On the Strength of Owicki-Gries for Resources

Alexander Malkis and Laurent Mauborgne
IMDEA Software Institute
accepted 2011-08-28, published 2011-10-14, last updated 2023-11-17

Abstract. In multithreaded programs data are often separated into lock-protected resources. Properties of those resources are typically verified by modular, Owicki-Gries-like methods. The modularity of the Owicki-Gries method has its price: proving some properties may require manual introduction of auxiliary variables. What properties can be proven without the burden of introducing auxiliary variables? We answer this question in the abstract interpretation framework. On one hand, we reveal a lattice structure of the method and supply a syntax-based abstract transformer that describes the method exactly. On the other hand, we bound the loss of precision from above and below by transition-relation-independent weakly relational closures. On infinitely many programs the closures coincide and describe the precision loss exactly; in general, the bounds are strict. We prove the absence of a general exact closure-based fixpoint characterization of the accuracy of the Owicki-Gries method, both in the collecting semantics and in certain trace semantics.

1 Introduction

The paper will characterize the accuracy of a popular verification method for proving safety properties of concurrent programs that operate on resources.

A program operating on resources is a multithreaded program in which threads communicate via sequentially consistent shared memory and in which all shared variables are partitioned into disjoint resources. Each resource may be available or busy. To access a variable belonging to a resource, a thread waits until the resource gets available and then starts a critical section for that resource, thus making the resource busy. While staying in the critical section, the thread can read and write the resource data, and no other thread can enter a critical section for the same resource, so no other thread can access the resource data. After the thread finishes accessing the resource, it exits the corresponding critical section, making the resource available.

Simple safety properties of such programs can be proven modularly. A modular proof of a program consists of an annotation per control flow location and an annotation per resource. Roughly, an annotation of a control flow location describes the valuations of the variables that the thread may access at that location. An annotation of a resource describes, roughly, the state of the resource when it is available. The annotations of locations have to be sequentially consistent similarly to the standard Hoare-style assertion logic, but with two changes: when a thread acquires a resource, the proof may assume that the invariant of the acquired resource holds, and on releasing a resource the resource invariant should be reestablished.
Such modularity incurs a loss of precision: for many programs, too strong but valid properties cannot be proven by the method. To prove such properties, the program can be manually augmented with so-called auxiliary variables. A set of variables is called auxiliary if, intuitively, projecting the traces of the program to the other variables gives the same result as removing all the statements involving the auxiliary variables and projecting afterwards. A modular proof is created for the augmented program, then the proven property is projected onto the original variables. The ability to use auxiliary variables makes the proof system complete. So far, auxiliary variables have been introduced purely manually, while the construction of the remaining proof can be automated.

We will estimate the loss of precision inherent to the core of the Owicki-Gries method, which consists of all the proof rules of the Owicki-Gries logic except the ability to use auxiliary variables, in abstract interpretation.

We will show a rich lattice structure of the Owicki-Gries-core proofs and a syntax-based abstract transformer describing the Owicki-Gries core exactly.

We will observe that there is no transition-relation-independent approximation operator that exactly characterizes the loss of precision of the Owicki-Gries core in the collecting semantics. We will also note the absence of equivalent trace-based characterizations of certain kinds.

We will find an approximation operator that induces a useful upper bound on this set, i.e., that will describe how much precision the Owicki-Gries core always loses. This approximation operator depends only on the syntactic structure of the program, but not on its exact transition relation. If a property is provable by the Owicki-Gries core, it is provable by abstract interpretation with this approximation.

We will present an approximation operator inducing a lower bound on the set, i.e., describing how much precision the Owicki-Gries core always retains. This approximation operator also depends only on the syntactic structure of the program, but not on its exact transition relation. If a property is provable by abstract interpretation with this approximation, it is provable by the Owicki-Gries core.

In passing, we will demonstrate an infinite class of simple programs for which both bounds are equal and a program on which both bounds are strict.

In short, the main results and their position are depicted in Fig. 1.

Fig. 1: Precision of analyses. The upper bound is $\rho$, the lower bound is $\bar{\rho}$. In addition to $\rho$, we will consider a simpler lower bound $\rho_c$, which is coarser than $\rho$, but easier to understand.
The rigorous formalization, computations, proofs, recommendations for practitioners, and comparison to abstract interpretations for general programs are found in the appendix.

2 Resource-manipulating language and its semantics

2.1 Language RPL

Now we briefly recall the parallel language RPL (Restricted Parallel Language, rigorously defined in [25]) in which shared data are separated into resources and access to a resource is granted exclusively.

Let threads be indexed by the elements of the set $\mathit{Tid}$ and, without loss of generality, start their executions together. Threads operate on data variables from the set $\mathit{DataVar}$. A resource is a set of data variables; the resources are disjoint. Let $\mathit{Res}$ be the set of all resources.

A statement is either

– an atomic statement, i.e., an assignment or an “assume $\phi$” (which skips if the argument expression evaluates to true and blocks otherwise),
– a sequential composition of two statements, an if-then-else, or a while loop,
– a critical section $\mathit{with r when } \phi \mathit{ do } C \mathit{ endwith}$ where $r$ is a resource, $\phi$ a formula over data variables and $C$ some statement. We write $\mathit{with r do } C \mathit{ endwith}$ when $\phi$ is true.

A thread executes a statement.

A data variable is called local to thread $t$ if all the assignments to the variable are syntactically in $t$. If a variable appears in thread $t$, it should belong to a resource or be local to $t$. If a variable belongs to a resource $r$, it can appear only inside a critical section for $r$, i.e., inside a “$\mathit{with r...}$” statement.

Each resource $r$ is associated with a set of proof variables $\mathit{ProofVar}(r)$, which are all data variables that are not assigned except maybe in critical sections for $r$. All our examples will satisfy $\mathit{ProofVar}(r) = r$ (in general, $\mathit{ProofVar}(r) \supseteq r$).

An RPL program is described by a set of threads, a set of resources and an initial condition on the variables.

2.2 Semantics of RPL

To connect to abstract interpretation, we describe programs in RPL as transition systems.

For each thread $t$ we introduce a fresh non-data program counter variable $\mathit{pc}_t$, which

– is local to thread $t$, but not to any other thread, and
– doesn’t belong to any resource, and
– takes values from the set of control flow locations $\mathit{PL}$ (Program Location).

Let $\mathit{PCVar}$ be the set of all program counter variables and $\mathit{Var} = \mathit{DataVar} \cup \mathit{PCVar}$.

We associate each control flow point $p \in \mathit{PL}$ with a set $\mathit{rsc}(p)$ of resources $r$ such that $p$ is inside a $\mathit{with r...}$ statement.

We allow the same control flow location, say, $p$, to occur in different threads.
A state of a program is a map from $\text{Var}$ to the set of values $\text{Val}$ that includes $\text{PL}$ and the ranges of all data variables. We are going to consider consistent states only: those are states that

- map program counters to elements of $\text{PL}$ and
- satisfy mutual exclusion: the sets of resources held by different threads are disjoint.

A thread $t$ holds a resource $r$ in a consistent state $v$ if $r \in rsc(v(pc_t))$. A resource $r$ is busy in a consistent state $v$ if some thread holds it in $v$, otherwise $r$ is available in $v$.

Each statement of thread $t$ induces a set of transitions $v \rightarrow_t v'$ where $v, v'$ are consistent states. The transitions induced by the non-$\text{with}$ statements are straightforward. The statement $\text{with } r \text{ when } \phi \text{ do } C$ blocks when $r$ is busy or when $\phi$ does not hold, otherwise it changes the control flow location to the initial control flow location of $C$; going out of the critical section is an unconditional change of the control flow location.

Let $\text{init}$ be the set of initial states corresponding to the initial condition and let the successor map

$$ \text{post}(S) = \{ v' \mid \exists v \in S, t \in \text{Tid}: v \rightarrow_t v' \} $$

return the set of all one-step successors of a set of consistent states.

The syntactic structure of an RPL program is given by: thread identifiers, control flow locations, values, resources, locals and program counter variables of the threads, proof variables, map $rsc$. A syntactic structure is just a tuple of basic mathematical objects (sets, variables, maps). It also exists independently of an RPL program.

3 Owicki-Gries-core proofs

3.1 Lattice of Owicki-Gries-core proofs

Now we formalize the core of the Owicki-Gries proof system. We abstract away from the details of logic, handling sets of variable valuations instead of formulas.

Fix an arbitrary syntactic structure.

A program annotation $(I, M)$ consists of

- a resource invariant $I_r$ for each resource $r$, which is a set of valuations of proof variables of $r$,
- a control flow annotation $M_{p,t}$ for each control flow location $p$ and each thread $t$, containing valuations of data variables which are local to $t$ or which are proof variables of a resource held at $p$.

