x = \mathsf{null} \wedge pl = \mathcal{R} + 1) \right) * \mathsf{Locked}\,(pl, \pi^x) \\ * \mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, u^x) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, d) * \mathsf{var}\,(\mathtt{ul}, pl) \end{array} \right. \right\} \end{array} \right\}$$

$\texttt{lock(n.leftL)}$;

$$\left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l} I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x, \pi^x) \ * \exists \mathsf{R}_{n.l}. [\mathcal{A}]^{\mathsf{R}_{n.l}}_{\frac{1}{2}} * [\mathcal{L}]^{\mathsf{R}_{n.l}}_1 * [\mathcal{U}]^{\mathsf{R}_{n.l}}_1 * \mathsf{ownsR}\left(l^x, n, u^x, \frac{3}{4}\right) \\ * \Subset^{\mathsf{R}, n, l^x, u^x} * \boxed{n.lL \to 1 * \mathsf{ownsR}\left(l^x, n, u^x, \frac{1}{4}\right)}^{\mathsf{R}_{n.l}}_{\mathsf{LC}(\mathsf{R}_{n.l}, n, u^x)} \\ * \exists pl. \left((u^x \neq \mathsf{null} \wedge pl = u^x.nL) \vee (u^x = \mathsf{null} \wedge pl = \mathcal{R}+1)\right) * \mathsf{Locked}\,(pl, \pi^x) \\ * \mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, u^x) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, d) * \mathsf{var}\,(\mathtt{ul}, pl) \end{array} \right\} \right\}$$

$$\left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l} I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x, \pi^x) \ * \mathsf{ownsR}\left(l^x, n, u^x, \frac{3}{4}\right) * \Subset^{\mathsf{R}, n, l^x, u^x} \\ * \exists pl. \left((u^x \neq \mathsf{null} \wedge pl = u^x.nL) \vee (u^x = \mathsf{null} \wedge pl = \mathcal{R}+1)\right) * \mathsf{Locked}\,(pl, \pi^x) \\ * \mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, u^x) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, d) * \mathsf{var}\,(\mathtt{ul}, pl) \end{array} \right\} \right\}$$

$\texttt{l:= [n.left]}$;

$$\left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l} I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x, \pi^x) \ * \mathsf{ownsR}\left(l^x, n, u^x, \frac{3}{4}\right) * \Subset^{\mathsf{R}, n, l^x, u^x} \\ * \exists pl. \left((u^x \neq \mathsf{null} \wedge pl = u^x.nL) \vee (u^x = \mathsf{null} \wedge pl = \mathcal{R}+1)\right) * \mathsf{Locked}\,(pl, \pi^x) \\ * \mathsf{var}\,(\mathtt{n}, n) * \boxed{\mathsf{var}\,(\mathtt{l}, l^x)} * \mathsf{var}\,(\mathtt{u}, u^x) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, d) * \mathsf{var}\,(\mathtt{ul}, pl) \end{array} \right\} \right\}$$

$$\left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l} I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x, \pi^x) \ * \mathsf{ownsR}\left(l^x, n, u^x, \frac{3}{4}\right) * \boxed{n.l \overset{\frac{1}{2}}{\mapsto} l^x} \\ * \left(\begin{array}{l} \left(\ l^x \neq \mathsf{null} \ \wedge \ l^x.r \overset{\frac{1}{2}}{\mapsto} n * \ \mathsf{isRLock}\left(l^x, u^x, \frac{1}{2}\right) \ \right) \\ \vee \left(\ l^x = \mathsf{null} \wedge u^x \neq \mathsf{null} \wedge u^x.d \overset{\frac{1}{2}}{\mapsto} n * \ \mathsf{isDLock}\left(u^x, \frac{1}{2}\right) \ \right) \\ \vee \left(\ l^x = \mathsf{null} \wedge u^x = \mathsf{null} \wedge \mathcal{R} \to n * n.l \overset{\frac{1}{2}}{\mapsto} l^x * \mathsf{isLLock}\left(n, u^x, \frac{1}{2}\right) \ \right) \end{array} \right) \\ * \exists pl. \left((u^x \neq \mathsf{null} \wedge pl = u^x.nL) \vee (u^x = \mathsf{null} \wedge pl = \mathcal{R}+1)\right) * \mathsf{Locked}\,(pl, \pi^x) \\ * \mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, l^x) * \mathsf{var}\,(\mathtt{u}, u^x) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, d) * \mathsf{var}\,(\mathtt{ul}, pl) \end{array} \right\} \right\}$$

$\texttt{if l} \neq \mathsf{null} \ \texttt{then} \quad \texttt{lock(l.rightL)}$
$\texttt{else if u} \neq \mathsf{null} \ \texttt{then} \quad \texttt{lock(u.firstL)}$;

$$\left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l} I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x, \pi^x) \ * \ * \boxed{\mathsf{ownsR}\left(n, l^x, u^x, \frac{1}{2}\right)} * n.l \overset{\frac{1}{2}}{\mapsto} l^x \\ * \left(\begin{array}{l} \left(\begin{array}{l} l^x \neq \mathsf{null} \ \wedge \ l^x.r \overset{\frac{1}{2}}{\mapsto} n \\ * \exists \mathsf{R}_{l.r}. [\mathcal{A}]^{\mathsf{R}_{l.r}}_{\frac{1}{2}} * \boxed{[\mathcal{L}]^{\mathsf{R}_{l.r}}_1 * [\mathcal{U}]^{\mathsf{R}_{l.r}}_1 * \ni^{l^x, n, u^x}} \\ * \boxed{l^x.rL \to 1 * \mathsf{ownsR}\left(l^x, n, u^x, \frac{1}{4}\right)}^{\mathsf{R}_{l.r}}_{\mathsf{RC}(\mathsf{R}_{l.r}, l^x, u^x)} \end{array} \right) \\ \vee \left(\begin{array}{l} l^x = \mathsf{null} \wedge u^x \neq \mathsf{null} \wedge u^x.d \overset{\frac{1}{2}}{\mapsto} n \\ * \exists \mathsf{R}_{u.d}. [\mathcal{A}]^{\mathsf{R}_{u.d}}_{\frac{1}{2}} * \boxed{[\mathcal{L}]^{\mathsf{R}_{u.d}}_1 * [\mathcal{U}]^{\mathsf{R}_{u.d}}_1 * \Subset^{u^x, n}} \\ * \boxed{u^x.dL \to 1 * \mathsf{ownsR}\left(\mathsf{null}, n, u^x, \frac{1}{4}\right)}^{\mathsf{R}_{u.d}}_{\mathsf{DC}(\mathsf{R}_{u.d}, u^x)} \end{array} \right) \\ \vee \left(\begin{array}{l} l^x = \mathsf{null} \wedge u^x = \mathsf{null} \wedge \mathcal{R} \to n * n.l \overset{\frac{1}{2}}{\mapsto} l^x \\ * \mathsf{isLLock}\,(n, l^x, u^x) \ \frac{1}{2} * \mathsf{ownsR}\left(l^x, n, u^x, \frac{1}{4}\right) \end{array} \right) \end{array} \right) \\ * \exists pl. \left((u^x \neq \mathsf{null} \wedge pl = u^x.nL) \vee (u^x = \mathsf{null} \wedge pl = \mathcal{R}+1)\right) * \mathsf{Locked}\,(pl, \pi^x) \\ * \mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, l^x) * \mathsf{var}\,(\mathtt{u}, u^x) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, d) * \mathsf{var}\,(\mathtt{ul}, pl) \end{array} \right\} \right\}$$

$$\left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l} I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x, \pi^x) \ * \ n.l \overset{1}{\mapsto} l^x * \exists \mathsf{R}_{n.l}. \, [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{2}} [\mathcal{A}]^{\mathsf{R}_{n.l}}_{1} * [\mathcal{L}]^{\mathsf{R}_{n.l}}_{1} * [\mathcal{U}]^{\mathsf{R}_{n.l}}_{1} \\ * \boxed{n.lL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{n.l}}_{\mathsf{LC}(\mathsf{R}_{n.l}, n, u^x)} \qquad * \mathsf{Right}\,(n, r^x, u^x) \\ * \left(\begin{array}{l} \left(\begin{array}{l} l^x \neq \mathsf{null} \ \wedge \ l^x.r \overset{1}{\mapsto} n * \exists \mathsf{R}_{l.r}. \\ [\mathcal{A}]^{\mathsf{R}_{l.r}}_{\frac{1}{2}} * [\mathcal{L}]^{\mathsf{R}_{l.r}}_{1} * [\mathcal{U}]^{\mathsf{R}_{l.r}}_{1} * \boxed{l^x.rL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{l.r}}_{\mathsf{RC}(\mathsf{R}_{l.r}, l^x, u^x)} \end{array} \right) \\ \vee \left(\begin{array}{l} l^x = \mathsf{null} \wedge u^x \neq \mathsf{null} \wedge u^x.d \overset{1}{\mapsto} n * \exists \mathsf{R}_{u.d}. \\ [\mathcal{A}]^{\mathsf{R}_{u.d}}_{\frac{1}{2}} * [\mathcal{L}]^{\mathsf{R}_{u.d}}_{1} * [\mathcal{U}]^{\mathsf{R}_{u.d}}_{1} * \boxed{u^x.dL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{u.d}}_{\mathsf{DC}(\mathsf{R}_{u.d}, u^x)} \end{array} \right) \\ \vee \left(l^x = \mathsf{null} \wedge u^x = \mathsf{null} \wedge \mathcal{R} \to n * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}} \right) \end{array} \right) \\ * \exists pl. \left((u^x \neq \mathsf{null} \wedge pl = u^x.nL) \vee (u^x = \mathsf{null} \wedge pl = \mathcal{R} + 1) \right) * \mathsf{Locked}\,(pl, \pi^x) \\ * \mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, l^x) * \mathsf{var}\,(\mathtt{u}, u^x) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, d) * \mathsf{var}\,(\mathtt{ul}, pl) \end{array} \right\} \right\}$$

//Do the same for the right hand side

`lock(n.rightL) ; r:= [n.right] ;`

`if r` $\neq$ `null then lock(r.leftL)  else if u` $\neq$ `null then lock(u.lastL) ;`

$$\left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l} I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x, \pi^x) \ * \ \exists \mathsf{R}_{n.l}. \, [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{2}} [\mathcal{A}]^{\mathsf{R}_{n.l}}_{1} * [\mathcal{L}]^{\mathsf{R}_{n.l}}_{1} * [\mathcal{U}]^{\mathsf{R}_{n.l}}_{1} \\ * n.l \overset{1}{\mapsto} l^x * n.r \overset{1}{\mapsto} r^x * \boxed{n.lL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{n.l}}_{\mathsf{LC}(\mathsf{R}_{n.l}, n, u^x)} \\ * \left(\begin{array}{l} \left(\begin{array}{l} l^x \neq \mathsf{null} \ \wedge \ l^x.r \overset{1}{\mapsto} n * \exists \mathsf{R}_{l.r}. \\ [\mathcal{A}]^{\mathsf{R}_{l.r}}_{\frac{1}{2}} * [\mathcal{L}]^{\mathsf{R}_{l.r}}_{1} * [\mathcal{U}]^{\mathsf{R}_{l.r}}_{1} * \boxed{l^x.rL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{l.r}}_{\mathsf{RC}(\mathsf{R}_{l.r}, l^x, u^x)} \end{array} \right) \\ \vee \left(\begin{array}{l} l^x = \mathsf{null} \wedge u^x \neq \mathsf{null} \wedge u^x.d \overset{1}{\mapsto} n * \exists \mathsf{R}_{u.d}. \\ [\mathcal{A}]^{\mathsf{R}_{u.d}}_{\frac{1}{2}} * [\mathcal{L}]^{\mathsf{R}_{u.d}}_{1} * [\mathcal{U}]^{\mathsf{R}_{u.d}}_{1} * \boxed{u^x.dL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{u.d}}_{\mathsf{DC}(\mathsf{R}_{u.d}, u^x)} \end{array} \right) \\ \vee \left(l^x = \mathsf{null} \wedge u^x = \mathsf{null} \wedge \mathcal{R} \to n * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}} \right) \end{array} \right) \\ * \exists \mathsf{R}_{n.r}. \, [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{2}} [\mathcal{A}]^{\mathsf{R}_{n.r}}_{1} * [\mathcal{L}]^{\mathsf{R}_{n.r}}_{1} * [\mathcal{U}]^{\mathsf{R}_{n.r}}_{1} * \boxed{n.rL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}}}^{\mathsf{R}_{n.r}}_{\mathsf{RC}(\mathsf{R}_{n.r}, n, u^x)} \\ * \left(\begin{array}{l} \left(\begin{array}{l} r^x \neq \mathsf{null} \ \wedge \ r^x.l \overset{1}{\mapsto} n * \exists \mathsf{R}_{r.l}. \\ [\mathcal{A}]^{\mathsf{R}_{r.l}}_{\frac{1}{2}} * [\mathcal{L}]^{\mathsf{R}_{r.l}}_{1} * [\mathcal{U}]^{\mathsf{R}_{r.l}}_{1} * \boxed{r^x.lL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}}}^{\mathsf{R}_{r.l}}_{\mathsf{LC}(\mathsf{R}_{r.l}, r^x, u^x)} \end{array} \right) \\ \vee \left(\begin{array}{l} r^x = \mathsf{null} \wedge u^x \neq \mathsf{null} \wedge u^x.e \overset{1}{\mapsto} n * \exists \mathsf{R}_{u.e}. \\ [\mathcal{A}]^{\mathsf{R}_{u.e}}_{\frac{1}{2}} * [\mathcal{L}]^{\mathsf{R}_{u.e}}_{1} * [\mathcal{U}]^{\mathsf{R}_{u.e}}_{1} * \boxed{u^x.eL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}}}^{\mathsf{R}_{u.e}}_{\mathsf{EC}(\mathsf{R}_{u.e}, u^x)} \end{array} \right) \\ \vee \left(r^x = \mathsf{null} \wedge u^x = \mathsf{null} \wedge [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}} \right) \end{array} \right) \\ * \exists pl. \left((u^x \neq \mathsf{null} \wedge pl = u^x.nL) \vee (u^x = \mathsf{null} \wedge pl = \mathcal{R} + 1) \right) * \mathsf{Locked}\,(pl, \pi^x) \\ * \mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, l^x) * \mathsf{var}\,(\mathtt{u}, u^x) * \mathsf{var}\,(\mathtt{r}, r^x) * \mathsf{var}\,(\mathtt{d}, d) * \mathsf{var}\,(\mathtt{ul}, pl) \end{array} \right\} \right\}$$

`unlock(ul) ;`

`if l` $\neq$ `null then  [l.right] := r else if u` $\neq$ `null then  [u.first] := r ;`

