Formalization of Ownership Transfer in Universe Types

Peter Müller and Arsenii Rudich

ETH Technical Report 556

Abstract

Ownership is a powerful concept to structure the object store and to control aliasing and modifications of objects. This paper presents an ownership type system for a Java-like programming language. Like our earlier Universe type system, Universe Types with Transfer (UTT) enforce the owner-as-modifier discipline. This discipline does not restrict aliasing, but requires modifications of an object to be initiated by its owner. This allows owner objects to control state changes of owned objects, for instance, to maintain invariants. UTT combines ownership type checking with a modular static analysis to control references to transferable objects. UTT is very flexible because it permits temporary aliases, even across certain method calls. Nevertheless, it guarantees statically that a cluster of objects is externally-unique when it is transferred and, thus, that ownership transfer is type safe. UTT provides the same encapsulation as Universe Types and requires only negligible annotation overhead.

Contents

1 Syntax

$$
\begin{array}{lcl}
CL & :: & = class\ C\ extends\ D\ \{\overline{Cl};\ \overline{T}\ \overline{f};\ \overline{M}\} \\
\\
M & ::= & T\ mt(T\ x)\ locVar(\overline{T\ y})\ \{e;\} \\
\\
e & ::= & x = y \\
 & | & x = y.f \\
 & | & x.f := y \\
 & | & x = y.mt(z) \\
 & | & x = new\ T() \\
 & | & x = (T)y \\
 & | & e_1; e_2 \\
 & | & x = release(y) \\
 & | & x = capture\ \langle m \rangle\ (y) \\
\\
T & ::= & m\ C \\
m & ::= & \texttt{any} \mid \texttt{peer} \mid \texttt{rep}\ \langle Cl \rangle \mid \texttt{uniq}
\end{array}
$$

Notation:

- $x,\ y,\ z \in$ `VarID` ranges over local variables and formal parameters, including `this`
- $C \in$ `ClassID` ranges over classes' names
- $mt \in$ `MethodID` ranges over methods' names
- $f \in$ `FieldID` ranges over fields' names
- $T \in$ `Type` ranges over Universe types
- $m \in$ `MOD` ranges over Universe types modifiers
- $Cl \in$ `Clt` ranges over clusters

Note: In purpose of simplification we:

- forbidden nested expression. Any program can be transformed to this form via introducing additional local variables which represent temporal values.

- suppose that any method has only one parameter. It is not hard to generalize in case of arbitrary parameters number.
- suppose that all local variables are declared at the begin of a method.It is not hard transform a program to this form via collection variables declaration in the method body.
- to return result of a method invocation we use special local variable `res`.
- All classes' fields and local variable have unique names.
- All input parameters have fixed name p.
- If methods have equal names then they have equal signatures.

2 Auxiliary functions and definitions

2.1 General constructions

In purpose of abbreviation we use next constructions:

$$\begin{array}{lll} x = & \texttt{if}(b_1) & \texttt{then}\ t_1 \\ \texttt{else} & \texttt{if}(b_2) & \texttt{then}\ t_2 \\ & \ldots & \\ \texttt{else} & \texttt{if}(b_n) & \texttt{then}\ t_n \\ \texttt{else} & t_{n+1} & \end{array} \Leftrightarrow \bigwedge_{i=1}^{n+1}((\bigwedge_{j=1}^{i-1} \neg b_i) \wedge b_j \Rightarrow x = t_i)$$

where $b_{n+1} = \top$
We use next operations on sequences, and mappings:

- $\epsilon = \langle\rangle$
- $\langle a_1, \ldots, a_n\rangle \circ \langle b_1, \ldots, b_m\rangle = \langle a_1, \ldots, a_n, b_1, \ldots, b_m\rangle$
- $\langle a_1, \ldots, a_n\rangle \downarrow_i = \texttt{if}(i \in [1..n])\ \texttt{then}\ a_i\ \texttt{else undefined}$
- $M[a \mapsto b] = (M \setminus \{\langle a,\ \_\rangle\}) \cup \{\langle a, b\rangle\}$
- $\texttt{dom}(\{\langle a_1,\ b_1\rangle, \ldots,\ \langle a_n,\ b_n\rangle\}) = \{a_1, \ldots, a_n\}$
- $\texttt{rng}(\{\langle a_1,\ b_1\rangle, \ldots,\ \langle a_n,\ b_n\rangle\}) = \{b_1, \ldots, b_n\}$

2.2 Clusters

$\texttt{Clt}$ is an unrestricted set which contains all clusters.
$\texttt{Clt} = \texttt{CltRep} \cup \texttt{CltFree}$ $\texttt{CltRep} \cap \texttt{CltFree} = \varnothing$
$\texttt{CltRep}$ is an unrestricted set which contains all clusters owned by some object.
$\texttt{CltFree}$ is an unrestricted set which contains all unowned clusters.
We have a special cluster $Cl_{\texttt{this}}$ which contains object's representation.
$Cl_{\texttt{this}} \in \texttt{CltRep}$

To be able generate new unique cluster we assume that $\texttt{CltFree}$ has next structure: $\texttt{CltFree} = \{\texttt{CF}_i | i \in \texttt{N}\}$

$\texttt{CF}_i$ satisfies the next axiom: $\forall\ i, j\ i \neq j \Rightarrow \texttt{CF}_i \neq \texttt{CF}_j$

2.3 Ownership type modifiers

A user can use next type modediers: $\texttt{any}$, $\texttt{peer}$, $\texttt{rep}\,\langle Cl \rangle$, $\texttt{uniq}$. Also we use type modifier $\texttt{this}$. A user can't use it directly but it can be deduced during the type checking procedure invocation. $\texttt{this}$ is type modifier which corresponds to the $\texttt{this}$ reference.

We denote meta-type modifiers like
$\texttt{MOD} = \{\texttt{any},\ \texttt{peer},\ \texttt{rep}\,\langle Cl \rangle,\ \texttt{uniq},\ \texttt{this} \mid Cl \in \texttt{Clt}\}$

2.4 Type combinators

We define a type combinator $\rhd_U$. We use it for expressing field access and methods invocation.

$$
\begin{array}{lllll}
\texttt{peer} & \rhd_U & \texttt{peer} & \rightarrow & \texttt{peer} \\
\texttt{rep}\,\langle Cl \rangle & \rhd_U & \texttt{peer} & \rightarrow & \texttt{rep}\,\langle Cl \rangle \\
\texttt{this} & \rhd_U & x & \rightarrow & x \\
x & \rhd_U & \texttt{uniq} & \rightarrow & \texttt{uniq} \\
x & \rhd_U & y & \rightarrow & \texttt{any}
\end{array}
$$

We define a type combinator $\rhd_U$ in the next way:
$(m_1\ C_1) \rhd_U (m_2\ C_2) = (m_1 \rhd_U m_2)\ C_2$

2.5 Subtype relation

We define subtype relation on the Java classes in the next way:

$$C \sqsubseteq C \qquad \frac{C \sqsubseteq D \quad D \sqsubseteq E}{C \sqsubseteq E} \qquad \frac{\textit{class } C \textit{ extends } D\ \{\ldots\}}{C \sqsubseteq D}$$

We define subtype relation on the universe type's modifiers in the next way:

$$\frac{m = m' \vee m' = \texttt{any}}{m \leq m'}$$

We define subtype relation on the universe types in the next way:

$$\frac{m \leq m' \quad C \sqsubseteq C'}{m\ C \leq m'\ C'}$$

2.6 Universe types's function

To access universe types' components we use next functions:

$$\frac{T = m\ C}{\texttt{class}(T) = C} \qquad \frac{T = m\ C}{\texttt{mod}(T) = m}$$

In purpose of brevity we allow use universe type in any expression in which we can use universe type modifiers. For example if we expect that expression $F[\_]$ get as parameter type modifier then $F[T] \stackrel{def}{=} F[\texttt{mod}(T)]$

2.7 Lookup functions

- The function $\texttt{fields}(C)$ yields the identifiers of all fields that are declared in or inherited by class C.

$$\frac{}{\texttt{fields}(\textit{Object}) = \epsilon} \qquad \frac{\textit{class } C \textit{ extends } D\{\ \_\ ; \overline{T f};\ \_\ \}}{\texttt{fields}(C) = \overline{f} \circ \texttt{fields}(D)}$$

- The function $\texttt{fType}(C, f)$ yields the type of field f as declared in class C. The result is `undefined` if f is not declared in C. Since identifiers

are assumed to be globally unique, there is only one declaration for each field identifier.

$$\frac{\textit{class } C \textit{ extends } \_\ \{\ \_\ ; \ldots T f \ldots ;\ \_\ \}}{\texttt{fType}(C, f) = T}$$

- The function $\texttt{mType}(C, mt)$ yields the signature of method mt as declared in class C. The result is `undefined` if mt is not declared in C. We do not allow overloading of methods; therefore, the method identifier is sufficient to uniquely identify a method.

$$\frac{\textit{class } C \textit{ extends } \_\ \{\ \_\ ;\ \_\ ; \ldots T_r\ mt(T_p p) \ldots\}}{\texttt{mType}(C, mt) = T_p \rightarrow T_r}$$

- The function $\texttt{mBody}(C, mt)$ yields a mt's body expression.

$$\frac{\textit{class } C \textit{ extends } \_\ \{\ \_\ ;\ \_\ ; \ldots\ \_\ mt(\ \_\ )\ \_\ \{e;\} \ldots\}}{\texttt{mBody}(C, mt) = e}$$

$$\frac{\textit{class } C \textit{ extends } D\{\text{no method } mt\}}{\texttt{mBody}(C, mt) = \texttt{mBody}(D, mt)}$$

- Method mt respects the rules for overriding if it does not override a method or if all overridden methods have the identical signatures.

$$\frac{\begin{array}{c}\forall C' : C' \leq C \Rightarrow \\ \texttt{mType}(C', mt)\ \texttt{undefined} \vee \texttt{mType}(C) = \texttt{mType}(C')\end{array}}{\texttt{override}(C, mt)}$$

- The function `mLoc` yields the names of local variables as declared in class C:

$$\frac{\textit{class } C \textit{ extends } \_\ \{\ \_\ ;\ \_\ ; \ldots\ \_\ mt(\ \_\ ) locVar(\overline{T\ y})\{\ \_\ \} \ldots\}}{\texttt{mLoc}(C, mt) = \overline{y}}$$

- The function $\texttt{Clt}_C$ yields the clusters of class C:

$$\frac{class\ C\ extends\ \_\ \{\overline{Cl};\ \_\ ;\ \_\ \}}{\texttt{Clt}_C = \overline{Cl}}$$

- The function $\texttt{CltAll}_C$ yields the clusters of class C and its superclasses:

$$\frac{}{\texttt{CltAll}_{Object} = \varnothing} \qquad \frac{class\ C\ extends\ D\ \_}{\texttt{CltAll}_C = \texttt{Clt}_C \cup \texttt{CltAll}_D}$$

2.8 Unusable variables

Note: we consider unusable variables set for fixed:

- Class C
- Method mt
- Statical environment Γ

To represent data flow analyze information we use special set which contains all inaccessible (unusable) variables. It is subset of $\texttt{Var} = \texttt{Loc} \cup \texttt{Field}$ where:

- $\texttt{Loc} = \{v \ \in \texttt{dom}(\Gamma) |\ \Gamma(v) \in \{\texttt{rep}\,\langle Cl\rangle\,,\ \texttt{uniq}\}\}$
- $\texttt{Field} = \{f \in \texttt{fields}(C,\ mt) |\ \texttt{fType}(C, f) = \texttt{rep}\,\langle Cl\rangle\}$

To change am unusable set we use next operations:

- $\texttt{consumeAliases}(U, v) = U \cup$
  $\{x \in \texttt{Var} | \Gamma(v) = \Gamma(x)\} \cup \{f \in \texttt{fields}(C,\ mt) | \Gamma(v) = \texttt{fType}(C, f))\}$
- $\texttt{consumeUniq}(U, T_{res}, v) =$
  $\texttt{if}(T_{res} \neq \texttt{any} \wedge \Gamma(v) = \texttt{uniq})\ \texttt{then}\ U \cup \{v\}\ \texttt{else}\ U$
- $\texttt{consumeLocals}(U) = U \cup \{v \in \texttt{Loc} \mid \Gamma(v) = \texttt{rep}\,\langle Cl_f\rangle \wedge f \in \texttt{Field}\}$

3 Unusable set's generation rules

In this section we express change of unusable set during expression type checking or evaluation. We use $\Gamma \in \texttt{Env} = \overline{\texttt{VarID Type}}$ for the declaration environment, which maps formal parameters to their types. A unusable set's generation rules has the form $\Gamma; U \vdash_{DE} e : U'$ and expresses that after expression e type checking or evaluation the unusable set change from U to U'.

In some situations we need to know an unusable set before method invocation. Uu-Pre-Invk rule generate such unusable set.

$$\frac{U' = \texttt{consumeUniq}(U, \Gamma(x), y) \setminus \{x\}}{\Gamma; U \vdash_{DE} x = y : U'} \quad [\text{Uu-Assign}]$$

$$\frac{}{\Gamma; U \vdash_{DE} x = y.f : U \setminus \{x\}} \quad [\text{Uu-Field-Read}]$$

$$\frac{\begin{array}{c} U' = \texttt{if}(y = \texttt{this}) \\ \texttt{then}\ U \setminus \{f\}\ \texttt{else}\ U \end{array}}{\Gamma; U \vdash_{DE} y.f = x : U'} \quad [\text{Uu-Field-Write}]$$

$$\frac{\begin{array}{c} \texttt{mType}(\Gamma(\texttt{class}(y)), mt) = T_p \rightarrow T_r \\ U_1 = \texttt{consumeUniq}(U, T_p, z) \\ U_2 = \texttt{if}(\Gamma(y) \notin \{\texttt{peer},\ \texttt{this}\})\ \texttt{then}\ U_1 \\ \texttt{else}\ \texttt{consumeLocals}(\texttt{consumeUniq}(U_1, T_p, z)) \end{array}}{\Gamma; U \vdash_{DE} y.mt(z) : U'} \quad [\text{Uu-Pre-Invk}]$$

$$\frac{\Gamma; U \vdash DEy.mt(z) : U'}{\Gamma; U \vdash_{DE} x = y.mt(z) : U' \setminus \{x\}} \quad [\text{Uu-Invk}]$$

$$\frac{}{\Gamma; U \vdash_{DE} x = new\ T() : U \setminus \{x\}} \quad [\text{Uu-New}]$$

$$\frac{U' = \texttt{consumeUniq}(U, \Gamma(x), y) \setminus \{x\}}{\Gamma; U \vdash_{DE} x = (T)y : U'} \quad [\text{Uu-Cast}]$$

$$\frac{\Gamma; U \vdash_{DE} e_1 : U_1 \quad \Gamma; U_1 \vdash_{DE} e_2 : U_2}{\Gamma; U \vdash_{DE} e_1; e_2 : U_2} \qquad [\text{Uu-Comp}]$$

$$\frac{U' = \texttt{consumeAliases}(U, y) \setminus \{x\}}{\Gamma; U \vdash_{DE} x = \mathit{release}(y) : U'} \qquad [\text{Uu-Release}]$$

$$\frac{U' = U \cup \{y\} \setminus \{x\}}{\Gamma; U \vdash_{DE} x = \mathit{capture}\,\langle m \rangle\,(y) : U'} \qquad [\text{Uu-Capture}]$$

4 Type rules

A judgment has the form $\Gamma; U \vdash e$ and expresses that expression e is well-typed in a declaration environment Γ. U is an unusable set before the expression evaluation.

We use an auxiliary predicate $\texttt{RepInDom} : \texttt{MOD} \times \mathcal{P}(\texttt{Clt})$ to check is the type's domain belong to the proper domains set or not.

$\texttt{RepInDom}(m, \mathit{CltSet}) \stackrel{def}{=} m = \texttt{rep}\,\langle Cl \rangle \Rightarrow Cl \in \mathit{CltSet}$

$\texttt{IsWritable} : \texttt{MOD} \rightarrow \texttt{Bool}$

$\texttt{IsWritable}(m) = m \in \{\texttt{peer},\ \texttt{this},\ \texttt{rep}\,\langle Cl \rangle \mid Cl \in \texttt{Clt}\}$

The function $\Gamma_{C,\ mt}$ yields the static environment of method mt as declared in class C:

$$\frac{\mathit{class}\ C\ \mathit{extends}\ \_\ \{\ \_\ ;\ \_\ ; \ldots T_r\ mt(T_p\ x)\ locVar(\overline{T\ y})\ \{\ \_\ \} \ldots\}}{\Gamma_{C,\ mt} = \{\langle p, T_p \rangle,\ \overline{\langle y,\ T \rangle},\ \langle \texttt{this}, \texttt{this}\ C \rangle,\ \langle \texttt{res}, T_r \rangle\}}$$

$$\frac{\begin{array}{c} y \notin U \\ \Gamma(y) \leq \Gamma(x) \end{array}}{\Gamma; U \vdash x = y} \qquad [\text{T-Assign}]$$

$$\frac{\begin{array}{c} T_f = \texttt{fType}(\texttt{class}(\Gamma(y)),\ f) \\ \Gamma(y) \rhd_U T_f \leq \Gamma(x) \\ y \notin U \\ y = \texttt{this} \Rightarrow f \notin U \end{array}}{\Gamma; U \vdash x = y.f} \qquad [\text{T-Field-Read}]$$

$$\frac{\begin{array}{c} T_f = \texttt{fType}(\texttt{class}(\Gamma(y)),\ f) \\ \Gamma(x) \leq \Gamma(y) \rhd_U T_f \\ \texttt{IsWritable}(\Gamma(y)) \\ T_f = \texttt{rep}\ \langle Cl \rangle \Rightarrow \Gamma(y) = \texttt{this} \\ x, y \notin U \end{array}}{\Gamma; U \vdash y.f = x} \qquad [\text{T-Field-Write}]$$

$$\frac{\begin{array}{c} \texttt{mType}(C, mt) = T_p \rightarrow T_r \\ \Gamma(z) \leq \Gamma(y) \rhd_U T_p \\ \Gamma(y) \rhd_U T_r \leq \Gamma(x) \\ T_p = \texttt{rep}\ \langle Cl \rangle \Rightarrow \Gamma(y) = \texttt{this} \\ y, z \notin U \\ \Gamma; U \vdash_{DE} y.mt(z) : U' \\ \texttt{Field} \cap U' = \varnothing \end{array}}{\Gamma; U \vdash x = y.mt(z)} \qquad [\text{T-Invk}]$$

$$\frac{\begin{array}{c} \texttt{IsWritable}(T) \\ C = \texttt{class}(\Gamma(\texttt{this})) \\ \texttt{RepInDom}(T,\ \texttt{CltAll}_C) \\ T \leq \Gamma(x) \end{array}}{\Gamma; U \vdash x = new\ T()} \qquad [\text{T-New}]$$

$$\frac{\begin{array}{c} T \leq \Gamma(x) \\ C = \texttt{class}(\Gamma(\texttt{this})) \\ \texttt{RepInDom}(T,\ \texttt{CltAll}_C) \\ m_y = \texttt{mod}(\Gamma(y)) \\ m = \texttt{mod}(T) \\ m_y \leq m \vee (m_y = \texttt{any} \wedge \texttt{IsWritable}(\Gamma(m))) \\ y \notin U \end{array}}{\Gamma; U \vdash x = (T)y} \qquad [\text{T-Cast}]$$

$$\frac{\begin{array}{c}\Gamma; U \vdash e_1 \\ \Gamma; U \vdash_{DE} e_1 : U' \\ \Gamma; U' \vdash e_2\end{array}}{\Gamma; U \vdash e_1; e_2} \qquad [\text{T-Comp}]$$

$$\frac{\begin{array}{c}\Gamma(x) = \texttt{uniq} \\ \Gamma(y) = \texttt{rep}\,\langle Cl \rangle \\ Cl \neq Cl_{\texttt{this}} \\ \texttt{class}(\Gamma(y)) \sqsubseteq \texttt{class}(\Gamma(x)) \\ y \notin U\end{array}}{\Gamma; U \vdash x = release(y)} \qquad [\text{T-Release}]$$

$$\frac{\begin{array}{c}\texttt{IsWritable}(m) \\ C = \texttt{class}(\Gamma(\texttt{this})) \\ \texttt{RepInDom}(m,\ \texttt{CltAll}_C) \\ \Gamma(x) = m \\ \Gamma(y) = \texttt{uniq} \\ \texttt{class}(\Gamma(y)) \sqsubseteq \texttt{class}(\Gamma(x)) \\ y \notin U\end{array}}{\Gamma; U \vdash x = capture\,\langle m \rangle\,(y)} \qquad [\text{T-Capture}]$$

$$\frac{\begin{array}{c}\texttt{RepInDom}(\overline{T} \circ T_r \circ T_p,\ \texttt{CltAll}_C) \\ \Gamma_{C,\ mt}; \varnothing \vdash e \\ \Gamma_{C,\ mt}; \varnothing \vdash_{DE} e : U \\ (\texttt{Field} \cup \{\texttt{res}\}) \cap U = \varnothing\end{array}}{T_r\ mt(T_p\ x)\ locVar(\overline{T\ y})\ \{e;\} \in C} \qquad [\text{Wf-Method}]$$

$$\frac{\begin{array}{c}\overline{M} \in C \\ \texttt{RepInDom}(\overline{f}, \texttt{Clt}_C) \\ \overline{f} \neq \texttt{uniq}\end{array}}{class\ C\{\overline{Cl};\ \overline{T}\ \overline{f};\ \overline{M}\}} \qquad [\text{Wf-Class}]$$

5 Runtime Model

5.1 Heap Model

Fig. 1 summarizes our heap model. To distinguish sorts of the runtime model from their static counterparts, we use the prefix $^{\texttt{r}}$.

$$
\begin{array}{rcll}
\mathtt{h} & \in & \mathtt{Heap} & = \mathtt{Addr!} \rightarrow \mathtt{Obj} \\
\iota! & \in & \mathtt{Addr!} & = \text{Set of Addresses} \\
\iota & \in & \mathtt{Addr} & = \mathtt{Addr!} \cup \{\mathtt{null^r}\} \\
\mathtt{o} & \in & \mathtt{Obj} & = \mathtt{ClassID} \times \mathtt{Owners} \times \mathtt{Fields} \\
\mathtt{Fds} & \in & \mathtt{Fields} & = \mathtt{FieldID} \rightarrow \mathtt{Addr} \\
\mathtt{ow} & \in & \mathtt{Owners} & = \mathtt{Clt} \times \mathtt{Addr} \\
\Gamma^{\mathtt{r}} & \in & \mathtt{Env^r} & = \overline{\mathtt{VarID\ Addr}} \\
\mathtt{Fr} & \in & \mathtt{Frames} & = \mathtt{Env^r} \times \mathtt{Env} \times \mathcal{P}(\mathtt{VarID}) \\
\mathtt{FrSt} & \in & \mathtt{FramesStack} & = \overline{\mathtt{Frames}} \\
\sigma & \in & \mathtt{States} & = \mathtt{Heap} \times \mathtt{FramesStack} \\
\sigma_{pr} & \in & \mathtt{States}_{pr} & = \mathtt{Heap} \times \mathtt{Env^r}
\end{array}
$$

Figure 1: Definitions for the heap model.

A heap (sort `Heap`) maps addresses to objects. The set of addresses (`Addr`) contains the special null-reference $\mathtt{null^r}$. An object (`Obj`) consist of its runtime type and a mapping from field identifiers to the addresses stored in the fields.