We say that a consistent state $v$ satisfies $I_r$ (resp. $M_{p,t}$), if the projection of $v$ to $\text{ProofVar}(r)$ (resp. to local data variables of $t$ and all proof variables of all resources in $rsc(p)$) is in $I_r$ (resp. in $M_{p,t}$).

A program annotation $(I, M)$ denotes the set of all consistent states $v$ such that

- for each resource $r$ which is available in $v$, the state $v$ satisfies $I_r$, and
- for each thread $t$, the state $v$ satisfies $M_{(pc_t),t}$.

We define $\gamma_{\text{OG}}(I, M)$ as the set of all consistent states denoted by $(I, M)$.

Now fix an arbitrary RPL program obeying the given syntactic structure.

An Owicki-Gries-core proof of the program is a program annotation that satisfies the following conditions.
It is sequentially consistent, which means the following: consider any transition \( v \rightarrow v' \) from a control flow location \( p \) to a control flow location \( p' \) such that \( v \) satisfies \( M_{p,t} \). There are three cases.

- The transition does not cross the border of a critical section. Then \( v' \) should satisfy \( M_{p',t} \).
- The transition starts a critical section of a resource \( r \). Additionally, assume that \( v \) satisfies \( I_r \). Then \( v' \) should satisfy \( M_{p',t} \).
- The transition finishes a critical section of a resource \( r \). Then \( v' \) should satisfy both \( M_{p',t} \) and \( I_r \).

It admits the initial states, i.e., denotes a superset of \( \text{init} \).

These Hoare-style rules treat critical sections specially. First, on entering a critical section, we additionally assume the resource invariant. Second, on leaving a critical section, we should prove the resource invariant.

Every Owicki-Gries-core proof denotes an inductive invariant. A set of consistent states \( S \) is **Owicki-Gries-core provable** if there is an Owicki-Gries-core proof that denotes a subset of \( S \).

Interestingly, the set of program annotations of a fixed program forms a complete lattice with respect to componentwise inclusion order. Restricting this order to the set of Owicki-Gries-core proofs gives a complete lattice of Owicki-Gries-core proofs, even a Moore family. So each program has a unique smallest Owicki-Gries-core proof. This proof denotes the strongest Owicki-Gries-core-provable property. To investigate the power of the method, we will look at the smallest Owicki-Gries-core proofs and strongest Owicki-Gries-core-provable properties.

### 3.2 Examples

Now we will look at examples of programs with their smallest Owicki-Gries-core proofs. On Readers-Writers, as well as for a whole class of similarly simple programs, all proof methods will have the same precision, on Upper all proof methods will have different precision and on the class SepThreads no precision loss will be observed at all.

We will use Owicki-style notation. In particular, “\( \text{resource control}(ww, ar, aw) \)” means that the resource named \( \text{control} \) contains exactly \( ww, ar \) and \( aw \).

**Example 1 (Readers-Writers).** A number of threads share a file simultaneously: \( n > 1 \) need reading access and \( m > 1 \) writing access. Any number of readers may access the file simultaneously, but a writer must have exclusive access. In Fig. 2, all the data variables range over nonnegative integers by default, subtracting a positive value from 0 blocks.
The strongest Owicki-Gries-core-provable property is

\[
\{v \in \text{ConsState} \mid v(ww), v(ar) \in \mathbb{N}_0 \land v(aw) \in \{0, 1\} \\
\land \forall i \in \{1, \ldots, n\}: \quad \langle v(pc_{\text{reader}, i}) \rangle \in \{\text{read, read} \mid x \in \{\text{start, finish}\} \\
\land y \in \{A, B, C\}\} \land v(pc_{\text{reader}, i}) = \text{startread}B \Rightarrow v(ww) = 0 \\
\land v(pc_{\text{reader}, i}) = \text{startread}C \Rightarrow v(ww) = 0 < v(ar) \}
\land \forall j \in \{1, \ldots, m\}: \quad \langle v(pc_{\text{writer}, j}) \rangle \in \{\text{write, write} \mid x \in \{\text{ask, start, finish}\} \\
\land y \in \{A, B, C\}\} \land v(pc_{\text{writer}, j}) = \text{askwrite}C \Rightarrow v(ww) > 0 \\
\land v(pc_{\text{writer}, j}) = \text{startwrite}B \Rightarrow v(ar) = v(aw) = 0 \\
\land v(pc_{\text{writer}, j}) = \text{startwrite}C \Rightarrow v(ar) = 0 < v(aw) \\
\land v(pc_{\text{writer}, j}) = \text{finishwrite}C \Rightarrow v(aw) = 0\}. \]
There are states in this set in which more than one writer is at write. Thus no Owicki-Gries-core proof can show that a writer has exclusive access. The smallest Owicki-Gries-core proof can prove a slightly weaker property, namely that the value of $aw$, which tracks the number of writers, never exceeds 1.

Example 2 (Upper). The program Upper in Fig. 3 will be used for showing differences between the Owicki-Gries-core proofs and the upper bound later. The range of the data variables is $\{0,1\}$. The computation is trivial: no thread can make a step. The majority of the program text serves to create a particular distribution of variables into locals and resources. There are exactly two reachable states, namely the initial ones. The smallest

<table>
<thead>
<tr>
<th>Initially $u \neq z = x = y = l$</th>
<th>resource $r(u,z), r'(x,y)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>// Thread 1</td>
<td>// Thread 2</td>
</tr>
<tr>
<td>A: ${l = x}$</td>
<td>0: ${y = z}$</td>
</tr>
<tr>
<td>B: ${l = x = u \neq z}$</td>
<td>assume false;</td>
</tr>
<tr>
<td>with $r$ when $l = u$ do</td>
<td>P: with $r'$ do</td>
</tr>
<tr>
<td>C: ${y \geq l = x = u \neq z}$</td>
<td>Q: $x := 0$</td>
</tr>
<tr>
<td>D: ${y \geq l = u \neq z \wedge x = 0}$</td>
<td>R: endwith;</td>
</tr>
<tr>
<td>master;</td>
<td>S: with $r$ do</td>
</tr>
<tr>
<td>E: ${l = u \neq z \wedge x = 0}$</td>
<td>T: $u := 0$</td>
</tr>
<tr>
<td>assume false</td>
<td>U: $z := 0$</td>
</tr>
<tr>
<td>F: endwith;</td>
<td>V: endwith;</td>
</tr>
<tr>
<td>G: with $r'$ do</td>
<td>W:</td>
</tr>
<tr>
<td>H: $x := 0$</td>
<td></td>
</tr>
<tr>
<td>I: endwith;</td>
<td></td>
</tr>
<tr>
<td>J: with $r$ do</td>
<td></td>
</tr>
<tr>
<td>K: $u := 0$</td>
<td></td>
</tr>
<tr>
<td>L: endwith;</td>
<td></td>
</tr>
<tr>
<td>M: $l := 0$</td>
<td></td>
</tr>
<tr>
<td>N:</td>
<td></td>
</tr>
</tbody>
</table>

Fig. 3: Program Upper and its smallest Owicki-Gries-core proof. Control flow locations following “assume false” are annotated by \{false\} by default.

Owicki-Gries-core proof denotes many more states, e.g., $[u \mapsto 0, z \mapsto 1, x \mapsto 0, y \mapsto 1, l \mapsto 0, pc_1 \mapsto k, pc_2 \mapsto 0]$.

Example 3 (Simple). A program belongs to the class Simple if it has at most one resource, and if the resource exists, then it contains no local variables and all its proof variables belong to the resource. Readers-Writers is a family of programs from Simple.

Example 4 (SepThreads). The class SepThreads (Separate Threads) consists of all programs that have no resources and whose initial states are exactly those that satisfy
the initial conditions of all the threads (a proper subset of such states is disallowed). For such programs the smallest Owicki-Gries-core proof denotes the set of reachable states.

4 Owicki-Gries core as abstract interpretation

4.1 Owicki-Gries-core proofs are the post-fixpoints of a sound abstract successor map

Our first step to try to give a measure of the precision of the Owicki-Gries core will be to cast it in the abstract interpretation framework. An Owicki-Gries-core proof is clearly an abstraction of the set of reachable states of a program. So we will give a characterization of Owicki-Gries core as a post-fixpoint of a sound abstraction of the successor map post of an RPL program. The map mimics the application of the Owicki-Gries-core proof conditions.