`else [ul-1]:= r ;`

`if r` $\neq$ `null then  [r.left] := l else if u` $\neq$ `null then  [u.last] := l ;`

$$
\left\{ \bigvee_{I \in SI\downarrow} \left\{
\begin{array}{l}
I^{\mathsf{out}}(\mathbf{x}) = (l^x, u^x, r^x, \pi^x) \ \wedge \ \ n.l \to l^x * n.r \to r^x \\
* \exists \mathsf{R}_{n.l}, \mathsf{R}_{n.r}. \, [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{2}} [\mathcal{A}]^{\mathsf{R}_{n.l}}_1 * [\mathcal{L}]^{\mathsf{R}_{n.l}}_1 * [\mathcal{U}]^{\mathsf{R}_{n.l}}_1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{2}} [\mathcal{A}]^{\mathsf{R}_{n.r}}_1 * [\mathcal{L}]^{\mathsf{R}_{n.r}}_1 * [\mathcal{U}]^{\mathsf{R}_{n.r}}_1 \\
* \boxed{n.rL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}}}^{\mathsf{R}_{n.r}}_{\mathsf{RC}(\mathsf{R}_{n.r}, n, u^x)} * \boxed{n.lL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{n.l}}_{\mathsf{LC}(\mathsf{R}_{n.l}, n, u^x)} \\
* \left(\begin{array}{l} \left(\begin{array}{l} l^x \neq \mathsf{null} \ \wedge \ \ l^x.r \overset{1}{\mapsto} r^x * \exists \mathsf{R}_{l.r}. \\ [\mathcal{A}]^{\mathsf{R}_{l.r}}_{\frac{1}{2}} * [\mathcal{L}]^{\mathsf{R}_{l.r}}_1 * [\mathcal{U}]^{\mathsf{R}_{l.r}}_1 * \boxed{l^x.rL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{l.r}}_{\mathsf{RC}(\mathsf{R}_{l.r}, l^x, u^x)} \end{array} \right) \\
\vee \left(\begin{array}{l} l^x = \mathsf{null} \wedge u^x \neq \mathsf{null} \wedge \ u^x.d \overset{1}{\mapsto} r^x * \exists \mathsf{R}_{u.d}. \\ [\mathcal{A}]^{\mathsf{R}_{u.d}}_{\frac{1}{2}} * [\mathcal{L}]^{\mathsf{R}_{u.d}}_1 * [\mathcal{U}]^{\mathsf{R}_{u.d}}_1 * \boxed{u^x.dL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{u.d}}_{\mathsf{DC}(\mathsf{R}_{u.d}, u^x)} \end{array} \right) \\
\vee \left(l^x = \mathsf{null} \wedge u^x = \mathsf{null} \wedge \ \mathcal{R} \to r^x * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}} \right) \end{array} \right) \\
* \left(\begin{array}{l} \left(\begin{array}{l} r^x \neq \mathsf{null} \ \wedge \ \ r^x.l \overset{1}{\mapsto} l^x * \exists \mathsf{R}_{r.l}. \\ [\mathcal{A}]^{\mathsf{R}_{r.l}}_{\frac{1}{2}} * [\mathcal{L}]^{\mathsf{R}_{r.l}}_1 * [\mathcal{U}]^{\mathsf{R}_{r.l}}_1 * \boxed{r^x.lL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}}}^{\mathsf{R}_{r.l}}_{\mathsf{LC}(\mathsf{R}_{r.l}, r^x, u^x)} \end{array} \right) \\
\vee \left(\begin{array}{l} r^x = \mathsf{null} \wedge u^x \neq \mathsf{null} \wedge \ u^x.e \overset{1}{\mapsto} l^x * \exists \mathsf{R}_{u.e}. \\ [\mathcal{A}]^{\mathsf{R}_{u.e}}_{\frac{1}{2}} * [\mathcal{L}]^{\mathsf{R}_{u.e}}_1 * [\mathcal{U}]^{\mathsf{R}_{u.e}}_1 * \boxed{u^x.eL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}}}^{\mathsf{R}_{u.e}}_{\mathsf{EC}(\mathsf{R}_{u.e}, u^x)} \end{array} \right) \\
\vee \left(r^x = \mathsf{null} \wedge u^x = \mathsf{null} \wedge [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}} \right) \end{array} \right) \\
* \exists pl. \left((u^x \neq \mathsf{null} \wedge pl = u^x.nL) \vee (u^x = \mathsf{null} \wedge pl = \mathcal{R} + 1) \right) * \mathsf{isLock}\,(pl, \pi^x) \\
* \mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, l^x) * \mathsf{var}\,(\mathtt{u}, u^x) * \mathsf{var}\,(\mathtt{r}, r^x) * \mathsf{var}\,(\mathtt{d}, d) * \mathsf{var}\,(\mathtt{ul}, pl)
\end{array}
\right\} \right\}
$$

$$
\left\{ \bigvee_{I \in SI\downarrow} \left\{
\begin{array}{l}
I^{\mathsf{out}}(\mathbf{x}) \dot{=} (l^x, u^x, r^x, \pi^x) \ * \ \ n.l \to l^x * n.r \to r^x \\
* \ \mathsf{tree}\,(I \uplus I_2, \mathbf{x}, \varnothing) \ \wedge \ I_2 \in \mathcal{I}_D \wedge I_2{}^{\mathsf{in}}(\mathbf{x}) = (r^x, l^x) \\
* \exists \mathsf{R}_{n.l}, \mathsf{R}_{n.r}. \, [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{2}} [\mathcal{A}]^{\mathsf{R}_{n.l}}_1 * [\mathcal{L}]^{\mathsf{R}_{n.l}}_1 * [\mathcal{U}]^{\mathsf{R}_{n.l}}_1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{2}} [\mathcal{A}]^{\mathsf{R}_{n.r}}_1 * [\mathcal{L}]^{\mathsf{R}_{n.r}}_1 * [\mathcal{U}]^{\mathsf{R}_{n.r}}_1 \\
* \boxed{n.rL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}}}^{\mathsf{R}_{n.r}}_{\mathsf{RC}(\mathsf{R}_{n.r}, n, u^x)} * \boxed{n.lL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{n.l}}_{\mathsf{LC}(\mathsf{R}_{n.l}, n, u^x)} \\
* \left(\begin{array}{l} \left(\begin{array}{l} l^x \neq \mathsf{null} \ \wedge \ \ l^x.r \overset{1}{\mapsto} r^x * \exists \mathsf{R}_{l.r}. \\ [\mathcal{A}]^{\mathsf{R}_{l.r}}_{\frac{1}{2}} * [\mathcal{L}]^{\mathsf{R}_{l.r}}_1 * [\mathcal{U}]^{\mathsf{R}_{l.r}}_1 * \boxed{l^x.rL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{l.r}}_{\mathsf{RC}(\mathsf{R}_{l.r}, l^x, u^x)} \end{array} \right) \\
\vee \left(\begin{array}{l} l^x = \mathsf{null} \wedge u^x \neq \mathsf{null} \wedge u^x.d \overset{1}{\mapsto} r^x * \exists \mathsf{R}_{u.d}. \\ [\mathcal{A}]^{\mathsf{R}_{u.d}}_{\frac{1}{2}} * [\mathcal{L}]^{\mathsf{R}_{u.d}}_1 * [\mathcal{U}]^{\mathsf{R}_{u.d}}_1 * \boxed{u^x.dL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{u.d}}_{\mathsf{DC}(\mathsf{R}_{u.d}, u^x)} \end{array} \right) \\
\vee \left(l^x = \mathsf{null} \wedge u^x = \mathsf{null} \wedge \mathcal{R} \to r^x * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}} \right) \end{array} \right) \\
* \left(\begin{array}{l} \left(\begin{array}{l} r^x \neq \mathsf{null} \ \wedge \ \ r^x.l \overset{1}{\mapsto} l^x * \exists \mathsf{R}_{r.l}. \\ [\mathcal{A}]^{\mathsf{R}_{r.l}}_{\frac{1}{2}} * [\mathcal{L}]^{\mathsf{R}_{r.l}}_1 * [\mathcal{U}]^{\mathsf{R}_{r.l}}_1 * \boxed{r^x.lL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}}}^{\mathsf{R}_{r.l}}_{\mathsf{LC}(\mathsf{R}_{r.l}, r^x, u^x)} \end{array} \right) \\
\vee \left(\begin{array}{l} r^x = \mathsf{null} \wedge u^x \neq \mathsf{null} \wedge u^x.e \overset{1}{\mapsto} l^x * \exists \mathsf{R}_{u.e}. \\ [\mathcal{A}]^{\mathsf{R}_{u.e}}_{\frac{1}{2}} * [\mathcal{L}]^{\mathsf{R}_{u.e}}_1 * [\mathcal{U}]^{\mathsf{R}_{u.e}}_1 * \boxed{u^x.eL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}}}^{\mathsf{R}_{u.e}}_{\mathsf{EC}(\mathsf{R}_{u.e}, u^x)} \end{array} \right) \\
\vee \left(r^x = \mathsf{null} \wedge u^x = \mathsf{null} \wedge [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}} \right) \end{array} \right) \\
* \mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, l^x) * \mathsf{var}\,(\mathtt{u}, u^x) * \mathsf{var}\,(\mathtt{r}, r^x) * \mathsf{var}\,(\mathtt{d}, d) * \mathsf{var}\,(\mathtt{ul}, -)
\end{array}
\right\} \right\}
$$

$$
\begin{array}{l}
\texttt{if l} \neq \mathsf{null}\ \texttt{then unlock(l.rightL) else if u} \neq \mathsf{null}\ \texttt{then unlock(u.firstL)}\,; \\
\texttt{if r} \neq \mathsf{null}\ \texttt{then unlock(r.leftL) else if u} \neq \mathsf{null}\ \texttt{then unlock(u.lastL)}\,; \\
\left\{ \bigvee_{I \in SI\downarrow} \left\{ \begin{array}{l}
I^{\mathsf{out}}(\mathbf{x}) \doteq (l^x, u^x, r^x, \pi^x) \ *\ n.l \to l^x * n.r \to r^x \\
*\mathsf{tree}\,(I \uplus I_2, \mathbf{x}, \varnothing) \ \wedge\ I_2 \in \mathcal{I}_D \wedge I_2{}^{\mathsf{in}}(\mathbf{x}) = (r^x, l^x) \\
*\exists \mathsf{R}_{n.l}, \mathsf{R}_{n.r}.\ \boxed{[\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{3}{4}}}\,[\mathcal{A}]^{\mathsf{R}_{n.l}}_1 * [\mathcal{L}]^{\mathsf{R}_{n.l}}_1 * [\mathcal{U}]^{\mathsf{R}_{n.l}}_1 * \boxed{[\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{3}{4}}}\,[\mathcal{A}]^{\mathsf{R}_{n.r}}_1 * [\mathcal{L}]^{\mathsf{R}_{n.r}}_1 \\
*[\mathcal{U}]^{\mathsf{R}_{n.r}}_1 * \boxed{n.rL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}}}^{\mathsf{R}_{n.r}}_{\mathsf{RC}(\mathsf{R}_{n.r},n,u^x)} * \boxed{n.lL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{n.l}}_{\mathsf{LC}(\mathsf{R}_{n.l},n,u^x)}
\end{array} \right\} \right. \\
\left. \times \{ *\mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, -) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, d) * \mathsf{var}\,(\mathtt{ul}, -) \} \right\} \\
\left\{ \begin{array}{l}
\bigvee_{I \in SI\downarrow} \left\{ \boxed{\langle \mathsf{tree}\,(\mathbf{x}, \varnothing) \rangle^{I \uplus I_2}} \ \wedge\ I_2 \in \mathcal{I}_D \right\} \\
*n.l \to - * n.r \to - * \exists \mathsf{R}_{n.l}, \mathsf{R}_{n.r}.\, [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{3}{4}} [\mathcal{A}]^{\mathsf{R}_{n.l}}_1 * [\mathcal{L}]^{\mathsf{R}_{n.l}}_1 * [\mathcal{U}]^{\mathsf{R}_{n.l}}_1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{3}{4}} [\mathcal{A}]^{\mathsf{R}_{n.r}}_1 \\
*[\mathcal{L}]^{\mathsf{R}_{n.r}}_1 * [\mathcal{U}]^{\mathsf{R}_{n.r}}_1 * \boxed{n.rL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}}}^{\mathsf{R}_{n.r}}_{\mathsf{RC}(\mathsf{R}_{n.r},n,u^x)} * \boxed{n.lL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{n.l}}_{\mathsf{LC}(\mathsf{R}_{n.l},n,u^x)} \\
*\exists d, e.\, n.d \to d * n.dL \to 0 * n.e \to e * n.eL \to 0 * n.nL \to 0 \\
* \|t\|^{(d,e)(\mathsf{null},n,\mathsf{null})} * n.u \to u^x * n.uL \to - \\
\times \{ \mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, -) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, d) * \mathsf{var}\,(\mathtt{ul}, -) \}
\end{array} \right\} \\
\left\{ \ \|t\|^{(d,e)(\mathsf{null},n,\mathsf{null})} \times \{\mathsf{var}\,(\mathtt{d}, d)\} \ \right\}\ \texttt{disposeForest(d)}\ \left\{ \ \mathsf{emp} \times \{\mathsf{var}\,(\mathtt{d}, -)\} \ \right\} \\
\left\{ \begin{array}{l}
\bigvee_{I \in SI\downarrow} \left\{ \ \langle \mathsf{tree}\,(\mathbf{x}, \varnothing) \rangle^{I \uplus I_2} \ \wedge\ I_2 \in \mathcal{I}_D \ \right\} \\
*n.l \to - * n.r \to - * \exists \mathsf{R}_{n.l}, \mathsf{R}_{n.r}.\, [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{3}{4}} [\mathcal{A}]^{\mathsf{R}_{n.l}}_1 * [\mathcal{L}]^{\mathsf{R}_{n.l}}_1 * [\mathcal{U}]^{\mathsf{R}_{n.l}}_1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{3}{4}} [\mathcal{A}]^{\mathsf{R}_{n.r}}_1 \\
*[\mathcal{L}]^{\mathsf{R}_{n.r}}_1 * [\mathcal{U}]^{\mathsf{R}_{n.r}}_1 * \boxed{n.rL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.r}}_{\frac{1}{4}}}^{\mathsf{R}_{n.r}}_{\mathsf{RC}(\mathsf{R}_{n.r},n,u^x)} * \boxed{n.lL \to 1 * [\mathcal{W}]^{\mathsf{R}_{n.l}}_{\frac{1}{4}}}^{\mathsf{R}_{n.l}}_{\mathsf{LC}(\mathsf{R}_{n.l},n,u^x)} \\
*\exists d, e.\, n.d \to - * n.dL \to 0 * n.e \to - * n.eL \to 0 * n.nL \to 0 * n.u \to u^x * n.uL \to - \\
\times \{ \mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, -) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, -) * \mathsf{var}\,(\mathtt{ul}, -) \}
\end{array} \right\} \\
//\text{Use the } [\mathcal{W}] \text{ tokens on } \mathsf{R}_{n.lL} \text{ and } \mathsf{R}_{n.rL}. \\
\left\{ \begin{array}{l}
\bigvee_{I \in SI\downarrow} \left\{ \ \langle \mathsf{tree}\,(\mathbf{x}, \varnothing) \rangle^{I \uplus I_2} \ \wedge\ I_2 \in \mathcal{I}_D \ \right\} \ * \\
\exists \mathsf{R}_{n.l}.\ \boxed{[\mathcal{W}]^{\mathsf{R}_{n.l}}_1} * [\mathcal{A}]^{\mathsf{R}_{n.l}}_1 * [\mathcal{L}]^{\mathsf{R}_{n.l}}_1 * [\mathcal{U}]^{\mathsf{R}_{n.l}}_1 * \boxed{n.lL \to 1 * \boxed{n.l \to - * n.u \overset{\frac{1}{4}}{\mapsto} u^x}^{\mathsf{R}_{n.l}}_{\mathsf{LC}(\mathsf{R}_{n.l},n,-)}}^{\mathsf{R}_{n.l}} * \\
\exists \mathsf{R}_{n.r}.\ \boxed{[\mathcal{W}]^{\mathsf{R}_{n.r}}_1} * [\mathcal{A}]^{\mathsf{R}_{n.r}}_1 * [\mathcal{L}]^{\mathsf{R}_{n.r}}_1 * [\mathcal{U}]^{\mathsf{R}_{n.r}}_1 * \boxed{n.rL \to 1 * \boxed{n.r \to - * n.u \overset{\frac{1}{4}}{\mapsto} u^x}^{\mathsf{R}_{n.r}}_{\mathsf{RC}(\mathsf{R}_{n.r},n,u^x)}} \\
*\exists d, e.\, n.d \to - * n.dL \to 0 * n.e \to - * n.eL \to 0 * n.nL \to 0 * \boxed{n.u \overset{\frac{1}{2}}{\mapsto} u^x} * n.uL \to - \\
\times \{ \mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, -) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, -) * \mathsf{var}\,(\mathtt{ul}, -) \}
\end{array} \right\} \\
//\text{Destroy the } \mathsf{R}_{n.r} \text{ and } \mathsf{R}_{n.l} \text{ regions since we have all tokens on them.} \\
\left\{ \begin{array}{l}
\bigvee_{I \in SI\downarrow} \left\{ \ \langle \mathsf{tree}\,(\mathbf{x}, \varnothing) \rangle^{I \uplus I_2} \ \wedge\ I_2 \in \mathcal{I}_D \ \right\} * \boxed{n.lL \to 1 * n.l \to - * n.rL \to 1 * n.r \to - * n.u \overset{1}{\mapsto} -} \\
*\exists d, e.\, n.d \to - * n.dL \to 0 * n.e \to - * n.eL \to 0 * n.nL \to 0 * n.uL \to - \\
\times \{ \mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, -) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, -) * \mathsf{var}\,(\mathtt{ul}, -) \}
\end{array} \right\} \\
\texttt{disposeNode(n)} \\
\left\{ \begin{array}{l}
\bigvee_{I \in SI\downarrow} \left\{ \ \langle \mathsf{tree}\,(\mathbf{x}, \varnothing) \rangle^{I \uplus I_2} \ \wedge\ I_2 \in \mathcal{I}_D \ \right\} \\
\times \{ \mathsf{var}\,(\mathtt{n}, n) * \mathsf{var}\,(\mathtt{l}, -) * \mathsf{var}\,(\mathtt{u}, -) * \mathsf{var}\,(\mathtt{r}, -) * \mathsf{var}\,(\mathtt{d}, -) * \mathsf{var}\,(\mathtt{ul}, -) \}
\end{array} \right\} \\
\}
\left\{ \ \bigvee_{I \in SI\downarrow} \left\{ \ \langle \mathsf{tree}\,(\mathbf{x}, \varnothing) \rangle^{I \uplus I_2} \ \wedge\ I_2 \in \mathcal{I}_D \ \right\} \times \{\mathsf{var}\,(\mathtt{n}, n)\} \ \right\}
\end{array}
$$