5.2 Operations on Heap and Objects

$$
\begin{array}{l}
\cdot[\cdot.\cdot := \cdot] \ :: \ \mathtt{Heap} \times \mathtt{Addr!} \times \mathtt{FieldID} \times \mathtt{Addr} \rightarrow \mathtt{Heap} \\
\quad \mathtt{h}[\iota\,.\,f := \iota'] = \mathtt{h}[\iota \mapsto \langle \mathtt{h}(\iota) \downarrow_1,\ \mathtt{h}(\iota) \downarrow_2,\ \mathtt{h}(\iota) \downarrow_3 [f \mapsto \iota']\rangle]
\end{array}
$$

$$
\begin{array}{lcl}
\cdot(\cdot.\cdot) \ :: \ \mathtt{Heap} \times \mathtt{Addr!} \times \mathtt{FieldID} \rightarrow \mathtt{Addr} & & \\
\quad \mathtt{h}(\iota\,.\,f) & = & \mathtt{h}(\iota) \downarrow_3 (f)
\end{array}
$$

$$
\begin{array}{lcl}
\mathtt{class^r} :: \mathtt{Heap} \times \mathtt{Addr!} \rightarrow \mathtt{ClassID} & & \\
\quad \mathtt{class^r}(\mathtt{h}, \iota) & = & \mathtt{h}(\iota) \downarrow_1
\end{array}
$$

$$
\begin{array}{lcl}
\mathtt{owner} :: \mathtt{Heap} \times \mathtt{Addr!} \rightarrow \mathtt{Owners} & & \\
\quad \mathtt{owner}(\mathtt{h}, \iota) & = & \mathtt{h}(\iota) \downarrow_2
\end{array}
$$

$$
\begin{array}{lcl}
\mathtt{owners} :: \mathtt{Heap} \times \mathtt{Addr!} \rightarrow \mathcal{P}(\mathtt{Owners}) & & \\
\quad \mathtt{owners}(\mathtt{h}, \iota) & \in & \mathtt{owners}(\mathtt{h}, \iota) \\
\quad \iota' \in \mathtt{owners}(\mathtt{h}, \iota) \wedge \iota' \downarrow_2 \neq \mathtt{null^r} & \Rightarrow & \mathtt{owner}(\mathtt{h}, \iota' \downarrow_2) \in \mathtt{owners}(\mathtt{h}, \iota)
\end{array}
$$

$$
\begin{array}{lll}
\texttt{transfer} :: \texttt{Heap} \times \texttt{Addr!} \times \texttt{Owners} \to \texttt{Heap} & & \\
\quad \texttt{transfer}(\texttt{h}, \iota, \texttt{ow}) & = & \texttt{h}[\iota \mapsto \langle \texttt{ow},\ \texttt{h}(\iota) \downarrow_2,\ \texttt{h}(\iota) \downarrow_3 \rangle] \\
\\
\texttt{transferCl} :: \texttt{Heap} \times \texttt{Addr} \times \texttt{Owners} \to \texttt{Heap} & & \\
\quad \texttt{transferCl}(\texttt{h}, \iota, \texttt{ow}) & = & \texttt{if}(\iota = \texttt{null}^{\texttt{r}})\ \texttt{then h} \\
\quad \texttt{else transfer}(\ldots \texttt{transfer}(\texttt{transfer}(\texttt{h}, \iota_1, \texttt{ow}), \iota_2, \texttt{ow}) \ldots, \iota_n, \texttt{ow}) & & \\
\quad \texttt{where}\ \{\iota_1,\ \iota_2, \ldots,\ \iota_n\} = \{\iota' \mid \texttt{owner}(\texttt{h},\ \iota') = \texttt{owner}(\texttt{h},\ \iota)\} & & \\
\\
\texttt{newClt} :: \texttt{Heap} \to \texttt{CltFree} & & \\
\quad Cl = \texttt{newClt}(\texttt{h}) & \Rightarrow & Cl \notin \texttt{owner}(\texttt{h},\ \texttt{dom}(\texttt{h})) \downarrow_1 \\
\\
\texttt{mod2Ow} :: \texttt{Heap} \times \texttt{MOD} \times \texttt{Addr!} \to \texttt{Owners} & & \\
\quad \texttt{mod2Ow}(\texttt{h},\ m,\ \iota) = \texttt{if} & (m = \texttt{rep}\ \langle Cl \rangle) & \texttt{then}\ \langle Cl,\ \iota \rangle \\
\quad \texttt{else if} & (m = \texttt{peer}) & \texttt{then owner}(\texttt{h},\ \iota) \\
\quad \texttt{else if} & (m = \texttt{uniq}) & \texttt{then}\ \langle \texttt{newClt}(\texttt{h}),\ \texttt{null}^{\texttt{r}} \rangle \\
\quad \texttt{else} & & \texttt{undefined} \\
\\
\texttt{new} :: \texttt{Heap} \times \texttt{ClassID} \times \texttt{Owners} \to \texttt{Addr!} \times \texttt{Heap} & & \\
\quad \texttt{new}(\texttt{h},\ C,\ \texttt{ow}) & = & \langle \iota,\ \texttt{h}[\iota \mapsto \langle C,\ \texttt{ow},\ \texttt{Fds} \rangle] \rangle \\
\quad \texttt{where}\ \iota \notin \texttt{dom}(\texttt{h}) \wedge \texttt{Fds}(\texttt{fields}(C)) = \texttt{null}^{\texttt{r}} & & \\
\\
\texttt{prj} :: \texttt{States} \to \texttt{States}_{pr} & & \\
\quad \texttt{prj}(\langle \texttt{h},\ \langle \Gamma^{\texttt{r}},\ \Gamma,\ U \rangle \circ \texttt{FrSt} \rangle) & = & \langle \texttt{h},\ \Gamma^{\texttt{r}} \rangle \\
\\
\texttt{RefNum} :: \texttt{Heap} \times \texttt{Frames} \times \texttt{Owners} \times \texttt{MOD} \to \texttt{N} & & \\
\quad \texttt{RefNum}(\texttt{h}, \langle \Gamma^{\texttt{r}},\ \Gamma,\ U \rangle, \texttt{ow}, m) = & & \\
\quad \mid \{x \mid \texttt{mod}(\Gamma(x)) = m \wedge \texttt{owner}(\texttt{h}, \Gamma^{\texttt{r}}(x)) = \texttt{ow} \wedge x \notin U\} \mid & & \\
\\
\texttt{RefNum} :: \texttt{Heap} \times \texttt{FramesStack} \times \texttt{Owners} \times \texttt{MOD} \to \texttt{N} & & \\
\quad \texttt{RefNum}(\texttt{h}, \overline{\texttt{Fr}}, \texttt{ow}, m) = \sum_{\texttt{Fr} \in \overline{\texttt{Fr}}} \texttt{RefNum}(\texttt{h}, \texttt{Fr}, \texttt{ow}, m) & &
\end{array}
$$

5.3 Operational semantic

A judgment has the form $\texttt{h}; \texttt{FrSt}; e \rightsquigarrow \texttt{h}'; \Gamma^{\texttt{r}}$ and expresses evaluation of an expression e.

$$\frac{\Gamma^{\mathtt{r}\prime} = \Gamma^{\mathtt{r}}[x \mapsto \Gamma^{\mathtt{r}}(y)]}{\mathtt{h}; \langle \Gamma^{\mathtt{r}},\ \Gamma,\ U\rangle \circ \mathtt{FrSt}; x = y \rightsquigarrow \mathtt{h}; \Gamma^{\mathtt{r}\prime}} \quad [\text{OS-Assign}]$$

$$\frac{\begin{array}{c}\Gamma^{\mathtt{r}}(y) \neq \mathtt{null}^{\mathtt{r}} \\ \Gamma^{\mathtt{r}\prime} = \Gamma^{\mathtt{r}}[x \mapsto \mathtt{h}(\Gamma^{\mathtt{r}}(y)\,.\,f)]\end{array}}{\mathtt{h}; \langle \Gamma^{\mathtt{r}},\ \Gamma,\ U\rangle \circ \mathtt{FrSt}; x = y.f \rightsquigarrow \mathtt{h}; \Gamma^{\mathtt{r}\prime}} \quad [\text{OS-Field-Read}]$$

$$\frac{\begin{array}{c}\Gamma^{\mathtt{r}}(x) \neq \mathtt{null}^{\mathtt{r}} \\ \mathtt{h}' = \mathtt{h}[\Gamma^{\mathtt{r}}(x)\,.\,f := \Gamma^{\mathtt{r}}(y)]\end{array}}{\mathtt{h}; \langle \Gamma^{\mathtt{r}},\ \Gamma,\ U\rangle \circ \mathtt{FrSt}; x.f := y \rightsquigarrow \mathtt{h}'; \Gamma^{\mathtt{r}}} \quad [\text{OS-Field-Write}]$$

$$\frac{\begin{array}{c}\iota = \Gamma^{\mathtt{r}}(y) \\ \iota \neq \mathtt{null}^{\mathtt{r}} \\ C = \mathtt{class}^{\mathtt{r}}(\iota) \\ \mathtt{mLoc}(C,\ mt) = \overline{v} \\ \mathtt{mType}(C, mt) = T_p \rightarrow T_r \\ \Gamma; U \vdash_{DE} y.mt(z) : U' \\ \Gamma^{\mathtt{r}}{}_1 = \{\langle p,\ \Gamma^{\mathtt{r}}(z)\rangle,\ \overline{\langle v,\ \mathtt{null}^{\mathtt{r}}\rangle},\ \langle \mathtt{this},\ \iota\rangle,\ \langle \mathtt{res},\ \mathtt{null}^{\mathtt{r}}\rangle\} \\ \mathtt{Fr}_1 = \langle \Gamma^{\mathtt{r}}{}_1,\ \Gamma_{C,\ mt},\ \varnothing\rangle \\ \mathtt{Fr}_2 = \langle \Gamma^{\mathtt{r}},\ \Gamma,\ U'\rangle \\ \mathtt{h}; \mathtt{Fr}_1 \circ \mathtt{Fr}_2 \circ \mathtt{FrSt}; \mathtt{mBody}(C,\ mt) \rightsquigarrow \mathtt{h}'; \Gamma^{\mathtt{r}}{}_2 \\ \Gamma^{\mathtt{r}}{}_3 = \Gamma^{\mathtt{r}}{}_1[x \mapsto \Gamma^{\mathtt{r}}{}_2(\mathtt{res})]\end{array}}{\mathtt{h}; \langle \Gamma^{\mathtt{r}},\ \Gamma,\ U\rangle \circ \mathtt{FrSt}; x = y.mt(z) \rightsquigarrow \mathtt{h}'; \Gamma^{\mathtt{r}}{}_3} \quad [\text{OS-Invk}]$$

$$\frac{\begin{array}{c}\mathtt{ow} = \mathtt{mod2Ow}(\mathtt{h},\ \mathtt{mod}(T),\ \Gamma^{\mathtt{r}}(\mathtt{this})) \\ \langle \iota,\ \mathtt{h}'\rangle = \mathtt{new}(\mathtt{h},\ \mathtt{class}(T),\ \mathtt{ow}) \\ \Gamma^{\mathtt{r}\prime} = \Gamma^{\mathtt{r}}[x \mapsto \iota]\end{array}}{\mathtt{h}; \langle \Gamma^{\mathtt{r}},\ \Gamma,\ U\rangle \circ \mathtt{FrSt}; x = new\ T() \rightsquigarrow \mathtt{h}'; \Gamma^{\mathtt{r}\prime}} \quad [\text{OS-New}]$$

$$\frac{\begin{array}{c}\mathtt{ow} = \mathtt{mod2Ow}(\mathtt{h},\ \mathtt{mod}(T),\ \Gamma^{\mathtt{r}}(\mathtt{this})) \\ \mathtt{mod}(T) \neq \mathtt{any} \Rightarrow \mathtt{ow} = \mathtt{owner}(\mathtt{h},\ \Gamma^{\mathtt{r}}(y)) \\ \mathtt{class}^{\mathtt{r}}(\Gamma^{\mathtt{r}}(y)) \sqsubseteq \mathtt{class}(T) \\ \Gamma^{\mathtt{r}\prime} = \Gamma^{\mathtt{r}}[x \mapsto \Gamma^{\mathtt{r}}(y)]\end{array}}{\mathtt{h}; \langle \Gamma^{\mathtt{r}},\ \Gamma,\ U\rangle \circ \mathtt{FrSt}; x = (T)y \rightsquigarrow \mathtt{h}; \Gamma^{\mathtt{r}\prime}} \quad [\text{OS-Cast}]$$

$$\frac{\begin{array}{c}\mathtt{h}; \langle \Gamma^{\mathtt{r}},\ \Gamma,\ U\rangle \circ \mathtt{FrSt}; e_1 \rightsquigarrow \mathtt{h}_1; {\Gamma^{\mathtt{r}}}_1 \\ \Gamma; U \vdash_{DE} e_1 : U' \\ \mathtt{h}; \langle {\Gamma^{\mathtt{r}}}_1,\ \Gamma,\ U'\rangle \circ \mathtt{FrSt}; e_2 \rightsquigarrow \mathtt{h}_2; {\Gamma^{\mathtt{r}}}_2\end{array}}{\mathtt{h}; \langle \Gamma^{\mathtt{r}},\ \Gamma,\ U\rangle \circ \mathtt{FrSt}; e_1; e_2 \rightsquigarrow \mathtt{h}_2; {\Gamma^{\mathtt{r}}}_2} \quad [\text{OS-Comp}]$$

$$\frac{\begin{array}{c}\mathtt{ow} = \mathtt{mod2Ow}(\mathtt{h},\ \mathtt{uniq},\ \Gamma^{\mathtt{r}}(\mathtt{this})) \\ \mathtt{h}' = \mathtt{transferCl}(\mathtt{h},\ \Gamma^{\mathtt{r}}(y),\ \mathtt{ow}) \\ \Gamma^{\mathtt{r}\prime} = \Gamma^{\mathtt{r}}[x \mapsto \Gamma^{\mathtt{r}}(y)]\end{array}}{\mathtt{h}; \langle \Gamma^{\mathtt{r}},\ \Gamma,\ U\rangle \circ \mathtt{FrSt}; x = \mathit{release}(y) \rightsquigarrow \mathtt{h}'; \Gamma^{\mathtt{r}\prime}} \quad [\text{OS-Release}]$$

$$\frac{\begin{array}{c}\mathtt{ow} = \mathtt{mod2Ow}(\mathtt{h},\ m,\ \Gamma^{\mathtt{r}}(\mathtt{this})) \\ \mathtt{h}' = \mathtt{transferCl}(\mathtt{h},\ \Gamma^{\mathtt{r}}(y),\ \mathtt{ow}) \\ \Gamma^{\mathtt{r}\prime} = \Gamma^{\mathtt{r}}[x \mapsto \Gamma^{\mathtt{r}}(y)]\end{array}}{\mathtt{h}; \langle \Gamma^{\mathtt{r}},\ \Gamma,\ U\rangle \circ \mathtt{FrSt}; x = \mathit{capture}\,\langle m\rangle\,(y) \rightsquigarrow \mathtt{h}'; \Gamma^{\mathtt{r}\prime}} \quad [\text{OS-Capture}]$$

6 Type safety

$$\frac{}{\mathtt{h}; \iota_0 \vdash_{wf} \mathtt{null^r} : m} \quad [\textsc{Wf-Null}]$$

$$\frac{}{\mathtt{h}; \iota_0 \vdash_{wf} \iota : \mathtt{any}} \quad [\textsc{Wf-Any}]$$

$$\frac{\mathtt{owner}(\mathtt{h},\ \iota) = \mathtt{owner}(\mathtt{h},\ \iota_0)}{\mathtt{h}; \iota_0 \vdash_{wf} \iota : \mathtt{peer}} \quad [\textsc{Wf-Peer}]$$

$$\frac{\iota = \iota_0}{\mathtt{h}; \iota_0 \vdash_{wf} \iota : \mathtt{this}} \quad [\textsc{Wf-This}]$$

$$\frac{\mathtt{owner}(\mathtt{h},\ \iota) = \langle Cl,\ \iota_0 \rangle}{\mathtt{h}; \iota_0 \vdash_{wf} \iota : \mathtt{rep}\, \langle Cl \rangle} \quad [\textsc{Wf-Rep}]$$

$$\frac{\begin{array}{c}\mathtt{owner}(\mathtt{h},\ \iota) = \langle Cl,\ \mathtt{null^r} \rangle \\ Cl \in \mathtt{CltFree}\end{array}}{\mathtt{h}; \iota_0 \vdash_{wf} \iota : \mathtt{uniq}} \quad [\textsc{Wf-Uniq}]$$

$$\frac{\iota \neq \mathtt{null^r} \Rightarrow C \sqsubseteq \mathtt{class^r}(\mathtt{h},\ \iota)}{\mathtt{h} \vdash_{wf} \iota : C} \quad [\textsc{Wf-Class}]$$

$$\frac{\begin{array}{c}\mathtt{h} \vdash_{wf} \iota : C \\ \mathtt{h}; \iota_0 \vdash_{wf} \iota : m\end{array}}{\mathtt{h}; \iota_0 \vdash_{wf} \iota : m\ C} \quad [\textsc{Wf-Type}]$$

$$\frac{\begin{array}{c}\forall \iota \in \mathtt{dom}(\mathtt{h}) :\ C = \mathtt{class^r}(\mathtt{h},\ \iota) \forall f \in \mathtt{fields}(C) : \\ \mathtt{h} \vdash_{wf} \mathtt{h}(\iota\,.\,f) : \mathtt{class}(\mathtt{fType}(C,\ f))\end{array}}{\vdash_{wf} \mathtt{h}} \quad [\textsc{WF-Heap-Cl}]$$

$$\frac{\begin{array}{c}\forall \iota \in \mathtt{dom}(\mathtt{h}) :\ C = \mathtt{class^r}(\mathtt{h},\ \iota) \forall f \in \mathtt{fields}(C) : \\ \langle \iota,\ f \rangle \notin \{\iota_0\} \times U \Rightarrow \\ \mathtt{h}; \iota \vdash_{wf} \mathtt{h}(\iota\,.\,f) : \mathtt{mod}(\mathtt{fType}(C,\ f))\end{array}}{U; \iota_0 \vdash_{wf} \mathtt{h}} \quad [\textsc{WF-Heap}]$$

$$\frac{\begin{array}{c}\mathtt{dom}(\Gamma^{\mathtt{r}}) = \mathtt{dom}(\Gamma) \\ \mathtt{dom}(\Gamma) \supseteq U \\ \mathtt{mod}(\Gamma(\mathtt{this})) = \mathtt{this} \\ \forall v \in \mathtt{dom}(\Gamma^{\mathtt{r}}) \setminus U \ : \ \mathtt{h}; \Gamma^{\mathtt{r}}(\mathtt{this}) \vdash_{wf} \Gamma^{\mathtt{r}}(v) : \Gamma(v)\end{array}}{\mathtt{h} \vdash_{wf} \Gamma^{\mathtt{r}}; \Gamma; U} \quad [\text{WF-Frame}]$$

$$\frac{\forall \iota \in \mathtt{dom}(\mathtt{h}) \ : \ \iota \notin \mathtt{owners}(\mathtt{h},\ \iota) \downarrow_2}{\mathtt{WfTree}(\mathtt{h})} \quad [\text{WF-Tree}]$$

$$\frac{\overline{\mathtt{h} \vdash_{wf} \Gamma^{\mathtt{r}}; \Gamma; U}}{\mathtt{h} \vdash_{wf} \overline{\langle \Gamma^{\mathtt{r}},\ \Gamma,\ U \rangle}} \quad [\text{WF-FrSt}]$$

$$\frac{\forall Cl \in \mathtt{CltFree}\ \mathtt{RefNum}(\mathtt{h}, \mathtt{FrSt}, \langle Cl,\ \mathtt{null}^{\mathtt{r}} \rangle, \mathtt{uniq}) \leq 1}{\mathtt{h} \vdash_{Uniq} \mathtt{FrSt}} \quad [\text{WF-Uniq-Glob}]$$

$$\frac{\forall Cl \in \mathtt{CltRep} \setminus \{Cl_{\mathtt{this}}\}\ \mathtt{RefNum}(\mathtt{h}, \mathtt{FrSt}, \langle Cl,\ \iota \rangle, \mathtt{rep}\ \langle Cl \rangle) = 0}{\mathtt{h}; \mathtt{FrSt} \vdash_{Inv} \iota} \quad [\text{WF-Inv-Obj}]$$

$$\frac{\begin{array}{c}(\{\mathtt{owner}(\mathtt{h},\ \Gamma^{\mathtt{r}}(\mathtt{this}))\} \cup \\ \cup \{\mathtt{owner}(\mathtt{h},\ \Gamma^{\mathtt{r}}(x)) \mid \Gamma^{\mathtt{r}}(x) \neq \mathtt{null}^{\mathtt{r}} \wedge \Gamma(x) = \mathtt{uniq} \wedge x \notin U\}) \cap \\ \cap \mathtt{owners}(\mathtt{h},\ \iota) \neq \varnothing\end{array}}{\mathtt{ExtOwn}(\mathtt{h},\ \langle \Gamma^{\mathtt{r}},\ \Gamma,\ U \rangle,\ \iota)} \quad [\text{Ext-Own-Tr}]$$

$$\frac{\begin{array}{c}\mathtt{FrSt} = \langle \Gamma^{\mathtt{r}},\ \Gamma,\ U \rangle \circ \mathtt{FrSt}' \\ \iota_0 = \Gamma^{\mathtt{r}}(\mathtt{this}) \\ \mathtt{h}; \mathtt{FrSt}' \vdash_{Inv} \iota_0 \\ \forall \iota \ : \ \mathtt{ExtOwn}(\mathtt{h},\ \mathtt{Fr},\ \iota) \wedge \iota \neq \iota_0 \Rightarrow \mathtt{h}; \mathtt{FrSt} \vdash_{Inv} \iota\end{array}}{\mathtt{h} \vdash_{Inv} \mathtt{FrSt}} \quad [\text{WF-Inv-Glob}]$$

$$\frac{\begin{array}{c}\mathtt{Fr}_0 \circ \overline{\mathtt{Fr}} = \langle {\Gamma^{\mathtt{r}}}_0,\ \Gamma_0,\ U_0 \rangle \circ \overline{\langle \Gamma^{\mathtt{r}},\ \Gamma,\ U \rangle} \\ \forall Cl \in \mathtt{CltFree} : \langle Cl,\ \mathtt{null}^{\mathtt{r}} \rangle \notin \mathtt{owners}(\mathtt{h},\ {\Gamma^{\mathtt{r}}}_0(\mathtt{this})) \\ \overline{\mathtt{owner}(\mathtt{h},\ \Gamma^{\mathtt{r}}(\mathtt{this})) \in \mathtt{owners}(\mathtt{h},\ {\Gamma^{\mathtt{r}}}_0(\mathtt{this}))}\end{array}}{\mathtt{ThisOw}(\mathtt{h},\ \mathtt{Fr}_0 \circ \overline{\mathtt{Fr}})} \quad [\text{WF-This-Ow}]$$

$$\frac{\begin{array}{c}\texttt{FrSt} = \langle \Gamma^{\texttt{r}},\ \Gamma,\ U\rangle \circ \texttt{FrSt}' \\ \vdash_{wf} \texttt{h} \\ U; \Gamma^{\texttt{r}}(\texttt{this}) \vdash_{wf} \texttt{h} \\ \texttt{h} \vdash_{wf} \texttt{FrSt} \\ \texttt{h} \vdash_{Uniq} \texttt{FrSt} \\ \texttt{h} \vdash_{Inv} \texttt{FrSt} \\ \texttt{WfTree}(\texttt{h}) \\ \texttt{ThisOw}(\texttt{h},\ \texttt{FrSt})\end{array}}{\vdash_{wf} \langle \texttt{h},\ \texttt{FrSt}\rangle} \quad [\text{WF-St}]$$

$$\frac{\begin{array}{c}\forall \iota \in \texttt{dom}(\texttt{h}) : \neg\texttt{ExtOwn}(\texttt{h},\ \texttt{Fr},\ \iota) \Rightarrow \\ \texttt{h}(\iota) = \texttt{h}'(\iota) \wedge \neg\texttt{ExtOwn}(\texttt{h}',\ \texttt{Fr}',\ \iota)\end{array}}{\texttt{OwAsMod}(\texttt{h},\ \texttt{h}',\ \texttt{Fr},\ \texttt{Fr}')} \quad [\text{Ow-As-Mod}]$$