For a program annotation \((I, M)\), we define the sound Owicki-Gries-core abstract successor map \(\text{post}^{\#}_{\text{OG}}(I, M) = (I', M')\), which applies the sequential consistency once:

- \(I'_r\) is the smallest superset of \(I_r\) that contains all valuations \(w\) of proof variables of \(r\) such that there is a transition \(v \rightarrow v'\) (for some thread \(t\)) that exits a critical section for \(r\), \(v\) satisfies \(M_{v(pc)t}\), and \(w\) equals the projection of \(v'\) on the proof variables of \(r\);
- \(M'_{p't}\) is the smallest superset of \(M_{p't}\) that contains all valuations \(w\) of local data variables of thread \(t\) and proof variables of resources held at location \(p'\) such that there is a transition \(v \rightarrow v'\) such that \(v\) satisfies \(M_{v(pc)t}\), \(v\) satisfies \(I\), if the transition starts a critical section for \(r\), \(v'(pc)=p'\), and \(w\) equals the projection of \(v'\) to local data variables of \(t\) and to the proof variables of resources held at \(p'\).

This operator is, as the name says, sound with respect to the successor map.

Let \((I^{\text{init}}, M^{\text{init}})\) be the annotation describing the initial states only:

- \(I^{\text{init}}\) is the set of all valuations of proof variables of \(r\) in the initial states;
- \(M^{\text{init}}_{p't}\) is the set of valuations of local data variables of thread \(t\) in the initial states.

The Owicki-Gries-core abstract transformer \(F^{\#}_{\text{OG}}(I, M)\) is constructed as the pointwise union of \((I^{\text{init}}, M^{\text{init}})\) and \(\text{post}^{\#}_{\text{OG}}(I, M)\). The set of post-fixpoints of \(F^{\#}_{\text{OG}}\) coincides with the set of Owicki-Gries-core proofs; thus the following theorem holds.

**Theorem 5 (Equivalence).** The least fixpoint of \(F^{\#}_{\text{OG}}\) is the smallest Owicki-Gries-core proof.

4.2 Characteristic closures for Owicki-Gries core?

An elegant way of describing the precision of an approximation of a semantics given in fixpoint form is through the use of closures. A closure \(\rho\) is a monotone operator that is idempotent (\(\rho(\rho(x)) = \rho(x)\)) and extensive (\(\rho(x) \geq x\)). Given a concrete domain \((D, \leq)\) and a monotone function \(F: D \rightarrow D\), the closure \(\rho\) on \(D\) defines an approximation of the concrete semantics \(\text{lfp}(F)\) in the sense that \(\text{lfp}(F) \leq \text{lfp}(\rho \circ F)\). Such a description shows the actual loss of information, as the fixpoints of the closure are exactly the abstract elements that describe the approximation, and applying the closure to one concrete element exactly shows what information is lost for that element.
In our case, we have a concrete domain of sets of consistent states ordered by inclusion, and the semantics is given as the least fixpoint of the successor map \( \text{post} \) over the initial states. Then we exhibited an approximation \( \text{post}^{\alpha}_{OG} \) of that successor map. In order to describe its precision, it would be nice to find a closure \( \rho \) such that \( \text{post}^{\alpha}_{OG} \) is exactly the best transformer for \( \rho \circ \text{post} \). Finding one closure for each program is not difficult (just take the closure with two fixpoints, one being the strongest Owicki-Gries-core-provable property and the other the set of all consistent states), but this would not be very informative. Instead, because the concrete domain is entirely fixed by the syntactic structure of the program, we would like to find a \( \rho \) that would be fixed for a given syntactic structure. Alas, the next section shows that it is not possible in general.

5 Absence of equivalent characterizations by closures

The main result of this section is unfortunately negative: assuming we start from a reachable state semantics, there is no way to describe the strongest Owicki-Gries-core proof for a given syntactic structure using closures.

**Theorem 6 (No Equivalence).** There is a syntactic structure such that for consistent states defined through the syntactic structure and the concrete domain being the powerset of consistent states, there is no closure \( \rho \) on the powerset of consistent states such that for any multithreaded program having the given syntactic structure and for any property \( S \) of consistent states we have

\[
S \text{ is Owicki-Gries-core provable } \iff \text{lfp}(\lambda x. \rho(\text{init} \cup \text{post}(x))) \subseteq S.
\]

One such syntactic structure is given by program Upper from Example 2.

In fact, we can prove an even stronger property, as the proof requires only that \( \rho \) is monotone. Even more, the same proof holds even if we restrict the validity of the equivalence to a given transition relation:

**Theorem 7.** Under the same syntactic structure as in Thm. 6, there is no family of monotone maps \( \Xi \) indexed by transition relations, such that \( \Xi \) preserves least fixpoints \((\forall \text{ transition relations } \tau_1, \tau_2: \text{lfp}(\tau_1) = \text{lfp}(\tau_2) \Rightarrow \text{lfp}(\Xi_{\tau_1}) = \text{lfp}(\Xi_{\tau_2}))\), and for any property \( S \) of consistent states we have

\[
S \text{ is Owicki-Gries-core provable } \iff \text{lfp}(\Xi_{\text{init}, \text{post}(x)}) \subseteq S.
\]

Theorem 6 shows that if we start by approximating traces by states and wish to describe the Owicki-Gries-core proof system using closures, we can only hope for bounds framing the proof system. We will provide such bounds in the next two sections. If we are willing to work with closures on sets of traces instead of sets of states, it might be possible to find some equivalence. But such an equivalence cannot be obtained directly by collecting the states of traces obtained from abstract interpretation with a closure. Let \( \tilde{\alpha} \) be the abstraction which associates to a set of traces the set of consistent states appearing in the traces.
Theorem 8. Under the same syntactic structure as in Thm. 6, there is no monotone operator \( \tilde{\rho} \) on the powerset of traces of consistent states such that for any multithreaded program having the given syntactic structure, set of initial traces \( \tilde{\text{init}} \) and the trace extension operator post and for any property \( S \) of consistent states we have

\[
S \text{ is Owicki-Gries-core provable } \iff \tilde{\alpha}(\text{lfp}(\lambda x. \tilde{\rho}(\tilde{\text{init}} \cup \tilde{\text{post}}(x)))) \subseteq S.
\]

6 Upper bound on precision

Now we will show a closure operator such that the best abstract interpretation of the program with this approximation allows proving a larger set of properties than those provable by the Owicki-Gries core. The approximation will depend only on the syntactic structure, but not on the exact transition relation of a program.

Definition 9 (Owicki-Gries-core annotation closure). For a given syntactic structure, let \( \rho(Q) \) be the approximation defined as the set of consistent states \( v \) such that:

\begin{itemize}
  \item if a resource \( r \) is available in \( v \), then there is some other state in \( Q \) that coincides with \( v \) on the proof variables of \( r \) and in which \( r \) is available;
  \item and for any thread \( t \) there is a state in \( Q \) that coincides with \( v \) on local variables (including the program counter) of \( t \) and on the proof variables of the resources held by \( t \) in \( v \).
\end{itemize}

Then \( \rho \) is a closure on the powerset of consistent states. We call it the Owicki-Gries-core annotation closure.

The reason why we call this closure an Owicki-Gries-core annotation closure is because it is the closure corresponding to the Galois connection defined by \( \gamma_{OG} \) (which gives the set of consistent states denoted by a program annotation).

Now fix an arbitrary program and let \( \rho \) be defined by its syntactic structure.

Theorem 10 (Upper bound). Abstract interpretation with \( \rho \) is at least as strong as the Owicki-Gries core. Formally:

\[
\text{lfp}(\lambda x. \rho(\text{init} \cup \text{post}(x))) \subseteq \text{the strongest Owicki-Gries-core-provable property}.
\]

From the high-level view, the best transformer using this closure is capable of taking into account global computation instead of local successor computation in the Owicki-Gries core. It is as if before checking sequential consistency we take into account annotations not only of one thread, but of all the threads, gaining precision.

Furthermore, the Owicki-Gries-core annotation closure shows where the information is always lost. For instance, if a syntactic structure says that locals are disjoint among themselves and from all the proof variables of the resources, and if two states outside of critical sections are given, then any combination of the locals and resource variables of those states is in the approximation of those two states.
Example 11 (Readers-Writers). For the program Readers-Writers from Example 1 the least fixpoint of $\text{lfp}(\lambda x. \rho(\text{init} \cup \text{post}(x)))$ coincides with the strongest Owikki-Gries-core-provable property. This property is coarser than the set of reachable states. For example, in one execution $\text{writer}_1$ can reach $\text{write}$, in another execution $\text{writer}_2$ can reach $\text{write}$, and the initial state satisfies $\text{w} = \text{r} = \text{w} = 0$, so $\rho$ produces a combined state where both writers are at $\text{write}$, other threads are at their initial locations and all data variables have value 0. Thus, no Owikki-Gries-core proof can restore the dependency between the threads and prove mutual exclusion between the writers.