Bibliography

[1] Thomas Dinsdale-Young, Lars Birkedal, Philippa Gardner, Matthew Parkinson, and Hongseok Yang. Views: Compositional reasoning for concurrent programs. *SIGPLAN Not.*, 48(1):287–300, January 2013.

[2] Matthew Parkinson, Richard Bornat, and Cristiano Calcagno. Variables as resource in hoare logics. In *Proceedings of the 21st Annual IEEE Symposium on Logic in Computer Science*, LICS '06, pages 137–146, Washington, DC, USA, 2006. IEEE Computer Society.

A. Abstract (de)Allocation ($\tau : \mathbb{T} \to \mathbb{C}$)

In the lemmata given in this report, we use the following notation for brevity.

$$\langle\langle t \rangle\rangle_I^{(i,j)(l,u,r)} \triangleq \mathsf{treeFrag}\,(I,t)\,(i,j)\,(l,u,r)$$

Lemma 9 (Abstract Allocation/Deallocation)**.** For all $\mathbf{a} \in \textsc{SAdd} \cup \{\mathcal{R}\}$, $\mathbf{x}, \mathbf{y} \in \textsc{SAdd}$, $t, t' \in \textsc{Data}_{\mathbb{T}}$ and $I \in \mathcal{I}_\tau$,

$$\mathsf{tree}\left(I, a, t \circ_{\mathbf{x}} t'\right) \equiv \exists \mathbf{y} \in \textsc{SAdd}, in, out.\, \mathsf{tree}\left(I', \mathbf{a}, t \circ_{\mathbf{x}} \mathbf{y}\right) * \mathsf{tree}\left(I', \mathbf{y}, t'\right)$$

with

$$I' \triangleq \left(I^{\mathsf{in}}[\mathbf{y} \mapsto in], I^{\mathsf{out}}[\mathbf{y} \mapsto out]\right)$$

Proof. Let

$$k \triangleq \begin{cases} \left(I^{\mathsf{in}}(\mathbf{a}), I^{\mathsf{out}}(\mathbf{a})\right) & \text{if } \mathbf{a} \in \textsc{SAdd} \\ ((i,j)(\mathsf{null}, \mathsf{null}, \mathsf{null})) & \text{if } \mathbf{a} \in \{\mathcal{R}\} \end{cases}$$

for some i, j. Then we have:

$$\begin{aligned}
\mathsf{tree}\,(I, \mathbf{a}, t \circ_{\mathbf{x}} t') = \;& \langle\langle t \circ_{\mathbf{x}} t' \rangle\rangle_I^k \\
\text{By Lemma 10} = \;& \exists \mathbf{y}, in, out. \\
& \langle\langle t \circ_{\mathbf{x}} \mathbf{y} \rangle\rangle^k_{I\uplus[\mathbf{y}\mapsto in],[\mathbf{y}\mapsto out]} * \langle \mathsf{tree}\,(\mathbf{y}, t') \rangle^{I\uplus[\mathbf{y}\mapsto in],[\mathbf{y}\mapsto out]} \\
= \;& \exists \mathbf{y}, out, in. \\
& \langle \mathsf{tree}\,(\mathbf{a}, t \circ_{\mathbf{x}} \mathbf{y}) \rangle^{I\uplus[\mathbf{y}\mapsto in],[\mathbf{y}\mapsto out]} * \langle \mathsf{tree}\,(\mathbf{y}, t') \rangle^{I\uplus[\mathbf{y}\mapsto in],[\mathbf{y}\mapsto out]} \\
= \;& \exists \mathbf{y}, out, in. \\
& \mathsf{tree}\,(I', \mathbf{a}, t \circ_{\mathbf{x}} \mathbf{y}) * \mathsf{tree}\,(I', \mathbf{y}, t')
\end{aligned}$$

□

Lemma 10 (Crust Inclusion)**.**

$$\begin{aligned}
& \forall t, t' \in \textsc{Data}_{\mathbb{T}}. \\
& \forall i, j, l, u, r, t\,. \\
& \forall I \in \mathcal{I}_\tau\,. \\
& \mathbf{x} \in \mathit{addrs}\,(t) \implies \\
& \qquad \langle\langle t \circ_{\mathbf{x}} t' \rangle\rangle_I^{(i,j)(l,u,r)} \\
& \qquad = \\
& \qquad \exists \mathbf{y} \in \textsc{SAdd}.\, \exists out \in \textsc{Out}_\tau, in \in \textsc{In}_\tau. \\
& \langle\langle t \circ_{\mathbf{x}} \mathbf{y} \rangle\rangle^{(i,j)(l,u,r)}_{I\uplus[\mathbf{y}\mapsto in],[\mathbf{y}\mapsto out]} * \langle \mathbf{y} \to t' \rangle^{I\uplus[\mathbf{y}\mapsto in],[\mathbf{y}\mapsto out]}
\end{aligned}$$

Proof. By induction over the structure of t. In the following proofs we write S for SAdd for brevity.

Case 1. $t = \varnothing$
This case holds trivially as $\mathbf{x} \notin \mathit{addrs}(\varnothing)$.

Case 2. $t = \mathbf{z}$
If $\mathbf{z} \neq \mathbf{x}$, then the case holds vacuously since this contradicts our assumption that $\mathbf{x} \in \mathit{addrs}(t)$.
If $\mathbf{z} = \mathbf{x}$, then for arbitrary i, j, l, u, r, t, pick a fresh abstract address $\mathbf{y} \in$ SAdd, and let:

$$\mathit{in} = (i, j), \quad \mathit{out} = (l, u, r)$$

then we have:

$$\begin{aligned}
\langle\langle \mathbf{z} \circ_{\mathbf{x}} t' \rangle\rangle_I^{(i,j)(l,u,r)} &= \langle\langle t' \rangle\rangle_I^{(i,j)(l,u,r)} \\
(\text{Lemma 11}) &= \langle\langle t' \rangle\rangle_{I \uplus [\mathbf{z} \mapsto \mathit{in}], [\mathbf{z} \mapsto \mathit{out}]}^{(i,j)(l,u,r)} \\
&= \langle\langle t' \rangle\rangle_{I[\mathbf{y} \mapsto \mathit{in}], [\mathbf{y} \mapsto \mathit{out}]}^{(i,j)(l,u,r)} * \langle\langle \mathbf{y} \rangle\rangle_{I \uplus [\mathbf{y} \mapsto \mathit{in}], [\mathbf{y} \mapsto \mathit{out}]}^{(i,j)(l,u,r)} \\
&= \langle \mathbf{y} \to t' \rangle^{I \uplus [\mathbf{y} \mapsto \mathit{in}], [\mathbf{y} \mapsto \mathit{out}]} * \langle\langle \mathbf{z} \circ_{\mathbf{x}} \mathbf{y} \rangle\rangle_{I \uplus [\mathbf{y} \mapsto \mathit{in}], [\mathbf{y} \mapsto \mathit{out}]}^{(i,j)(l,u,r)}
\end{aligned}$$

Case 3. $t = n[t'']$
If $\mathbf{x} \notin \mathit{addrs}(t'')$, then the case holds vacuously since this contradicts our assumption that $\mathbf{x} \in \mathit{addrs}(n[t''])$. If $\mathbf{x} \in \mathit{addrs}(t'')$, then for arbitrary i, j, l, u, r, t we have

$$\begin{aligned}
\langle\langle t \circ_{\mathbf{x}} t' \rangle\rangle_I^{(i,j)(l,u,r)} &= \langle\langle n[t''] \circ_{\mathbf{x}} t' \rangle\rangle_I^{(i,j)(l,u,r)} \\
&= \langle\langle n[t'' \circ_{\mathbf{x}} t'] \rangle\rangle_I^{(i,j)(l,u,r)} \\
&= (i \doteq j \doteq n) * n.u \to u * \exists d, e. \\
&\quad \mathsf{Left}(n, l, u) * \mathsf{Right}(n, r, u) \\
&\quad * \mathsf{First}(n, d) * \mathsf{Last}(n, e) \\
&\quad * \langle\langle t'' \circ_{\mathbf{x}} t' \rangle\rangle_I^{(d,e)(\mathsf{null}, n, \mathsf{null})} \\
(\text{I. H.}) &= (i \doteq j \doteq n) * n.u \to u * \exists d, e. \\
&\quad \mathsf{Left}(n, l, u) * \mathsf{Right}(n, r, u) \\
&\quad * \mathsf{First}(n, d) * \mathsf{Last}(n, e) \\
&\quad \exists \mathbf{y}, \mathit{in}, \mathit{out}. \\
&\quad \langle\langle t'' \circ_{\mathbf{x}} \mathbf{y} \rangle\rangle_{I \uplus [\mathbf{y} \mapsto \mathit{in}], [\mathbf{y} \mapsto \mathit{out}]}^{(d,e)(\mathsf{null}, n, \mathsf{null})} * \langle \mathbf{y} \to t' \rangle^{I \uplus [\mathbf{y} \mapsto \mathit{in}], [\mathbf{y} \mapsto \mathit{out}]} \\
&= \exists \mathbf{y}, \mathit{in}, \mathit{out}. \\
&\quad \langle\langle n[t'' \circ_{\mathbf{x}} \mathbf{y}] \rangle\rangle_{I \uplus [\mathbf{y} \mapsto \mathit{in}], [\mathbf{y} \mapsto \mathit{out}]}^{(i,j)(l,u,r)} * \langle \mathbf{y} \to t' \rangle^{I \uplus [\mathbf{y} \mapsto \mathit{in}], [\mathbf{y} \mapsto \mathit{out}]}
\end{aligned}$$

Case 4. $t = t_1 \otimes t_2$

Case 4.1 $\mathbf{x} \notin addrs(t_1) \wedge \mathbf{x} \notin addrs(t_2)$
This case holds trivially since it contradicts our assumption that $\mathbf{x} \in addrs(t_1 \otimes t_2)$.

Case 4.2 $\mathbf{x} \in addrs(t_1) \wedge \mathbf{x} \notin addrs(t_2)$.