7 Type safety proof

7.1 The main theorem

Theorem 7.1.

$$\left.\begin{array}{l}\vdash_{wf} \langle \boldsymbol{h},\ \boldsymbol{FrSt}\rangle \\ \boldsymbol{FrSt} = \boldsymbol{Fr} \circ \boldsymbol{FrSt}_0 \\ \boldsymbol{Fr} = \langle \Gamma^{r},\ \Gamma,\ U\rangle \\ \Gamma; U \vdash e \\ \Gamma; U \vdash_{DE} e : U' \\ \boldsymbol{h}; \boldsymbol{FrSt}; e \rightsquigarrow \boldsymbol{h}'; \Gamma^{r'} \\ \boldsymbol{Fr}' = \langle \Gamma^{r'},\ \Gamma,\ U'\rangle \\ \boldsymbol{FrSt}' = \boldsymbol{Fr}' \circ \boldsymbol{FrSt}_0\end{array}\right\} \Rightarrow \left\{\begin{array}{l}\vdash_{wf} \langle \boldsymbol{h}',\ \boldsymbol{FrSt}'\rangle \\ \boldsymbol{OwAsMod}(\boldsymbol{h},\ \boldsymbol{h}',\ \boldsymbol{Fr},\ \boldsymbol{Fr}')\end{array}\right.$$

Proof.

$$\vdash_{wf} \langle \texttt{h},\ \texttt{FrSt}\rangle \Rightarrow \left\{\begin{array}{ll}\vdash_{wf} \texttt{h} & (1) \\ U; \Gamma^{\texttt{r}}(\texttt{this}) \vdash_{wf} \texttt{h} & (2) \\ \texttt{h} \vdash_{wf} \texttt{FrSt} & (3) \\ \texttt{h} \vdash_{Uniq} \texttt{FrSt} & (4) \\ \texttt{h} \vdash_{Inv} \texttt{FrSt} & (5) \\ \texttt{WfTree}(\texttt{h}) & (6) \\ \texttt{ThisOw}(\texttt{h},\ \texttt{FrSt}) & (7)\end{array}\right.$$

- OS-Assign

$U' = \texttt{consumeUniq}(U, \Gamma(x), y) \setminus \{x\}$
$\Gamma^{\mathtt{r}\prime} = \Gamma^{\mathtt{r}}[x \mapsto \Gamma^{\mathtt{r}}(y)]$

$(2) \overset{Lem.\ 7.14}{\Rightarrow} U'; \Gamma^{\mathtt{r}\prime}(\texttt{this}) \vdash_{wf} \texttt{h}\ (8)$
T-Assign $\Rightarrow y \notin U \overset{(3)}{\Rightarrow} \texttt{h}; \Gamma^{\mathtt{r}}(\texttt{this}) \vdash_{wf} \Gamma^{\mathtt{r}}(y) : \Gamma(y) \Rightarrow$
$\overset{Lem.\ 7.21 \wedge Lem.\ 7.22 \wedge (3)}{\Rightarrow} \texttt{h} \vdash_{wf} \texttt{FrSt}'\ (9)$
$\texttt{FrSt}'' = \langle \Gamma^{\mathtt{r}},\ \Gamma,\ \texttt{consumeUniq}(U, \Gamma(x), y) \rangle \circ \texttt{FrSt}_0$
$(4) \overset{Lem.\ 7.29 \wedge (3)}{\Rightarrow} \texttt{h} \vdash_{Uniq} \texttt{FrSt}''\ (10)$
$(3) \wedge (4) \Rightarrow (\Gamma^{\mathtt{r}}(y) \neq \texttt{null}^{\mathtt{r}} \wedge \Gamma(x) = \texttt{uniq} \Rightarrow$
$\texttt{RefNum}(\texttt{h}, \texttt{FrSt}'', \texttt{owner}(\texttt{h},\ (\Gamma^{\mathtt{r}}(y)), \texttt{uniq}) = 0)) \overset{Lem.\ 7.30 \wedge (10)}{\Rightarrow} \texttt{h} \vdash_{Uniq} \texttt{FrSt}'\ (11)$
$(5) \wedge (9) \overset{Lem.\ 7.37}{\Rightarrow} \texttt{h} \vdash_{Inv} \texttt{FrSt}'\ (12)$
$(7) \overset{Lem.\ 7.49}{\Rightarrow} \texttt{ThisOw}(\texttt{h},\ \texttt{FrSt}')\ (13)$
$(1) \wedge (8) \wedge (9) \wedge (11) \wedge (12) \wedge (6) \wedge (13) \Rightarrow \vdash_{wf} \langle \texttt{h}',\ \texttt{FrSt}' \rangle$
$Lem.\ 7.55 \Rightarrow \texttt{OwAsMod}(\texttt{h},\ \texttt{h},\ \texttt{Fr},\ \texttt{Fr}')$

- OS-Field-Read

$U' = U \setminus \{x\}$
$\Gamma^{\mathtt{r}}(y) \neq \texttt{null}^{\mathtt{r}}$
$\Gamma^{\mathtt{r}\prime} = \Gamma^{\mathtt{r}}[x \mapsto \texttt{h}(\Gamma^{\mathtt{r}}(y) \,.\, f)]$

$(2) \overset{Lem.\ 7.14}{\Rightarrow} U'; \Gamma^{\mathtt{r}\prime}(\texttt{this}) \vdash_{wf} \texttt{h}\ (8)$
T-Field-Read $\Rightarrow y \notin U \overset{(3)}{\Rightarrow} \texttt{h}; \Gamma^{\mathtt{r}}(\texttt{this}) \vdash_{wf} \Gamma^{\mathtt{r}}(y) : \Gamma(y) \overset{Lem.\ 7.15}{\Rightarrow}$
$\texttt{h}; \Gamma^{\mathtt{r}}(\texttt{this}) \vdash_{wf} \texttt{h}(\Gamma^{\mathtt{r}}(y) \,.\, f) : T \rhd_U \texttt{fType}(\texttt{class}^{\mathtt{r}}(\Gamma^{\mathtt{r}}(y)),\ f) \Rightarrow$
$\overset{Lem.\ 7.21 \wedge Lem.\ 7.22 \wedge (3)}{\Rightarrow} \texttt{h} \vdash_{wf} \texttt{FrSt}'\ (9)$
T-Field-Read $\Rightarrow \Gamma(x) \neq \texttt{uniq} \overset{Lem.\ 7.30 \wedge Lem.\ 7.29 \wedge (4)}{\Rightarrow} \texttt{h} \vdash_{Uniq} \texttt{FrSt}'\ (10)$
$(5) \wedge (9) \overset{Lem.\ 7.37}{\Rightarrow} \texttt{h} \vdash_{Inv} \texttt{FrSt}'\ (11)$
$(7) \overset{Lem.\ 7.49}{\Rightarrow} \texttt{ThisOw}(\texttt{h},\ \texttt{FrSt}')\ (12)$
$(1) \wedge (8) \wedge (9) \wedge (10) \wedge (11) \wedge (6) \wedge (12) \Rightarrow \vdash_{wf} \langle \texttt{h}',\ \texttt{FrSt}' \rangle$
$Lem.\ 7.55 \Rightarrow \texttt{OwAsMod}(\texttt{h},\ \texttt{h},\ \texttt{Fr},\ \texttt{Fr}')$

- OS-Field-Write

$U' = \texttt{if}(y = \texttt{this})\ \texttt{then}\ U \setminus \{f\}\ \texttt{else}\ U$
$\texttt{h}' = \texttt{h}[\Gamma^{\texttt{r}}(x).f := \Gamma^{\texttt{r}}(y)]$

(1) $\overset{Lem.\ 7.11}{\Rightarrow} \vdash_{wf} \texttt{h}'$ (8)
(3) $\Rightarrow \texttt{h}; \Gamma^{\texttt{r}}(this) \vdash_{wf} \Gamma^{\texttt{r}}(y) : \Gamma(y) \wedge \texttt{h}; \Gamma^{\texttt{r}}(this) \vdash_{wf} \Gamma^{\texttt{r}}(x) : \Gamma(x) \Rightarrow$
$\overset{Lem.\ 7.3 \wedge \text{T-Field-Write}}{\Rightarrow} \texttt{h}; \Gamma^{\texttt{r}}(y) \vdash_{wf} \Gamma^{\texttt{r}}(x) : \texttt{fType}(\texttt{class}^{\texttt{r}}(\Gamma^{\texttt{r}}(x)),\ f) \Rightarrow$
$\overset{Lem.\ 7.15 \wedge (2)}{\Rightarrow} U'; \Gamma^{\texttt{r}\prime}(\texttt{this}) \vdash_{wf} \texttt{h}'$ (9)
(3) $\overset{Lem.\ 7.21 \wedge Lem.\ 7.23}{\Rightarrow} \texttt{h}' \vdash_{wf} \texttt{FrSt}'$ (10)
(4) $\overset{Lem.\ 7.29 \wedge Lem.\ 7.31}{\Rightarrow} \texttt{h}' \vdash_{Uniq} \texttt{FrSt}'$ (11)
(5) $\overset{Lem.\ 7.37 \wedge Lem.\ 7.38}{\Rightarrow} \texttt{h}' \vdash_{Inv} \texttt{FrSt}'$ (12)
(6) $\overset{Lem.\ 7.45}{\Rightarrow} \texttt{WfTree}(\texttt{h}')$ (13)
(7) $\overset{Lem.\ 7.49 \wedge Lem.\ 7.50}{\Rightarrow} \texttt{ThisOw}(\texttt{h}',\ \texttt{FrSt}')$ (14)
$(8) \wedge (9) \wedge (10) \wedge (11) \wedge (12) \wedge (13) \wedge (14) \Rightarrow \vdash_{wf} \langle \texttt{h}',\ \texttt{FrSt}' \rangle$
$Lem.\ 7.55 \wedge Lem.\ 7.56 \Rightarrow \texttt{OwAsMod}(\texttt{h},\ \texttt{hFr}',\ \texttt{Fr},\ \texttt{Fr}')$

- OS-Invk

$U_1 = \texttt{consumeUniq}(U, T_p, z)$
$U_2 = \texttt{consumeLocals}(U_1)$
$\Gamma^{\texttt{r}}{}_1 = \{\langle p,\ \Gamma^{\texttt{r}}(z)\rangle,\ \overline{\langle v,\ \texttt{null}^{\texttt{r}}\rangle},\ \langle \texttt{this},\ \iota\rangle,\ \langle \texttt{res},\ \texttt{null}^{\texttt{r}}\rangle\}$
$\texttt{Fr}_1 = \langle \Gamma^{\texttt{r}}{}_1,\ \Gamma_{C,\ mt},\ \varnothing\rangle$
$\texttt{Fr}_2 = \langle \Gamma^{\texttt{r}},\ \Gamma,\ U_2\rangle$
$\texttt{FrSt}_1 = \texttt{Fr}_1 \circ \texttt{Fr}_2 \circ \texttt{FrSt}_0$
$\texttt{h}; \texttt{FrSt}_1; \texttt{mBody}(C,\ mt) \rightsquigarrow \texttt{h}'; \Gamma^{\texttt{r}}{}_2$
$\Gamma; U_2 \vdash_{DE} y.mt(z) : U_3$
$\texttt{Fr}_3 = \langle \Gamma^{\texttt{r}}{}_2,\ \Gamma_{C,\ mt},\ U_3\rangle$
$\texttt{FrSt}_2 = \texttt{Fr}_3 \circ \texttt{Fr}_2 \circ \texttt{FrSt}_0$
$\Gamma^{\texttt{r}}{}_3 = \Gamma^{\texttt{r}}{}_1[x \mapsto \Gamma^{\texttt{r}}{}_2(\texttt{res})]$
$U_4 = U_2 \setminus \{x\}$
$\texttt{Fr}' = \langle \Gamma^{\texttt{r}}{}_3,\ \Gamma_{C,\ mt},\ U_4\rangle$

$(2) \overset{Lem.\ 7.14}{\Rightarrow} U_2; \Gamma^{\texttt{r}}(\texttt{this}) \vdash_{wf} \texttt{h} \overset{Lem.\ 7.17}{\Rightarrow} \varnothing; \Gamma^{\texttt{r}}{}_1(\texttt{this}) \vdash_{wf} \texttt{h}\ (9)$
$(3) \wedge \text{T-Invk} \overset{Lem.\ 7.21 \wedge Lem.\ 7.24}{\Rightarrow} \texttt{h} \vdash_{wf} \texttt{FrSt}_1\ (10)$
$(4) \overset{Lem.\ 7.29 \wedge Lem.\ 7.32}{\Rightarrow} (5) \overset{Lem.\ 7.37 \wedge Lem.\ 7.39}{\Rightarrow} \texttt{h} \vdash_{Inv} \texttt{FrSt}_1\ (12)$
$(7) \overset{Lem.\ 7.49 \wedge Lem.\ 7.51}{\Rightarrow} \texttt{ThisOw}(\texttt{h},\ \texttt{FrSt}_1)\ (13)$
$(1) \wedge (9) \wedge (10) \wedge (11) \wedge (12) \wedge (6) \wedge (13) \Rightarrow \vdash_{wf} \langle \texttt{h},\ \texttt{FrSt}_2\rangle \overset{\texttt{Ind.}}{\Rightarrow}{}^{\texttt{step}}$

$$\Rightarrow \begin{cases} \vdash_{wf} \langle \texttt{h}',\ \texttt{FrSt}_2\rangle & (14) \\ \texttt{OwAsMod}(\texttt{h},\ \texttt{h}',\ \texttt{Fr}_1,\ \texttt{Fr}_3) & (15) \end{cases}$$

$$(14) \Rightarrow \begin{cases} \vdash_{wf} \texttt{h}' & (16) \\ \texttt{FrSt}_2; \texttt{h}' \vdash_{wf} & (17) \\ U_3; \Gamma^{\texttt{r}}{}_2(\texttt{this}) \vdash_{wf} \texttt{h} & (18) \\ \texttt{h}' \vdash_{Uniq} \texttt{FrSt}_2 & (19) \\ \texttt{h}' \vdash_{Inv} \texttt{FrSt}_2 & (20) \\ \texttt{WfTree}(\texttt{h}') & (21) \\ \texttt{ThisOw}(\texttt{h}',\ \texttt{FrSt}_2) & (22) \end{cases}$$

$\text{T-Invk} \Rightarrow U_3 \cap \texttt{FieldID} = \varnothing \overset{Lem.\ 7.17 \wedge (17)}{\Rightarrow} U_2; \Gamma^{\mathtt{r}}(\texttt{this}) \vdash_{wf} \texttt{h}' \Rightarrow$
$\overset{Lem.\ 7.14}{\Rightarrow} U_4; \Gamma^{\mathtt{r}}{}_3(\texttt{this}) \vdash_{wf} \texttt{h}'$ (23)
(18) $\overset{Lem.\ 7.25}{\Rightarrow} \texttt{h}' \vdash_{wf} \texttt{Fr}_2 \circ \texttt{FrSt}_0 \overset{Lem.\ 7.22}{\Rightarrow} \texttt{h}' \vdash_{wf} \texttt{FrSt}'$ (24)
(19) $\overset{Lem.\ 7.33}{\Rightarrow} \texttt{h}' \vdash_{Uniq} \texttt{Fr}_2 \circ \texttt{FrSt}_0 \overset{Lem.\ 7.30}{\Rightarrow} \texttt{h}' \vdash_{Uniq} \texttt{FrSt}'$ (25)
(20) $\wedge$ (15) $\overset{Lem.\ 7.40 \wedge Lem.\ 7.41}{\Rightarrow} \texttt{h}' \vdash_{Inv} \texttt{Fr}_2 \circ \texttt{FrSt}_0 \overset{Lem.\ 7.37}{\Rightarrow} \texttt{h}' \vdash_{Inv} \texttt{FrSt}'$ (26)
(22) $\wedge$ (15) $\overset{Lem.\ 7.53 \wedge Lem.\ 7.53}{\Rightarrow} \texttt{ThisOw}(\texttt{h}',\ \texttt{Fr}_2 \circ \texttt{FrSt}_0) \overset{Lem.\ 7.49}{\Rightarrow} \texttt{ThisOw}(\texttt{h}',\ \texttt{FrSt}')$ (27)
(16) $\wedge$ (23) $\wedge$ (24) $\wedge$ (25) $\wedge$ (26) $\wedge$ (21) $\wedge$ (27) $\Rightarrow \vdash_{wf} \langle \texttt{h}',\ \texttt{FrSt}' \rangle$
$Lem.$ 7.55 $\Rightarrow \texttt{OwAsMod}(\texttt{h},\ \texttt{h},\ \texttt{Fr},\ \texttt{Fr}_2)$ (28)
$Lem.$ 7.55 $\Rightarrow \texttt{OwAsMod}(\texttt{h},\ \texttt{h},\ \texttt{Fr}_2,\ \texttt{Fr}_1) \overset{Lem.\ 7.59 \wedge (15)}{\Rightarrow} \texttt{OwAsMod}(\texttt{h},\ \texttt{h}',\ \texttt{Fr}_2,\ \texttt{Fr}_3) \Rightarrow$
$\overset{Lem.\ 7.57}{\Rightarrow} \texttt{OwAsMod}(\texttt{h},\ \texttt{h}',\ \texttt{Fr}_2,\ \texttt{Fr}_2)$ (29)
(28) $\wedge$ (29) $\overset{Lem.\ 7.59}{\Rightarrow} \texttt{OwAsMod}(\texttt{h},\ \texttt{h}',\ \texttt{Fr},\ \texttt{Fr}_2) \overset{Lem.\ 7.55}{\Rightarrow} \texttt{OwAsMod}(\texttt{h},\ \texttt{h}',\ \texttt{Fr},\ \texttt{Fr}')$

- OS-New

$U' = U \setminus \{x\}$
$\texttt{ow} = \texttt{mod2Ow}(\texttt{h},\ \texttt{mod}(T),\ \Gamma^{\mathtt{r}}(\texttt{this}))$
$\langle \iota,\ \texttt{h}' \rangle = \texttt{new}(\texttt{h},\ \texttt{class}(T),\ \texttt{ow})$
$\Gamma^{\mathtt{r}\prime} = \Gamma^{\mathtt{r}}[x \mapsto \iota]$

(1) $\overset{Lem.\ 7.12}{\Rightarrow} \vdash_{wf} \texttt{h}'$ (8)
(2) $\overset{Lem.\ 7.14}{\Rightarrow} U'; \Gamma^{\mathtt{r}\prime}(\texttt{this}) \vdash_{wf} \texttt{h} \overset{Lem.\ 7.18}{\Rightarrow} U'; \Gamma^{\mathtt{r}\prime}(\texttt{this}) \vdash_{wf} \texttt{h}'$ (9)
(3) $\overset{Lem.\ 7.26 \wedge (3)}{\Rightarrow} \texttt{h}' \vdash_{wf} \texttt{FrSt}$ (10)
$Lem.$ 7.4 $\Rightarrow \texttt{h}; \Gamma^{\mathtt{r}}(\texttt{this}) \vdash_{wf} \iota : T \overset{Lem.\ 7.6 \wedge \text{T-New}}{\Rightarrow} \texttt{h}; \Gamma^{\mathtt{r}}(\texttt{this}) \vdash_{wf} \iota : \Gamma(x) \Rightarrow$
$\overset{Lem.\ 7.22 \wedge (10)}{\Rightarrow} \texttt{h}' \vdash_{wf} \texttt{FrSt}'$ (11)
$\texttt{mod}(T) = \texttt{uniq} \Rightarrow \texttt{ow} = \langle \texttt{newClt}(\texttt{h}),\ \texttt{null}^{\mathtt{r}} \rangle \Rightarrow \texttt{RefNum}(\texttt{h}', \texttt{FrSt}, \texttt{ow}, \texttt{uniq}) = 0$ (12)
(4) $\overset{Lem.\ 7.34}{\Rightarrow} \texttt{h}' \vdash_{Uniq} \texttt{FrSt} \overset{Lem.\ 7.30 \wedge (12)}{\Rightarrow} \texttt{h}' \vdash_{Uniq} \texttt{FrSt}'$ (13)
(5) $\overset{Lem.\ 7.42}{\Rightarrow} \texttt{h}' \vdash_{Inv} \texttt{FrSt} \overset{Lem.\ 7.37}{\Rightarrow} \texttt{h}' \vdash_{Inv} \texttt{FrSt}'$ (13)
(6) $\overset{Lem.\ 7.46}{\Rightarrow} \texttt{WfTree}(\texttt{h}')$ (14)
(7) $\overset{Lem.\ 7.52}{\Rightarrow} \texttt{ThisOw}(\texttt{h}',\ \texttt{FrSt}) \overset{Lem.\ 7.49}{\Rightarrow} \texttt{ThisOw}(\texttt{h}',\ \texttt{FrSt}')$ (15)
(8) $\wedge$ (9) $\wedge$ (10) $\wedge$ (12) $\wedge$ (13) $\wedge$ (14) $\wedge$ (15) $\Rightarrow \vdash_{wf} \langle \texttt{h}',\ \texttt{FrSt}' \rangle$
$Lem.$ 7.58 $\Rightarrow \texttt{OwAsMod}(\texttt{h},\ \texttt{h}',\ \texttt{FrSt},\ \texttt{FrSt}')$

- OS-Cast

$$
\begin{array}{l}
U' = \texttt{consumeUniq}(U, \Gamma(x), y) \setminus \{x\} \\
\texttt{ow} = \texttt{mod2Ow}(\texttt{h},\ \texttt{mod}(T),\ \Gamma^{\texttt{r}}(\texttt{this})) \\
\texttt{mod}(T) \neq \texttt{any} \Rightarrow \texttt{ow} = \texttt{owner}(\texttt{h},\ \Gamma^{\texttt{r}}(y)) \\
\texttt{class}^{\texttt{r}}(\Gamma^{\texttt{r}}(y)) \sqsubseteq \texttt{class}(T) \\
\Gamma^{\texttt{r}\prime} = \Gamma^{\texttt{r}}[x \mapsto \Gamma^{\texttt{r}}(y)]
\end{array}
$$

$$
\begin{array}{l}
(2) \overset{Lem.\ 7.14}{\Rightarrow} U'; \Gamma^{\texttt{r}\prime}(\texttt{this}) \vdash_{wf} \texttt{h}\ (8) \\
(3) \overset{Lem.\ 7.4}{\Rightarrow} \texttt{h}; \Gamma^{\texttt{r}}(\texttt{this}) \vdash_{wf} \Gamma^{\texttt{r}}(y) : T \Rightarrow \\
\overset{Lem.\ 7.21 \wedge Lem.\ 7.22 \wedge (3)}{\Rightarrow} \texttt{h} \vdash_{wf} \texttt{FrSt}'\ (9) \\
\texttt{FrSt}'' = \langle \Gamma^{\texttt{r}},\ \Gamma,\ \texttt{consumeUniq}(U, \Gamma(x), y) \rangle \circ \texttt{FrSt}_0 \\
(4) \overset{Lem.\ 7.29 \wedge (3)}{\Rightarrow} \texttt{h} \vdash_{Uniq} \texttt{FrSt}''\ (10) \\
(3) \wedge (4) \Rightarrow (\Gamma^{\texttt{r}}(y) \neq \texttt{null}^{\texttt{r}} \wedge \Gamma(x) = \texttt{uniq} \Rightarrow \\
\texttt{RefNum}(\texttt{h}, \texttt{FrSt}'', \texttt{owner}(\texttt{h},\ (\Gamma^{\texttt{r}}(y)), \texttt{uniq}) = 0)) \overset{Lem.\ 7.30 \wedge (10)}{\Rightarrow} \texttt{h} \vdash_{Uniq} \texttt{FrSt}'\ (11) \\
(5) \wedge (9) \overset{Lem.\ 7.37}{\Rightarrow} \texttt{h} \vdash_{Inv} \texttt{FrSt}'\ (12) \\
(7) \overset{Lem.\ 7.49}{\Rightarrow} \texttt{ThisOw}(\texttt{h},\ \texttt{FrSt}')\ (13) \\
(1) \wedge (8) \wedge (9) \wedge (11) \wedge (12) \wedge (6) \wedge (13) \Rightarrow \vdash_{wf} \langle \texttt{h}',\ \texttt{FrSt}' \rangle \\
Lem.\ 7.55 \Rightarrow \texttt{OwAsMod}(\texttt{h},\ \texttt{h},\ \texttt{Fr},\ \texttt{Fr}')
\end{array}
$$