Example 12 (Upper). For the program Upper from Example 2 abstract interpretation with $\rho$ produces the set of reachable states, which is properly included into every Owikki-Gries-core-provable property. The reason for this discrepancy is that locals of one thread and resources held by a different thread overlap. Such an overlap constrains the output of $\rho$, but not an Owikki-Gries-core proof. Considering such overlaps actually improves precision!

Example 13 (Simple). For the programs of the class Simple abstract interpretation with $\rho$ produces the same result as the smallest Owikki-Gries-core proof. The reason, as we will see, is that abstract interpretation with the lower bound will produce the same result as abstract interpretation with the upper bound.

Example 14 (SepThreads). For the programs of the class SepThreads of Example 4 abstract interpretation with $\rho$ produces the same result as the smallest Owikki-Gries-core proof. The reason is that the smallest Owikki-Gries-core proof already denotes the set of reachable states.

7 Lower bound on precision

Now we will show a nontrivial Cartesian-like closure such that abstract interpretation with this closure can prove only properties weaker than or equal to the strongest Owikki-Gries-core-provable property. In fact, we will even show two such closures. One closure (namely $\bar{\rho}$) will describe a better lower bound, while the other (namely $\rho_c$) is easier to comprehend.

The definitions of both bounds require some preparation.

For a family of sets $\mathcal{X} = \{X_1, \ldots, X_n\}$, let $\text{Part}(\mathcal{X})$, called partition of $\mathcal{X}$, be the set of all nonempty $Y_1 \cap \cdots \cap Y_n$ where each $Y_i$ is either $X_i$ or its complement $(\bigcup \mathcal{X}) \setminus X_i$ ($1 \leq i \leq n$). Elements of a partition are called blocks.

Let us fix an arbitrary syntactic structure. Our lower bounds will depend on the syntactic structure but be the same for all the programs that obey this syntactic structure. Let $RL$ be the family of sets containing all resources $r$ and all sets of locals $\text{Local}_t$ for all threads $t$ as elements. Let $\overline{RL}$ be the partition of $RL$.

For example, for the syntactic structure of Upper the set $RL$ has exactly four elements: the locals of the first thread $\{t, x, p_{c_1}\}$, the locals of the second thread $\{y, z, p_{c_2}\}$, the resource $r = \{u, z\}$, and the resource $r' = \{x, y\}$. The corresponding partition has exactly six blocks: $\{u\}, \{x\}, \{y\}, \{z\}, \{t, p_{c_1}\}, \{p_{c_2}\}$. 

7.1 Simple cartesian closure

The simpler approximation is defined as follows.

**Definition 15 (Cartesian closure).** Given a set of consistent states \( Q \), the Cartesian approximation \( \rho_c \) returns all the consistent states from the product of projections of \( Q \) onto the blocks in \( RL \).

In other words, \( \rho_c(Q) \) contains exactly those consistent states \( v \) such that for each block there is a state \( \tilde{v} \in Q \) that agrees with \( v \) on the variables of the block. We call this approximation *Cartesian*, since it is similar to the closure that can be derived from the Cartesian pair of adjoint maps from [10], p. 172. As the name says, \( \rho_c \) is a closure.

This approximation breaks all the dependencies between the blocks and retains all dependencies inside a block.

For example, for the syntactic structure of the program Upper the variables \( l \) and \( pc_1 \) belong to the same block. Thus, if in a set of states every state at some fixed control flow location satisfies \( l = 0 \), each state from the Cartesian approximation of this set will also satisfy \( l = 0 \) for that control flow location.

Abstract interpretation with \( \rho_c \) generates a property which is always weaker than or equal to the strongest Owicki-Gries-core-provable property.

7.2 More precise lower bound closure

The following definition strengthens \( \rho_c \) in two ways. Firstly, we impose restrictions on \( \tilde{v} \) from the definition of \( \rho_c \). Such restrictions will depend on the block. Secondly, we look at the prophecy variables: those are variables which are never written and which don’t belong to a resource. Prophecy variables form a separate block; now we restore all the dependencies between this block and those locals of any thread that are not resource variables.

**Definition 16 (Lower Bound closure).** Given a set of consistent states \( Q \), its approximation \( \bar{\rho}(Q) \) contains exactly those consistent states \( v \) such that both of the following conditions are satisfied.

- For every block in \( RL \) that is contained in a resource,
  * if the resource is available in \( v \), then there is some \( \tilde{v} \in Q \) in which the resource is also available
  * and which coincides with \( v \) on the block;
  * if some thread holds the resource in \( v \), then there is some \( \tilde{v} \in Q \) which coincides with \( v \) on all the variables
  * that are local to this thread but do not belong to any resource, or
  * that belong to the block.

- For every thread there is a state in \( Q \) that coincides with \( v \) on each variable
  * that is a local variable of the thread but
  * does not belong to any resource.
As the name says, $\bar{\rho}$ is a closure. It is at least as precise as $\rho_c$. Both closures do not depend on the exact transition relation of a program. The closure $\bar{\rho}$ induces the tightest lower bound we could prove. It shows the dependencies that are always retained, creating a basis for the construction of future refinement algorithms (possibly following [20]).

Now fix an arbitrary RPL program that has the assumed syntactic structure.

The proof of the lower bound relies on several claims about the strongest property provable by abstract interpretation with $\bar{\rho}$. The following claim is the most important one.

**Lemma 17.** Let $Q$ be the strongest property provable by abstract interpretation with $\bar{\rho}$. Consider a transition of a thread $t$ from a consistent state $v$ to a consistent state $v'$, let the transition start a critical section. Let $\tilde{v} \in Q$ such that $v$ agrees with $\tilde{v}$ on the locals of $t$ and on the variables of the resources held by $t$ before the transition. Let $\hat{v} \in Q$ such that $v$ agrees with $\hat{v}$ on the variables of the resource being acquired. Then there is a state in $Q$ that agrees with $v'$ on the locals of thread $t$ and on the variables of the resources held by the thread after the transition.

The lower bound theorem follows from the lemma.

**Theorem 18 (Lower bound).** The core of Owicki-Gries can prove at least as many properties as abstract interpretation with $\bar{\rho}$ or $\rho_c$. Formally:

$$\text{the strongest Owicki-Gries-core–provable property} \subseteq \text{lfp}(\lambda x. \bar{\rho}(\text{init} \cup \text{post}(x)))$$

$$\subseteq \text{lfp}(\lambda x. \rho_c(\text{init} \cup \text{post}(x))) .$$

**Example 19 (Readers-Writers).** For the program Readers-Writers from Example 1 abstract interpretation with $\rho_c$ produces the set of all consistent states where readers are at ...read..., writers are at ...write..., and $ww$, $ar$, $aw$ are nonnegative. The Owicki-Gries core and abstract interpretation with $\bar{\rho}$ can prove stronger properties, e.g., that at location askwriteC the value of $ww$ is positive. Intuitively, when a resource is busy, Cartesian abstraction always breaks the dependency between the resource variables and the control flow, while $\bar{\rho}$ and the Owicki-Gries core sometimes retain the dependency.

**Example 20 (Upper).** For the program Upper from Example 2 abstract interpretation using either $\rho_c$ or $\bar{\rho}$ produces the same result: the set of all states such that the first thread is at any location between A and E, the second thread is at 0 and all data variables take arbitrary values from $\{0, 1\}$. The Owicki-Gries core can prove stronger properties; for instance, it can show that at location E the value of $x$ is zero. Intuitively, the dependency between resource variables and control flow is always broken in Cartesian abstraction but is sometimes retained in the Owicki-Gries core.

**Example 21 (Simple).** For the programs from the class Simple from Example 3 the approximations $\bar{\rho}$ and $\rho$ are so close to each other that abstract interpretations with both produce the same property. Since they define the lower and upper bounds on the precision of the Owicki-Gries core, the Owicki-Gries core can prove exactly the same properties as those provable by abstract interpretation with any of the two approximations. If a program from Simple does not have the empty resource, then $\bar{\rho}$ and $\rho$ coincide exactly, approximating a set of states $Q$ by the set of all consistent states $v$ such that both of the following conditions hold.

13
If there is a resource and it is available in \( v \), there is some state in \( Q \) that coincides with \( v \) on the resource and in which the resource is available.

For each thread there is a state in \( Q \) which coincides with \( v \) on the variables of the thread and, if the resource is present and is held, on the variables of the resource.