Proof.

$$
\begin{aligned}
\langle\langle t \circ_{\mathbf{x}} t' \rangle\rangle_I^{(i,j)(l,u,r)} &= \langle\langle (t_1 \otimes t_2) \circ_{\mathbf{x}} t' \rangle\rangle_I^{(i,j)(l,u,r)} \\
&= \langle\langle (t_1 \circ_{\mathbf{x}} t') \otimes t_2 \rangle\rangle_I^{(i,j)(l,u,r)} \\
&= \exists p, q.\, \langle\langle t_1 \circ_{\mathbf{x}} t' \rangle\rangle_I^{(i,p)(l,u,q)} * \langle\langle t_2 \rangle\rangle_I^{(q,j)(p,u,r)} \\
\text{(I. H.)} &= \exists p, q.\, \exists \mathbf{y}, out, in. \\
&\quad \langle\langle t_1 \circ_{\mathbf{x}} \mathbf{y} \rangle\rangle_{I\uplus[\mathbf{y}\mapsto in],[\mathbf{y}\mapsto out]}^{(i,p)(l,u,q)} * \langle \mathbf{y} \to t' \rangle^{I\uplus[\mathbf{y}\mapsto in],[\mathbf{y}\mapsto out]} \\
&\quad * \langle\langle t_2 \rangle\rangle_I^{(q,j)(p,u,r)} \\
\text{Lemma 11} &= \exists p, q.\, \exists \mathbf{y}, out, in. \\
&\quad \langle\langle t_1 \circ_{\mathbf{x}} \mathbf{y} \rangle\rangle_{I\uplus[\mathbf{y}\mapsto in],[\mathbf{y}\mapsto out]}^{(i,p)(l,u,q)} * \langle \mathbf{y} \to t' \rangle^{I\uplus[\mathbf{y}\mapsto in],[\mathbf{y}\mapsto out]} \\
&\quad * \langle\langle t_2 \rangle\rangle_{I\uplus[\mathbf{y}\mapsto in],[\mathbf{y}\mapsto out]}^{(q,j)(p,u,r)} \\
&= \exists \mathbf{y}, out, in. \\
&\quad \langle\langle (t_1 \otimes t_2) \circ_{\mathbf{x}} \mathbf{y} \rangle\rangle_{I\uplus[\mathbf{y}\mapsto in],[\mathbf{y}\mapsto out]}^{(i,j)(l,u,r)} \\
&\quad * \langle \mathbf{y} \to t' \rangle^{I\uplus[\mathbf{y}\mapsto in],[\mathbf{y}\mapsto out]}
\end{aligned}
$$

□

Case 4.3 $\mathbf{x} \notin addrs(t_1) \wedge \mathbf{x} \in addrs(t_2)$.
The proof of this case is analogous to that of the previous case and is omitted here.

Case 4.4 $\mathbf{x} \in addrs(t_1) \wedge \mathbf{x} \in addrs(t_2)$
This case holds trivially since $t = t_1 \otimes t_2 \notin \textsc{Data}_{\mathbb{T}}$.

Lemma 11.

$$
\begin{aligned}
&\forall i, j, l, u, r, \forall t \in \textsc{Data}_{\mathbb{T}},\ \forall I_c, I_d, I_1, I_2 \in \mathcal{I}_\tau \\
&\left(\mathrm{dom}({I_1}^{\mathsf{in}}) \cup \mathrm{dom}({I_1}^{\mathsf{out}}) \cup \mathrm{dom}({I_2}^{\mathsf{in}}) \cup \mathrm{dom}({I_2}^{\mathsf{out}})\right) \cap addrs(t) = \varnothing \\
&\Longrightarrow \\
&\langle\langle t \rangle\rangle_{I_c, I_d}^{(i,j)(l,u,r)} = \langle\langle t \rangle\rangle_{I_c \uplus I_1, I_d \uplus I_2}^{(i,j)(l,u,r)}
\end{aligned}
$$

B. Auxiliary Lemmas ($\tau : \mathbb{T} \to \mathbb{C}$)

The following lemmata are used in the soundness proof of translation $\tau : \mathbb{T} \to \mathbb{C}$. Lemma 12 is used in the proof of lemma 5 (in particular the proof of `deleteTree` axiom correctness). Lemmata 13 and 14 are used in the proof of lemma 12.

Lemma 12 (Crust Elimination)**.**

$$
\begin{array}{l}
\forall t \in \textsc{Data}_{\mathbb{T}}.\ \forall I \in \mathcal{I}_{\tau}.\ \forall i, j, l, u, r, t, gp \\
\mathit{addrs}(t) = \varnothing \implies \\
\qquad \begin{pmatrix} (l \neq \mathsf{null} \wedge \mathsf{Right}(l, i, u) * l.u \to u) \\ \vee (l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{First}(u, i) * u.u \to gp) \\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
\qquad * \begin{pmatrix} (r \neq \mathsf{null} \wedge \mathsf{Left}(r, j, u) * r.u \to u) \\ \vee (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{Last}(u, j) * u.u \to gp) \\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
\qquad\qquad * \langle\langle t \rangle\rangle_I^{(i,j)(l,u,r)} \\
\qquad\qquad\qquad \equiv \\
\begin{pmatrix} (l \neq \mathsf{null} \wedge l.r \to i * l.rL \to 0 * l.u \to u) \\ \vee (l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.d \to i * u.dL \to 0 * u.u \to gp) \\ \vee (l \doteq \mathsf{null} * u \doteq \mathsf{null}) \end{pmatrix} \\
* \begin{pmatrix} (r \neq \mathsf{null} \wedge r.l \to j * r.lL \to 0 * r.u \to u) \\ \vee (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.e \to j * u.eL \to 0 * u.u \to gp) \\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
\qquad\qquad * ||t||^{(i,j)(l,u,r)}
\end{array}
$$

where the crust-less tree context translation function is defined inductively as:

$$
\begin{array}{rcl}
||\varnothing||^{(i,j)(l,u,r)} & \triangleq & (i \doteq r) * (j \doteq l) \\
\\
||n[ct]||^{(i,j)(l,u,r)} & \triangleq & (i \doteq j \doteq n) * n.u \to u * \exists d, e. \\
& & * n.l \to l * n.lL \to 0 * n.r \to r * n.rL \to 0 \\
& & * n.d \to d * n.dL \to 0 * n.e \to e * n.eL \to 0 \\
& & * ||ct||^{(d,e)(\mathsf{null},n,\mathsf{null})} \\
\\
||\mathbf{x}||^{(i,j)(l,u,r)} & \triangleq & \text{undefined} \\
\\
||ct_1 \otimes ct_2||^{(i,j)(l,u,r)} & \triangleq & \exists p, q.\ ||ct_1||^{(i,p)(l,u,q)} * ||ct_2||^{(q,j)(p,u,r)}
\end{array}
$$

Proof. There are two cases to consider:

Case 1. $t = \varnothing$

$$
\begin{array}{rcl}
 & & \begin{pmatrix} (l \neq \mathsf{null} \wedge \mathsf{Right}\,(l,i,u) * l.u \to u) \\ \vee (l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{First}\,(u,i) * u.u \to gp) \\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
 & & * \begin{pmatrix} (r \neq \mathsf{null} \wedge \mathsf{Left}\,(r,j,u) * r.u \to u) \\ \vee (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{Last}\,(u,j) * u.u \to gp) \\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
 & & * \langle\langle \varnothing \rangle\rangle_I^{(i,j)(l,u,r)} \\
 & \equiv & \begin{pmatrix} (l \neq \mathsf{null} \wedge \mathsf{Right}\,(l,r,u) * l.u \to u) \\ \vee (l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{First}\,(u,r) * u.u \to gp) \\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
 & & * \begin{pmatrix} (r \neq \mathsf{null} \wedge \mathsf{Left}\,(r,l,u) * r.u \to u) \\ \vee (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{Last}\,(u,l) * u.u \to gp) \\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
 & & * ||\varnothing||^{(i,j)(l,u,r)} \\
\text{Lemma 13} \equiv & & \begin{pmatrix} \big(l \neq \mathsf{null} \wedge l.u \to u * l.rL \to 0 * l.r \to i\big) \\ \vee \big(l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.u \to gp * u.dL \to 0 * u.d \to i\big) \\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
 & & * \begin{pmatrix} \big(r \neq \mathsf{null} \wedge r.u \to u * r.lL \to 0 * r.l \to j\big) \\ \vee \big(r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.u \to gp * u.eL \to 0 * u.e \to j\big) \\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
 & & * ||\varnothing||^{(i,j)(l,u,r)}
\end{array}
$$

Case 2. $t \neq \varnothing$

$$
\begin{aligned}
& \begin{pmatrix} (l \neq \mathsf{null} \wedge \mathsf{Right}\,(l,i,u) * l.u \to u) \\ \vee (l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{First}\,(u,i) * u.u \to gp) \\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
& * \begin{pmatrix} (r \neq \mathsf{null} \wedge \mathsf{Left}\,(r,j,u) * r.u \to u) \\ \vee (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{Last}\,(u,j) * u.u \to gp) \\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
& * \langle\langle t \rangle\rangle_I^{(i,j)(l,u,r)} \\
\text{Lemma 14} \equiv\ & \begin{pmatrix} (l \neq \mathsf{null} \wedge \mathsf{Right}\,(l,i,u) * l.u \to u) \\ \vee (l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{First}\,(u,i) * u.u \to gp) \\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
& * \begin{pmatrix} (r \neq \mathsf{null} \wedge \mathsf{Left}\,(r,j,u) * r.u \to u) \\ \vee (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{Last}\,(u,j) * u.u \to gp) \\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
& * \mathsf{Left}\,(i,l,u) * \mathsf{Right}\,(j,r,u) \\
& * \left(\begin{pmatrix} i.l \to l * i.lL \to 0 \\ j.r \to r * j.rL \to 0 \end{pmatrix} \mathrel{-\!\!*} \|t\|^{(i,j)(l,u,r)} \right) \\
\text{Lemma 13} \equiv\ & \begin{pmatrix} \big(l \neq \mathsf{null} \wedge l.u \to u * l.rL \to 0 * l.r \to i\big) \\ \vee \big(l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.u \to gp * u.dL \to 0 * u.d \to i\big) \\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
& * \begin{pmatrix} \big(r \neq \mathsf{null} \wedge r.u \to u * r.lL \to 0 * r.l \to j\big) \\ \vee \big(r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.u \to gp * u.eL \to 0 * u.e \to j\big) \\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
& * i.l \to l * i.lL \to 0 * j.r \to r * j.rL \to 0 \\
& * \left(\begin{pmatrix} i.l \to l * i.lL \to 0 \\ j.r \to r * j.rL \to 0 \end{pmatrix} \mathrel{-\!\!*} \|t\|^{(i,j)(l,u,r)} \right) \\
\equiv\ & \begin{pmatrix} \big(l \neq \mathsf{null} \wedge l.u \to u * l.rL \to 0 * l.r \to i\big) \\ \vee \big(l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.u \to gp * u.dL \to 0 * u.d \to i\big) \\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
& * \begin{pmatrix} \big(r \neq \mathsf{null} \wedge r.u \to u * r.lL \to 0 * r.l \to j\big) \\ \vee \big(r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.u \to gp * u.eL \to 0 * u.e \to j\big) \\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
& * \|t\|^{(i,j)(l,u,r)}
\end{aligned}
$$

□

Lemma 13.

$$\forall l, u, r, gp.$$
$$\begin{pmatrix}(l \neq \mathsf{null} \wedge \mathsf{Right}\,(l, r, u) * l.u \to u)\\ \vee (l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{First}\,(u, r) * u.u \to gp)\\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null})\end{pmatrix}$$
$$* \begin{pmatrix}(r \neq \mathsf{null} \wedge \mathsf{Left}\,(r, l, u) * r.u \to u)\\ \vee (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{Last}\,(u, l) * u.u \to gp)\\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null})\end{pmatrix}$$
$$\equiv$$
$$\begin{pmatrix}(l \neq \mathsf{null} \wedge l.r \to r * l.rL \to 0 * l.u \to u)\\ \vee (l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.d \to r * u.dL \to 0 * u.u \to gp)\\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null})\end{pmatrix}$$
$$* \begin{pmatrix}(r \neq \mathsf{null} \wedge r.l \to l * r.lL \to 0 * r.u \to u)\\ \vee (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.e \to l * u.eL \to 0 * u.u \to gp)\\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null})\end{pmatrix}$$

Proof.

$$\begin{pmatrix}(l \neq \mathsf{null} \wedge \mathsf{Right}\,(l, r, u) * l.u \to u)\\ \vee (l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{First}\,(u, r) * u.u \to gp)\\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null})\end{pmatrix}$$
$$* \begin{pmatrix}(r \neq \mathsf{null} \wedge \mathsf{Left}\,(r, l, u) * r.u \to u)\\ \vee (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{Last}\,(u, l) * u.u \to gp)\\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null})\end{pmatrix}$$
$$\equiv \begin{pmatrix}\begin{pmatrix} l \neq \mathsf{null} \wedge \mathsf{Right}\,(l, r, u) * l.u \to u\\ \begin{pmatrix}(r \neq \mathsf{null} \wedge \mathsf{Left}\,(r, l, u) * r.u \to u)\\ \vee (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{Last}\,(u, l) * u.u \to gp)\\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null})\end{pmatrix}\end{pmatrix}\\ \vee \begin{pmatrix} l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{First}\,(u, r) * u.u \to gp)\\ \begin{pmatrix}(r \neq \mathsf{null} \wedge \mathsf{Left}\,(r, l, u) * r.u \to u)\\ \vee (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{Last}\,(u, l) * u.u \to gp)\end{pmatrix}\end{pmatrix}\\ \vee \begin{pmatrix} l = \mathsf{null} \wedge u = \mathsf{null} \wedge\\ \begin{pmatrix}(r \neq \mathsf{null} \wedge \mathsf{Left}\,(r, l, u) * r.u \to u)\\ \vee (r \doteq \mathsf{null})\end{pmatrix}\end{pmatrix}\end{pmatrix}$$
//Use $[\mathcal{W}]$ tokens to get resources out.