- OS-Comp

$$
\begin{array}{l}
\Gamma; U \vdash_{DE} e_1; e_2 : U'' \\
\texttt{Fr}_1 = \langle \Gamma^{\texttt{r}}{}_1,\ \Gamma,\ U' \rangle \\
\vdash_{wf} \langle \texttt{h},\ \texttt{FrSt} \rangle \overset{\texttt{Ind.}}{\Rightarrow}{}^{\texttt{step}} \begin{cases} \vdash_{wf} \langle \texttt{h}_1,\ \texttt{Fr}_1 \circ \texttt{FrSt} \rangle & (7) \\ \texttt{OwAsMod}(\texttt{h},\ \texttt{h}_1,\ \texttt{Fr},\ \texttt{Fr}_1) & (8) \end{cases} \\
\texttt{Fr}_2 = \langle \Gamma^{\texttt{r}}{}_2,\ \Gamma,\ U'' \rangle \\
(7) \overset{\texttt{Ind.}}{\Rightarrow}{}^{\texttt{step}} \begin{cases} \vdash_{wf} \langle \texttt{h}_2,\ \texttt{Fr}_2 \circ \texttt{FrSt} \rangle \\ \texttt{OwAsMod}(\texttt{h}_1,\ \texttt{h}_2,\ \texttt{Fr}_1,\ \texttt{Fr}_2) \quad (9) \end{cases} \\
(8) \wedge (9) \overset{Lem.\ 7.59}{\Rightarrow} \texttt{OwAsMod}(\texttt{h},\ \texttt{h}_2,\ \texttt{Fr}_1,\ \texttt{Fr}_2)
\end{array}
$$

- OS-Release

$U' = \texttt{consumeAliases}(U, y) \setminus \{x\}$
$\texttt{ow} = \texttt{mod2Ow}(\texttt{h},\ \texttt{uniq},\ \Gamma^{\texttt{r}}(\texttt{this}))$
$\texttt{h}' = \texttt{transferCl}(\texttt{h},\ \Gamma^{\texttt{r}}(y),\ \texttt{ow})$
$\Gamma^{\texttt{r}\prime} = \Gamma^{\texttt{r}}[x \mapsto \Gamma^{\texttt{r}}(y)]$

(1) $\overset{Lem.\ 7.13}{\Rightarrow} \vdash_{wf} \texttt{h}'$ (8)
(2) $\overset{Lem.\ 7.19 \wedge Lem.\ 7.14}{\Rightarrow} U'; \Gamma^{\texttt{r}\prime}(\texttt{this}) \vdash_{wf} \texttt{h}'$ (9)
(3) $\wedge$ (5) $\overset{Lem.\ 7.27 \wedge Lem.\ 7.21}{\Rightarrow} \texttt{h}' \vdash_{wf} \texttt{FrSt}'$ (10)
(3) $\wedge$ (4) $\overset{Lem.\ 7.35 \wedge Lem.\ 7.29}{\Rightarrow} \texttt{h}' \vdash_{Uniq} \texttt{FrSt}'$ (11)
(3) $\wedge$ (5) $\wedge$ (7) $\overset{Lem.\ 7.43 \wedge Lem.\ 7.37}{\Rightarrow} \texttt{h}' \vdash_{Inv} \texttt{FrSt}'$ (12)
(6) $\overset{Lem.\ 7.47}{\Rightarrow} \texttt{WfTree}(\texttt{h}')$ (13)
(7) $\overset{Lem.\ 7.54 \wedge Lem.\ 7.49}{\Rightarrow} \texttt{ThisOw}(\texttt{h}',\ \texttt{FrSt}')$ (14)
(8) $\wedge$ (9) $\wedge$ (10) $\wedge$ (11) $\wedge$ (12) $\wedge$ (13) $\wedge$ (14) $\Rightarrow \vdash_{wf} \langle \texttt{h}',\ \texttt{FrSt}' \rangle$
(3) $\wedge$ $Lem.$ 7.60 $\wedge$ $Lem.$ 7.55 $\Rightarrow \texttt{OwAsMod}(\texttt{h},\ \texttt{h}',\ \texttt{Fr},\ \texttt{Fr}')$

- OS-Capture

$U' = U \cup \{y\} \setminus \{x\}$
$\texttt{ow} = \texttt{mod2Ow}(\texttt{h},\ m,\ \Gamma^{\texttt{r}}(\texttt{this}))$
$\texttt{h}' = \texttt{transferCl}(\texttt{h},\ \Gamma^{\texttt{r}}(y),\ \texttt{ow})$
$\Gamma^{\texttt{r}\prime} = \Gamma^{\texttt{r}}[x \mapsto \Gamma^{\texttt{r}}(y)]$

(1) $\overset{Lem.\ 7.13}{\Rightarrow} \vdash_{wf} \texttt{h}'$ (8)
(2) $\overset{Lem.\ 7.20 \wedge Lem.\ 7.14}{\Rightarrow} U'; \Gamma^{\texttt{r}\prime}(\texttt{this}) \vdash_{wf} \texttt{h}'$ (9)
(3) $\wedge$ (5) $\overset{Lem.\ 7.28 \wedge Lem.\ 7.21}{\Rightarrow} \texttt{h}' \vdash_{wf} \texttt{FrSt}'$ (10)
(3) $\wedge$ (4) $\overset{Lem.\ 7.36 \wedge Lem.\ 7.29}{\Rightarrow} \texttt{h}' \vdash_{Uniq} \texttt{FrSt}'$ (11)
(3) $\wedge$ (5) $\wedge$ (7) $\overset{Lem.\ 7.44 \wedge Lem.\ 7.37}{\Rightarrow} \texttt{h}' \vdash_{Inv} \texttt{FrSt}'$ (12)
(6) $\overset{Lem.\ 7.48}{\Rightarrow} \texttt{WfTree}(\texttt{h}')$ (13)
(7) $\overset{Lem.\ 7.54 \wedge Lem.\ 7.49}{\Rightarrow} \texttt{ThisOw}(\texttt{h}',\ \texttt{FrSt}')$ (14)
(8) $\wedge$ (9) $\wedge$ (10) $\wedge$ (11) $\wedge$ (12) $\wedge$ (13) $\wedge$ (14) $\Rightarrow \vdash_{wf} \langle \texttt{h}',\ \texttt{FrSt}' \rangle$
(3) $\wedge$ $Lem.$ 7.61 $\wedge$ $Lem.$ 7.55 $\Rightarrow \texttt{OwAsMod}(\texttt{h},\ \texttt{h}',\ \texttt{Fr},\ \texttt{Fr}')$

□

7.2 Auxiliary lemmas

$$\begin{aligned}
&\texttt{RepSet} :: \texttt{Heap} \times \texttt{Addr!} \rightarrow \mathcal{P}(\texttt{Addr!})\\
&\quad \texttt{RepSet}(\texttt{h}, \iota) \quad = \quad \{\iota' \in \texttt{dom}(\texttt{h}) \mid \texttt{owner}(\texttt{h},\ \iota') \downarrow_2 = \iota\}\\
&\texttt{RepTrSet} :: \texttt{Heap} \times \texttt{Addr!} \rightarrow \mathcal{P}(\texttt{Addr!})\\
&\quad \texttt{RepTrSet}(\texttt{h}, \iota) \quad = \quad \{\iota' \in \texttt{dom}(\texttt{h}) \mid \iota \in \texttt{owners}(\texttt{h},\ \iota') \downarrow_2\}\\
&\texttt{PeerSet} :: \texttt{Heap} \times \texttt{Addr!} \rightarrow \mathcal{P}(\texttt{Addr!})\\
&\quad \texttt{PeerSet}(\texttt{h}, \iota) \quad = \quad \{\iota' \in \texttt{dom}(\texttt{h}) \mid \texttt{owner}(\texttt{h},\ \iota) = \texttt{owner}(\texttt{h},\ \iota')\}
\end{aligned}$$

Lemma 7.1.

$$\boldsymbol{h}; \iota_0 \vdash_{wf} \iota : \boldsymbol{uniq} \Rightarrow \boldsymbol{h}; \iota_0' \vdash_{wf} \iota : \boldsymbol{uniq}$$

Proof.

$$\begin{aligned}
&\texttt{h}; \iota_0 \vdash_{wf} \iota : \texttt{uniq} \Rightarrow \texttt{owner}(\texttt{h},\ \iota) = \langle Cl,\ \texttt{null}^{\texttt{r}}\rangle \wedge\\
&Cl \in \texttt{CltFree} \Rightarrow \texttt{h}; \iota_0' \vdash_{wf} \iota : \texttt{uniq}
\end{aligned}$$

□

Lemma 7.2.

$$\left.\begin{array}{ll}
\boldsymbol{h}; \iota_0 \vdash_{wf} \iota : T & (1)\\
\boldsymbol{h}; \iota \vdash_{wf} \iota' : T' & (2)
\end{array}\right\} \Rightarrow \boldsymbol{h}; \iota_0 \vdash_{wf} \iota' : T \rhd_U T'$$

Proof.

$$T = C\ m$$
$$T' = C'\ m'$$
$$(2) \Rightarrow C' \sqsubseteq \texttt{class}^{\texttt{r}}(\texttt{h},\ \iota')\ (3)$$

$$m = \texttt{peer} \wedge m' = \texttt{peer} \overset{(1)\wedge(2)}{\Rightarrow}$$
$$\texttt{owner}(\texttt{h},\ \iota_0) = \texttt{owner}(\texttt{h},\ \iota) \wedge \texttt{owner}(\texttt{h},\ \iota) = \texttt{owner}(\texttt{h},\ \iota') \Rightarrow$$
$$\texttt{owner}(\texttt{h},\ \iota_0) = \texttt{owner}(\texttt{h},\ \iota') \Rightarrow \texttt{h}; \iota_0 \vdash_{wf} \iota' : \texttt{peer}\ (4)$$

$$m = \texttt{rep}\,\langle Cl\rangle \wedge m' = \texttt{peer} \overset{(1)\wedge(2)}{\Rightarrow}$$
$$\texttt{owner}(\texttt{h},\ \iota) = \langle \iota_0,\ Cl\rangle \wedge \texttt{owner}(\texttt{h},\ \iota) = \texttt{owner}(\texttt{h},\ \iota') \Rightarrow$$
$$\langle \iota_0,\ Cl\rangle = \texttt{owner}(\texttt{h},\ \iota') \Rightarrow \texttt{h}; \iota_0 \vdash_{wf} \iota' : \texttt{rep}\,\langle Cl\rangle\ \ (5)$$

$$m = \texttt{this} \overset{(1)}{\Rightarrow} \iota = \iota_0 \overset{(2)}{\Rightarrow} \texttt{h}; \iota_0 \vdash_{wf} \iota' : m'\ (6)$$

$$m' = \texttt{uniq} \overset{(2)\wedge Lem.\ 7.1}{\Rightarrow} \texttt{h}; \iota_0 \vdash_{wf} \iota' : \texttt{uniq}\ (7)$$

$$\texttt{In all other cases}\ m \rhd_U m' = \texttt{any} \Rightarrow \texttt{h}; \iota_0 \vdash_{wf} \iota' : \texttt{any}\ (8)$$

$$(4) \wedge (5) \wedge (6) \wedge (7) \wedge (8) \Rightarrow \texttt{h}; \iota_0 \vdash_{wf} \iota' : m \rhd_U m'\ (9)$$

$$(2) \wedge (9) \Rightarrow \texttt{h}; \iota_0 \vdash_{wf} \iota' : T \rhd_U T'$$

□

Lemma 7.3.

$$\left.\begin{array}{ll} \boldsymbol{h}; \iota_0 \vdash_{wf} \iota : T & (1) \\ \boldsymbol{h}; \iota_0 \vdash_{wf} \iota' : T \rhd_U T' & (2) \\ \mathit{IsWritable}(T) & (3) \\ T' = \boldsymbol{rep}\,\langle Cl\rangle \Rightarrow T = \boldsymbol{this} & (4) \end{array}\right\} \Rightarrow \boldsymbol{h}; \iota \vdash_{wf} \iota' : T'$$

Proof.

$T = C\ m$
$T' = C'\ m'$
$(2) \Rightarrow C' \sqsubseteq \texttt{class}^{\texttt{r}}(\texttt{h},\ \iota')\ (5)$

$m = \texttt{peer} \wedge m' = \texttt{peer} \overset{(1)\wedge(2)}{\Rightarrow}$
$\texttt{owner}(\texttt{h},\ \iota_0) = \texttt{owner}(\texttt{h},\ \iota) \wedge \texttt{owner}(\texttt{h},\ \iota_0) = \texttt{owner}(\texttt{h},\ \iota') \Rightarrow$
$\texttt{owner}(\texttt{h},\ \iota) = \texttt{owner}(\texttt{h},\ \iota') \Rightarrow \texttt{h}; \iota \vdash_{wf} \iota' : \texttt{peer}\ (6)$

$m = \texttt{rep}\,\langle Cl\rangle \wedge m' = \texttt{peer} \overset{(1)\wedge(2)}{\Rightarrow}$
$\texttt{owner}(\texttt{h},\ \iota) = \langle \iota_0,\ Cl\rangle \wedge \texttt{owner}(\texttt{h},\ \iota)' = \langle \iota_0,\ Cl\rangle \Rightarrow$
$\texttt{owner}(\texttt{h},\ \iota) = \texttt{owner}(\texttt{h},\ \iota') \Rightarrow \texttt{h}; \iota \vdash_{wf} \iota' : \texttt{peer}\ (7)$

$m = \texttt{this} \overset{(1)}{\Rightarrow} \iota = \iota_0 \overset{(2)}{\Rightarrow} \texttt{h}; \iota \vdash_{wf} \iota' : m'\ (8)$

$m' = \texttt{uniq} \overset{(2)\wedge Lem.\ 7.1}{\Rightarrow} \texttt{h}; \iota \vdash_{wf} \iota' : \texttt{uniq}\ (9)$

$m' = \texttt{any} \Rightarrow \texttt{h}; \iota \vdash_{wf} \iota' : \texttt{any}\ (10)$

$m \setminus m'$	$\texttt{rep}\,\langle\_\rangle$	peer	any	uniq
$\texttt{rep}\,\langle\_\rangle$	(4)	(7)	(10)	(9)
peer	(4)	(6)	(10)	(9)
this	(8)	(8)	(8)(10)	(8)(9)
any	(3)(4)	(3)	(3)(10)	(3)(9)
uniq	(3)(4)	(3)	(3)(10)	(3)(9)

$\Rightarrow \texttt{h}; \iota \vdash_{wf} \iota' : m'\ (11)$

$(5) \wedge (11) \Rightarrow \texttt{h}; \iota \vdash_{wf} \iota' : T'$

□

Lemma 7.4.

$$\left.\begin{array}{ll} \mathit{owner}(\mathit{h},\ \iota) = \mathit{mod2Ow}(\mathit{h},\ m,\ \iota_0) & (1) \\ m \neq \mathit{any} & (2) \end{array}\right\} \Rightarrow \mathit{h}; \iota_0 \vdash_{wf} \iota : m$$

Proof.

$$m = \texttt{rep}\,\langle Cl\rangle \overset{(1)}{\Rightarrow} \texttt{owner}(\texttt{h},\ \iota) = \langle Cl,\ \iota\rangle \Rightarrow \texttt{h}; \iota_0 \vdash_{wf} \iota : \texttt{rep}\,\langle Cl\rangle \ \ (3)$$
$$m = \texttt{peer} \overset{(1)}{\Rightarrow} \texttt{owner}(\texttt{h},\ \iota) = \texttt{owner}(\texttt{h},\ \iota_0) \Rightarrow \texttt{h}; \iota_0 \vdash_{wf} \iota : \texttt{peer}\ (4)$$
$$m = \texttt{uniq} \overset{(1)}{\Rightarrow} \langle Cl,\ \texttt{null}^{\texttt{r}}\rangle \wedge Cl \in \texttt{CltFree} \Rightarrow \texttt{h}; \iota_0 \vdash_{wf} \iota : \texttt{uniq}\ (5)$$
$$(2) \wedge (3) \wedge (4) \wedge (5) \Rightarrow \texttt{h}; \iota_0 \vdash_{wf} \iota : m$$

□

Lemma 7.5.

$$\left.\begin{array}{ll} \mathit{class}^{r}(\mathit{h},\ \iota) = C & (1) \\ \mathit{h}' = \mathit{transfer}(\mathit{h},\ \iota_{tr},\ \mathit{ow}) & (2) \end{array}\right\} \Rightarrow \mathit{class}^{r}(\mathit{h}',\ \iota) = C$$

Proof.

$$\begin{array}{l} \texttt{class}^{\texttt{r}}(\texttt{h}',\ \iota) = (\texttt{h}[\iota_{tr} \mapsto \langle \texttt{h}(\iota_{tr}) \downarrow_1,\ \texttt{ow},\ \texttt{h}(\iota_{tr}) \downarrow_3\rangle]) \downarrow_1 \overset{(2)}{=} \\ = \left\{\begin{array}{l} \iota = \iota_{tr} \Rightarrow \langle \texttt{h}(\iota_{tr}) \downarrow_1,\ \texttt{ow},\ \texttt{h}(\iota_{tr}) \downarrow_3\rangle \downarrow_1 \\ \iota \neq \iota_{tr} \Rightarrow \texttt{h}(\iota_{tr}) \downarrow_1 = \end{array}\right. = \texttt{h}(\iota_{tr}) \downarrow_1 = \\ = \texttt{class}^{\texttt{r}}(\texttt{h},\ \iota) \overset{(1)}{=} C \end{array}$$

□

Lemma 7.6.

$$\left.\begin{array}{ll} \mathit{h}; \iota_0 \vdash_{wf} \iota : T & (1) \\ T \leq T' & (2) \end{array}\right\} \Rightarrow \mathit{h}; \iota_0 \vdash_{wf} \iota : T'$$

Proof.

$$\begin{array}{l} T = C\ m \\ T' = C'\ m' \\ (2) \Rightarrow \left\{\begin{array}{ll} m \leq m' & (3) \\ C \sqsubseteq C' & (4) \end{array}\right. \\ (3) \Rightarrow \left\{\begin{array}{l} m = m' \overset{(1)}{\Rightarrow} \texttt{h}; \iota_0 \vdash_{wf} \iota : m' \\ m' = \texttt{any} \Rightarrow \texttt{h}; \iota_0 \vdash_{wf} \iota : \texttt{any} \end{array}\right. \\ \Rightarrow \texttt{h}; \iota_0 \vdash_{wf} \iota : m'\ (5) \\ (1) \wedge (4) \Rightarrow C' \sqsubseteq \texttt{class}^{\texttt{r}}(\texttt{h},\ \iota)\ (6) \\ (5) \wedge (6) \Rightarrow \texttt{h}; \iota_0 \vdash_{wf} \iota : T' \end{array}$$

□

Lemma 7.7.

$$\left.\begin{array}{ll} \boldsymbol{h}; \iota_0 \vdash_{wf} \iota : T & (1) \\ \boldsymbol{h}' = \boldsymbol{transferCl}(\boldsymbol{h},\ \iota_{tr},\ \boldsymbol{ow}) & (2) \\ m \in \{\boldsymbol{uniq},\ \boldsymbol{rep}\,\langle Cl\rangle\} \Rightarrow \boldsymbol{owner}(\boldsymbol{h},\ \iota) \neq \boldsymbol{owner}(\boldsymbol{h},\ \iota_{tr}) & (3) \\ \boldsymbol{owner}(\boldsymbol{h},\ \iota_{tr}) \downarrow_2 = Cl & (4) \end{array}\right\} \Rightarrow \boldsymbol{h}'; \iota_0 \vdash_{wf} \iota : T$$

Proof.

$T = C\ m$

$(1) \Rightarrow C \sqsubseteq \mathtt{class^r}(\mathtt{h},\ \iota) \overset{Lem.\ 7.5}{\Rightarrow} C \sqsubseteq \mathtt{class^r}(\mathtt{h}',\ \iota)$ (5)

$m = \mathtt{rep}\,\langle Cl'\rangle \overset{(1)}{\Rightarrow} \mathtt{owner}(\mathtt{h},\ \iota) = \langle Cl',\ \iota_0\rangle \overset{(3)\wedge(4)}{\Rightarrow} \mathtt{owner}(\mathtt{h}',\ \iota) = \langle Cl',\ \iota_0\rangle \Rightarrow$
$\Rightarrow \mathtt{h}'; \iota_0 \vdash_{wf} \iota : \mathtt{rep}\,\langle Cl'\rangle$ (6)

$m = \mathtt{peer} \overset{(1)}{\Rightarrow} \mathtt{owner}(\mathtt{h},\ \iota_0) = \mathtt{owner}(\mathtt{h},\ \iota) \Rightarrow$
$\left\{\begin{array}{l} \iota,\ \iota' \in \mathtt{PeerSet}(\mathtt{h},\ \iota_{tr}) \Rightarrow \mathtt{owner}(\mathtt{h}',\ \iota_0) = \mathtt{ow} \wedge \mathtt{owner}(\mathtt{h}',\ \iota) = \mathtt{ow} \\ \iota,\ \iota' \notin \mathtt{PeerSet}(\mathtt{h},\ \iota_{tr}) \Rightarrow \mathtt{owner}(\mathtt{h}',\ \iota_0) = \mathtt{owner}(\mathtt{h}',\ \iota) \end{array}\right. \Rightarrow$
$\Rightarrow \mathtt{owner}(\mathtt{h}',\ \iota_0) = \mathtt{owner}(\mathtt{h}',\ \iota) \Rightarrow \mathtt{h}'; \iota_0 \vdash_{wf} \iota : \mathtt{peer}$ (7)

$m = \mathtt{uniq} \overset{(1)}{\Rightarrow} \mathtt{owner}(\mathtt{h},\ \iota) = \langle Cl,\ \mathtt{null^r}\rangle \wedge Cl \in \mathtt{CltFree} \overset{(3)}{\Rightarrow}$
$\Rightarrow \mathtt{owner}(\mathtt{h}',\ \iota) = \langle Cl,\ \mathtt{null^r}\rangle \wedge Cl \in \mathtt{CltFree} \Rightarrow \mathtt{h}'; \iota_0 \vdash_{wf} \iota : \mathtt{uniq}$ (8)

$m = \mathtt{this} \overset{(1)}{\Rightarrow} \iota = \iota_0 \Rightarrow \mathtt{h}'; \iota_0 \vdash_{wf} \iota : \mathtt{this}$ (9)

$\mathtt{h}'; \iota_0 \vdash_{wf} \iota : \mathtt{any}$ (10)

$(6) \wedge (7) \wedge (8) \wedge (9) \wedge (10) \Rightarrow \mathtt{h}'; \iota_0 \vdash_{wf} \iota : m$ (11)

$(5) \wedge (11) \Rightarrow \mathtt{h}'; \iota_0 \vdash_{wf} \iota : T$

□

Lemma 7.8.

$$\left.\begin{array}{ll} \boldsymbol{h}; \iota_0 \vdash_{wf} \iota : T & (1) \\ \boldsymbol{owner}(\boldsymbol{h},\ \iota_0) = \boldsymbol{owner}(\boldsymbol{h}',\ \iota_0) & (2) \\ \boldsymbol{owner}(\boldsymbol{h},\ \iota) = \boldsymbol{owner}(\boldsymbol{h}',\ \iota) & (3) \\ \boldsymbol{class^r}(\boldsymbol{h},\ \iota) = \boldsymbol{class^r}(\boldsymbol{h}',\ \iota) & (4) \end{array}\right\} \Rightarrow \boldsymbol{h}'; \iota_0 \vdash_{wf} \iota : T$$

Proof.