**Example 22 (SepThreads).** For the programs from the class SepThreads from Example 4 the approximations \( \bar{\rho} \) and \( \rho \) coincide. Since they define the lower and upper bounds on the precision of the Owicki-Gries core, the Owicki-Gries core can prove exactly the same properties as those provable by abstract interpretation with any of the two approximations. Due to the absence of any thread interactions and independence of initial states of the threads, the mentioned methods can prove the strongest inductive property, namely the set of states reachable from the initial ones. Informally spoken, all dependencies between the locals of each thread are retained.

### 8 Related work

Historically, conditional critical regions were introduced in [16]. The thesis [25] of Owicki and her paper with Gries [26] describe the original proof method for RPL. Modular reasoning about RPL has not been characterized in terms of abstract interpretation via closures [8] so far.

For general multithreaded programs (i.e. without separation of data into resources), Owicki-Gries-style reasoning without auxiliary variables is equivalent to multithreaded Cartesian abstraction. The result was first mentioned without proof in [11], and the proof appears in [20].

Clarke [6] has considered a subset of integer RPL programs with only one resource, where, roughly, only additions of constants inside the critical sections are allowed, and the property to be checked is either mutual exclusion of PV-semaphores or deadlock freedom. With a predefined choice of integer auxiliary variables, the least fixpoint of a particular functional is a resource invariant that precisely tells whether the property holds or not. Two overapproximations are given: a fixed-formula resource invariant and an invariant computed by a polyhedral analysis with widening. Our work, on the contrary, does not impose any restrictions on the program form. Our results hold for even more programs than the RPL ones, e.g., where the critical sections are not well-nested.

The work of Owicki on RPL is the basis of a variety of modular programming languages equipped with proof methods of different degrees of completeness and automation.

Concurrent separation logic (CSL) [24] equips RPL with separation logic as a formula language. CSL is also incomplete without the rule of auxiliary variables, so the question of precision arises. Removing secondly important features of CSL for the sake of clarity (as in [5]) and considering variables in the heap makes our lower bound also apply to such CSL versions.

Chalice [19] is a language for verification of object-oriented concurrent programs with heap, equipped with an RPL-like proof system. Due to the powerful permission system, the proof system is in general stronger than that of Owicki, so our lower bound
on precision carries over to Chalice for programs that can be directly represented both
in RPL and in Chalice.

VCC [23] is a verifier for multithreaded C. When accessing structures in a lock-based
manner, VCC requires the user to provide invariants of C structs. On obtaining
ownership of a structure, the resource invariant is assumed; on relinquishing
ownership, the resource invariant has to be reestablished. Ghost contracts of lock-
manipulating functions control the ownership transfer. Our lower bound applies to VCC
as well.

9 Discussion

9.1 Challenges

Discussing the precision loss reveals several open problems.

Example 20 shows a gap between the accuracy of the Owicki-Gries core and the
lower bound. Can the lower bound closure be strengthened?

The main inequivalence result assumes that the concrete domain is the powerset of
consistent states. For the powerset of traces, we only know inequivalence for a subclass
of abstract interpretations. Is there an exact characterization of the Owicki-Gries core
by abstract interpretation on the powerset of traces?

We have shown what variable dependencies does the Owicki-Gries core break. Can
these dependencies be restored on demand? Is there an automatic counterexample-
guided abstraction refinement of the Owicki-Gries core, perhaps based on auxiliary
variables [7], unions of Cartesian products [20], or abstract threads [18]?

Can one characterize the precision loss of the Owicki-Gries core by completeness
notions of [15]?

Can one formalize CSL in abstract interpretation in a way that would reveal the
involved approximation?

9.2 Conclusion

We have examined a modular method (Owicki-Gries core) for proving safety properties
of a widely-used class of multithreaded programs.

The considered class contains structured programs in which shared data are par-
titioned into resources and are accessed only in critical sections that ensure mutually
exclusive access to resources. The method provides a clean basis for other more so-
phisticated proof methods like Concurrent Separation Logic, Chalice, or VCC. The
Owicki-Gries core is polynomial in the number of threads, but without manually adding
auxiliary variables it cannot prove many properties of concurrent programs.

The Owicki-Gries core is, intuitively, expected to succeed for properties whose de-
pendence on thread coupling is low, and is expected to fail if complicated thread inter-
actions have to be analyzed. We have made this notion precise, providing a characteriza-
tion of the set of Owicki-Gries-core-provable properties. We have demonstrated an ab-
stract transformer corresponding to the Owicki-Gries core: the least fixpoint of the ab-
stract transformer denotes exactly the strongest Owicki-Gries-core-provable property.
To quantify the loss of precision inherent to modularity, we have provided a superset and a subset of Owicki-Gries-core-provable properties, described by abstract interpretations with closure operators that depend on the syntactic structure of the program only. These bounds coincide for a class of simple programs. We have also shown a principal inability to provide an exact characterization of the set of properties in terms of closures that depend only on the syntactic structure.

10 Acknowledgements

We thank Byron Cook and Microsoft Research Cambridge for support in the initial stages of the work. The work was also partially supported by the Verisoft project of the German science foundation DFG. We thank Josh Berdine and Viktor Vafeiadis for helpful comments and discussions.

References

A RPL

We formalize RPL (restricted programming language) of [25] as a transition system as follows.

A syntactic structure is a tuple

\[(Tid, PL, Val, Res, (Local_t, pc_t)_{t \in Tid}, ProofVar, rsc)\]

where all the following conditions hold.

- \(Tid, PL, Val\) are any sets with \(PL \subseteq Val\).
- \( \text{Res} \) is a set\(^1\) of disjoint\(^2\) sets.
- For each \( t \in \text{Tid} \) we have \( pc_t \in \text{Local}_t \setminus \cup \text{Res} \).
- For all different \( t, \bar{t} \in \text{Tid} \) we have \( pc_t \not\in \text{Local}_{\bar{t}} \).
- \( \text{ProofVar} : \text{Res} \to \wp(\text{Datavar}) \) is extensive, where \( \wp \) is the powerset symbol, \( \text{PCVar} = \{ pc_t \mid t \in \text{Tid} \} \) and \( \text{Datavar} = \cup \text{Res} \cup \cup_{t \in \text{Tid}} \text{Local}_t \setminus \text{PCVar} \).
- \( \text{rsc} : \text{PL} \to \wp(\text{Res}) \). Notice that \( \text{rsc} \) is independent\(^3\) of \( \text{Tid} \).

The elements of \( \text{ProofVar}(r) \) are called \text{proof variables}\(^4\) of a resource \( r (r \in \text{Res}) \). Given a syntactic structure as above, let \( \text{Var} = \cup \text{Res} \cup \cup_{t \in \text{Tid}} \text{Local}_t \). A \text{consistent state} is an element of

\[
\text{ConsState} = \{ v \in \text{Var} \to \text{Val} \mid \forall t \in \text{Tid} : v(pc_t) \in \text{PL} \text{ and } \forall \bar{t} \in \text{Tid} \setminus \{ t \} : \text{rsc}(v(pc_t)) \cap \text{rsc}(v(pc_{\bar{t}})) = \emptyset \}.
\]

A resource \( r \) is held by \( t \in \text{Tid} \) if \( r \in \text{ConsState} \). A resource \( r \) is busy in \( v \in \text{ConsState} \) if \( r \in \cup_{t \in \text{Tid}} \text{rsc}(v(pc_t)) \), otherwise \( r \) is available in \( v \).

The restriction of a map \( w \) to a set \( V \) is \( w|_V = \{ (a, b) \in w \mid a \in V \} \). Two maps \( v, w \) coincide on a set \( V \), written \( v \sim_v w \), if \( v|_V = w|_V \).

An \text{RPL transition system obeying a syntactic structure} as above is a tuple

\[
(\text{init}, (\rightarrow_t)_{t \in \text{Tid}})
\]

such that \( \text{init} \subseteq \text{ConsState} \), for all \( t \in \text{Tid} \) we have \( \rightarrow_t \subseteq \text{ConsState} \) \( \land \forall v \in \text{init} : \text{rsc}(v(pc_t)) = \emptyset \), and all the conditions below hold:

- for all \( x \in \text{Datavar} \) and \( t \in \text{Tid} \) we have

\[
\forall t \in \text{Tid} \setminus \{ t \} , (v, v') \in \rightarrow_t : v(x) = v'(x) \Rightarrow x \in \text{Local}_t ;
\]

- for all \( r \in \text{Res} \) we have

\[
\text{ProofVar}(r) = \left\{ x \in \text{Datavar} \mid \forall t \in \text{Tid} , (v, v') \in \rightarrow_t : \left( v(x) = v'(x) \right. \left. \lor r \in \text{rsc}(v(pc_t)) \cap \text{rsc}(v'(pc_t)) \right) \right\} ;
\]

- for all \( t \in \text{Tid} , (v, v') \in \rightarrow_t , R = \text{rsc}(v(pc_t)) , R' = \text{rsc}(v'(pc_t)) , R = \text{Res} \setminus (R \cup R') \) all the following conditions hold:

\(^1\) In her thesis, Owicki did not explicitly forbid resources that do not protect any variables, though she mentions no examples with such empty resources. We explicitly allow them. However, we introduce a restriction: in our formulation, the empty resource, if it exists, should be unique. We don’t consider this restriction important: we have never come across meaningful academic or real-life programs with empty resources.