$$
\left(\begin{array}{l}
\left(\begin{array}{l}
l \neq \mathsf{null} \wedge \exists \mathsf{R}_{l.r}.\, [\mathcal{L}]_1^{\mathsf{R}_{l.r}} * [\mathcal{U}]_1^{\mathsf{R}_{l.r}} * [\mathcal{W}]_1^{\mathsf{R}_{l.r}} * l.u \overset{\frac{1}{2}}{\mapsto} u \\
\left(\begin{array}{l}
\left(\begin{array}{l}
r \neq \mathsf{null} \wedge \exists \mathsf{R}_{r.l}.\, [\mathcal{L}]_1^{\mathsf{R}_{r.l}} * [\mathcal{U}]_1^{\mathsf{R}_{r.l}} * [\mathcal{W}]_1^{\mathsf{R}_{r.l}} * r.u \overset{\frac{1}{2}}{\mapsto} u \\
* l.r \to r * r.l \to l * \boxed{l.rL \to 0 * l.u \overset{\frac{1}{4}}{\mapsto} u * r.u \overset{\frac{1}{4}}{\mapsto} u}^{\mathsf{R}_{l.r}}_{\mathsf{RC}(\mathsf{R}_{l.r},l,u)} \\
* \boxed{r.lL \to 0 * l.u \overset{\frac{1}{4}}{\mapsto} u * r.u \overset{\frac{1}{4}}{\mapsto} u}^{\mathsf{R}_{r.l}}_{\mathsf{LC}(\mathsf{R}_{r.l},r,u)}
\end{array}\right) \\
* \left(\begin{array}{l}
r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \exists \mathsf{R}_{u.e}.\, [\mathcal{L}]_1^{\mathsf{R}_{u.e}} * [\mathcal{U}]_1^{\mathsf{R}_{u.e}} * [\mathcal{W}]_1^{\mathsf{R}_{u.e}} * u.u \overset{\frac{1}{2}}{\mapsto} gp \\
* l.r \to r * u.e \to l * \boxed{l.rL \to 0 * l.u \overset{\frac{1}{4}}{\mapsto} u * u.u \overset{\frac{1}{4}}{\mapsto} gp}^{\mathsf{R}_{l.r}}_{\mathsf{RC}(\mathsf{R}_{l.r},l,u)} \\
* \boxed{u.eL \to 0 * l.u \overset{\frac{1}{4}}{\mapsto} u * u.u \overset{\frac{1}{4}}{\mapsto} gp}^{\mathsf{R}_{u.e}}_{\mathsf{EC}(\mathsf{R}_{u.e},u)}
\end{array}\right) \\
\vee \left(\begin{array}{l}
r = \mathsf{null} \wedge u = \mathsf{null} \wedge l.u \overset{\frac{1}{4}}{\mapsto} u * \boxed{l.u \overset{\frac{1}{4}}{\mapsto} u * l.r \to r}^{\mathsf{R}_{l.r}}_{\mathsf{RC}(\mathsf{R}_{l.r},l,u)}
\end{array}\right)
\end{array}\right) \\
\equiv \left(\begin{array}{l}
l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \exists \mathsf{R}_{u.d}.\, [\mathcal{L}]_1^{\mathsf{R}_{u.d}} * [\mathcal{U}]_1^{\mathsf{R}_{u.d}} * [\mathcal{W}]_1^{\mathsf{R}_{u.d}} * u.u \overset{\frac{1}{2}}{\mapsto} gp \\
\left(\begin{array}{l}
\left(\begin{array}{l}
r \neq \mathsf{null} \wedge \exists \mathsf{R}_{r.l}.\, [\mathcal{A}]_1^{\mathsf{R}_{r.l}} * [\mathcal{L}]_1^{\mathsf{R}_{r.l}} * [\mathcal{U}]_1^{\mathsf{R}_{r.l}} * [\mathcal{W}]_1^{\mathsf{R}_{r.l}} * r.u \overset{\frac{1}{2}}{\mapsto} u \\
* u.d \to r * r.l \to l * \boxed{u.dL \to 0 * u.u \overset{\frac{1}{4}}{\mapsto} gp * r.u \overset{\frac{1}{4}}{\mapsto} u}^{\mathsf{R}_{u.d}}_{\mathsf{DC}(\mathsf{R}_{u.d},u)} \\
* \boxed{r.lL \to 0 * u.u \overset{\frac{1}{4}}{\mapsto} gp * r.u \overset{\frac{1}{4}}{\mapsto} u}^{\mathsf{R}_{r.l}}_{\mathsf{LC}(\mathsf{R}_{r.l},r,u)}
\end{array}\right) \\
\vee \left(\begin{array}{l}
r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \exists \mathsf{R}_{r.l}.\, [\mathcal{L}]_1^{\mathsf{R}_{u.e}} * [\mathcal{U}]_1^{\mathsf{R}_{u.e}} * [\mathcal{W}]_1^{\mathsf{R}_{u.e}} \\
* \boxed{u.dL \to 0 * u.u \overset{\frac{1}{4}}{\mapsto} gp * u.d \to r}^{\mathsf{R}_{u.d}}_{\mathsf{DC}(\mathsf{R}_{u.d},u)} \\
* \boxed{u.eL \to 0 * u.u \overset{\frac{1}{4}}{\mapsto} gp * u.e \to l}^{\mathsf{R}_{u.e}}_{\mathsf{EC}(\mathsf{R}_{u.e},u)}
\end{array}\right)
\end{array}\right) \\
\vee \left(\begin{array}{l}
l = \mathsf{null} \wedge u = \mathsf{null} \wedge \\
\left(\begin{array}{l}
r \neq \mathsf{null} \wedge \wedge \exists \mathsf{R}_{r.l}.\, [\mathcal{L}]_1^{\mathsf{R}_{r.l}} * [\mathcal{U}]_1^{\mathsf{R}_{r.l}} * [\mathcal{W}]_1^{\mathsf{R}_{r.l}} \\
* \boxed{r.lL \to 0 * r.l \to l * r.u \overset{\frac{1}{4}}{\mapsto} u}^{\mathsf{R}_{r.l}}_{\mathsf{LC}(\mathsf{R}_{r.l},r,u)}
\end{array}\right) \\
\vee (r \doteq \mathsf{null})
\end{array}\right)
\end{array}\right)
$$

//Destroy $\mathsf{R}_{l.r}, \mathsf{R}_{u.d}, \mathsf{R}_{r.l}, \mathsf{R}_{u.e}$ regions since we have all tokens on them.

$$
\equiv \quad \begin{pmatrix} \big(l \neq \mathsf{null} \wedge l.u \to u * l.rL \to 0 * l.r \to r\big) \\ \vee \big(l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.u \to gp * u.dL \to 0 * u.d \to r\big) \\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix}
$$
$$
\quad * \begin{pmatrix} \big(r \neq \mathsf{null} \wedge r.u \to u * r.lL \to 0 * r.l \to l\big) \\ \vee \big(r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.u \to gp * u.eL \to 0 * u.e \to l\big) \\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix}
$$

□

Lemma 14.

$$\begin{array}{l}\forall t \in \textsc{Data}_{\mathbb{T}}.\ \forall i, j, l, u, r, t, gp \\ addrs(t) = \varnothing \wedge t \neq \varnothing \implies \\ \qquad\qquad \langle\langle t \rangle\rangle_I^{(i,j)(l,u,r)} \\ \qquad\qquad\qquad \equiv \\ \qquad\qquad \mathsf{Left}(i,l,u) * \mathsf{Right}(j,r,u) \\ \qquad * \left(\begin{pmatrix} i.l \to l * i.lL \to 0 \\ j.r \to r * j.rL \to 0 \end{pmatrix} \mathrel{-\!\!*} ||t||^{(i,j)(l,u,r)} \right)\end{array}$$

Proof. By induction over the structure of t.

Case $t = \varnothing$
This case holds vacuously as it contradicts the assumption that $t \neq \varnothing$.

Case $t = \mathbf{x}$
This case holds vacuously as $addrs(t) \neq \varnothing$.

Case $t = n[t']$
If $addrs(t') \neq \varnothing$, this case holds vacuously as it contradicts our assumption that $addrs(n[t']) = \varnothing$. On the other hand, if $addrs(t') = \varnothing$, we have:

$$\begin{array}{rcl} \langle\langle n[t'] \rangle\rangle_I^{(i,j)(l,u,r)} & \equiv & (i \doteq j \doteq n) * n.u \to u * \exists d, e. \\ & & \mathsf{Left}(n,l,u) * \mathsf{Right}(n,r,u) * \mathsf{First}(n,d) * \mathsf{Last}(n,e) \\ & & * \langle\langle t' \rangle\rangle_I^{(d,e)(\mathsf{null},n,\mathsf{null})} \\ \text{(I.H.)} & \equiv & (i \doteq j \doteq n) * n.u \to u * \exists d, e. \\ & & \mathsf{Left}(n,l,u) * \mathsf{Right}(n,r,u) * \mathsf{First}(n,d) * \mathsf{Last}(n,e) \\ & & * \mathsf{Left}(d, \mathsf{null}, n) * \mathsf{Right}(e, \mathsf{null}, n) \\ & & * \left(\begin{pmatrix} d.l \to \mathsf{null} * d.lL \to 0 \\ e.r \to \mathsf{null} * e.rL \to 0 \end{pmatrix} \mathrel{-\!\!*} ||t'||^{(d,e)(\mathsf{null},n,\mathsf{null})} \right) \\ \text{Lemma 13} & \equiv & (i \doteq j \doteq n) * n.u \to u * \exists d, e. \\ & & * \mathsf{Left}(n,l,u) * \mathsf{Right}(n,r,u) \\ & & * n.d \to d * n.dL \to 0 * n.e \to e * n.eL \to 0 \\ & & * d.l \to \mathsf{null} * d.lL \to 0 * e.r \to \mathsf{null} * e.rL \to 0 \\ & & * \left(\begin{pmatrix} d.l \to \mathsf{null} * d.lL \to 0 \\ e.r \to \mathsf{null} * e.rL \to 0 \end{pmatrix} \mathrel{-\!\!*} ||t'||^{(d,e)(\mathsf{null},n,\mathsf{null})} \right) \end{array}$$

$$
\begin{aligned}
\equiv\ & (i \doteq j \doteq n) * n.u \to u * \exists d, e. \\
& * \mathsf{Left}\,(n, l, u) * \mathsf{Right}\,(n, r, u) \\
& * n.d \to d * n.dL \to 0 * n.e \to e * n.eL \to 0 * n.nL \to 0 \\
& * \|t'\|^{(d,e)(\mathsf{null},n,\mathsf{null})} \\
\equiv\ & \mathsf{Left}\,(i, l, u) * \mathsf{Right}\,(j, r, u) \\
& * \begin{pmatrix} i.l \to l * i.lL \to 0 \\ j.r \to r * j.rL \to 0 \end{pmatrix} \mathrel{-\!\!*} \|n[t']\|^{(i,j)(l,u,r)}
\end{aligned}
$$

Case $t = t_1 \otimes t_2$
If $addrs\,(t_1) \neq \varnothing \vee addrs\,(t_2) \neq \varnothing$, this case holds vacuously as it contradicts our assumption that $addrs\,(t) = \varnothing$. If $addrs\,(t_1) = \varnothing \wedge addrs\,(t_2) = \varnothing$ then we have the following four cases:

Case 1. $t_1 = \varnothing \wedge t_2 = \varnothing$
This case holds vacuously as we have: $t = t_1 \otimes t_2 = \varnothing \otimes \varnothing = \varnothing$

Case 2. $t_1 = \varnothing \wedge t_2 \neq \varnothing$

$$
\begin{aligned}
\langle\langle t_1 \otimes t_2 \rangle\rangle_I^{(i,j)(l,u,r)} \equiv\ & \langle\langle \varnothing \otimes t_2 \rangle\rangle_I^{(i,j)(l,u,r)} \\
\equiv\ & \langle\langle t_2 \rangle\rangle_I^{(i,j)(l,u,r)} \\
(\text{I.H.}) \equiv\ & \mathsf{Left}\,(n, l, u) * \mathsf{Right}\,(n, r, u) \\
& * \begin{pmatrix} i.l \to l * i.lL \to 0 \\ j.r \to r * j.rL \to 0 \end{pmatrix} \mathrel{-\!\!*} \|t_2\|^{(i,j)(l,u,r)} \\
\equiv\ & \mathsf{Left}\,(n, l, u) * \mathsf{Right}\,(n, r, u) \\
& * \begin{pmatrix} i.l \to l * i.lL \to 0 \\ j.r \to r * j.rL \to 0 \end{pmatrix} \mathrel{-\!\!*} \|t_1 \otimes t_2\|^{(i,j)(l,u,r)}
\end{aligned}
$$

Case 3. $t_1 \neq \varnothing \wedge t_2 = \varnothing$
This case is analogous to the previous case and is omitted here.

Case 4. $t_1 \neq \varnothing \wedge t_2 \neq \varnothing$

$$
\begin{aligned}
& \langle\langle t_1 \otimes t_2 \rangle\rangle_I^{(i,j)(l,u,r)} \\
\equiv\ & \exists p, q.\, \langle\langle t_1 \rangle\rangle_I^{(i,p)(l,u,q)} * \langle\langle t_2 \rangle\rangle_I^{(q,j)(p,u,r)} \\
(\text{I.H.}) \equiv\ & \exists p, q.\, \mathsf{Left}\,(i,l,u) * \mathsf{Right}\,(p,q,u) \\
& * \begin{pmatrix} i.l \to l * i.lL \to 0 \\ p.r \to q * p.rL \to 0 \end{pmatrix} \mathrel{-\!\!*} \|t_1\|^{(i,p)(l,u,q)} \\
& * \mathsf{Left}\,(q,p,u) * \mathsf{Right}\,(j,r,u) \\
& * \begin{pmatrix} q.l \to p * i.lL \to 0 \\ j.r \to r * j.rL \to 0 \end{pmatrix} \mathrel{-\!\!*} \|t_2\|^{(q,j)(p,u,q)} \\
\text{Lemma 13} \equiv\ & \mathsf{Left}\,(i,l,u) * \mathsf{Right}\,(j,r,u) \\
& \exists p, q.\, p.r \to q * p.rL \to 0 * q.l \to p * q.lL \to 0 \\
& * \begin{pmatrix} i.l \to l * i.lL \to 0 \\ p.r \to q * p.rL \to 0 \\ q.l \to p * i.lL \to 0 \\ j.r \to r * j.rL \to 0 \end{pmatrix} \mathrel{-\!\!*} \begin{pmatrix} \|t_1\|^{(i,p)(l,u,q)} \\ * \|t_2\|^{(q,j)(p,u,q)} \end{pmatrix} \\
\equiv\ & \mathsf{Left}\,(i,l,u) * \mathsf{Right}\,(j,r,u) \\
& * \begin{pmatrix} i.l \to l * i.lL \to 0 \\ j.r \to r * j.rL \to 0 \end{pmatrix} \mathrel{-\!\!*} \begin{pmatrix} \|t_1 \otimes t_2\|^{(i,j)(l,u,r)} \end{pmatrix}
\end{aligned}
$$

□

C. Abstract (de)Allocation ($\theta : \mathbb{T} \to \mathbb{C}$)

In the lemmata given in this report, we use the following notation for brevity.

$$\langle\langle t \rangle\rangle_I^{(i,j)(l,u,r)(\pi)} \triangleq \mathsf{treeFrag}\,(I,t)\,(i,j)\,(l,u,r)\,(\pi)$$

Lemma 15 (Abstract Allocation/Deallocation)**.** For all $\mathbf{a} \in \textsc{SAdd} \uplus \{\mathcal{R}\}$, $\mathbf{x}, \mathbf{y} \in \textsc{SAdd}$, $t, t' \in \textsc{Data}_{\mathbb{T}}$ and $I \in \mathcal{I}_\theta$,

$$\mathsf{tree}\left(I, \mathbf{a}, t \circ_{\mathbf{x}} t'\right) \equiv \exists \mathbf{y} \in \textsc{SAdd}, in, out.\, \mathsf{tree}\left(I', \mathbf{a}, t \circ_{\mathbf{x}} \mathbf{y}\right) * \mathsf{tree}\left(I', \mathbf{y}, t'\right)$$

with

$$I' \triangleq \left(I^{\mathsf{in}}[\mathbf{y} \mapsto in], I^{\mathsf{out}}[\mathbf{y} \mapsto out]\right)$$