$T = C\ m$

$(1) \Rightarrow C \sqsubseteq \texttt{class}^{\texttt{r}}(\texttt{h},\ \iota) \overset{(4)}{\Rightarrow} C \sqsubseteq \texttt{class}^{\texttt{r}}(\texttt{h}',\ \iota)\ (5)$

$m = \texttt{rep}\,\langle Cl\rangle \overset{(1)}{\Rightarrow} \texttt{owner}(\texttt{h},\ \iota) = \langle Cl,\ \iota_0\rangle \overset{(3)}{\Rightarrow} \texttt{owner}(\texttt{h}',\ \iota) = \langle Cl,\ \iota_0\rangle \Rightarrow$
$\Rightarrow \texttt{h}'; \iota_0 \vdash_{wf} \iota : \texttt{rep}\,\langle Cl\rangle\ \ (6)$

$m = \texttt{peer} \overset{(1)}{\Rightarrow} \texttt{owner}(\texttt{h},\ \iota_0) = \texttt{owner}(\texttt{h},\ \iota) \overset{(2)\wedge(3)}{\Rightarrow}$
$\Rightarrow \texttt{owner}(\texttt{h}',\ \iota_0) = \texttt{owner}(\texttt{h}',\ \iota) \Rightarrow \texttt{h}'; \iota_0 \vdash_{wf} \iota : \texttt{peer}\ (7)$

$m = \texttt{uniq} \overset{(1)}{\Rightarrow} \texttt{owner}(\texttt{h},\ \iota) = \langle Cl,\ \texttt{null}^{\texttt{r}}\rangle \wedge Cl \in \texttt{CltFree} \overset{(3)}{\Rightarrow}$
$\Rightarrow \texttt{owner}(\texttt{h}',\ \iota) = \langle Cl,\ \texttt{null}^{\texttt{r}}\rangle \wedge Cl \in \texttt{CltFree} \Rightarrow \texttt{h}'; \iota_0 \vdash_{wf} \iota : \texttt{uniq}\ (8)$

$m = \texttt{this} \overset{(1)}{\Rightarrow} \iota = \iota_0 \Rightarrow \texttt{h}'; \iota_0 \vdash_{wf} \iota : \texttt{this}\ (9)$

$\texttt{h}'; \iota_0 \vdash_{wf} \iota : \texttt{any}\ (10)$

$(6) \wedge (7) \wedge (8) \wedge (9) \wedge (10) \Rightarrow \texttt{h}'; \iota_0 \vdash_{wf} \iota : m\ (11)$

$(5) \wedge (11) \Rightarrow \texttt{h}'; \iota_0 \vdash_{wf} \iota : T$

□

Lemma 7.9.

$$\left.\begin{array}{ll} \mathit{h}; \iota_0 \vdash_{wf} \iota : T & (1) \\ \langle \iota',\ \mathit{h}'\rangle = \mathit{new}(\mathit{h},\ C,\ \mathit{ow}) & (2) \end{array}\right\} \Rightarrow \mathit{h}'; \iota_0 \vdash_{wf} \iota : T$$

Proof.

$$(1) \overset{(2)\wedge \textit{Lem. 7.8}}{\Rightarrow} \texttt{h}'; \iota_0 \vdash_{wf} \iota : T$$

□

Lemma 7.10.

$$\left.\begin{array}{ll} \mathit{h}; \iota_0 \vdash_{wf} \iota : T & (1) \\ \mathit{h}' = \mathit{h}[\iota_0'.f := \iota'] & (2) \end{array}\right\} \Rightarrow \mathit{h}'; \iota_0 \vdash_{wf} \iota : T$$

Proof.

$$(1) \overset{(2)\wedge \textit{Lem. 7.8}}{\Rightarrow} \texttt{h}'; \iota_0 \vdash_{wf} \iota : T$$

□

7.3 heap's class well-formedness lemmas

Lemma 7.11.

$$\left.\begin{array}{ll} \vdash_{wf} \boldsymbol{h} & (1) \\ \iota_0 \in \boldsymbol{dom}(\boldsymbol{h}) & (2) \\ \boldsymbol{h}' = \boldsymbol{h}[\iota_0 \,.\, f' := \iota'] & (3) \\ \boldsymbol{h} \vdash_{wf} \iota' : \boldsymbol{class}(\boldsymbol{fType}(\boldsymbol{class}^{\mathtt{r}}(\iota_0),\ f')) & (4) \end{array}\right\} \Rightarrow \vdash_{wf} \boldsymbol{h}'$$

Proof.

$$\begin{array}{l} \forall \iota \in \mathtt{dom}(\mathtt{h}') :\ C = \mathtt{class}^{\mathtt{r}}(\mathtt{h}',\ \iota) \forall f \in \mathtt{fields}(C) : \\ \left\{\begin{array}{l} \iota = \iota_0 \wedge f' = f \overset{(4)}{\Rightarrow} \\ \iota \neq \iota_0 \vee f' \neq f \Rightarrow \mathtt{h}'(\iota \,.\, f) = \mathtt{h}(\iota \,.\, f) \overset{(1)}{\Rightarrow} \end{array}\right. \\ \Rightarrow \mathtt{h}' \vdash_{wf} \mathtt{h}'(\iota \,.\, f) : \mathtt{class}(\mathtt{fType}(C,\ f)) \Rightarrow \vdash_{wf} \mathtt{h}' \end{array}$$

□

Lemma 7.12.

$$\left.\begin{array}{ll} \vdash_{wf} \boldsymbol{h} & (1) \\ \langle \iota',\ \boldsymbol{h}' \rangle = \boldsymbol{new}(\boldsymbol{h},\ C,\ \boldsymbol{ow}) & (2) \end{array}\right\} \Rightarrow \vdash_{wf} \boldsymbol{h}'$$

Proof.

$$\begin{array}{l} \forall \iota \in \mathtt{dom}(\mathtt{h}') :\ C = \mathtt{class}^{\mathtt{r}}(\mathtt{h}',\ \iota) \forall f \in \mathtt{fields}(C) : \\ \left\{\begin{array}{l} \iota = \iota' \overset{(2)}{\Rightarrow} \mathtt{h}'(\iota \,.\, f) = \mathtt{null}^{\mathtt{r}} \Rightarrow \\ \iota \neq \iota' \Rightarrow \mathtt{h}'(\iota \,.\, f) = \mathtt{h}(\iota \,.\, f) \overset{(1)}{\Rightarrow} \end{array}\right. \\ \Rightarrow \mathtt{h}' \vdash_{wf} \mathtt{h}'(\iota \,.\, f) : \mathtt{class}(\mathtt{fType}(C,\ f)) \Rightarrow \vdash_{wf} \mathtt{h}' \end{array}$$

□

Lemma 7.13.

$$\left.\begin{array}{ll} \vdash_{wf} \boldsymbol{h} & (1) \\ \boldsymbol{h}' = \boldsymbol{transferCl}(\boldsymbol{h},\ \iota_{tr},\ \boldsymbol{ow}) & (2) \end{array}\right\} \Rightarrow \vdash_{wf} \boldsymbol{h}'$$

Proof.

$$\begin{array}{l} \forall \iota \in \mathtt{dom}(\mathtt{h}') :\ C = \mathtt{class}^{\mathtt{r}}(\mathtt{h}',\ \iota) \forall f \in \mathtt{fields}(C) : \\ \left\{\begin{array}{l} \mathtt{class}^{\mathtt{r}}(\mathtt{h},\ \iota) = \mathtt{class}^{\mathtt{r}}(\mathtt{h}',\ \iota) \\ \mathtt{h}(\iota \,.\, f)) = \mathtt{h}'(\iota \,.\, f)) = \iota' \\ \mathtt{class}^{\mathtt{r}}(\mathtt{h}, \iota') = \mathtt{class}^{\mathtt{r}}(\mathtt{h}',\ \iota') \\ \mathtt{h} \vdash_{wf} \mathtt{h}(\iota \,.\, f) : \mathtt{class}(\mathtt{fType}(C,\ f)) \end{array}\right. \Rightarrow \\ \Rightarrow \mathtt{h}' \vdash_{wf} \mathtt{h}'(\iota \,.\, f) : \mathtt{class}(\mathtt{fType}(C,\ f)) \Rightarrow \vdash_{wf} \mathtt{h}' \end{array}$$

□

7.4 heap's well-formedness lemmas

Lemma 7.14.

$$\left.\begin{array}{ll} U; \iota_0 \vdash_{wf} \boldsymbol{h} & (1) \\ U' \cap \mathit{FieldID} \subseteq U \cap \mathit{FieldID} & (2) \end{array}\right\} \Rightarrow U'; \iota_0 \vdash_{wf} \boldsymbol{h}$$

Proof.

$$\begin{array}{l} \forall \iota \in \mathtt{dom}(\mathtt{h}) : \ C = \mathtt{class}^{\mathtt{r}}(\mathtt{h},\ \iota) \forall f \in \mathtt{fields}(C) : \\ \langle \iota,\ \{\iota_0\} \times U \overset{(2)}{\Rightarrow} \langle \iota,\ \{\iota_0\} \times U' \overset{(1)}{\Rightarrow} \mathtt{h}; \iota \vdash_{wf} \mathtt{h}(\iota\,.\,f) : \mathtt{mod}(\mathtt{fType}(C,\ f)) \\ \Rightarrow \mathtt{FrSt}_2; \mathtt{h} \vdash_{wf} \end{array}$$

□

Lemma 7.15.

$$\left.\begin{array}{ll} \vdash_{wf} \boldsymbol{h} & (1) \\ U; \iota_0 \vdash_{wf} \boldsymbol{h} & (2) \\ \boldsymbol{h}; \iota_0 \vdash_{wf} \iota_0' : T & (3) \\ T = C\ m & \\ m = \mathit{this} \Rightarrow f \notin U & (4) \\ \iota_0' \neq \mathit{null}^r & (5) \end{array}\right\} \Rightarrow \boldsymbol{h}; \iota_0 \vdash_{wf} \boldsymbol{h}(\iota_0'\,.\,f) : T \rhd_U \mathit{fType}(C,\ f)$$

Proof.

$$\begin{array}{l} (1) \wedge (2) \wedge (4) \Rightarrow \mathtt{h}; \iota_0' \vdash_{wf} \mathtt{h}(\iota_0'\,.\,f) : \mathtt{fType}(C,\ f) \overset{(3) \wedge \mathit{Lem.}\ 7.2}{\Rightarrow} \\ \Rightarrow \mathtt{h}; \iota_0 \vdash_{wf} \mathtt{h}(\iota_0'\,.\,f) : T \rhd_U \mathtt{fType}(C,\ f) \end{array}$$

□

Lemma 7.16.

$$\left.\begin{array}{ll} U; \iota_0 \vdash_{wf} \boldsymbol{h} & (1) \\ \boldsymbol{h}; \iota_0' \vdash_{wf} \iota' : \mathit{mod}(\mathit{fType}(\mathit{class}^r(\iota_0'),\ f)) & (2) \\ \boldsymbol{h}' = \boldsymbol{h}[\iota_0'\,.\,f' := \iota'] & (3) \\ \boldsymbol{h}; \iota_0 \vdash_{wf} \iota_0' : m & (4) \\ U' = \mathit{if}(m = \mathit{this})\ \mathit{then}\ U \setminus \{f\}\ \mathit{else}\ U & (5) \end{array}\right\} \Rightarrow U'; \iota_0 \vdash_{wf} \boldsymbol{h}'$$

Proof.

$$\begin{array}{l}
\forall \iota \in \mathtt{dom}(\mathtt{h}') : \; C = \mathtt{class}^{\mathtt{r}}(\mathtt{h}', \; \iota) \forall f \in \mathtt{fields}(C) : \\
\langle \iota, \; f \rangle \notin \{\iota_0\} \times U' \overset{(3)\wedge(4)}{\Rightarrow} \\
\left\{ \begin{array}{l} \iota \neq \iota_0' \vee f \neq f' \Rightarrow \mathtt{h}(\iota \,.\, f) = \mathtt{h}'(\iota \,.\, f) \overset{(1)}{\Rightarrow} \\ \iota = \iota_0' \wedge f = f' \overset{(2)}{\Rightarrow} \end{array} \right. \; \mathtt{h}'; \iota \vdash_{wf} \mathtt{h}'(\iota \,.\, f) : \mathtt{mod}(\mathtt{fType}(C, \; f)) \\
\Rightarrow U'; \iota_0 \vdash_{wf} \mathtt{h}'
\end{array}$$

□

Lemma 7.17.

$$\left. \begin{array}{ll} U; \iota_0 \vdash_{wf} \boldsymbol{h} & (1) \\ U \cap \mathit{FieldID} = \varnothing & (2) \end{array} \right\} \Rightarrow U'; \iota_0' \vdash_{wf} \boldsymbol{h}$$

Proof.

$$\begin{array}{l}
\forall \iota \in \mathtt{dom}(\mathtt{h}) : \; C = \mathtt{class}^{\mathtt{r}}(\mathtt{h}, \; \iota) \forall f \in \mathtt{fields}(C) : \\
\langle \iota, \; f \rangle \notin \{\iota_0'\} \times U' \Rightarrow \langle \iota, \; f \rangle \notin \{\iota_0\} \times U \overset{(1)}{\Rightarrow} \\
\mathtt{h}; \iota \vdash_{wf} \mathtt{h}(\iota \,.\, f) : \mathtt{mod}(\mathtt{fType}(C, \; f)) \\
\Rightarrow U'; \iota_0' \vdash_{wf} \mathtt{h}
\end{array}$$

□

Lemma 7.18.

$$\left. \begin{array}{ll} U; \iota_0 \vdash_{wf} \boldsymbol{h} & (1) \\ \langle \iota', \; \boldsymbol{h}' \rangle = \mathit{new}(\boldsymbol{h}, \; C, \; \mathit{ow}) & (2) \end{array} \right\} \Rightarrow U; \iota_0 \vdash_{wf} \boldsymbol{h}'$$

Proof.

$$\begin{array}{l}
\forall \iota \in \mathtt{dom}(\mathtt{h}') : \; C = \mathtt{class}^{\mathtt{r}}(\mathtt{h}', \; \iota) \forall f \in \mathtt{fields}(C) : \\
\langle \iota, \; f \rangle \notin \{\iota_0\} \times U \overset{(2)}{\Rightarrow} \\
\left\{ \begin{array}{l} \iota \neq \iota' \Rightarrow \mathtt{h}(\iota \,.\, f) = \mathtt{h}'(\iota \,.\, f) \overset{(1)}{\Rightarrow} \\ \iota = \iota' \Rightarrow \mathtt{h}'(\iota \,.\, f) = \mathtt{null}^{\mathtt{r}} \end{array} \right. \; \mathtt{h}'; \iota \vdash_{wf} \mathtt{h}'(\iota \,.\, f) : \mathtt{mod}(\mathtt{fType}(C, \; f)) \\
\Rightarrow U; \iota_0 \vdash_{wf} \mathtt{h}'
\end{array}$$

□

Lemma 7.19.

$$\left.\begin{array}{ll} \Gamma(y) = \textit{rep}\,\langle Cl\rangle & (1) \\ \textit{h}; \iota_0 \vdash_{wf} \iota_{tr} : \textit{rep}\,\langle Cl\rangle & (2) \\ \textit{h}' = \textit{transferCl}(\textit{h},\ \iota_{tr},\ \textit{ow}) & (3) \\ U; \iota_0 \vdash_{wf} \textit{h} & (4) \\ U' = \textit{consumeAliases}(U, y) & (5) \end{array}\right\} \Rightarrow U'; \iota_0 \vdash_{wf} \textit{h}'$$

Proof.

$$\begin{array}{l} \forall \iota \in \mathtt{dom}(\mathtt{h}') :\ C = \mathtt{class}^{\mathtt{r}}(\mathtt{h}',\ \iota) \forall f \in \mathtt{fields}(C) : \\ \langle \iota,\ f\rangle \notin \{\iota_0\} \times U' \overset{(1)\wedge(2)\wedge(3)\wedge(5)}{\Rightarrow} \\ \mathtt{mod}(\mathtt{fType}(C,\ f)) \neq \mathtt{rep}\,\langle Cl\rangle \vee \iota \neq \iota_0 \overset{(4)\wedge \textit{Lem. 7.7}}{\Rightarrow} \\ \mathtt{h}'; \iota \vdash_{wf} \mathtt{h}'(\iota\,.\,f) : \mathtt{mod}(\mathtt{fType}(C,\ f)) \\ \Rightarrow U'; \iota_0 \vdash_{wf} \mathtt{h}' \end{array}$$

□

Lemma 7.20.

$$\left.\begin{array}{ll} \textit{h}; \iota_0 \vdash_{wf} \iota_{tr} : \textit{uniq} & (1) \\ \textit{h}' = \textit{transferCl}(\textit{h},\ \iota_{tr},\ \textit{ow}) & (2) \\ U; \iota_0 \vdash_{wf} \textit{h} & (3) \end{array}\right\} \Rightarrow U; \iota_0 \vdash_{wf} \textit{h}'$$

Proof.

$$\begin{array}{l} \forall \iota \in \mathtt{dom}(\mathtt{h}') :\ C = \mathtt{class}^{\mathtt{r}}(\mathtt{h}',\ \iota) \forall f \in \mathtt{fields}(C) : \\ \langle \iota,\ f\rangle \notin \{\iota_0\} \times U \overset{(1)\wedge(3)}{\Rightarrow} \\ \mathtt{mod}(\mathtt{fType}(C,\ f)) \neq \mathtt{rep}\,\langle Cl\rangle \vee \mathtt{owner}(\mathtt{h},\ \iota) \neq \mathtt{owner}(\mathtt{h},\ \iota_{tr}) \overset{(2)\wedge \textit{Lem. 7.7}}{\Rightarrow} \\ \mathtt{h}'; \iota \vdash_{wf} \mathtt{h}'(\iota\,.\,f) : \mathtt{mod}(\mathtt{fType}(C,\ f)) \\ \Rightarrow U; \iota_0 \vdash_{wf} \mathtt{h}' \end{array}$$

□

7.5 Frames stack's well-formedness lemmas

Lemma 7.21.

$$\left.\begin{array}{ll} \textit{h} \vdash_{wf} \Gamma^r; \Gamma; U & (1) \\ U' \cap \textit{VarID} \subseteq U \cap \textit{VarID} & (2) \end{array}\right\} \Rightarrow \textit{h} \vdash_{wf} \Gamma^r; \Gamma; U'$$

Proof.

$$(1) \Rightarrow \begin{cases} \mathtt{dom}(\Gamma^{\mathtt{r}}) = \mathtt{dom}(\Gamma) & (3) \\ \mathtt{dom}(\Gamma) \supseteq U & (4) \\ \mathtt{mod}(\Gamma(\mathtt{this})) = \mathtt{this} & (5) \\ \forall v \in \mathtt{dom}(\Gamma^{\mathtt{r}}) \setminus U \ : \ \mathtt{h}; \Gamma^{\mathtt{r}}(\mathtt{this}) \vdash_{wf} \Gamma^{\mathtt{r}}(v) : \Gamma(v) & (6) \end{cases}$$

$$(2) \wedge (6) \Rightarrow \forall v \in \mathtt{dom}(\Gamma^{\mathtt{r}}) \setminus U' \ : \ \mathtt{h}; \Gamma^{\mathtt{r}}(\mathtt{this}) \vdash_{wf} \Gamma^{\mathtt{r}}(v) : \Gamma(v) \ (7)$$

$$(3) \wedge (4) \wedge (5) \wedge (7) \Rightarrow \mathtt{h} \vdash_{wf} \Gamma^{\mathtt{r}}; \Gamma; U'$$

□

Lemma 7.22.

$$\left.\begin{array}{ll} \boldsymbol{h} \vdash_{wf} \Gamma^{r}; \Gamma; U & (1) \\ U' = U \cup \{x\} & (2) \\ \Gamma^{r\prime} = \Gamma^{r}[x \mapsto \iota'] & (3) \\ \boldsymbol{h}; \Gamma^{r}(\boldsymbol{this}) \vdash_{wf} \iota' : \Gamma(x) & (4) \\ x \in \boldsymbol{dom}(\Gamma) & (5) \end{array}\right\} \Rightarrow \boldsymbol{h} \vdash_{wf} \Gamma^{r\prime}; \Gamma; U'$$

Proof.

$$\begin{cases} \mathtt{dom}(\Gamma^{\mathtt{r}}) = \mathtt{dom}(\Gamma) & (6) \\ \mathtt{dom}(\Gamma) \supseteq U & (7) \\ \mathtt{mod}(\Gamma(\mathtt{this})) = \mathtt{this} & (8) \\ \forall v \in \mathtt{dom}(\Gamma^{\mathtt{r}}) \setminus U \ : \ \mathtt{h}; \Gamma^{\mathtt{r}}(\mathtt{this}) \vdash_{wf} \Gamma^{\mathtt{r}}(v) : \Gamma(v) & (9) \end{cases}$$

$$v \in \mathtt{dom}(\Gamma^{\mathtt{r}\prime}) \setminus U' \begin{cases} v = x \overset{(4)}{\Rightarrow} \\ v \neq x \overset{(9)}{\Rightarrow} \end{cases} \mathtt{h}; \Gamma^{\mathtt{r}\prime}(\mathtt{this}) \vdash_{wf} \Gamma^{\mathtt{r}\prime}(v) : \Gamma(v) \ (10)$$

$$(5) \wedge (6) \Rightarrow \mathtt{dom}(\Gamma^{\mathtt{r}\prime}) = \mathtt{dom}(\Gamma) \ (11)$$

$$(11) \wedge (7) \wedge (8) \wedge (10) \Rightarrow \mathtt{h} \vdash_{wf} \Gamma^{\mathtt{r}\prime}; \Gamma; U'$$

□

Lemma 7.23.

$$\left.\begin{array}{ll} \boldsymbol{h} \vdash_{wf} \Gamma^{r}; \Gamma; U & (1) \\ \iota_0 \in \boldsymbol{dom}(\boldsymbol{h}) & (2) \\ \boldsymbol{h}' = \boldsymbol{h}[\iota_0 \,.\, f := \iota] & (3) \end{array}\right\} \Rightarrow \boldsymbol{h}' \vdash_{wf} \Gamma^{r}; \Gamma; U$$

Proof.

$$(1) \Rightarrow \begin{cases} \mathtt{dom}(\Gamma^{\mathtt{r}}) = \mathtt{dom}(\Gamma) & (4) \\ \mathtt{dom}(\Gamma) \supseteq U & (5) \\ \mathtt{mod}(\Gamma(\mathtt{this})) = \mathtt{this} & (6) \\ \forall v \in \mathtt{dom}(\Gamma^{\mathtt{r}}) \setminus U \ : \ \mathtt{h}; \Gamma^{\mathtt{r}}(\mathtt{this}) \vdash_{wf} \Gamma^{\mathtt{r}}(v) : \Gamma(v) & (7) \end{cases}$$

$(7) \Rightarrow \forall v \in \mathtt{dom}(\Gamma^{\mathtt{r}}) \setminus U \ : \ \mathtt{h}; \Gamma^{\mathtt{r}}(\mathtt{this}) \vdash_{wf} \Gamma^{\mathtt{r}}(v) : \Gamma(v)$

$\overset{(3) \wedge Lem.\ 7.10}{\Rightarrow} \mathtt{h}'; \Gamma^{\mathtt{r}}(\mathtt{this}) \vdash_{wf} \Gamma^{\mathtt{r}}(v) : \Gamma(v)$ (8)

$(4) \wedge (5) \wedge (6) \wedge (8) \Rightarrow \mathtt{h}' \vdash_{wf} \Gamma^{\mathtt{r}}; \Gamma; U$

□

Lemma 7.24.

$$\left.\begin{array}{ll} \boldsymbol{h} \vdash_{wf} \Gamma^{r}; \Gamma; U & (1) \\ \Gamma^{r\prime} = \{\langle p,\ \Gamma^{r}(z)\rangle,\ \overline{\langle v,\ \boldsymbol{null}^{r}\rangle},\ \langle \boldsymbol{this},\ \Gamma^{r}(y)\rangle,\ \langle \boldsymbol{res},\ \boldsymbol{null}^{r}\rangle\} & (2) \\ \Gamma' = \{\langle p, T_p\rangle,\ \overline{\langle v,\ T\rangle},\ \langle \boldsymbol{this}, \boldsymbol{this\ class}^{r}(\Gamma^{r}(y))\rangle,\ \langle \boldsymbol{res}, T_r\rangle\} & (3) \\ \Gamma(z) \leq \Gamma(y) \rhd_U T_p & (4) \end{array}\right\} \Rightarrow \boldsymbol{h} \vdash_{wf} \Gamma^{r\prime}; \Gamma'; \varnothing$$

Proof.