\(^2\) Following Owicki, we consider the general case, allowing nonempty intersection between any element of \( \text{Res} \) and any \( \text{Local}_t (t \in \text{Tid}) \). If we enforced mutual disjointness between all \( r \in \text{Res} \) and all \( \text{Local}_t (t \in \text{Tid}) \), we would get a tighter lower bound, but only because the proof system would get weaker.

\(^3\) This way of modeling turned out to be simpler than, say, making control flow locations of different threads disjoint, or making \( \text{rsc} \) dependent on the thread.

\(^4\) Owicki described \text{ProofVar} as a proof-related notion. Since proof variables of a resource capture a syntactic property of the transition relation of a program, we view proof variables as a syntactic notion, despite their name. A lightweight presentation [26] omits the notion of proof variables, obtaining a simpler but significantly weaker proof system.
For an RPL transition system $T$:

(1) $v \in \mathbb{L}_{\text{init}}(1) \text{Local}_i V'$
(2) $v \in \mathbb{L}_R V'$
(3) $R \neq R' \Rightarrow v \notin \mathbb{W}_R(V)$
(4) For all $w \in \text{ConsState}$, if $v \in (\text{Local}_i \cup R) w$ and $\forall r \in R' \setminus R : r \notin \mathbb{rsc}(w(\text{PCVar}))$, then there is some $w'$ such that $w \rightarrow_i w'$ and $v \in (\text{Local}_i \cup R) w'$
(5) $(R \setminus R') \cup (R' \setminus R) \leq 1$

**Remark 23.** Notice that in (4), $w'$ additionally satisfies $w' \in \text{ConsState}$ and $(v \in \mathbb{W}_R(V) \Rightarrow v' \in \mathbb{W}_R(V))$.

**Proof.** Follows from $\rightarrow_i \subseteq \text{ConsState}^2$ and $v' [\text{by (2)}] \approx \mathbb{W}_R(V) [\text{by assumption}]$.

Fix an RPL transition system as above. A set of states is mapped to a set of their successors by the function

$$\text{post} : \mathbb{P}(\text{ConsState}) \rightarrow \mathbb{P}(\text{ConsState}), \quad S \mapsto \{ v' \mid \exists v \in S, t \in \text{Tid} : v \rightarrow_i v' \}.$$ 

The goal of verification is, given a set of states $\text{safe} \subseteq \text{ConsState}$, to prove that

$$\text{lfp}(\lambda S, \text{init} \cup \text{post}(S)) \subseteq \text{safe}.$$ 

## B Owicki-Gries for RPL

Fix a syntactic structure $(\text{Tid}, \text{PL}, \text{Val}, \text{Res}, (\text{Local}, \text{pc})_{r \in \text{Tid}}, \text{ProofVar}, \text{rsc})$ for the whole section B.

### B.1 Definition of Owicki-Gries core

For each $t \in \text{Tid}$ let $\text{LocalDataVar}_t = \text{Local}_i \setminus \{ \text{pc}_t \}$ be the set of local data variables. A program annotation is an element of

$$PA = \prod_{r \in \text{Res}} ((\text{LocalDataVar}_t \cup \text{ProofVar}(\text{rsc}(p))) \rightarrow \text{Val}).$$

A program annotation $P$ denotes a set of states given by

$$\gamma_{\text{OG}}(P) = \{ v \in \text{ConsState} \mid \forall r \in \text{Res} \setminus \bigcup \text{rsc}(v(\text{PCVar})): v|_{\text{ProofVar}(r)} \in I_r \text{ and } \forall t \in \text{Tid} : v|_{\text{LocalDataVar}_t \cup \text{ProofVar}(\text{rsc}(v(\text{pc}_t)))} \in M_r(\text{pc}_t) \}.$$ 

For an RPL transition system $T = (\text{init}, (\rightarrow_i)_{r \in \text{Tid}})$ that obeys the given syntactic structure, an Owicki-Gries-core proof of $T$ is a program annotation $P := (I_r)_{r \in \text{Res}} (M_p)_{p \in \text{PL}}$ such that the following holds:
– sequential consistency: for all \( t \in \text{Tid} \), \((v, v') \in \to_r, p = v(pc_i), p' = v'(pc_i), R = rsc(p), R' = rsc(p')\), if

\[
v|_{\text{LocalDataVar} \cup \text{ProofVar}(R)} \in M_{p,t} \land \forall r \in R' \setminus R : v|_{\text{ProofVar}(r)} \in I_r,
\]

then

\[
v|_{\text{LocalDataVar} \cup \text{ProofVar}(R')} \in M_{p',t} \land \forall r \in R' \setminus R : v|_{\text{ProofVar}(r)} \in I_r;
\]

– initial condition: \( \text{init} \subseteq \gamma_{\text{OG}}(P) \).

An Owicki-Gries-core proof \( P \) proves a property \( \text{safe} \subseteq \text{ConsState} \) if \( \gamma_{\text{OG}}(P) \subseteq \text{safe} \).

### B.2 Lattice of Owicki-Gries-core proofs

The set of program annotations is ordered by pointwise inclusion:

\[
((I_r)_{r \in \text{Res}}, (M_{p,t})_{p \in \text{PL}, t \in \text{Tid}}) \subseteq ((I'_r)_{r \in \text{Res}}, (M'_{p,t})_{p \in \text{PL}, t \in \text{Tid}})
\]

iff \( \forall r \in \text{Res} : I_r \subseteq I'_r \) and \( \forall p \in \text{PL}, t \in \text{Tid} : M_{p,t} \subseteq M'_{p,t} \).

Then the least upper bound is the pointwise union \( \sqcup \), the greatest lower bound is a pointwise intersection \( \sqcap \), and the lattice is complete.

Consider the lattice

\[
D = \mathcal{P}(\text{ConsState}),
\]

ordered by inclusion. This lattice is certainly complete.

**Proposition 24.** \( \gamma_{\text{OG}} : \text{PA} \rightarrow D \) is a complete meet-morphism.

**Proof.** Let \( A \) be a set of program annotations and \(((I_r)_{r \in \text{Res}}, (M_{p,t})_{p \in \text{PL}, t \in \text{Tid}}) = \sqcap A \). We have to show that \( \gamma_{\text{OG}}(\sqcap A) \) and \( \sqcap \gamma_{\text{OG}}(A) \) coincide.

\( \subseteq \) : Let \( v \in \gamma_{\text{OG}}(\sqcap A) \). Then \( \forall r \in \text{Res} \setminus \bigcup rsc(v(\text{PCVar})) : v|_{\text{ProofVar}(r)} \in J_r \) and \( \forall t \in \text{Tid} : v|_{\text{LocalDataVar} \cup \text{ProofVar}(rsc(v(pc_i)))} \in N_{v(pc_i)}t \). The definition of \( \sqcap \) implies that for all \( B = ((I'_r)_{r \in \text{Res}}, (M'_{p,t})_{p \in \text{PL}, t \in \text{Tid}}) \subseteq A \) we have \( \forall r \in \text{Res} \setminus \bigcup rsc(v(\text{PCVar})) : v|_{\text{ProofVar}(r)} \in I'_r \) and \( \forall t \in \text{Tid} : v|_{\text{LocalDataVar} \cup \text{ProofVar}(rsc(v(pc_i)))} \in M'_{v(pc_i)}t \), i.e., \( v \in \gamma_{\text{OG}}(B) \). Since \( B \in A \) was arbitrary, we have \( v \in \sqcap \gamma_{\text{OG}}(A) \).