Proof. Let

$$k \triangleq \begin{cases} \left(I^{\mathsf{in}}(\mathbf{a}), I^{\mathsf{out}}(\mathbf{a})\right) & \text{if } \mathbf{a} \in \textsc{SAdd} \\ ((i,j)(\mathsf{null}, \mathsf{null}, \mathsf{null}, 1)) & \text{if } \mathbf{a} \in \{\mathcal{R}\} \end{cases}$$

for some i, j. Then we have:

$$\begin{array}{rcl} \mathsf{tree}\,(I, \mathbf{a}, t \circ_{\mathbf{x}} t') = & \langle\langle t \circ_{\mathbf{x}} t' \rangle\rangle_I^k & \\ \text{By Lemma 16} = & \exists \mathbf{y}, in, out. & \\ & \langle\langle t \circ_{\mathbf{x}} \mathbf{y} \rangle\rangle^k_{I \uplus [\mathbf{y} \mapsto in], [\mathbf{y} \mapsto out]} * \langle \mathbf{y} \to t' \rangle^{I \uplus [\mathbf{y} \mapsto in], [\mathbf{y} \mapsto out]} & \\ = & \exists \mathbf{y}, out, in. & \\ & \langle \mathbf{a} \to t \circ_{\mathbf{x}} \mathbf{y} \rangle^{I \uplus [\mathbf{y} \mapsto in], [\mathbf{y} \mapsto out]} * \langle \mathbf{y} \to t' \rangle^{I \uplus [\mathbf{y} \mapsto in], [\mathbf{y} \mapsto out]} & \\ = & \exists \mathbf{y}, out, in. & \\ & \mathsf{tree}\,(I', \mathbf{a}, t \circ_{\mathbf{x}} \mathbf{y}) * \mathsf{tree}\,(I', \mathbf{y}, t') & \end{array}$$

□

Lemma 16 (Crust Inclusion)**.**

$$\begin{array}{l} \forall t, t' \in \textsc{Data}_{\mathbb{T}}. \\ \forall i, j, l, u, r, t, \pi\ . \\ \mathbf{x} \in addrs\,(t) \implies \\ \qquad \langle\langle t \circ_{\mathbf{x}} t' \rangle\rangle_I^{(i,j)(l,u,r)(\pi)} \\ \qquad = \\ \exists \mathbf{y} \in \textsc{SAdd}.\, \exists out \in \textsc{Out}_\theta, in \in \textsc{In}_\theta. \\ \langle\langle t \circ_{\mathbf{x}} \mathbf{y} \rangle\rangle^{(i,j)(l,u,r)(\pi)}_{I \uplus [\mathbf{y} \mapsto in], [\mathbf{y} \mapsto out]} * \langle \mathbf{y} \to t' \rangle^{I \uplus [\mathbf{y} \mapsto in], [\mathbf{y} \mapsto out]} \end{array}$$

Proof. By induction over the structure of t. In the following proofs we write S for SAdd for brevity.

Case 1. $t = \varnothing$
This case holds trivially as $\mathbf{x} \notin \mathit{addrs}(\varnothing)$.

Case 2. $t = \mathbf{z}$
If $\mathbf{z} \neq \mathbf{x}$, then the case holds vacuously since this contradicts our assumption that $\mathbf{x} \in \mathit{addrs}(t)$.
If $\mathbf{z} = \mathbf{x}$, then for arbitrary i, j, l, u, r, t, π, pick a fresh abstract address $\mathbf{y} \in$ SAdd, and let:

$$\mathit{in} = (i, j), \quad \mathit{out} = (l, u, r, \pi)$$

then we have:

$$\begin{aligned}
\langle\langle \mathbf{z} \circ_{\mathbf{x}} t' \rangle\rangle_I^{(i,j)(l,u,r)(\pi)} &= \langle\langle t' \rangle\rangle_I^{(i,j)(l,u,r)(\pi)} \\
\text{(Lemma 17)} &= \langle\langle t' \rangle\rangle_{I \uplus [\mathbf{z} \mapsto \mathit{in}], [\mathbf{z} \mapsto \mathit{out}]}^{(i,j)(l,u,r)(\pi)} \\
&= \langle\langle t' \rangle\rangle_{I[\mathbf{y} \mapsto \mathit{in}], [\mathbf{y} \mapsto \mathit{out}]}^{(i,j)(l,u,r)(\pi)} * \langle\langle \mathbf{y} \rangle\rangle_{I \uplus [\mathbf{y} \mapsto \mathit{in}], [\mathbf{y} \mapsto \mathit{out}]}^{(i,j)(l,u,r)(\pi)} \\
&= \langle \mathbf{y} \to t' \rangle^{I \uplus [\mathbf{y} \mapsto \mathit{in}], [\mathbf{y} \mapsto \mathit{out}]} * \langle\langle \mathbf{z} \circ_{\mathbf{x}} \mathbf{y} \rangle\rangle_{I \uplus [\mathbf{y} \mapsto \mathit{in}], [\mathbf{y} \mapsto \mathit{out}]}^{(i,j)(l,u,r)(\pi)}
\end{aligned}$$

Case 3. $t = n[t'']$
If $\mathbf{x} \notin \mathit{addrs}(t'')$, then the case holds vacuously since this contradicts our assumption that $\mathbf{x} \in \mathit{addrs}(n[t''])$. If $\mathbf{x} \in \mathit{addrs}(t'')$, then for arbitrary i, j, l, u, r, t, π we have

$$
\begin{array}{rcl}
\langle\langle t \circ_{\mathbf{x}} t' \rangle\rangle_I^{(i,j)(l,u,r)(\pi)} & = & \langle\langle n[t''] \circ_{\mathbf{x}} t' \rangle\rangle_I^{(i,j)(l,u,r)(\pi)} \\
& = & \langle\langle n[t'' \circ_{\mathbf{x}} t'] \rangle\rangle_I^{(i,j)(l,u,r)(\pi)} \\
& = & \exists d, e, \pi_1, \pi_2.\, \pi_1, \pi_2 > 0 \wedge \pi_1 + \pi_2 = 1 \wedge \\
& & (i = j = n) \wedge \\
& & \mathsf{isPLock}\,(u, \pi) * n.u \to u \\
& & \left(\begin{array}{l} (u \neq \mathsf{null} \wedge n.uL = u.nL) \\ \vee (u = \mathsf{null} \wedge n.uL = \mathcal{R} + 1) \end{array} \right) \\
& & * \mathsf{Left}\,(n, l, u) * \mathsf{Right}\,(n, r, u) \\
& & * \mathsf{First}\,(n, d) * \mathsf{Last}\,(n, e) \\
& & * \mathsf{isPLock}\,(n, \pi_1) \\
& & * \langle\langle t'' \circ_{\mathbf{x}} t' \rangle\rangle_I^{(d,e)(\mathsf{null},n,\mathsf{null})(\pi_2)} \\
(\text{I. H.}) & = & \exists d, e, \pi_1, \pi_2.\, \pi_1, \pi_2 > 0 \wedge \pi_1 + \pi_2 = 1 \wedge \\
& & (i = j = n) \wedge \\
& & \mathsf{isPLock}\,(u, \pi) * n.u \to u \\
& & \left(\begin{array}{l} (u \neq \mathsf{null} \wedge n.uL = u.nL) \\ \vee (u = \mathsf{null} \wedge n.uL = \mathcal{R} + 1) \end{array} \right) \\
& & * \mathsf{Left}\,(n, l, u) * \mathsf{Right}\,(n, r, u) \\
& & * \mathsf{First}\,(n, d) * \mathsf{Last}\,(n, e) \\
& & * \mathsf{isPLock}\,(n, \pi_1) \\
& & \exists \mathbf{y}, in, out. \\
& & \langle\langle t'' \circ_{\mathbf{x}} \mathbf{y} \rangle\rangle_{I \uplus [\mathbf{y} \mapsto in], [\mathbf{y} \mapsto out]}^{(d,e)(\mathsf{null},n,\mathsf{null})(\pi_2)} * \langle \mathbf{y} \to t' \rangle^{I \uplus [\mathbf{y} \mapsto in], [\mathbf{y} \mapsto out]} \\
& = & \exists \mathbf{y}, in, out. \\
& & \langle\langle n[t'' \circ_{\mathbf{x}} \mathbf{y}] \rangle\rangle_{I \uplus [\mathbf{y} \mapsto in], [\mathbf{y} \mapsto out]}^{(i,j)(l,u,r)(\pi)} * \langle \mathbf{y} \to t' \rangle^{I \uplus [\mathbf{y} \mapsto in], [\mathbf{y} \mapsto out]}
\end{array}
$$

Case 4. $t = t_1 \otimes t_2$

Case 4.1 $\mathbf{x} \notin addrs\,(t_1) \wedge \mathbf{x} \notin addrs\,(t_2)$
This case holds trivially since it contradicts our assumption that $\mathbf{x} \in addrs\,(t_1 \otimes t_2)$.

Case 4.2 $\mathbf{x} \in addrs\,(t_1) \wedge \mathbf{x} \notin addrs\,(t_2)$.

Proof.

$$
\begin{aligned}
\langle\langle t \circ_{\mathbf{x}} t' \rangle\rangle_I^{(i,j)(l,u,r)(\pi)} &= \langle\langle (t_1 \otimes t_2) \circ_{\mathbf{x}} t' \rangle\rangle_I^{(i,j)(l,u,r)(\pi)} \\
&= \langle\langle (t_1 \circ_{\mathbf{x}} t') \otimes t_2 \rangle\rangle_I^{(i,j)(l,u,r)(\pi)} \\
&= \exists p, q, \pi_1, \pi_2 .\, \pi_1 + \pi_2 = \pi \wedge \\
&\quad \langle\langle t_1 \circ_{\mathbf{x}} t' \rangle\rangle_I^{(i,p)(l,u,q)(\pi_1)} * \langle\langle t_2 \rangle\rangle_I^{(q,j)(p,u,r)(\pi_2)} \\
\text{(I. H.)} &= \exists p, q, \pi_1, \pi_2 .\, \pi_1 + \pi_2 = \pi \wedge \\
&\quad \exists \mathbf{y}, out, in. \\
&\quad \langle\langle t_1 \circ_{\mathbf{x}} \mathbf{y} \rangle\rangle_{I\uplus[\mathbf{y}\mapsto in],[\mathbf{y}\mapsto out]}^{(i,p)(l,u,q)(\pi_1)} * \langle \mathbf{y} \to t' \rangle^{I\uplus[\mathbf{y}\mapsto in],[\mathbf{y}\mapsto out]} \\
&\quad * \langle\langle t_2 \rangle\rangle_I^{(q,j)(p,u,r)(\pi_2)} \\
\text{Lemma 17} &= \exists p, q, \pi_1, \pi_2 .\, \pi_1 + \pi_2 = \pi \wedge \\
&\quad \exists \mathbf{y}, out, in. \\
&\quad \langle\langle t_1 \circ_{\mathbf{x}} \mathbf{y} \rangle\rangle_{I\uplus[\mathbf{y}\mapsto in],[\mathbf{y}\mapsto out]}^{(i,p)(l,u,q)(\pi_1)} * \langle \mathbf{y} \to t' \rangle^{I\uplus[\mathbf{y}\mapsto in],[\mathbf{y}\mapsto out]} \\
&\quad * \langle\langle t_2 \rangle\rangle_{I\uplus[\mathbf{y}\mapsto in],[\mathbf{y}\mapsto out]}^{(q,j)(p,u,r)(\pi_2)} \\
&= \exists \mathbf{y}, out, in. \\
&\quad \langle\langle (t_1 \otimes t_2) \circ_{\mathbf{x}} \mathbf{y} \rangle\rangle_{I\uplus[\mathbf{y}\mapsto in],[\mathbf{y}\mapsto out]}^{(i,j)(l,u,r)(\pi)} \\
&\quad * \langle \mathbf{y} \to t' \rangle^{I\uplus[\mathbf{y}\mapsto in],[\mathbf{y}\mapsto out]}
\end{aligned}
$$

□

Case 4.3 $\mathbf{x} \notin addrs(t_1) \wedge \mathbf{x} \in addrs(t_2)$.
The proof of this case is analogous to that of the previous case and is omitted here.

Case 4.4 $\mathbf{x} \in addrs(t_1) \wedge \mathbf{x} \in addrs(t_2)$
This case holds trivially since $t = t_1 \otimes t_2 \notin \text{DATA}_{\mathbb{T}}$.

Lemma 17.

$$
\begin{aligned}
&\forall i, j, l, u, r, \pi, \forall t \in \text{DATA}_{\mathbb{T}},\ \forall I_c, I_d, I_1, I_2 \in \mathcal{I}_\theta \\
&\big(\text{dom}(I_1{}^{\mathsf{in}}) \cup \text{dom}(I_1{}^{\mathsf{out}}) \cup \text{dom}(I_2{}^{\mathsf{in}}) \cup \text{dom}(I_2{}^{\mathsf{out}})\big) \cap addrs(t) = \varnothing \\
&\Longrightarrow \\
&\langle\langle t \rangle\rangle_{I_c,I_d}^{(i,j)(l,u,r)(\pi)} = \langle\langle t \rangle\rangle_{I_c\uplus I_1,I_d\uplus I_2}^{(i,j)(l,u,r)(\pi)}
\end{aligned}
$$

D. Auxiliary Lemmas ($\theta : \mathbb{T} \to \mathbb{C}$)

The following lemmata are used in the soundness proof of translation $\theta : \mathbb{T} \to \mathbb{C}$. Lemma 18 is used in the proof of lemma 8 (in particular the proof of `deleteTree` axiom correctness). Lemmata 19 and 20 are used in the proof of lemma 18.