$\mathtt{dom}(\Gamma^{\mathtt{r}\prime}) = \{p,\ \overline{v},\ \mathtt{this},\ \mathtt{res}\} = \mathtt{dom}(\Gamma') \Rightarrow \mathtt{dom}(\Gamma^{\mathtt{r}\prime}) = \mathtt{dom}(\Gamma')$ (5)

$\mathtt{dom}(\Gamma') \supseteq \varnothing$ (6)

$\mathtt{mod}(\Gamma'(\mathtt{this})) = \mathtt{this}$ (7)

$(1) \Rightarrow \mathtt{h}; \Gamma^{\mathtt{r}}(\mathtt{this}) \vdash_{wf} \Gamma^{\mathtt{r}\prime}(\mathtt{this}) : \Gamma(y) \wedge \mathtt{h}; \Gamma^{\mathtt{r}}(\mathtt{this}) \vdash_{wf} \Gamma^{\mathtt{r}\prime}(p) : \Gamma(z) \wedge (4)$

$\overset{Lem.\ 7.3}{\Rightarrow} \mathtt{h}; \Gamma^{\mathtt{r}\prime}(\mathtt{this}) \vdash_{wf} \Gamma^{\mathtt{r}\prime}(p) : T_p$ (8)

$\Gamma^{\mathtt{r}\prime}(\mathtt{this}) = \Gamma^{\mathtt{r}\prime}(\mathtt{this}) \Rightarrow \mathtt{h}; \Gamma^{\mathtt{r}\prime}(\mathtt{this}) \vdash_{wf} \Gamma^{\mathtt{r}\prime}(\mathtt{this}) : \Gamma'(\mathtt{this})$ (9)

$\Gamma^{\mathtt{r}\prime}(\overline{v}) = \mathtt{null}^{\mathtt{r}} \Rightarrow \mathtt{h}; \Gamma^{\mathtt{r}\prime}(\overline{v}) \vdash_{wf} \Gamma^{\mathtt{r}\prime}(\overline{v}) : \Gamma'(\overline{v})$ (10)

$\Gamma^{\mathtt{r}\prime}(\mathtt{res}) = \mathtt{null}^{\mathtt{r}} \Rightarrow \mathtt{h}; \Gamma^{\mathtt{r}\prime}(\mathtt{res}) \vdash_{wf} \Gamma^{\mathtt{r}\prime}(\mathtt{res}) : \Gamma'(\mathtt{res})$ (11)

$(8) \wedge (9) \wedge (10) \wedge (11) \Rightarrow \forall v \in \mathtt{dom}(\Gamma^{\mathtt{r}\prime}) \setminus \varnothing \ : \ \mathtt{h}; \Gamma^{\mathtt{r}\prime}(\mathtt{this}) \vdash_{wf} \Gamma^{\mathtt{r}\prime}(v) : \Gamma'(v)$ (12)

$(5) \wedge (6) \wedge (7) \wedge (12) \Rightarrow \mathtt{h} \vdash_{wf} \Gamma^{\mathtt{r}\prime}; \Gamma'; \varnothing$

□

Lemma 7.25.

$$\left.\begin{array}{ll} \boldsymbol{FrSt} = \boldsymbol{Fr} \circ \boldsymbol{FrSt}' & \\ \boldsymbol{h} \vdash_{wf} \boldsymbol{FrSt} & (1) \end{array}\right\} \Rightarrow \boldsymbol{h} \vdash_{wf} \boldsymbol{FrSt}'\boldsymbol{h}$$

Proof.

$$\mathtt{Fr} \circ \mathtt{FrSt}' = \langle \Gamma^{\mathtt{r}}{}_0,\ \Gamma^{\mathtt{r}}{}_0,\ \Gamma^{\mathtt{r}}{}_0 \rangle \circ \overline{\langle \Gamma^{\mathtt{r}},\ \Gamma,\ U \rangle}$$
$$(1) \Rightarrow \mathtt{h}_0 \vdash_{wf} \Gamma^{\mathtt{r}}{}_0; \Gamma^{\mathtt{r}}{}_0; \Gamma^{\mathtt{r}}{}_0 \wedge \overline{\mathtt{h} \vdash_{wf} \Gamma^{\mathtt{r}}; \Gamma^{\mathtt{r}}; \Gamma^{\mathtt{r}}} \Rightarrow \overline{\mathtt{h} \vdash_{wf} \Gamma^{\mathtt{r}}; \Gamma^{\mathtt{r}}; \Gamma^{\mathtt{r}}} \Rightarrow \mathtt{h} \vdash_{wf} \mathtt{FrSt}'\mathtt{h}$$

□

Lemma 7.26.

$$\left.\begin{array}{ll} \boldsymbol{h} \vdash_{wf} \Gamma^{r}; \Gamma; U & (1) \\ \langle \iota,\ \boldsymbol{h}' \rangle = \boldsymbol{new}(\boldsymbol{h},\ C,\ \boldsymbol{ow}) & (2) \end{array}\right\} \Rightarrow \boldsymbol{h}' \vdash_{wf} \Gamma^{r}; \Gamma; U$$

Proof.

$$(1) \Rightarrow \left\{\begin{array}{ll} \mathtt{dom}(\Gamma^{\mathtt{r}}) = \mathtt{dom}(\Gamma) & (4) \\ \mathtt{dom}(\Gamma) \supseteq U & (5) \\ \mathtt{mod}(\Gamma(\mathtt{this})) = \mathtt{this} & (6) \\ \forall v \in \mathtt{dom}(\Gamma^{\mathtt{r}}) \setminus U \ :\ \mathtt{h}; \Gamma^{\mathtt{r}}(\mathtt{this}) \vdash_{wf} \Gamma^{\mathtt{r}}(v) : \Gamma(v) & (7) \end{array}\right.$$
$$(7) \Rightarrow \forall v \in \mathtt{dom}(\Gamma^{\mathtt{r}}) \setminus U \ :\ \mathtt{h}; \Gamma^{\mathtt{r}}(\mathtt{this}) \vdash_{wf} \Gamma^{\mathtt{r}}(v) : \Gamma(v)$$
$$\overset{(4) \wedge Lem.\ 7.9}{\Rightarrow} \mathtt{h}'; \Gamma^{\mathtt{r}}(\mathtt{this}) \vdash_{wf} \Gamma^{\mathtt{r}}(v) : \Gamma(v) \ (8)$$
$$(4) \wedge (5) \wedge (6) \wedge (8) \Rightarrow \mathtt{h}' \vdash_{wf} \Gamma^{\mathtt{r}}; \Gamma; U$$

□

Lemma 7.27.

$$\left.\begin{array}{ll} \boldsymbol{Fr} = \langle \Gamma^{r},\ \Gamma,\ U \rangle & \\ \boldsymbol{FrSt} = \boldsymbol{Fr} \circ \boldsymbol{FrSt}_0 & \\ \boldsymbol{Fr}' = \langle \Gamma^{r\prime},\ \Gamma,\ U' \rangle & \\ \boldsymbol{FrSt}' = \boldsymbol{Fr}' \circ \boldsymbol{FrSt}_0 & \\ \Gamma(y) = \boldsymbol{rep}\,\langle Cl \rangle & (1) \\ \Gamma(x) = \boldsymbol{uniq} & (2) \\ \boldsymbol{h} \vdash_{wf} \boldsymbol{FrSt} & (3) \\ \boldsymbol{h} \vdash_{Inv} \boldsymbol{FrSt} & (4) \\ \boldsymbol{ow} = \langle \boldsymbol{newClt}(\boldsymbol{h}),\ \boldsymbol{null}^{r} \rangle & (5) \\ \boldsymbol{h}' = \boldsymbol{transferCl}(\boldsymbol{h},\ \Gamma^{r}(y),\ \boldsymbol{ow}) & (6) \\ U' = \boldsymbol{consumeAliases}(U, y) \setminus \{x\} & (7) \\ \Gamma^{r\prime} = \Gamma^{r}[x \mapsto \Gamma^{r}(y)] & (8) \end{array}\right\} \Rightarrow \boldsymbol{h}' \vdash_{wf} \boldsymbol{FrSt}'$$

Proof.

$$(3) \wedge (4) \wedge (6) \overset{(4)\wedge \textit{Lem. 7.7}}{\Rightarrow} \mathtt{h}' \vdash_{wf} \mathtt{FrSt}_0 \ (9)$$

$$(3) \Rightarrow \begin{cases} \mathtt{dom}(\Gamma^{\mathtt{r}}) = \mathtt{dom}(\Gamma) & (10) \\ \mathtt{dom}(\Gamma) \supseteq U & (11) \\ \mathtt{mod}(\Gamma(\mathtt{this})) = \mathtt{this} & (12) \\ \forall v \in \mathtt{dom}(\Gamma^{\mathtt{r}}) \setminus U \ : \ \mathtt{h}; \Gamma^{\mathtt{r}}(\mathtt{this}) \vdash_{wf} \Gamma^{\mathtt{r}}(v) : \Gamma(v) & (13) \end{cases}$$

$$\forall v' \in \mathtt{dom}(\Gamma^{\mathtt{r}\prime}) \setminus U' \overset{(7)\wedge(8)}{\Rightarrow} \Gamma^{\mathtt{r}\prime}(v) \neq \mathtt{rep}\,\langle Cl \rangle \wedge v \neq y \overset{\textit{Lem. 7.7}\wedge(3)}{\Rightarrow}$$
$$\mathtt{h}'; \Gamma^{\mathtt{r}\prime}(\mathtt{this}) \vdash_{wf} \Gamma^{\mathtt{r}\prime}(v) : \Gamma'(v) \ (14)$$
$$(10) \wedge (11) \wedge (12) \wedge (14) \Rightarrow \mathtt{h}' \vdash_{wf} \Gamma^{\mathtt{r}}; \Gamma; U \ (15)$$
$$(9) \wedge (15) \Rightarrow \mathtt{h}' \vdash_{wf} \mathtt{FrSt}'$$

□

Lemma 7.28.

$$\left.\begin{array}{ll} \mathit{Fr} = \langle \Gamma^r,\ \Gamma,\ U \rangle & \\ \mathit{FrSt} = \mathit{Fr} \circ \mathit{FrSt}_0 & \\ \mathit{Fr}' = \langle \Gamma^{r\prime},\ \Gamma,\ U' \rangle & \\ \mathit{FrSt}' = \mathit{Fr}' \circ \mathit{FrSt}_0 & \\ \Gamma(y) = \mathit{uniq} & (1) \\ \Gamma(x) = \mathit{rep}\,\langle Cl \rangle & (2) \\ \mathit{h} \vdash_{wf} \mathit{FrSt} & (3) \\ \mathit{FrSt} \vdash_{Uniq} \mathit{h} & (4) \\ \mathit{ow} = \mathit{mod2Ow}(\mathit{h},\ m,\ \Gamma^r(\mathit{this})) & (5) \\ m \in \{\mathit{rep}\,\langle Cl \rangle\,,\ \mathit{peer}\} & (6) \\ \mathit{h}' = \mathit{transferCl}(\mathit{h},\ \Gamma^r(y),\ \mathit{ow}) & (7) \\ U' = U \cup \{y\} \setminus \{x\} & (8) \\ \Gamma^{r\prime} = \Gamma^r[x \mapsto \Gamma^r(y)] & (9) \end{array}\right\} \Rightarrow \mathit{h}' \vdash_{wf} \mathit{FrSt}'$$

Proof.

$$(3) \wedge (4) \wedge (6) \overset{(4)\wedge \textit{Lem. 7.7}}{\Rightarrow} \mathtt{h}' \vdash_{wf} \mathtt{FrSt}_0 \ (9)$$

$$(3) \Rightarrow \begin{cases} \mathtt{dom}(\Gamma^{\mathtt{r}}) = \mathtt{dom}(\Gamma) & (10) \\ \mathtt{dom}(\Gamma) \supseteq U & (11) \\ \mathtt{mod}(\Gamma(\mathtt{this})) = \mathtt{this} & (12) \\ \forall v \in \mathtt{dom}(\Gamma^{\mathtt{r}}) \setminus U \ : \ \mathtt{h}; \Gamma^{\mathtt{r}}(\mathtt{this}) \vdash_{wf} \Gamma^{\mathtt{r}}(v) : \Gamma(v) & (13) \end{cases}$$

$$\forall v' \in \mathtt{dom}(\Gamma^{\mathtt{r}\prime}) \setminus U' \overset{(7)\wedge(8)}{\Rightarrow} v \neq y \overset{\textit{Lem. 7.7}\wedge(3)}{\Rightarrow}$$
$$\mathtt{h}'; \Gamma^{\mathtt{r}\prime}(\mathtt{this}) \vdash_{wf} \Gamma^{\mathtt{r}\prime}(v) : \Gamma'(v) \ (14)$$
$$(10) \wedge (11) \wedge (12) \wedge (14) \Rightarrow \mathtt{h}' \vdash_{wf} \Gamma^{\mathtt{r}}; \Gamma; U \ (15)$$
$$(9) \wedge (15) \Rightarrow \mathtt{h}' \vdash_{wf} \mathtt{FrSt}'$$

□

7.6 Uniqueness's lemmas

Lemma 7.29.

$$\left.\begin{array}{ll} \mathit{FrSt} = \langle \Gamma^r,\ \Gamma,\ U\rangle \circ \mathit{FrSt}_0 & \\ \mathit{h} \vdash_{Uniq} \mathit{FrSt} & (1) \\ U' \cap \mathit{VarID} \subseteq U \cap \mathit{VarID} & (2) \\ \mathit{FrSt}' = \langle \Gamma^r,\ \Gamma,\ U'\rangle \circ \mathit{FrSt}_0 & \end{array}\right\} \Rightarrow \mathit{h} \vdash_{Uniq} \mathit{FrSt}'$$

Proof.

$$(1) \Rightarrow \forall Cl \in \mathtt{CltFree}\ \mathtt{RefNum}(\mathtt{h}, \mathtt{FrSt}, \langle Cl,\ \mathtt{null^r}\rangle, \mathtt{uniq}) \leq 1 \overset{(2)}{\Rightarrow}$$
$$\Rightarrow \mathtt{RefNum}(\mathtt{h}, \mathtt{FrSt}', \langle Cl,\ \mathtt{null^r}\rangle, \mathtt{uniq}) \leq 1 \Rightarrow \mathtt{h} \vdash_{Uniq} \mathtt{FrSt}'$$

□

Lemma 7.30.

$$\left.\begin{array}{ll} \mathit{FrSt} = \langle \Gamma^r,\ \Gamma,\ U\rangle \circ \mathit{FrSt}_0 & \\ \mathit{h} \vdash_{Uniq} \mathit{FrSt} & (1) \\ U' = U \cup \{x\} & (2) \\ \Gamma^{r\prime} = \Gamma^r[x \mapsto \iota'] & (3) \\ \iota' \neq \mathit{null}^r \wedge \Gamma(x) = \mathit{uniq} \Rightarrow & \\ \mathit{RefNum}(\mathit{h}, \mathit{FrSt}, \mathit{owner}(\mathit{h},\ \iota'), \mathit{uniq}) = 0 & (4) \\ \mathit{FrSt}' = \langle \Gamma^{r\prime},\ \Gamma,\ U'\rangle \circ \mathit{FrSt}_0 & \end{array}\right\} \Rightarrow \mathit{h} \vdash_{Uniq} \mathit{FrSt}'$$

Proof.

$$(1) \Rightarrow \forall Cl \in \mathtt{CltFree} \left\{\begin{array}{l} Cl = \mathtt{owner}(\mathtt{h},\ \iota') \downarrow_1 \overset{(3)\wedge(4)}{\Rightarrow} \\ Cl \neq \mathtt{owner}(\mathtt{h},\ \iota') \downarrow_1 \overset{(1)}{\Rightarrow} \end{array}\right.$$
$$\mathtt{RefNum}(\mathtt{h}, \mathtt{FrSt}', \langle Cl,\ \mathtt{null^r}\rangle, \mathtt{uniq}) \leq 1 \Rightarrow \mathtt{h} \vdash_{Uniq} \mathtt{FrSt}'$$

□

Lemma 7.31.

$$\left.\begin{array}{ll} \mathit{h} \vdash_{Uniq} \mathit{FrSt} & (1) \\ \iota_0 \in \mathit{dom}(\mathit{h}) & (2) \\ \mathit{h}' = \mathit{h}[\iota_0 \,.\, f := \iota] & (3) \end{array}\right\} \Rightarrow \mathit{h}' \vdash_{Uniq} \mathit{FrSt}$$

Proof.

$$(1) \Rightarrow \forall Cl \in \texttt{CltFree}\ \texttt{RefNum}(\texttt{h}, \texttt{FrSt}, \langle Cl,\ \texttt{null}^{\texttt{r}}\rangle, \texttt{uniq}) \leq 1 \overset{(2)\wedge(3)}{\Rightarrow}$$
$$\Rightarrow \texttt{RefNum}(\texttt{h}',\ \texttt{FrSt}, \langle Cl,\ \texttt{null}^{\texttt{r}}\rangle, \texttt{uniq}) \leq 1 \Rightarrow \texttt{h}' \vdash_{Uniq} \texttt{FrSt}$$

□

Lemma 7.32.

$$\left.\begin{array}{ll}
\mathit{FrSt} = \langle \Gamma^r,\ \Gamma,\ U\rangle \circ \mathit{FrSt}_0 & \\
\mathit{h} \vdash_{Uniq} \mathit{FrSt} & (1)\\
\Gamma^{r\prime} = \{\langle p,\ \Gamma^r(z)\rangle,\ \overline{\langle v,\ \mathit{null}^r\rangle},\ \langle \mathit{this},\ \Gamma^r(y)\rangle,\ \langle \mathit{res},\ \mathit{null}^r\rangle\} & (2)\\
\Gamma' = \{\langle p, T_p\rangle,\ \overline{\langle v,\ T\rangle},\ \langle \mathit{this}, \mathit{this\ class}^r(\Gamma^r(y))\rangle,\ \langle \mathit{res}, T_r\rangle\} & (3)\\
U' = \mathit{consumeUniq}(U, T_p, z) & (4)\\
\mathit{Fr}_1 = \langle \Gamma^{r\prime},\ \Gamma',\ \varnothing\rangle & \\
\mathit{Fr}_2 = \langle \Gamma^r,\ \Gamma,\ U'\rangle &
\end{array}\right\} \Rightarrow$$
$$\Rightarrow \mathit{h} \vdash_{Uniq} \mathit{Fr}_1 \circ \mathit{Fr}_2 \circ \mathit{FrSt}_0$$

Proof.

$$(1) \Rightarrow \forall Cl \in \texttt{CltFree} \setminus \{\texttt{owner}(\texttt{h},\ \Gamma^{\texttt{r}\prime}(p)) \downarrow_1\} \Rightarrow$$
$$\Rightarrow \texttt{RefNum}(\texttt{h}, \texttt{Fr}_1 \circ \texttt{Fr}_2 \circ \texttt{FrSt}_0, \langle Cl,\ \texttt{null}^{\texttt{r}}\rangle, \texttt{uniq}) \leq 1\ (5)$$
$$\Gamma'(p) \neq \texttt{uniq} \Rightarrow \texttt{owner}(\texttt{h},\ \Gamma^{\texttt{r}\prime}(p)) \downarrow_1 \notin Cl\ (6)$$
$$\Gamma'(p) = \texttt{uniq} \Rightarrow \texttt{RefNum}(\texttt{h}, \texttt{Fr}_1 \circ \texttt{Fr}_2 \circ \texttt{FrSt}_0, \langle Cl,\ \texttt{null}^{\texttt{r}}\rangle, \texttt{uniq}) =$$
$$= \texttt{RefNum}(\texttt{h}, \texttt{FrSt}, \langle Cl,\ \texttt{null}^{\texttt{r}}\rangle, \texttt{uniq}) \leq 1\ (7)$$
$$(5) \wedge (6) \wedge (7) \Rightarrow \texttt{h} \vdash_{Uniq} \texttt{Fr}_1 \circ \texttt{Fr}_2 \circ \texttt{FrSt}_0$$

□

Lemma 7.33.

$$\left.\begin{array}{ll}
\mathit{FrSt} = \mathit{Fr} \circ \mathit{FrSt}' & \\
\mathit{h} \vdash_{Uniq} \mathit{FrSt} & (1)
\end{array}\right\} \Rightarrow \mathit{h} \vdash_{Uniq} \mathit{FrSt}'$$

Proof.

$$\forall Cl \in \texttt{CltFree}\ (1) \Rightarrow \texttt{RefNum}(\texttt{h},\ \texttt{FrSt}',\ \langle Cl,\ \texttt{null}^{\texttt{r}}\rangle, \texttt{uniq}) \leq$$
$$\leq \texttt{RefNum}(\texttt{h},\ \texttt{FrSt}, \langle Cl,\ \texttt{null}^{\texttt{r}}\rangle, \texttt{uniq}) \leq 1 \Rightarrow \texttt{h}' \vdash_{Uniq} \texttt{FrSt}$$

□

Lemma 7.34.

$$\left.\begin{array}{ll} \boldsymbol{h} \vdash_{Uniq} \boldsymbol{FrSt} & (1) \\ \langle \iota,\ \boldsymbol{h}' \rangle = \boldsymbol{new}(\boldsymbol{h},\ C,\ \boldsymbol{ow}) & (2) \end{array}\right\} \Rightarrow \boldsymbol{h}' \vdash_{Uniq} \boldsymbol{FrSt}$$

Proof.