\( \supseteq \) : Let \( v \in \gamma_{\text{OG}}(B) \) for all \( B \in A \). Let \( r \in \text{Res} \setminus \bigcup rsc(v(\text{PCVar})) \). Then for each \( B = (I, M) \in A \) the definition of \( \gamma_{\text{OG}} \) gives \( v|_{\text{ProofVar}(r)} \in J_r \). Thus \( v|_{\text{ProofVar}(r)} \in J_r \). So \( \forall r \in \text{Res} \setminus \bigcup rsc(v(\text{PCVar})) : v|_{\text{ProofVar}(r)} \in J_r \). Now let \( t \in \text{Tid} \). For each \( B = (I, M) \in A \) the definition of \( \gamma_{\text{OG}} \) implies that \( v|_{\text{LocalDataVar} \cup \text{ProofVar}(rsc(v(pc_i)))} \in M_{v(pc_i)}t \); so \( N_{v(pc_i)}t \supseteq v|_{\text{LocalDataVar} \cup \text{ProofVar}(rsc(v(pc_i)))} \). Thus \( \forall t \in \text{Tid} : v|_{\text{LocalDataVar} \cup \text{ProofVar}(rsc(v(pc_i)))} \in N_{v(pc_i)}t \). We have shown \( v \in \gamma_{\text{OG}}(\sqcap A) \).

For the remainder of the subsection B.2, fix an RPL transition system \( T = (\text{init}, (\to_r)_{r \in \text{Tid}}) \) that obeys the given syntactic structure. Let \( \mathcal{D} \) be the set of Owicki-Gries-core proofs of \( T \). From \( \text{PA} \) it inherits the componentwise inclusion as the partial order, which we also denote by \( \subseteq \).
Theorem 25. \( (\mathcal{O}, \sqsubseteq) \) is a complete lattice with infimum being componentwise intersection \( \sqcap \).

Proof. Let \( A \) be a set of Owicki-Gries-core proofs. First we show that \( \bigcap A \) in \( PA \) is the infimum of \( A \) in \( \mathcal{O} \).

- Case \( A = \emptyset \). Let \( B = \bigcap_{(\text{ProofVar}(r) \to \text{Val}) \in \text{Res}, \{ (\text{LocalDataVar} \cup \bigcup_{r \in \text{Tid}} \text{ProofVar}(\text{rsc}(p))) \} \in \text{Val}_{p \in \text{Tid}} \} \). Certainly \( B \) is sequentially consistent. Since \( \gamma_{OG}(B) = \text{ConsState} \), \( B \) satisfies the initial condition. Thus \( B \in \mathcal{O} \). Notice that \( B \) is a lower bound of \( \emptyset \) and is greater than or equal to any other element of \( \mathcal{O} \). Thus \( B = \inf_{\mathcal{O}} \emptyset \).

- Case \( A \neq \emptyset \). Let \( B = \bigcap_{(I_t) \in \text{Res}, (M_{p,t}) \in \text{Tid}} = \bigcap A \). First we will show that \( B \) is an Owicki-Gries-core proof.

  Sequential consistency. Let \( t \in \text{Tid} \), \( (v, v') \in \gamma_{OG}, p = v (pC_t), p' = v' (pC_t), R = \text{rsc}(p), R' = \text{rsc}(p') \), \( v_{\text{LocalDataVar} \cup \text{ProofVar}(\text{rsc}(p))} \in M_{p,t} \) and \( \forall r \in R \setminus R' : v_{\text{ProofVar}(\text{rsc}(r))} \in L_r \).

  Then for all \( (J, N) \in A \) we have \( v_{\text{LocalDataVar} \cup \text{ProofVar}(\text{rsc}(p))} \in N_{p,t} \) and \( \forall r \in R \setminus R' : v_{\text{ProofVar}(\text{rsc}(r))} \in L_r \). Thus \( v_{\text{LocalDataVar} \cup \text{ProofVar}(\text{rsc}(p))} \in M_{p,t} \) and \( \forall r \in R \setminus R' : v_{\text{ProofVar}(\text{rsc}(r))} \in L_r \).

  Initial condition. For each \( P = ((I_t) \in \text{Res}, (M_{p,t}) \in \text{Tid}) \in A \) we have \( \text{init} \subseteq \gamma_{OG}(P) \).

  We have shown that \( B \in \mathcal{O} \). By definition \( B \) is less than or equal to any element of \( A \). Assume some other lower bound \( C \in \mathcal{O} \) for \( A \). Then \( C \subseteq P \) for each \( P \in A \), so \( C \) is less than or equal to the pointwise intersection over \( A \), i.e., \( C \sqsubseteq B \). Thus \( B \) is the greatest lower bound of \( A \) in \( \mathcal{O} \).

  We have shown that the greatest lower bound of any set of elements of the poset \( (\mathcal{O}, \sqsubseteq) \) exist. By Thm. 2 in Chap. 4 of [2] (alternatively Thm. 4.2 in [4]), \( \mathcal{O} \) is a complete lattice.

Notice that the infimum of \( \mathcal{O} \) is the tuple of empty sets iff \( \text{init} \) is empty; thus \( \mathcal{O} \) is a complete sublattice of \( PA \) only if \( \text{init} \) is empty. Usually verified programs have initial states, thus usually \( \mathcal{O} \) is not a complete sublattice of \( PA \).

In any case the least Owicki-Gries-core proof exists.

Corollary 26. The strongest Owicki-Gries-core provable property exists and is denoted by the smallest Owicki-Gries-core proof.

Proof. The set of Owicki-Gries-core-provable properties is \( \gamma_{OG}(\mathcal{O}) \). The infimum of this set is \( S := \bigcap \gamma_{OG}(\mathcal{O}) = \gamma_{OG}(\bigcap \mathcal{O}) \). Since \( \mathcal{O} \) is a complete lattice with pointwise intersection as infimum, \( \bigcap \mathcal{O} \in \mathcal{O} \). So \( S \) is itself Owicki-Gries-core provable. Notice that \( S \) is stronger than or equal to any other Owicki-Gries-core-provable property.

Proposition 27. Any Owicki-Gries-core proof denotes an inductive invariant:

\[
\forall P \in \mathcal{O}: \quad \text{init} \cup \text{post}(\gamma_{OG}(P)) \subseteq \gamma_{OG}(P).
\]
Proof. Let \((I, M) \in O\). We have to prove the following two claims.

"post \(\circ \gamma_{OG}(I, M) \subseteq \gamma_{OG}(I, M)\)". Let \(v' \in \text{post } \gamma_{OG}(I, M)\) and \(i \in \text{Tid}\) such that \(v \rightarrow_n v'\). Notice that by (1) we have \(v_{\langle pc_i \rangle}=v'_{\langle pc_i \rangle}\) for \(i \in \text{Tid} \setminus \{t\}\). Let \(R = \text{rsc}(v_{\langle pc_i \rangle})\) and \(R' = \text{rsc}(v'_{\langle pc_i \rangle})\). From \(v \in \gamma_{OG}(I, M)\) we get \(v_{\langle LocalDataV ar \cup ProofV ar \rangle} = M_{\langle pc_i \rangle} \ast R\). Now let \(r \in R' \setminus R\). From \(v \in \text{ConsState}\) and \(r \in \text{rsc}(v_{\langle pc_i \rangle})\) we get \(r \notin \bigcup_{i \in \text{Tid} \setminus \{t\}} \text{rsc}(v_{\langle pc_i \rangle}) = \{\text{since } v_{\langle pc_i \rangle} = v'_{\langle pc_i \rangle}\}\) for \(i \in \text{Tid} \setminus \{t\}\). Since \(r \notin R = \text{rsc}(v_{\langle pc_i \rangle})\), we conclude that \(r \notin \bigcup \text{rsc}(v_{\langle PCVar \rangle})\). Since \(v \in \gamma_{OG}(I, M)\), we obtain \(v_{\langle ProofV ar \rangle} \in I\). Thus \(v \in R' \setminus R: v_{\langle ProofV ar \rangle} \in I\) and \(\forall v \in R \setminus R': v_{\langle ProofV ar \rangle} \in I\).

Now we will show that \(v'\) is in \(\gamma_{OG}(I, M)\).

- Let \(r \in \text{Res} \setminus \bigcup \text{rsc}(v_{\langle PCVar \rangle})\). From \(i \in \text{Tid}\), \(v \rightarrow_n v'\) and the definition of \(ProofV ar\) we obtain that for all \(x \in ProofV ar\) we have \(v(x) = v'(x)\). So \(v_{\langle ProofV ar \rangle} = v'_{\langle ProofV ar \rangle}\). From (1) we know for \(i \in \text{Tid} \setminus \{t\}\) that \(v_{\langle pc_i \rangle} = v'_{\langle pc_i \rangle}\), thus \(\text{rsc}(v_{\langle pc_i \rangle}) = \text{rsc}(v'_{\langle pc_i \rangle})\) \(\notin r\). Consider two cases.