Lemma 18 (Crust Elimination)**.**

$$
\begin{array}{l}
\forall t \in \textsc{Data}_{\mathbb{T}}.\ \forall i,j,l,u,r,t,gp,\pi_1,\pi_2.\ \ \pi_1 + \pi_2 = 1 \\
addrs(t) = \varnothing \implies \\
\qquad \begin{pmatrix} (l \neq \mathsf{null} \wedge \mathsf{Right}(l,i,u) * l.u \to u) \\ \vee (l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{First}(u,i) * u.u \to gp) \\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
\qquad * \begin{pmatrix} (r \neq \mathsf{null} \wedge \mathsf{Left}(r,j,u) * r.u \to u) \\ \vee (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{Last}(u,j) * u.u \to gp) \\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
\qquad\qquad * \mathsf{isPLock}(u,\pi_1) * \langle\langle t \rangle\rangle_I^{(i,j)(l,u,r)(\pi_2)} \\
\qquad\qquad\qquad \equiv \\
\begin{pmatrix} (l \neq \mathsf{null} \wedge l.r \to i * l.rL \to 0 * l.u \to u) \\ \vee (l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.d \to i * u.dL \to 0 * u.u \to gp) \\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null} \wedge \mathcal{R} \to i) \end{pmatrix} \\
* \begin{pmatrix} (r \neq \mathsf{null} \wedge r.l \to j * r.lL \to 0 * r.u \to u) \\ \vee (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.e \to j * u.eL \to 0 * u.u \to gp) \\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
\quad * \big(\ (u \neq \mathsf{null} \wedge u.nL \to 0) \vee (u = \mathsf{null} \wedge \mathcal{R} + 1 \to 0)\ \big) \\
\qquad * \left((l = u = \mathsf{null} \wedge \mathcal{R} \to i) \vee \mathrm{emp}\right) * ||t||^{(i,j)(l,u,r)}
\end{array}
$$

where the crust-less tree context translation function is defined inductively as:

$$
\begin{array}{rcl}
||\varnothing||^{(i,j)(l,u,r)} & \triangleq & (i = r) \wedge (j = l) \\
\\
||n[ct]||^{(i,j)(l,u,r)} & \triangleq & (i = j = n) \wedge \\
& & \exists d, e.\, n.u \to u * n.nL \to 0 \\
& & * \left(\begin{array}{l} (u \neq \mathsf{null} \wedge n.uL \to u.nL) \\ \vee (u = \mathsf{null} \wedge n.uL \to t + 1) \end{array} \right) \\
& & * n.l \to l * n.lL \to 0 * n.r \to r * n.rL \to 0 \\
& & * n.d \to d * n.dL \to 0 * n.e \to e * n.eL \to 0 \\
& & ((l = u = r = \mathsf{null} \wedge \mathcal{R} \to i) \vee \mathrm{emp}) \\
& & * \, ||ct||^{(d,e)(\mathsf{null},n,\mathsf{null})} \\
\\
||\mathbf{x}||^{(i,j)(l,u,r)} & \triangleq & \text{undefined} \\
\\
||ct_1 \otimes ct_2||^{(i,j)(l,u,r)} & \triangleq & \exists p, q.\ ||ct_1||^{(i,p)(l,u,q)} * ||ct_2||^{(q,j)(p,u,r)}
\end{array}
$$

Proof. There are two cases to consider:

Case 1. $t = \varnothing$

$$
\begin{aligned}
& \begin{pmatrix} (l \neq \mathsf{null} \wedge \mathsf{Right}\,(l,i,u) * l.u \to u) \\ \vee (l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{First}\,(u,i) * u.u \to gp) \\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
& * \begin{pmatrix} (r \neq \mathsf{null} \wedge \mathsf{Left}\,(r,j,u) * r.u \to u) \\ \vee (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{Last}\,(u,j) * u.u \to gp) \\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
& * \mathsf{isPLock}\,(u,\pi_1) * \langle\langle \varnothing \rangle\rangle_I^{(i,j)(l,u,r)(\pi_2)} \\
\equiv\ & \begin{pmatrix} (l \neq \mathsf{null} \wedge \mathsf{Right}\,(l,i,u) * l.u \to u) \\ \vee (l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{First}\,(u,i) * u.u \to gp) \\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
& * \begin{pmatrix} (r \neq \mathsf{null} \wedge \mathsf{Left}\,(r,j,u) * r.u \to u) \\ \vee (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{Last}\,(u,j) * u.u \to gp) \\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
& * \mathsf{isPLock}\,(u,\pi_1) * \mathsf{isPLock}\,(u,\pi_2) \\
& \wedge i = r \wedge j = l * ((l = u = r = \mathsf{null} \wedge \mathcal{R} \to i) \vee \mathrm{emp}) \\
\equiv\ & \begin{pmatrix} (l \neq \mathsf{null} \wedge \mathsf{Right}\,(l,r,u) * l.u \to u) \\ \vee (l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{First}\,(u,r) * u.u \to gp) \\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
& * \begin{pmatrix} (r \neq \mathsf{null} \wedge \mathsf{Left}\,(r,l,u) * r.u \to u) \\ \vee (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{Last}\,(u,l) * u.u \to gp) \\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
& * \mathsf{isPLock}\,(u,1) * \|\varnothing\|^{(i,j)(l,u,r)} \\
& \wedge i = r \wedge j = l * ((l = u = r = \mathsf{null} \wedge \mathcal{R} \to i) \vee \mathrm{emp}) \\
\text{Lemma 19} \equiv\ & \begin{pmatrix} \big(l \neq \mathsf{null} \wedge l.u \to u * l.rL \to 0 * l.r \to i\big) \\ \vee \big(l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.u \to gp * u.dL \to 0 * u.d \to i\big) \\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
& * \begin{pmatrix} \big(r \neq \mathsf{null} \wedge r.u \to u * r.lL \to 0 * r.l \to j\big) \\ \vee \big(r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.u \to gp * u.eL \to 0 * u.e \to j\big) \\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
& * \big(\ \ (u \neq \mathsf{null} \wedge u.nL \to 0) \vee (u = \mathsf{null} \wedge \mathcal{R} + 1 \to 0)\ \ \big) \\
& * ((l = u = \mathsf{null} \wedge \mathcal{R} \to i) \vee \mathrm{emp}) * \|\varnothing\|^{(i,j)(l,u,r)}
\end{aligned}
$$

Case 2. $t \neq \varnothing$

$$
\begin{array}{rl}
 & \begin{pmatrix} (l \neq \mathsf{null} \wedge \mathsf{Right}\,(l,i,u) * l.u \to u) \\ \vee (l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{First}\,(u,i) * u.u \to gp) \\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
 & * \begin{pmatrix} (r \neq \mathsf{null} \wedge \mathsf{Left}\,(r,j,u) * r.u \to u) \\ \vee (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{Last}\,(u,j) * u.u \to gp) \\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
 & * \mathsf{isPLock}\,(u,\pi_1) * \langle\langle t \rangle\rangle_I^{(i,j)(l,u,r)(\pi_2)} \\
\text{Lemma 20} \equiv & \begin{pmatrix} (l \neq \mathsf{null} \wedge \mathsf{Right}\,(l,i,u) * l.u \to u) \\ \vee (l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{First}\,(u,i) * u.u \to gp) \\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
 & * \begin{pmatrix} (r \neq \mathsf{null} \wedge \mathsf{Left}\,(r,j,u) * r.u \to u) \\ \vee (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{Last}\,(u,j) * u.u \to gp) \\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
 & * \mathsf{isPLock}\,(u,\pi_1) * \mathsf{isPLock}\,(u,\pi_2) \\
 & * \mathsf{Left}\,(i,l,u) * \mathsf{Right}\,(j,r,u) \\
 & * \left(\begin{pmatrix} i.l \to l * i.lL \to 0 \\ j.r \to r * j.rL \to 0 \end{pmatrix} \mathrel{-\!\!*} ||t||^{(i,j)(l,u,r)} \right) \\
\text{Lemma 19} \equiv & \begin{pmatrix} \big(l \neq \mathsf{null} \wedge l.u \to u * l.rL \to 0 * l.r \to i\big) \\ \vee \big(l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.u \to gp * u.dL \to 0 * u.d \to i\big) \\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
 & * \begin{pmatrix} \big(r \neq \mathsf{null} \wedge r.u \to u * r.lL \to 0 * r.l \to j\big) \\ \vee \big(r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.u \to gp * u.eL \to 0 * u.e \to j\big) \\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
 & * ((l = u = \mathsf{null} \wedge i \neq \mathsf{null} \wedge \mathcal{R} \to i) \vee \mathrm{emp}) \\
 & * \mathsf{isPLock}\,(u,1) * i.l \to l * i.lL \to 0 * j.r \to r * j.rL \to 0 \\
 & * \left(\begin{pmatrix} i.l \to l * i.lL \to 0 \\ j.r \to r * j.rL \to 0 \end{pmatrix} \mathrel{-\!\!*} ||t||^{(i,j)(l,u,r)} \right) \\
\equiv & \begin{pmatrix} \big(l \neq \mathsf{null} \wedge l.u \to u * l.rL \to 0 * l.r \to i\big) \\ \vee \big(l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.u \to gp * u.dL \to 0 * u.d \to i\big) \\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
 & * \begin{pmatrix} \big(r \neq \mathsf{null} \wedge r.u \to u * r.lL \to 0 * r.l \to j\big) \\ \vee \big(r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.u \to gp * u.eL \to 0 * u.e \to j\big) \\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
 & * \big(\ \ (u \neq \mathsf{null} \wedge u.nL \to 0) \vee (u = \mathsf{null} \wedge \mathcal{R} + 1 \to 0) \ \big) \\
 & * ((l = u = \mathsf{null} \wedge \mathcal{R} \to i) \vee \mathrm{emp}) * ||t||^{(i,j)(l,u,r)}
\end{array}
$$

□

Lemma 19.

$$\forall l, u, r, gp.$$
$$\begin{pmatrix}(l \neq \mathsf{null} \wedge \mathsf{Right}\,(l, r, u) * l.u \to u)\\ \vee (l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{First}\,(u, r) * u.u \to gp)\\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null})\end{pmatrix}$$
$$* \begin{pmatrix}(r \neq \mathsf{null} \wedge \mathsf{Left}\,(r, l, u) * r.u \to u)\\ \vee (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{Last}\,(u, l) * u.u \to gp)\\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null})\end{pmatrix}$$
$$\equiv$$
$$\begin{pmatrix}(l \neq \mathsf{null} \wedge l.r \to r * l.rL \to 0 * l.u \to u)\\ \vee (l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.d \to r * u.dL \to 0 * u.u \to gp)\\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null})\end{pmatrix}$$
$$* \begin{pmatrix}(r \neq \mathsf{null} \wedge r.l \to l * r.lL \to 0 * r.u \to u)\\ \vee (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.e \to l * u.eL \to 0 * u.u \to gp)\\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null})\end{pmatrix}$$
$$* ((l = u = \mathsf{null} \wedge r \neq \mathsf{null} \wedge \mathcal{R} \to r) \vee \mathrm{emp})$$

Proof.

$$\begin{pmatrix}(l \neq \mathsf{null} \wedge \mathsf{Right}\,(l, r, u) * l.u \to u)\\ \vee (l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{First}\,(u, r) * u.u \to gp)\\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null})\end{pmatrix}$$
$$* \begin{pmatrix}(r \neq \mathsf{null} \wedge \mathsf{Left}\,(r, l, u) * r.u \to u)\\ \vee (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{Last}\,(u, l) * u.u \to gp)\\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null})\end{pmatrix}$$
$$\equiv \begin{pmatrix}\begin{pmatrix} l \neq \mathsf{null} \wedge \mathsf{Right}\,(l, r, u) * l.u \to u\\ \begin{pmatrix}(r \neq \mathsf{null} \wedge \mathsf{Left}\,(r, l, u) * r.u \to u)\\ \vee (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{Last}\,(u, l) * u.u \to gp)\\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null})\end{pmatrix}\end{pmatrix}\\ \vee \begin{pmatrix} l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{First}\,(u, r) * u.u \to gp)\\ \begin{pmatrix}(r \neq \mathsf{null} \wedge \mathsf{Left}\,(r, l, u) * r.u \to u)\\ \vee (r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \mathsf{Last}\,(u, l) * u.u \to gp)\end{pmatrix}\end{pmatrix}\\ \vee \begin{pmatrix} l = \mathsf{null} \wedge u = \mathsf{null} \wedge\\ \begin{pmatrix}(r \neq \mathsf{null} \wedge \mathsf{Left}\,(r, l, u) * r.u \to u)\\ \vee (r \doteq \mathsf{null})\end{pmatrix}\end{pmatrix}\end{pmatrix}$$

//Use $[\mathcal{W}]$ tokens to get resources out.

$$
\left(\begin{array}{l}
\left(\begin{array}{l}
l \neq \mathsf{null} \wedge \exists \mathsf{R}_{l.r}.\, [\mathcal{A}]_1^{\mathsf{R}_{l.r}} * [\mathcal{L}]_1^{\mathsf{R}_{l.r}} * [\mathcal{U}]_1^{\mathsf{R}_{l.r}} * [\mathcal{W}]_1^{\mathsf{R}_{l.r}} * l.u \overset{\frac{1}{2}}{\mapsto} u \\
* \left(\begin{array}{l}
\left(\begin{array}{l}
r \neq \mathsf{null} \wedge \exists \mathsf{R}_{r.l}.\, [\mathcal{A}]_1^{\mathsf{R}_{r.l}} * [\mathcal{L}]_1^{\mathsf{R}_{r.l}} * [\mathcal{U}]_1^{\mathsf{R}_{r.l}} * [\mathcal{W}]_1^{\mathsf{R}_{r.l}} * r.u \overset{\frac{1}{2}}{\mapsto} u \\
* l.r \to r * r.l \to l * \boxed{l.rL \to 0 * l.u \overset{\frac{1}{4}}{\mapsto} u * r.u \overset{\frac{1}{4}}{\mapsto} u}^{\mathsf{R}_{l.r}}_{\mathsf{RC}(\mathsf{R}_{l.r},l,u)} \\
* \boxed{r.lL \to 0 * l.u \overset{\frac{1}{4}}{\mapsto} u * r.u \overset{\frac{1}{4}}{\mapsto} u}^{\mathsf{R}_{r.l}}_{\mathsf{LC}(\mathsf{R}_{r.l},r,u)}
\end{array}\right) \\
\vee \left(\begin{array}{l}
r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \exists \mathsf{R}_{u.e}.\, [\mathcal{A}]_1^{\mathsf{R}_{u.e}} * [\mathcal{L}]_1^{\mathsf{R}_{u.e}} * [\mathcal{U}]_1^{\mathsf{R}_{u.e}} * [\mathcal{W}]_1^{\mathsf{R}_{u.e}} * u.u \overset{\frac{1}{2}}{\mapsto} gp \\
* l.r \to r * u.e \to l * \boxed{l.rL \to 0 * l.u \overset{\frac{1}{4}}{\mapsto} u * u.u \overset{\frac{1}{4}}{\mapsto} gp}^{\mathsf{R}_{l.r}}_{\mathsf{RC}(\mathsf{R}_{l.r},l,u)} \\
* \boxed{u.eL \to 0 * l.u \overset{\frac{1}{4}}{\mapsto} u * u.u \overset{\frac{1}{4}}{\mapsto} gp}^{\mathsf{R}_{u.e}}_{\mathsf{EC}(\mathsf{R}_{u.e},u)}
\end{array}\right) \\
\vee \left(r = \mathsf{null} \wedge u = \mathsf{null} \wedge l.u \overset{\frac{1}{4}}{\mapsto} u * \boxed{l.u \overset{\frac{1}{4}}{\mapsto} u * l.r \to r}^{\mathsf{R}_{l.r}}_{\mathsf{RC}(\mathsf{R}_{l.r},l,u)}\right)
\end{array}\right) \\
\equiv \left(\begin{array}{l}
l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \exists \mathsf{R}_{u.d}.\, [\mathcal{A}]_1^{\mathsf{R}_{u.d}} * [\mathcal{L}]_1^{\mathsf{R}_{u.d}} * [\mathcal{U}]_1^{\mathsf{R}_{u.d}} * [\mathcal{W}]_1^{\mathsf{R}_{u.d}} * u.u \overset{\frac{1}{2}}{\mapsto} gp \\
\left(\begin{array}{l}
\left(\begin{array}{l}
r \neq \mathsf{null} \wedge \exists \mathsf{R}_{r.l}.\, [\mathcal{A}]_1^{\mathsf{R}_{r.l}} * [\mathcal{L}]_1^{\mathsf{R}_{r.l}} * [\mathcal{U}]_1^{\mathsf{R}_{r.l}} * [\mathcal{W}]_1^{\mathsf{R}_{r.l}} * r.u \overset{\frac{1}{2}}{\mapsto} u \\
* u.d \to r * r.l \to l * \boxed{u.dL \to 0 * u.u \overset{\frac{1}{4}}{\mapsto} gp * r.u \overset{\frac{1}{4}}{\mapsto} u}^{\mathsf{R}_{u.d}}_{\mathsf{DC}(\mathsf{R}_{u.d},u)} \\
* \boxed{r.lL \to 0 * u.u \overset{\frac{1}{4}}{\mapsto} gp * r.u \overset{\frac{1}{4}}{\mapsto} u}^{\mathsf{R}_{r.l}}_{\mathsf{LC}(\mathsf{R}_{r.l},r,u)}
\end{array}\right) \\
\vee \left(\begin{array}{l}
r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge \exists \mathsf{R}_{r.l}.\, [\mathcal{A}]_1^{\mathsf{R}_{u.e}} * [\mathcal{L}]_1^{\mathsf{R}_{u.e}} * [\mathcal{U}]_1^{\mathsf{R}_{u.e}} * [\mathcal{W}]_1^{\mathsf{R}_{u.e}} \\
* \boxed{u.dL \to 0 * u.u \overset{\frac{1}{4}}{\mapsto} gp * u.d \to r}^{\mathsf{R}_{u.d}}_{\mathsf{DC}(\mathsf{R}_{u.d},u)} \\
* \boxed{u.eL \to 0 * u.u \overset{\frac{1}{4}}{\mapsto} gp * u.e \to l}^{\mathsf{R}_{u.e}}_{\mathsf{EC}(\mathsf{R}_{u.e},u)}
\end{array}\right)
\end{array}\right) \\
\vee \left(\begin{array}{l}
l = \mathsf{null} \wedge u = \mathsf{null} \wedge \\
\left(\begin{array}{l}
r \neq \mathsf{null} \wedge \wedge \exists \mathsf{R}_{r.l}.\, [\mathcal{A}]_1^{\mathsf{R}_{r.l}} * [\mathcal{L}]_1^{\mathsf{R}_{r.l}} * [\mathcal{U}]_1^{\mathsf{R}_{r.l}} * [\mathcal{W}]_1^{\mathsf{R}_{r.l}} \\
* \mathcal{R} \to r * \boxed{r.lL \to 0 * r.l \to l * r.u \overset{\frac{1}{4}}{\mapsto} u}^{\mathsf{R}_{r.l}}_{\mathsf{LC}(\mathsf{R}_{r.l},r,u)}
\end{array}\right) \\
\vee (r \doteq \mathsf{null})
\end{array}\right)
\end{array}\right)
$$