$$\begin{array}{l} \forall Cl \in \texttt{CltFree}\ (1) \Rightarrow \texttt{RefNum}(\texttt{h},\ \texttt{FrSt}',\ \langle Cl,\ \texttt{null}^{\texttt{r}} \rangle, \texttt{uniq}) = \\ = \texttt{RefNum}(\texttt{h},\ \texttt{FrSt}, \langle Cl,\ \texttt{null}^{\texttt{r}} \rangle, \texttt{uniq}) \leq 1 \Rightarrow \texttt{h}' \vdash_{Uniq} \texttt{FrSt} \end{array}$$

□

Lemma 7.35.

$$\left.\begin{array}{ll} \boldsymbol{Fr} = \langle \Gamma^r,\ \Gamma,\ U \rangle & \\ \boldsymbol{FrSt} = \boldsymbol{Fr} \circ \boldsymbol{FrSt}_0 & \\ \boldsymbol{Fr}' = \langle \Gamma^{r\prime},\ \Gamma,\ U' \rangle & \\ \boldsymbol{FrSt}' = \boldsymbol{Fr}' \circ \boldsymbol{FrSt}_0 & \\ \Gamma(y) = \boldsymbol{rep}\, \langle Cl \rangle & (1) \\ \boldsymbol{h} \vdash_{wf} \boldsymbol{FrSt} & (2) \\ \boldsymbol{FrSt} \vdash_{Uniq} \boldsymbol{h} & (3) \\ \boldsymbol{ow} = \langle \boldsymbol{null}^r,\ \boldsymbol{newClt}(\boldsymbol{h}) \rangle & (4) \\ \boldsymbol{h}' = \boldsymbol{transferCl}(\boldsymbol{h},\ \Gamma^r(y),\ \boldsymbol{ow}) & (5) \\ U' = \boldsymbol{consumeAliases}(U, y) \setminus \{x\} & (6) \\ \Gamma^{r\prime} = \Gamma^r[x \mapsto \Gamma^r(y)] & (7) \end{array}\right\} \Rightarrow \boldsymbol{h}' \vdash_{Uniq} \boldsymbol{FrSt}'$$

Proof.

$$\begin{array}{l} \forall Cl \in \texttt{CltFree} \setminus \{\texttt{ow} \downarrow_1\} \texttt{RefNum}(\texttt{h}',\ \texttt{FrSt}',\ \langle Cl,\ \texttt{null}^{\texttt{r}} \rangle, \texttt{uniq}) \overset{(2)\wedge(5)\wedge(6)}{\leq} \\ \leq \texttt{RefNum}(\texttt{h},\ \texttt{FrSt}, \langle Cl,\ \texttt{null}^{\texttt{r}} \rangle, \texttt{uniq}) \leq 1\ (8) \\ (4) \Rightarrow \texttt{RefNum}(\texttt{h},\ \texttt{FrSt},\ \langle \texttt{ow} \downarrow_1,\ \texttt{null}^{\texttt{r}} \rangle, \texttt{uniq}) = 0 \Rightarrow \\ \Rightarrow \texttt{RefNum}(\texttt{h}',\ \texttt{FrSt}',\ \langle \texttt{ow} \downarrow_1,\ \texttt{null}^{\texttt{r}} \rangle, \texttt{uniq}) = 1\ (9) \\ (8) \wedge (9) \Rightarrow \texttt{h}' \vdash_{Uniq} \texttt{FrSt}' \end{array}$$

□

Lemma 7.36.

$$\left.\begin{array}{ll}
\mathit{Fr} = \langle \Gamma^r,\ \Gamma,\ U\rangle & \\
\mathit{FrSt} = \mathit{Fr} \circ \mathit{FrSt}_0 & \\
\mathit{Fr}' = \langle \Gamma^{r\prime},\ \Gamma,\ U'\rangle & \\
\mathit{FrSt}' = \mathit{Fr}' \circ \mathit{FrSt}_0 & \\
\Gamma(y) = \mathit{uniq} & (1)\\
\mathit{h} \vdash_{wf} \mathit{FrSt} & (2)\\
\mathit{FrSt} \vdash_{Uniq} \mathit{h} & (3)\\
\mathit{ow} \neq \langle \mathit{null}^r,\ _\rangle & (4)\\
\mathit{h}' = \mathit{transferCl}(\mathit{h},\ \Gamma^r(y),\ \mathit{ow}) & (5)\\
U' = U \cup \{y\} \setminus \{x\} & (6)\\
\Gamma^{r\prime} = \Gamma^r[x \mapsto \Gamma^r(y)] & (7)
\end{array}\right\} \Rightarrow \mathit{h}' \vdash_{Uniq} \mathit{FrSt}'$$

Proof.

$$\begin{array}{l}
\forall Cl \in \mathtt{CltFree}\ (3) \Rightarrow \mathtt{RefNum}(\mathtt{h}',\ \mathtt{FrSt}',\ \langle Cl,\ \mathtt{null}^{\mathtt{r}}\rangle, \mathtt{uniq}) \overset{(2)\wedge(5)\wedge(6)}{\Rightarrow}\\
\leq \mathtt{RefNum}(\mathtt{h},\ \mathtt{FrSt}, \langle Cl,\ \mathtt{null}^{\mathtt{r}}\rangle, \mathtt{uniq}) \leq 1 \Rightarrow \mathtt{h}' \vdash_{Uniq} \mathtt{FrSt}'
\end{array}$$

□

7.7 Global invariant's lemmas

Lemma 7.37.

$$\left.\begin{array}{ll}
\mathit{Fr} = \langle \Gamma^r,\ \Gamma,\ U\rangle & \\
\mathit{Fr}' = \langle \Gamma^{r\prime},\ \Gamma,\ U'\rangle & \\
\mathit{FrSt} = \mathit{Fr} \circ \mathit{FrSt}_0 & \\
\mathit{FrSt}' = \mathit{Fr}' \circ \mathit{FrSt}_0 & \\
\mathit{h} \vdash_{Inv} \mathit{FrSt} & (1)\\
\Gamma^r(\mathit{this}) = \Gamma^{r\prime}(\mathit{this}) & (2)\\
\mathit{h} \vdash_{wf} \mathit{FrSt}' & (3)\\
\forall \iota\ :\ \mathit{ExtOwn}(\mathit{h},\ \mathit{Fr},\ \iota) \Rightarrow \mathit{ExtOwn}(\mathit{h},\ \mathit{Fr}',\ \iota) & (4)
\end{array}\right\} \Rightarrow \mathit{h} \vdash_{Inv} \mathit{FrSt}'$$

Proof.

$$\begin{array}{l}
\iota_0 = \Gamma^{\mathtt{r}}(\mathtt{this})\\
(1) \Rightarrow\\
\left\{\begin{array}{ll}
\mathtt{h}; \mathtt{FrSt}' \vdash_{Inv} \iota_0 & (5)\\
\forall \iota\ :\ \mathtt{ExtOwn}(\mathtt{h},\ \mathtt{Fr},\ \iota) \wedge \iota \neq \iota_0 \Rightarrow \mathtt{h}; \mathtt{FrSt} \vdash_{Inv} \iota & (6)
\end{array}\right.\\
(4) \wedge (3) \wedge (6) \Rightarrow \forall \iota\ :\ \mathtt{ExtOwn}(\mathtt{h}',\ \mathtt{Fr}',\ \iota) \wedge \iota \neq \iota_0 \Rightarrow \mathtt{h}'; \mathtt{FrSt}' \vdash_{Inv} \iota\ (7)\\
(5) \wedge (7) \Rightarrow \mathtt{h} \vdash_{Inv} \mathtt{FrSt}'
\end{array}$$

□

Lemma 7.38.

$$\left.\begin{array}{ll} \boldsymbol{h} \vdash_{Inv} \boldsymbol{FrSt} & (1) \\ \iota_0 \in \boldsymbol{dom}(\boldsymbol{h}) & (2) \\ \boldsymbol{h}' = \boldsymbol{h}[\iota_0 \,.\, f := \iota] & (3) \end{array}\right\} \Rightarrow \boldsymbol{h}' \vdash_{Inv} \boldsymbol{FrSt}$$

Proof.

$$(2) \wedge (3) \Rightarrow \forall \iota \in \mathtt{dom}(\mathtt{h}') \ : \ \mathtt{owner}(\mathtt{h},\ \iota) = \mathtt{owner}(\mathtt{h}',\ \iota) \overset{(2)}{\Rightarrow} \mathtt{h}' \vdash_{Inv} \mathtt{FrSt}$$

□

Lemma 7.39.

$$\left.\begin{array}{ll} \boldsymbol{Fr} = \langle \Gamma^r,\ \Gamma,\ U \rangle & \\ \boldsymbol{FrSt} = \boldsymbol{Fr} \circ \boldsymbol{FrSt}_0 & \\ \Gamma^{r\prime} = \{\langle p,\ \Gamma^r(z)\rangle,\ \overline{\langle v,\ \boldsymbol{null}^r\rangle},\ \langle \boldsymbol{this},\ \Gamma^r(y)\rangle,\ \langle \boldsymbol{res},\ \boldsymbol{null}^r\rangle\} & \\ \Gamma' = \{\langle p, T_p\rangle,\ \overline{\langle v,\ T\rangle},\ \langle \boldsymbol{this}, \boldsymbol{this\ class}^r(\Gamma^r(y))\rangle,\ \langle \boldsymbol{res}, T_r\rangle\} & \\ U' = \boldsymbol{if}(\Gamma(y) \notin \{\boldsymbol{peer},\ \boldsymbol{this}\})\ \boldsymbol{then}\ U\ \boldsymbol{else\ consumeLocals}(U) & \\ \boldsymbol{Fr}_1 = \langle \Gamma^{r\prime},\ \Gamma',\ \varnothing \rangle & \\ \boldsymbol{Fr}_2 = \langle \Gamma^r,\ \Gamma,\ U' \rangle & \\ \boldsymbol{FrSt}' = \boldsymbol{Fr}_1 \circ \boldsymbol{Fr}_2 \circ \boldsymbol{FrSt}_0 & \\ \boldsymbol{h} \vdash_{Inv} \boldsymbol{FrSt} & (1) \\ \boldsymbol{h} \vdash_{wf} \boldsymbol{FrSt} & (2) \\ \boldsymbol{h} \vdash_{wf} \boldsymbol{FrSt}' & (3) \\ \boldsymbol{IsWritable}(\boldsymbol{class}^r(\Gamma^r(y))) & (4) \end{array}\right\} \Rightarrow$$

$$\Rightarrow \boldsymbol{h} \vdash_{Inv} \boldsymbol{FrSt}'$$

Proof.

$\iota_0 = \Gamma^{\mathtt{r}}(\mathtt{this})$

$(1) \Rightarrow$

$$\left\{\begin{array}{ll} \mathtt{h}; \mathtt{FrSt}_0 \vdash_{Inv} \iota_0 & (5) \\ \forall \iota \ : \ \mathtt{ExtOwn}(\mathtt{h},\ \mathtt{Fr},\ \iota) \wedge \iota \neq \iota_0 \Rightarrow \mathtt{h}; \mathtt{FrSt} \vdash_{Inv} \iota & (6) \end{array}\right.$$

$\iota_0' = \Gamma^{\mathtt{r}\prime}(\mathtt{this})$

$(2) \wedge (3) \wedge (4) \Rightarrow (\forall \iota \ : \ \mathtt{ExtOwn}(\mathtt{h},\ \mathtt{Fr},\ \iota) \Rightarrow \mathtt{ExtOwn}(\mathtt{h},\ \mathtt{Fr}',\ \iota)) \Rightarrow$
$\mathtt{ExtOwn}(\mathtt{h}',\ \mathtt{Fr}',\ \iota) \wedge \iota \neq \iota_0' \Rightarrow \mathtt{h}'; \mathtt{Fr} \circ \mathtt{FrSt}_0 \vdash_{Inv} \iota$ (7)

$\Gamma(y) \in \{\mathtt{peer},\ \mathtt{this}\} \Rightarrow U' = \mathtt{consumeLocals}(U) \Rightarrow$
$\overset{(1)}{\Rightarrow} \mathtt{h}; \mathtt{FrSt}_1 \vdash_{Inv} \iota_0'$ (8)

$\Gamma(y) = \mathtt{rep}\ \langle Cl \rangle \overset{(1)}{\Rightarrow} \mathtt{h}; \mathtt{FrSt}_1 \vdash_{Inv} \iota_0'$ (9)

$(7) \wedge (8) \wedge (9) \Rightarrow \mathtt{h} \vdash_{Inv} \mathtt{FrSt}'$

□

Lemma 7.40.

$$\left.\begin{array}{ll}
\mathit{Fr}_1 = \langle \Gamma^r{}_1,\ \Gamma_1,\ U_1 \rangle & \\
\mathit{Fr}_2 = \langle \Gamma^r{}_2,\ \Gamma_2,\ U_2 \rangle & \\
\mathit{Fr}_3 = \langle \Gamma^r{}_3,\ \Gamma_3,\ U_3 \rangle & \\
\mathit{FrSt}_1 = \mathit{Fr}_1 \circ \mathit{FrSt}_0 & \\
\mathit{FrSt}_3 = \mathit{Fr}_3 \circ \mathit{FrSt}_1 & \\
h; \Gamma^r{}_1(\mathit{this}) \vdash_{wf} \Gamma^r{}_2(\mathit{this}) : \mathit{rep}\,\langle Cl \rangle & (1) \\
h \vdash_{Inv} \mathit{FrSt}_1 & (2) \\
h' \vdash_{Inv} \mathit{FrSt}_3 & (3) \\
\Gamma^r{}_2(\mathit{this}) = \Gamma^r{}_3(\mathit{this}) & (4) \\
\mathit{OwAsMod}(h,\ h',\ \mathit{Fr}_2,\ \mathit{Fr}_3) & (5)
\end{array}\right\} \Rightarrow h' \vdash_{Inv} \mathit{FrSt}_1$$

Proof.

$$\forall \iota\ : \mathtt{ExtOwn}(\mathtt{h}',\ \mathtt{Fr}_1,\ \Gamma^{\mathtt{r}}{}_1(\mathtt{this})) \overset{(1)}{\Rightarrow} \left\{ \begin{array}{l} \mathtt{ExtOwn}(\mathtt{h}',\ \mathtt{Fr}_2,\ \Gamma^{\mathtt{r}}{}_3(\mathtt{this})) \overset{(2)\wedge(5)}{\Rightarrow} \\ \mathtt{ExtOwn}(\mathtt{h}',\ \mathtt{Fr}_3,\ \Gamma^{\mathtt{r}}{}_3(\mathtt{this})) \overset{(3)}{\Rightarrow} \end{array} \right.$$
$$\mathtt{h}'; \mathtt{FrSt}_1 \vdash_{Inv} \iota \Rightarrow \mathtt{h}' \vdash_{Inv} \mathtt{FrSt}_1$$

□

Lemma 7.41.

$$\left.\begin{array}{ll}
\mathit{Fr}_1 = \langle \Gamma^r{}_1,\ \Gamma_1,\ U_1 \rangle & \\
\mathit{Fr}_2 = \langle \Gamma^r{}_2,\ \Gamma_2,\ U_2 \rangle & \\
\mathit{FrSt}_1 = \mathit{Fr}_1 \circ \mathit{FrSt}_0 & \\
\mathit{FrSt}_2 = \mathit{Fr}_2 \circ \mathit{FrSt}_1 & \\
h; \Gamma^r{}_1(\mathit{this}) \vdash_{wf} \Gamma^r{}_2(\mathit{this}) : \mathit{peer} & (1) \\
h \vdash_{Inv} \mathit{FrSt}_2 & (2)
\end{array}\right\} \Rightarrow h \vdash_{Inv} \mathit{FrSt}_1$$

Proof.

$$\forall \iota\ : \mathtt{ExtOwn}(\mathtt{h},\ \mathtt{Fr}_1,\ \Gamma^{\mathtt{r}}{}_2(\mathtt{this})) \overset{(1)}{\Rightarrow} \mathtt{ExtOwn}(\mathtt{h},\ \mathtt{Fr}_2,\ \Gamma^{\mathtt{r}}{}_2(\mathtt{this})) \overset{(2)}{\Rightarrow}$$
$$\Rightarrow \mathtt{h}; \mathtt{FrSt}_1 \vdash_{Inv} \iota \Rightarrow \mathtt{h} \vdash_{Inv} \mathtt{FrSt}_1$$

□

Lemma 7.42.

$$\left.\begin{array}{ll}
h \vdash_{Inv} \mathit{FrSt} & (1) \\
\langle \iota_{new},\ h' \rangle = \mathit{new}(h,\ C,\ \mathit{ow}) & (2)
\end{array}\right\} \Rightarrow h \vdash_{Inv} \mathit{FrSt}'$$

Proof.

$$(2) \Rightarrow \forall \iota \in \mathtt{dom}(\mathtt{h}') \setminus \{\iota_{new}\} \ : \ \mathtt{owner}(\mathtt{h},\ \iota) = \mathtt{owner}(\mathtt{h}',\ \iota) \overset{(1)}{\Rightarrow} \mathtt{h}' \vdash_{Inv} \mathtt{FrSt}$$

□

Lemma 7.43.

$$\left.\begin{array}{ll} \mathit{Fr} = \langle \Gamma^r,\ \Gamma,\ U \rangle & \\ \mathit{FrSt} = \mathit{Fr} \circ \mathit{FrSt}_0 & \\ \Gamma(y) = \mathit{rep}\,\langle Cl \rangle & (1) \\ \mathit{h} \vdash_{wf} \mathit{FrSt} & (2) \\ \mathit{FrSt} \vdash_{Inv} \mathit{h} & (3) \\ \mathit{ow} = \langle \mathit{null}^r,\ \mathit{newClt}(\mathit{h}) \rangle & (4) \\ \mathit{h}' = \mathit{transferCl}(\mathit{h},\ \Gamma^r(y),\ \mathit{ow}) & (5) \end{array}\right\} \Rightarrow \mathit{h}' \vdash_{Inv} \mathit{FrSt}$$

Proof.

$$\forall Cl \in \mathtt{CltRep}\, \iota \in \mathtt{dom}(\mathtt{h})(4) \wedge (5) \Rightarrow \mathtt{RefNum}(\mathtt{h}',\ \mathtt{FrSt},\ \langle Cl,\ \iota \rangle, \mathtt{rep}\,\langle Cl \rangle) \overset{(1)\wedge(2)\wedge(3)}{\leq}$$
$$\leq \mathtt{RefNum}(\mathtt{h},\ \mathtt{FrSt}, \langle Cl,\ \mathtt{null^r} \rangle, \mathtt{uniq}) \leq 1 \Rightarrow \mathtt{h}' \vdash_{Inv} \mathtt{FrSt}$$

□

Lemma 7.44.

$$\left.\begin{array}{ll} \mathit{Fr} = \langle \Gamma^r,\ \Gamma,\ U \rangle & \\ \mathit{FrSt} = \mathit{Fr} \circ \mathit{FrSt}_0 & \\ \Gamma(y) = \mathit{uniq} & (1) \\ \mathit{h} \vdash_{wf} \mathit{FrSt} & (2) \\ \mathit{FrSt} \vdash_{Inv} \mathit{h} & (3) \\ \mathit{ThisOw}(\mathit{h},\ \mathit{FrSt}) & (4) \\ \mathit{h}' = \mathit{transferCl}(\mathit{h},\ \Gamma^r(y),\ \mathit{ow}) & (5) \end{array}\right\} \Rightarrow \mathit{h}' \vdash_{Inv} \mathit{FrSt}$$

Proof.

$$\forall Cl \in \mathtt{CltRep}\, \iota \in \mathtt{dom}(\mathtt{h})(4) \wedge (5) \Rightarrow \mathtt{RefNum}(\mathtt{h},\ \mathtt{FrSt},\ \langle Cl,\ \iota \rangle, \mathtt{rep}\,\langle Cl \rangle) = 0 \overset{(1)\wedge(2)\wedge(3)}{\Rightarrow}$$
$$\leq \mathtt{RefNum}(\mathtt{h}'L,\ \mathtt{FrSt}, \langle Cl,\ \mathtt{null^r} \rangle, \mathtt{uniq}) = 0 \Rightarrow \mathtt{h}' \vdash_{Inv} \mathtt{FrSt}$$

□

7.8 Ownership tree's lemmas

Lemma 7.45.

$$\left.\begin{array}{ll} \mathit{WfTree}(h) & (1) \\ \iota_0 \in \mathit{dom}(h) & (2) \\ h' = h[\iota_0 \,.\, f := \iota] & (3) \end{array}\right\} \Rightarrow \mathit{WfTree}(h')$$

Proof.

$$\forall \iota \in \mathtt{dom}(\mathtt{h}') \ :\overset{(1)}{\Rightarrow} \iota \notin \mathtt{owners}(\mathtt{h},\ \iota) \downarrow_2 \overset{(2)\wedge(3)}{\Rightarrow}$$
$$\Rightarrow \iota \notin \mathtt{owners}(\mathtt{h}',\ \iota) \downarrow_2 \Rightarrow \mathtt{WfTree}(\mathtt{h}')$$

□

Lemma 7.46.

$$\left.\begin{array}{ll} \mathit{WfTree}(h) & (1) \\ \langle \iota_{new},\ h' \rangle = \mathit{new}(h,\ C,\ \mathit{ow}) & (2) \end{array}\right\} \Rightarrow \mathit{WfTree}(h')$$

Proof.

$$\forall \iota \in \mathtt{dom}(\mathtt{h}') \setminus \{\iota_{new}\} \ :\overset{(1)}{\Rightarrow} \iota \notin \mathtt{owners}(\mathtt{h},\ \iota) \downarrow_2 \overset{(2)}{\Rightarrow}$$
$$\Rightarrow \iota \notin \mathtt{owners}(\mathtt{h}',\ \iota) \downarrow_2 \Rightarrow \mathtt{WfTree}(\mathtt{h}')$$

□

Lemma 7.47.

$$\left.\begin{array}{ll} \mathit{WfTree}(h) & (1) \\ h' = \mathit{transferCl}(h,\ \iota_{tr},\ \mathit{ow}) & (2) \\ \mathit{ow} = \langle \mathit{newClt}(h),\ \mathit{null}^r \rangle & (3) \end{array}\right\} \Rightarrow \mathit{WfTree}(h')$$

Proof.

$$\forall \iota \in \mathtt{dom}(\mathtt{h}') \setminus \{\iota_{new}\} \ :\overset{(1)}{\Rightarrow} \iota \notin \mathtt{owners}(\mathtt{h},\ \iota) \downarrow_2 \overset{(2)\wedge(3)}{\Rightarrow}$$
$$\Rightarrow \iota \notin \mathtt{owners}(\mathtt{h}',\ \iota) \downarrow_2 \Rightarrow \mathtt{WfTree}(\mathtt{h}')$$

□

Lemma 7.48.

$$\left.\begin{array}{ll} \mathit{WfTree}(h) & (1) \\ h' = \mathit{transferCl}(h,\ \iota_{tr},\ \mathit{ow}) & (2) \\ \mathit{ow} = \mathit{mod2Ow}(h,\ m,\ \Gamma^r(\mathit{this})) & (3) \\ m \in \{\mathit{rep}\,\langle Cl \rangle\,,\ \mathit{peer}\} & (4) \\ \mathit{ThisOw}(h,\ \mathit{FrSt}) & (5) \\ h; \_ \vdash_{wf} \iota_{tr} : \mathit{uniq} & (6) \end{array}\right\} \Rightarrow \mathit{WfTree}(h')$$

Proof.

$$\forall \iota \in \mathtt{dom}(\mathtt{h}') \setminus \{\iota_{new}\} \ :\overset{(1)}{\Rightarrow} \iota \notin \mathtt{owners}(\mathtt{h},\ \iota) \downarrow_2 \overset{(2)\wedge(5)\wedge(6)}{\Rightarrow}$$
$$\Rightarrow \iota \notin \mathtt{owners}(\mathtt{h}',\ \iota) \downarrow_2 \Rightarrow \mathtt{WfTree}(\mathtt{h}')$$