//Destroy $\mathsf{R}_{l.r}, \mathsf{R}_{u.d}, \mathsf{R}_{r.l}, \mathsf{R}_{u.e}$ regions since we have all tokens on them.

$$
\begin{aligned}
\equiv\quad & \begin{pmatrix} \big(l \neq \mathsf{null} \wedge l.u \to u * l.rL \to 0 * l.r \to r\big) \\ \vee \big(l = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.u \to gp * u.dL \to 0 * u.d \to r\big) \\ \vee (l = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
& * \begin{pmatrix} \big(r \neq \mathsf{null} \wedge r.u \to u * r.lL \to 0 * r.l \to l\big) \\ \vee \big(r = \mathsf{null} \wedge u \neq \mathsf{null} \wedge u.u \to gp * u.eL \to 0 * u.e \to l\big) \\ \vee (r = \mathsf{null} \wedge u \doteq \mathsf{null}) \end{pmatrix} \\
& * \big((l = u = \mathsf{null} \wedge r \neq \mathsf{null} \wedge \mathcal{R} \to r) \vee \mathrm{emp}\big)
\end{aligned}
$$

□

Lemma 20.

$$\begin{array}{l}\forall t \in \textsc{Data}_{\mathbb{T}}.\ \forall i,j,l,u,r,t,gp,\pi_1,\pi_2.\ \ \pi_1+\pi_2=1\\ addrs(t)=\varnothing \wedge t \neq \varnothing \implies \\ \qquad\qquad \langle\langle t\rangle\rangle_I^{(i,j)(l,u,r)(\pi)} \\ \qquad\qquad\qquad \equiv \\ \qquad \mathsf{isPLock}(u,\pi) * \mathsf{Left}(i,l,u) * \mathsf{Right}(j,r,u) \\ \qquad * \left(\begin{pmatrix} i.l \to l * i.lL \to 0 \\ j.r \to r * j.rL \to 0 \end{pmatrix} \mathrel{-\!\!*} \|t\|^{(i,j)(l,u,r)}\right)\end{array}$$

Proof. By induction over the structure of t.

Case $t = \varnothing$
This case holds vacuously as it contradicts the assumption that $t \neq \varnothing$.

Case $t = \mathbf{x}$
This case holds vacuously as $addrs(t) \neq \varnothing$.

Case $t = n[t']$
If $addrs(t') \neq \varnothing$, this case holds vacuously as it contradicts our assumption that $addrs(n[t']) = \varnothing$. On the other hand, if $addrs(t') = \varnothing$, we have:

$$\begin{array}{rcl}\langle\langle n[t']\rangle\rangle_I^{(i,j)(l,u,r)(\pi)} & \equiv & (i=j=n) \wedge \exists d,e,\pi_3,\pi_4.\ \ \pi_3+\pi_4=1 \wedge \\ & & \begin{pmatrix}(u \neq \mathsf{null} \wedge n.uL \to u.nL) \\ \vee (u = \mathsf{null} \wedge n.uL \to \mathcal{R}+1)\end{pmatrix} * n.u \to u \\ & & * \mathsf{isPLock}(n,\pi_3) * \mathsf{isPLock}(u,\pi) * \mathsf{Left}(n,l,u) \\ & & * \mathsf{Right}(n,r,u) * \mathsf{First}(n,d) * \mathsf{Last}(n,e) \\ & & * \langle\langle t'\rangle\rangle_I^{(d,e)(\mathsf{null},n,\mathsf{null})(\pi_4)} \\ (\text{I.H.}) & \equiv & (i=j=n) \wedge \exists d,e,\pi_3,\pi_4.\ \ \pi_3+\pi_4=1 \wedge \\ & & \begin{pmatrix}(u \neq \mathsf{null} \wedge n.uL \to u.nL) \\ \vee (u = \mathsf{null} \wedge n.uL \to \mathcal{R}+1)\end{pmatrix} * n.u \to u \\ & & * \mathsf{isPLock}(n,\pi_3) * \mathsf{isPLock}(u,\pi) * \mathsf{Left}(n,l,u) \\ & & * \mathsf{Right}(n,r,u) * \mathsf{First}(n,d) * \mathsf{Last}(n,e) \\ & & * \mathsf{isPLock}(n,\pi_4) * \mathsf{Left}(d,\mathsf{null},n) * \mathsf{Right}(e,\mathsf{null},n) \\ & & * \left(\begin{pmatrix} d.l \to \mathsf{null} * d.lL \to 0 \\ e.r \to \mathsf{null} * e.rL \to 0 \end{pmatrix} \mathrel{-\!\!*} \|t'\|^{(d,e)(\mathsf{null},n,\mathsf{null})}\right)\end{array}$$

$$
\begin{aligned}
\text{Lemma 19} \quad \equiv \quad & (i = j = n) \wedge \exists d, e. \\
& \begin{pmatrix} (u \neq \mathsf{null} \wedge n.uL \to u.nL) \\ \vee (u = \mathsf{null} \wedge n.uL \to \mathcal{R} + 1) \end{pmatrix} * n.u \to u \\
& * \mathsf{isPLock}\,(u, \pi) * \mathsf{Left}\,(n, l, u) * \mathsf{Right}\,(n, r, u) \\
& * n.d \to d * n.dL \to 0 * n.e \to e * n.eL \to 0 \\
& * n.nL \to 0 * d.l \to \mathsf{null} * d.lL \to 0 * e.r \to \mathsf{null} * e.rL \to 0 \\
& * \left(\begin{pmatrix} d.l \to \mathsf{null} * d.lL \to 0 \\ e.r \to \mathsf{null} * e.rL \to 0 \end{pmatrix} \mathrel{-\!\!*} \|t'\|^{(d,e)(\mathsf{null},n,\mathsf{null})} \right) \\
\equiv \quad & (i = j = n) \wedge \exists d, e. \\
& \begin{pmatrix} (u \neq \mathsf{null} \wedge n.uL \to u.nL) \\ \vee (u = \mathsf{null} \wedge n.uL \to \mathcal{R} + 1) \end{pmatrix} * n.u \to u \\
& * \mathsf{isPLock}\,(u, \pi) * \mathsf{Left}\,(n, l, u) * \mathsf{Right}\,(n, r, u) \\
& * n.d \to d * n.dL \to 0 * n.e \to e * n.eL \to 0 * n.nL \to 0 \\
& * \|t'\|^{(d,e)(\mathsf{null},n,\mathsf{null})} \\
\equiv \quad & * \mathsf{isPLock}\,(u, \pi) * \mathsf{Left}\,(i, l, u) * \mathsf{Right}\,(j, r, u) \\
& * \begin{pmatrix} i.l \to l * i.lL \to 0 \\ j.r \to r * j.rL \to 0 \end{pmatrix} \mathrel{-\!\!*} \|n[t']\|^{(i,j)(l,u,r)}
\end{aligned}
$$

Case $t = t_1 \otimes t_2$
If $addrs\,(t_1) \neq \varnothing \vee addrs\,(t_2) \neq \varnothing$, this case holds vacuously as it contradicts our assumption that $addrs\,(t) = \varnothing$. If $addrs\,(t_1) = \varnothing \wedge addrs\,(t_2) = \varnothing$ then we have the following four cases:

Case 1. $t_1 = \varnothing \wedge t_2 = \varnothing$
This case holds vacuously as we have: $t = t_1 \otimes t_2 = \varnothing \otimes \varnothing = \varnothing$

Case 2. $t_1 = \varnothing \wedge t_2 \neq \varnothing$

$$
\begin{aligned}
\langle\langle t_1 \otimes t_2 \rangle\rangle_I^{(i,j)(l,u,r)(\pi)} \equiv \quad & \langle\langle \varnothing \otimes t_2 \rangle\rangle_I^{(i,j)(l,u,r)(\pi)} \\
\equiv \quad & \langle\langle t_2 \rangle\rangle_I^{(i,j)(l,u,r)(\pi)} \\
(\text{I.H.}) \equiv \quad & \mathsf{isPLock}\,(u, \pi) * \mathsf{Left}\,(n, l, u) * \mathsf{Right}\,(n, r, u) \\
& * \begin{pmatrix} i.l \to l * i.lL \to 0 \\ j.r \to r * j.rL \to 0 \end{pmatrix} \mathrel{-\!\!*} \|t_2\|^{(i,j)(l,u,r)} \\
\equiv \quad & \mathsf{isPLock}\,(u, \pi) * \mathsf{Left}\,(n, l, u) * \mathsf{Right}\,(n, r, u) \\
& * \begin{pmatrix} i.l \to l * i.lL \to 0 \\ j.r \to r * j.rL \to 0 \end{pmatrix} \mathrel{-\!\!*} \|t_1 \otimes t_2\|^{(i,j)(l,u,r)}
\end{aligned}
$$

Case 3. $t_1 \neq \varnothing \wedge t_2 = \varnothing$
This case is analogous to the previous case and is omitted here.

Case 4. $t_1 \neq \varnothing \wedge t_2 \neq \varnothing$

$$
\begin{aligned}
& \langle\langle t_1 \otimes t_2 \rangle\rangle_I^{(i,j)(l,u,r)(\pi)} \\
\equiv\ & \exists p, q, \pi_1, \pi_2.\ \pi_1 + \pi_2 = \pi \wedge \\
& \langle\langle t_1 \rangle\rangle_I^{(i,p)(l,u,q)(\pi_1)} * \langle\langle t_2 \rangle\rangle_I^{(q,j)(p,u,r)(\pi_2)} \\
(\text{I.H.}) \equiv\ & \exists p, q, \pi_1, \pi_2.\ \pi_1 + \pi_2 = \pi \wedge \\
& \mathsf{isPLock}\,(u, \pi_1) * \mathsf{Left}\,(i, l, u) * \mathsf{Right}\,(p, q, u) \\
& * \begin{pmatrix} i.l \to l * i.lL \to 0 \\ p.r \to q * p.rL \to 0 \end{pmatrix} \mathrel{-\!\!*} \|t_1\|^{(i,p)(l,u,q)} \\
& * \mathsf{isPLock}\,(u, \pi_2) * \mathsf{Left}\,(q, p, u) * \mathsf{Right}\,(j, r, u) \\
& * \begin{pmatrix} q.l \to p * i.lL \to 0 \\ j.r \to r * j.rL \to 0 \end{pmatrix} \mathrel{-\!\!*} \|t_2\|^{(q,j)(p,u,q)} \\
\text{Lemma 19} \equiv\ & \mathsf{isPLock}\,(u, \pi) * \mathsf{Left}\,(i, l, u) * \mathsf{Right}\,(j, r, u) \\
& \exists p, q.\, p.r \to q * p.rL \to 0 * q.l \to p * q.lL \to 0 \\
& * \begin{pmatrix} i.l \to l * i.lL \to 0 \\ p.r \to q * p.rL \to 0 \\ q.l \to p * i.lL \to 0 \\ j.r \to r * j.rL \to 0 \end{pmatrix} \mathrel{-\!\!*} \begin{pmatrix} \|t_1\|^{(i,p)(l,u,q)} \\ * \|t_2\|^{(q,j)(p,u,q)} \end{pmatrix} \\
\equiv\ & \mathsf{isPLock}\,(u, \pi_1) * \mathsf{Left}\,(i, l, u) * \mathsf{Right}\,(j, r, u) \\
& * \begin{pmatrix} i.l \to l * i.lL \to 0 \\ j.r \to r * j.rL \to 0 \end{pmatrix} \mathrel{-\!\!*} \begin{pmatrix} \|t_1 \otimes t_2\|^{(i,j)(l,u,r)} \end{pmatrix}
\end{aligned}
$$

□