□

7.9 This owners's lemmas

Lemma 7.49.

$$\left.\begin{array}{ll} \mathit{FrSt} = \langle \Gamma^{r}{}_0,\ \Gamma_0,\ U_0\rangle \circ \mathit{FrSt}_0 & \\ \mathit{FrSt}' = \langle \Gamma^{r'}{}_0,\ \Gamma_0,\ U'_0\rangle \circ \mathit{FrSt}_0 & \\ \mathit{ThisOw}(\mathit{h},\ \mathit{FrSt}) & (1) \\ \Gamma^{r}(\mathit{this}) = \Gamma^{r'}(\mathit{this}) & (2) \end{array}\right\} \Rightarrow \mathit{ThisOw}(\mathit{h},\ \mathit{FrSt}')$$

Proof.

$$\mathtt{FrSt}_0 = \overline{\langle \Gamma^{\mathtt{r}},\ \Gamma,\ U\rangle}$$
$$(1) \Rightarrow \left\{\begin{array}{ll} \forall Cl \in \mathtt{CltFree} : \langle Cl,\ \mathtt{null}^{\mathtt{r}}\rangle \notin \mathtt{owners}(\mathtt{h},\ \Gamma^{\mathtt{r}}{}_0(\mathtt{this})) & (3) \\ \overline{\mathtt{owner}(\mathtt{h},\ \Gamma^{\mathtt{r}}(\mathtt{this})) \in \mathtt{owners}(\mathtt{h},\ \Gamma^{\mathtt{r}}{}_0(\mathtt{this}))} & (4) \end{array}\right.$$
$$(3) \wedge (1) \wedge (2) \Rightarrow \overline{\forall Cl \in \mathtt{CltFree} : \langle Cl,\ \mathtt{null}^{\mathtt{r}}\rangle \notin \mathtt{owners}(\mathtt{h},\ \Gamma^{\mathtt{r}'}{}_0(\mathtt{this}))} \ (5)$$
$$(4) \wedge (1) \wedge (2) \Rightarrow \overline{\mathtt{owner}(\mathtt{h},\ \Gamma^{\mathtt{r}}(\mathtt{this})) \in \mathtt{owners}(\mathtt{h},\ \Gamma^{\mathtt{r}'}{}_0(\mathtt{this}))} \ (6)$$
$$(5) \wedge (6) \Rightarrow \mathtt{ThisOw}(\mathtt{h},\ \mathtt{FrSt}')$$

□

Lemma 7.50.

$$\left.\begin{array}{ll} \mathit{FrSt} = \langle \Gamma^{r}{}_0,\ \Gamma_0,\ U_0\rangle \circ \mathit{FrSt}_0 & \\ \mathit{FrSt}' = \langle \Gamma^{r'}{}_0,\ \Gamma_0,\ U_0\rangle \circ \mathit{FrSt}_0 & \\ \mathit{ThisOw}(\mathit{h},\ \mathit{FrSt}) & (1) \\ \iota_0 \in \mathit{dom}(\mathit{h}) & (2) \\ \mathit{h}' = \mathit{h}[\iota_0 . f := \iota] & (3) \end{array}\right\} \Rightarrow \mathit{ThisOw}(\mathit{h},\ \mathit{FrSt}')$$

Proof.

$$\mathtt{FrSt}_0 = \overline{\langle \Gamma^{\mathtt{r}},\ \Gamma,\ U\rangle}$$
$$(1) \Rightarrow \left\{\begin{array}{ll} \forall Cl \in \mathtt{CltFree} : \langle Cl,\ \mathtt{null}^{\mathtt{r}}\rangle \notin \mathtt{owners}(\mathtt{h},\ \Gamma^{\mathtt{r}}{}_0(\mathtt{this})) & (4) \\ \overline{\mathtt{owner}(\mathtt{h},\ \Gamma^{\mathtt{r}}(\mathtt{this})) \in \mathtt{owners}(\mathtt{h},\ \Gamma^{\mathtt{r}}{}_0(\mathtt{this}))} & (5) \end{array}\right.$$
$$(4) \wedge (1) \wedge (3) \Rightarrow \overline{\forall Cl \in \mathtt{CltFree} : \langle Cl,\ \mathtt{null}^{\mathtt{r}}\rangle \notin \mathtt{owners}(\mathtt{h},\ \Gamma^{\mathtt{r}'}{}_0(\mathtt{this}))} \ (6)$$
$$(5) \wedge (1) \wedge (3) \Rightarrow \overline{\mathtt{owner}(\mathtt{h},\ \Gamma^{\mathtt{r}}(\mathtt{this})) \in \mathtt{owners}(\mathtt{h},\ \Gamma^{\mathtt{r}'}{}_0(\mathtt{this}))} \ (7)$$
$$(6) \wedge (7) \Rightarrow \mathtt{ThisOw}(\mathtt{h},\ \mathtt{FrSt}')$$

□

Lemma 7.51.

$$\left.\begin{array}{ll} \mathit{Fr} = \langle {\Gamma^r}_0,\ \Gamma_0,\ U_0\rangle & \\ \mathit{Fr}' = \langle {\Gamma^{r'}}_0,\ \Gamma'_0,\ U'_0\rangle & \\ \mathit{FrSt} = \mathit{Fr} \circ \mathit{FrSt}_0 & \\ \mathit{FrSt}' = \mathit{Fr}' \circ \mathit{FrSt} & \\ \mathit{ThisOw}(\mathit{h},\ \mathit{FrSt}) & (1) \\ \mathit{h}; \Gamma^r(\mathit{this}) \vdash_{wf} \Gamma^{r'}(\mathit{this}) : m & (2) \\ \mathit{IsWritable}(m) & (3) \end{array}\right\} \Rightarrow \mathit{ThisOw}(\mathit{h},\ \mathit{FrSt}')$$

Proof.

$$\begin{array}{l} \mathtt{FrSt}_0 = \overline{\langle \Gamma^{\mathtt{r}},\ \Gamma,\ U\rangle} \\ (1) \Rightarrow \left\{\begin{array}{ll} \forall Cl \in \mathtt{CltFree} : \langle Cl,\ \mathtt{null}^{\mathtt{r}}\rangle \notin \mathtt{owners}(\mathtt{h},\ {\Gamma^{\mathtt{r}}}_0(\mathtt{this})) & (4) \\ \overline{\mathtt{owner}(\mathtt{h},\ \Gamma^{\mathtt{r}}(\mathtt{this})) \in \mathtt{owners}(\mathtt{h},\ {\Gamma^{\mathtt{r}}}_0(\mathtt{this}))} & (5) \end{array}\right. \\ (4) \wedge (1) \wedge (3) \Rightarrow \forall Cl \in \mathtt{CltFree} : \langle Cl,\ \mathtt{null}^{\mathtt{r}}\rangle \notin \mathtt{owners}(\mathtt{h},\ {\Gamma^{\mathtt{r}'}}_0(\mathtt{this})) \ (6) \\ (5) \wedge (1) \wedge (3) \Rightarrow \overline{\mathtt{owner}(\mathtt{h},\ \Gamma^{\mathtt{r}}(\mathtt{this})) \in \mathtt{owners}(\mathtt{h},\ {\Gamma^{\mathtt{r}'}}_0(\mathtt{this}))} \ (7) \\ (1) \wedge (3) \Rightarrow \mathtt{owner}(\mathtt{h},\ {\Gamma^{\mathtt{r}}}_0(\mathtt{this})) \in \mathtt{owners}(\mathtt{h},\ {\Gamma^{\mathtt{r}'}}_0(\mathtt{this})) \ (8) \\ (6) \wedge (7) \wedge (8) \Rightarrow \mathtt{ThisOw}(\mathtt{h},\ \mathtt{FrSt}') \end{array}$$

□

Lemma 7.52.

$$\left.\begin{array}{ll} \mathit{ThisOw}(\mathit{h},\ \mathit{FrSt}) & (1) \\ \langle \iota,\ \mathit{h}'\rangle = \mathit{new}(\mathit{h},\ C,\ \mathit{ow}) & (2) \end{array}\right\} \Rightarrow \mathit{ThisOw}(\mathit{h}',\ \mathit{FrSt})$$

Proof.

$$\begin{array}{l} \mathtt{FrSt}_0 = \overline{\langle \Gamma^{\mathtt{r}},\ \Gamma,\ U\rangle} \\ (1) \Rightarrow \left\{\begin{array}{ll} \forall Cl \in \mathtt{CltFree} : \langle Cl,\ \mathtt{null}^{\mathtt{r}}\rangle \notin \mathtt{owners}(\mathtt{h},\ {\Gamma^{\mathtt{r}}}_0(\mathtt{this})) & (3) \\ \overline{\mathtt{owner}(\mathtt{h},\ \Gamma^{\mathtt{r}}(\mathtt{this})) \in \mathtt{owners}(\mathtt{h},\ {\Gamma^{\mathtt{r}}}_0(\mathtt{this}))} & (4) \end{array}\right. \\ (3) \wedge (1) \wedge (2) \Rightarrow \forall Cl \in \mathtt{CltFree} : \langle Cl,\ \mathtt{null}^{\mathtt{r}}\rangle \notin \mathtt{owners}(\mathtt{h}',\ {\Gamma^{\mathtt{r}}}_0(\mathtt{this})) \ (5) \\ (4) \wedge (1) \wedge (2) \Rightarrow \overline{\mathtt{owner}(\mathtt{h}',\ \Gamma^{\mathtt{r}}(\mathtt{this})) \in \mathtt{owners}(\mathtt{h},\ {\Gamma^{\mathtt{r}}}_0(\mathtt{this}))} \ (6) \\ (5) \wedge (6) \Rightarrow \mathtt{ThisOw}(\mathtt{h}',\ \mathtt{FrSt}) \end{array}$$

□

Lemma 7.53.

$$\left.\begin{array}{ll} \mathit{Fr}_1 = \langle \Gamma^r{}_1,\ \Gamma_1,\ U_1 \rangle & \\ \mathit{Fr}_2 = \langle \Gamma^r{}_2,\ \Gamma_2,\ U_2 \rangle & \\ \mathit{FrSt}_1 = \mathit{Fr}_1 \circ \mathit{FrSt}_0 & \\ \mathit{FrSt}_2 = \mathit{Fr}_2 \circ \mathit{FrSt}_1 & \\ \mathit{h}; \Gamma^r{}_1(\mathit{this}) \vdash_{wf} \Gamma^r{}_2(\mathit{this}) : m & (1) \\ m \in \{\mathit{peer}, \mathit{this}, \mathit{rep}\,\langle Cl \rangle\} & (2) \\ \mathit{ThisOw}(\mathit{h},\ \mathit{FrSt}_2) & (3) \end{array}\right\} \Rightarrow \mathit{ThisOw}(\mathit{h},\ \mathit{FrSt}_1)$$

Proof.

$$\begin{array}{l} \mathtt{FrSt}_0 = \overline{\langle \Gamma^{\mathtt{r}},\ \Gamma,\ U \rangle} \\ (1) \Rightarrow \left\{ \begin{array}{ll} \forall Cl \in \mathtt{CltFree} : \langle Cl,\ \mathtt{null}^{\mathtt{r}} \rangle \notin \mathtt{owners}(\mathtt{h},\ \Gamma^{\mathtt{r}}{}_2(\mathtt{this})) & (4) \\ \overline{\mathtt{owner}(\mathtt{h},\ \Gamma^{\mathtt{r}}(\mathtt{this})) \in \mathtt{owners}(\mathtt{h},\ \Gamma^{\mathtt{r}}{}_2(\mathtt{this}))} & (5) \end{array} \right. \\ (4) \wedge (1) \wedge (2) \Rightarrow \overline{\forall Cl \in \mathtt{CltFree} : \langle Cl,\ \mathtt{null}^{\mathtt{r}} \rangle \notin \mathtt{owners}(\mathtt{h},\ \Gamma^{\mathtt{r}}{}_1(\mathtt{this}))} \ (6) \\ (5) \wedge (1) \wedge (2) \Rightarrow \overline{\mathtt{owner}(\mathtt{h},\ \Gamma^{\mathtt{r}}(\mathtt{this})) \in \mathtt{owners}(\mathtt{h},\ \Gamma^{\mathtt{r}}{}_1(\mathtt{this}))} \ (7) \\ (6) \wedge (7) \Rightarrow \mathtt{ThisOw}(\mathtt{h},\ \mathtt{FrSt}_1) \end{array}$$

□

Lemma 7.54.

$$\left.\begin{array}{ll} \mathit{Fr} = \langle \Gamma^r{}_0,\ \Gamma_0,\ U_0 \rangle & \\ \mathit{ThisOw}(\mathit{h},\ \mathit{FrSt}) & (1) \\ \mathit{h}' = \mathit{transferCl}(\mathit{h},\ \iota_{tr},\ \mathit{ow}) & (2) \\ \mathit{h}; \Gamma^r(\mathit{this}) \vdash_{wf} \iota_{tr} : m & (3) \\ m \in \{\mathit{rep}\,\langle Cl \rangle\,,\ \mathit{uniq}\} & (4) \end{array}\right\} \Rightarrow \mathit{ThisOw}(\mathit{h}',\ \mathit{FrSt})$$

Proof.

$$\begin{array}{l} \mathtt{FrSt}_0 = \overline{\langle \Gamma^{\mathtt{r}},\ \Gamma,\ U \rangle} \\ (1) \Rightarrow \left\{ \begin{array}{ll} \forall Cl \in \mathtt{CltFree} : \langle Cl,\ \mathtt{null}^{\mathtt{r}} \rangle \notin \mathtt{owners}(\mathtt{h},\ \Gamma^{\mathtt{r}}{}_0(\mathtt{this})) & (5) \\ \overline{\mathtt{owner}(\mathtt{h},\ \Gamma^{\mathtt{r}}(\mathtt{this})) \in \mathtt{owners}(\mathtt{h},\ \Gamma^{\mathtt{r}}{}_0(\mathtt{this}))} & (6) \end{array} \right. \\ (5) \wedge (2) \wedge (4) \Rightarrow \overline{\forall Cl \in \mathtt{CltFree} : \langle Cl,\ \mathtt{null}^{\mathtt{r}} \rangle \notin \mathtt{owners}(\mathtt{h}',\ \Gamma^{\mathtt{r}}{}_0(\mathtt{this}))} \ (7) \\ (6) \wedge (2) \wedge (4) \Rightarrow \overline{\mathtt{owner}(\mathtt{h}',\ \Gamma^{\mathtt{r}}(\mathtt{this})) \in \mathtt{owners}(\mathtt{h}',\ \Gamma^{\mathtt{r}}{}_0(\mathtt{this}))} \ (8) \\ (7) \wedge (8) \Rightarrow \mathtt{ThisOw}(\mathtt{h}',\ \mathtt{FrSt}) \end{array}$$

□

7.10 Owner as modifier's lemmas

Lemma 7.55.

$$\left.\begin{array}{ll} \mathit{Fr} = \langle \Gamma^r,\ \Gamma,\ U \rangle & \\ \mathit{Fr}' = \langle \Gamma^r,\ \Gamma',\ U' \rangle & \\ \{v \in U' | \Gamma'(v) = \mathit{uniq}\} \subseteq \{v \in U | \Gamma(v) = \mathit{uniq}\} & (1) \\ \mathit{owner}(\mathit{h},\ \Gamma^r(\mathit{this})) \in \mathit{owners}(\mathit{h},\ \Gamma^{r\prime}(\mathit{this})) & (2) \end{array}\right\} \Rightarrow \mathit{OwAsMod}(\mathit{h},\ \mathit{h},\ \mathit{Fr},\ \mathit{Fr}')$$

Proof.

$$\begin{array}{l} \forall \iota \in \mathtt{dom(h)} : \neg \mathtt{ExtOwn(h,\ Fr,\ } \iota) \overset{(1)\wedge(2)}{\Rightarrow} \\ \Rightarrow \mathtt{h}(\iota) = \mathtt{h}(\iota) \wedge \neg \mathtt{ExtOwn(h,\ Fr',\ } \iota) \Rightarrow \mathtt{OwAsMod(h,\ h,\ Fr,\ Fr')} \end{array}$$

□

Lemma 7.56.

$$\left.\begin{array}{ll} \mathit{Fr} = \langle \Gamma^r,\ \Gamma,\ U \rangle & \\ \iota_0 \in \mathit{dom}(\mathit{h}) & (1) \\ \mathit{h}; \Gamma^r(\mathit{this}) \vdash_{wf} \iota : m & (2) \\ \mathit{IsWritable}(m) & (3) \\ \mathit{h}' = \mathit{h}[\iota_0 . f := \iota] & (4) \end{array}\right\} \Rightarrow \mathit{OwAsMod}(\mathit{h},\ \mathit{h}',\ \mathit{Fr},\ \mathit{Fr})$$

Proof.

$$\begin{array}{l} \forall \iota \in \mathtt{dom(h)} : \neg \mathtt{ExtOwn(h,\ Fr,\ } \iota) \overset{(3)\wedge(4)}{\Rightarrow} \\ \Rightarrow \mathtt{h}(\iota) = \mathtt{h}'(\iota) \wedge \neg \mathtt{ExtOwn(h',\ Fr,\ } \iota) \Rightarrow \mathtt{OwAsMod(h,\ h',\ Fr,\ Fr)} \end{array}$$

□

Lemma 7.57.

$$\mathit{OwAsMod}(\mathit{h},\ \mathit{h}',\ \mathit{Fr},\ \mathit{Fr}')\ (1) \Rightarrow \mathit{OwAsMod}(\mathit{h},\ \mathit{h}',\ \mathit{Fr},\ \mathit{Fr})$$

Proof.

$$\begin{array}{l} \forall \iota \in \mathtt{dom(h)} : \neg \mathtt{ExtOwn(h,\ Fr,\ } \iota) \overset{(1)}{\Rightarrow} \\ \Rightarrow \mathtt{h}(\iota) = \mathtt{h}'(\iota) \wedge \neg \mathtt{ExtOwn(h,\ Fr',\ } \iota) \Rightarrow \\ \Rightarrow \mathtt{h}(\iota) = \mathtt{h}'(\iota) \wedge \neg \mathtt{ExtOwn(h,\ Fr,\ } \iota) \Rightarrow \mathtt{OwAsMod(h,\ h',\ Fr,\ Fr)} \end{array}$$

□

Lemma 7.58.

$$\left.\begin{array}{l} \mathit{Fr} = \langle \Gamma^r,\ \Gamma,\ U\rangle \\ U' = U \setminus \{x\} \\ \Gamma^{r\prime} = \Gamma^r[x \mapsto \iota] \\ \mathit{Fr}' = \langle \Gamma^{r\prime},\ \Gamma,\ U'\rangle \\ \langle \iota,\ h'\rangle = \mathit{new}(h,\ C,\ \mathit{ow}) \quad (1) \end{array}\right\} \Rightarrow \mathit{OwAsMod}(h,\ h',\ \mathit{Fr},\ \mathit{Fr}')$$

Proof.

$$\begin{array}{l} \forall \iota \in \mathtt{dom(h)} : \neg\mathtt{ExtOwn(h,\ Fr,\ }\iota\mathtt{)} \overset{(1)}{\Rightarrow} \\ \Rightarrow \mathtt{h}(\iota) = \mathtt{h}'(\iota) \wedge \neg\mathtt{ExtOwn(h',\ Fr',\ }\iota\mathtt{)} \Rightarrow \mathtt{OwAsMod(h,\ h',\ Fr,\ Fr')} \end{array}$$

□

Lemma 7.59.

$$\left.\begin{array}{ll} \mathit{OwAsMod}(h,\ h_1,\ \mathit{Fr},\ \mathit{Fr}_1) & (1) \\ \mathit{OwAsMod}(h_1,\ h_2,\ \mathit{Fr}_1,\ \mathit{Fr}_2) & (2) \end{array}\right\} \Rightarrow \mathit{OwAsMod}(h,\ h_2,\ \mathit{Fr},\ \mathit{Fr}_2)$$

Proof.

$$\begin{array}{l} \forall \iota \in \mathtt{dom(h)} : \\ \neg\mathtt{ExtOwn(h,\ Fr,\ }\iota\mathtt{)} \overset{(1)}{\Rightarrow} \left\{\begin{array}{ll} \mathtt{h}(\iota) = \mathtt{h}_1(\iota) & (3) \\ \neg\mathtt{ExtOwn(h_1,\ Fr_1,\ }\iota\mathtt{)} & (4) \end{array}\right. \\ (4) \overset{(2)}{\Rightarrow} \left\{\begin{array}{ll} \mathtt{h}_1(\iota) = \mathtt{h}_2(\iota) & (5) \\ \neg\mathtt{ExtOwn(h_2,\ Fr_2,\ }\iota\mathtt{)} & (6) \end{array}\right. \\ (3) \wedge (5) \Rightarrow \mathtt{h}(\iota) = \mathtt{h}_2(\iota)\ (7) \\ (6) \wedge (7) \Rightarrow \mathtt{OwAsMod(h,\ h_2,\ Fr,\ Fr_2)} \end{array}$$

□

Lemma 7.60.

$$\left.\begin{array}{ll} \mathit{Fr} = \langle \Gamma^r,\ \Gamma,\ U\rangle & \\ U' = U \setminus \{x\} & \\ \Gamma^{r\prime} = \Gamma^r[x \mapsto \Gamma^r(y)] & \\ \mathit{Fr}' = \langle \Gamma^{r\prime},\ \Gamma,\ U'\rangle & \\ h; \Gamma^r(\mathit{this}) \vdash_{wf} \Gamma^r(y) : \mathit{rep}\,\langle Cl\rangle & (1) \\ h' = \mathit{transferCl}(h,\ \Gamma^r(y),\ \mathit{ow}) & (2) \\ \Gamma(x) = \mathit{uniq} & (3) \end{array}\right\} \Rightarrow \mathit{OwAsMod}(h,\ h',\ \mathit{Fr},\ \mathit{Fr}')$$

Proof.

$$\forall \iota \in \mathtt{dom}(\mathtt{h}) : \neg\mathtt{ExtOwn}(\mathtt{h},\ \mathtt{Fr},\ \iota) \overset{(1)\wedge(2)}{\Rightarrow}$$
$$\Rightarrow \mathtt{h}(\iota) = \mathtt{h}'(\iota) \wedge \neg\mathtt{ExtOwn}(\mathtt{h}',\ \mathtt{Fr}',\ \iota) \Rightarrow \mathtt{OwAsMod}(\mathtt{h},\ \mathtt{h}',\ \mathtt{Fr},\ \mathtt{Fr}')$$

□

Lemma 7.61.

$$\left.\begin{array}{ll} \mathit{Fr} = \langle \Gamma^r,\ \Gamma,\ U \rangle & \\ \Gamma(y) = \mathit{uniq} & (1) \\ \mathit{h}' = \mathit{transferCl}(\mathit{h},\ \Gamma^r(y),\ \mathit{ow}) & (2) \end{array}\right\} \Rightarrow \mathit{OwAsMod}(\mathit{h},\ \mathit{h}',\ \mathit{Fr},\ \mathit{Fr})$$

Proof.

$$\forall \iota \in \mathtt{dom}(\mathtt{h}) : \neg\mathtt{ExtOwn}(\mathtt{h},\ \mathtt{Fr},\ \iota) \overset{(2)}{\Rightarrow}$$
$$\Rightarrow \mathtt{h}(\iota) = \mathtt{h}'(\iota) \wedge \neg\mathtt{ExtOwn}(\mathtt{h}',\ \mathtt{Fr}',\ \iota) \Rightarrow \mathtt{OwAsMod}(\mathtt{h},\ \mathtt{h}',\ \mathtt{Fr},\ \mathtt{Fr}')$$

□