  - Case \(r \in \text{rsc}(v_{\langle pc_i \rangle})\). Then \(r \in R' \setminus R\). By the above, \(v_{\langle ProofV ar \rangle} \in I\).
  - Case \(r \notin \text{rsc}(v_{\langle pc_i \rangle})\). Then \(r \notin \bigcup \text{rsc}(v_{\langle PCVar \rangle})\). Thus \(v_{\langle ProofV ar \rangle} \in I\). Therefore \(v_{\langle ProofV ar \rangle} \in I\).

So \(\forall r \in \text{Res} \setminus \bigcup \text{rsc}(v_{\langle PCVar \rangle})\): \(v_{\langle ProofV ar \rangle} \in I\).

- Let \(i \in \text{Tid}\). Consider two cases.

  - Case \(i = t\). By the above, \(v'_{\langle LocalDataVar \cup ProofV ar \rangle} = M_{\langle pc_i \rangle} \ast R\).
  - Case \(i \neq t\). From \(v_{\langle pc_i \rangle} = v'_{\langle pc_i \rangle}\) we get \(LocalDataVar \cup \bigcup ProofV ar \cup R\). From \(x \in LocalDataVar\), then (1) implies \(v(x) = v'(x)\). Otherwise \(x \in ProofV ar\) for some \(r \in \text{rsc}(v_{\langle pc_i \rangle})\). From \(v_{\langle ProofV ar \rangle} \in I\) we get \(r \notin \text{rsc}(v_{\langle pc_i \rangle})\). From \(x \in ProofV ar\) we obtain \(v(x) = v'(x)\). Combining together, \(v_{\langle LocalDataVar \cup ProofV ar \cup R \cup \text{rsc}(v_{\langle \langle pc_i \rangle})\rangle} = M_{\langle pc_i \rangle} \ast R\).

So \(\forall i \in \text{Tid}: v_{\langle LocalDataVar \cup ProofV ar \cup R \cup \text{rsc}(v_{\langle \langle pc_i \rangle})\rangle} = M_{\langle pc_i \rangle} \ast R\).

We have shown \(v' \in \gamma_{OG}(I, M)\).

"init \(\subseteq \gamma_{OG}(I, M)\)". By definition of an Owicki-Gries-core proof.

\[\Box\]

### B.3 Examples of Owicki-Gries-core proofs

For \(k \in \mathbb{N}^+\) let \(\mathbb{N}_k = \mathbb{N} \cap [1, k]\).

**Extension of Example 1.** The syntactic structure of Readers- Writers \((n, m > 1)\) is given by

- \(\text{Tid} = \{\text{reader}_i, \text{writer}_j | 1 \leq i \leq n, 1 \leq j \leq m\}\);
- \(\text{PL} = \{\text{startreadA}, \text{startreadB}, \text{startreadC}, \text{read}, \text{finishreadA}, \text{finishreadB}, \text{finishreadC}, \text{askwriteA}, \text{askwriteB}, \text{askwriteC}, \text{startwriteA}, \text{startwriteB}, \text{write}, \text{finishwriteA}, \text{finishwriteB}, \text{finishwriteC}\};
- \(\text{Val} = \text{PL} \cup \mathbb{N}_0\), where \(\mathbb{N}_0\) is the set of nonnegative integers;
- \(\text{Res} = \{\text{control}\} = \{\{\text{ww}, \text{ar}, \text{aw}\}\};

22
Sequentially consistent and the single initial state, say, \( M_{\text{init}} \), we have assumed at least two readers and two writers, there are no local data variables. Let 
\[
I_{\text{control}} = \{ v : \text{control} \to N_0 \mid v(aw) \leq 1 \},
\[
M \in \prod_{p \in \text{LocalVar} \cup \text{ProofVar}(rsc(p))} (LocalDataVar \cup \{ I \}) \to \text{Val} \) given by 
\[
M_{\text{read reader}_i} = M_{\text{read reader}_j} = \emptyset,
\[
M_{\text{start read}_A reader} = \{ v \in \{ \text{ww, ar, aw} \to N_0 \} \mid v(ww) = 0 \land v(aw) \leq 1 \},
\[
M_{\text{start read}_B reader} = \{ v \in \{ \text{ww, ar, aw} \to N_0 \} \mid v(ww) = 0 \land v(aw) \leq 1 \leq v(aw) \},
\[
M_{\text{finish read}_A reader} = M_{\text{finish read}_B reader} = \{ v \in \{ \text{ww, ar, aw} \to N_0 \} \mid v(aw) \leq 1 \} \text{ for } 1 \leq i \leq n,
\[
M_{\text{write}_A writer} = M_{\text{write}_B writer} = \{ \emptyset \},
\[
M_{\text{ask write}_A writer} = M_{\text{ask write}_B writer} = \{ v \in \{ \text{ww, ar, aw} \to N_0 \} \mid v(aw) \leq 1 \},
\[
M_{\text{ask write}_C writer} = \{ v \in \{ \text{ww, ar, aw} \to N_0 \} \mid v(aw) = 0 = v(aw) \},
\[
M_{\text{start write}_A writer} = \{ v \in \{ \text{ww, ar, aw} \to N_0 \} \mid v(aw) = 0 \land v(aw) = 1 \},
\[
M_{\text{start write}_B writer} = \{ v \in \{ \text{ww, ar, aw} \to N_0 \} \mid v(aw) = 0 \land v(aw) = 1 \},
\[
M_{\text{finish write}_A writer} = M_{\text{finish write}_B writer} = \{ v \in \{ \text{ww, ar, aw} \to N_0 \} \mid 0 = v(aw) \} \text{ for } 1 \leq j \leq n,
\]
the remaining \( M_i \) are empty sets.

Notice that \( P = \{ [\text{control} \to I_{\text{control}}, M] \} \) is an annotation of Readers-Writers. It is sequentially consistent and the single initial state, say, \( v_{\text{init}} \), satisfies \( v_{\text{init}}(ww) = v_{\text{init}}(ar) = 0 \), thus \( v_{\text{init}}[|p_{\text{read}}(\text{control})|] \in I_{\text{control}} \), so \( v_{\text{init}} \in \text{O(G)}(P) \). Thus \( P \) is an Owicki-Gries-core proof.

Now we will show that this proof is the smallest one. So let \( ([\text{control} \to I_{\text{control}}, \widehat{M}] \mid \) be an arbitrary Owicki-Gries-core proof for Readers-Writers.

First notice that by starting with the initial state and successively applying sequential consistency we obtain nonemptiness of certain annotation parts:

**Fact 1.** For every \( i \in \mathbb{N} \) and every \( l \in \{ \text{start read}_A reader, \text{read, finish read}_A \} \) we have \( \emptyset \in \widehat{M}_{\text{read reader}_i} \); for every \( j \in \mathbb{N} \) and every \( l \in \{ \text{ask write}_A writer, \text{start write}_A writer, \text{write}, \text{finish write}_A \} \) we have \( \emptyset \in \widehat{M}_{\text{write}_A writer} \).

Now we will show in three steps that for any \( (a, b, c) \in \mathbb{N}^3 \times \{ 0, 1 \} \) the map \( [\text{ww} \mapsto a, \text{ar} \mapsto b, \text{aw} \mapsto c] \) is in \( I_{\text{control}} \).

**Step 1.** If \( c = 0 \), we get \( [\text{ww} \mapsto 0, \text{ar} \mapsto 0, \text{aw} \mapsto c] \in I_{\text{control}} \) from the initial condition. If \( c = 1 \), apply sequential consistency to states \( v, v' \) with \( v(p_{\text{write}_A}) = \text{start write}_A \) and \( v' \) to \( [\text{ww} \mapsto 0, \text{ar} \mapsto 0, \text{aw} \mapsto 0] \in I_{\text{control}} \) to get \( [\text{ww} \mapsto 0, \text{ar} \mapsto 0, \text{aw} \mapsto 0] \in M_{\text{start write}_A writer} \). Applying sequential consistency to the next step of the same thread to get \( [\text{ww} \mapsto 0, \text{ar} \mapsto 0, \text{aw} \mapsto 1] \in M_{\text{start write}_A writer} \). Applying sequential consistency to the termination of the critical section, we obtain \( [\text{ww} \mapsto 0, \text{ar} \mapsto 0, \text{aw} \mapsto c] \in \widehat{I}_{\text{control}} \).

**Step 2.** Now we will prove by induction on \( b \) that for all \( b \geq 0, c \in \{ 0, 1 \} \) the map \( [\text{ww} \mapsto 0, \text{ar} \mapsto b, \text{aw} \mapsto c] \) is in \( I_{\text{control}} \). Notice that for \( b = 0 \) we already have \( [\text{ww} \mapsto 0, \text{ar} \mapsto 0, \text{aw} \mapsto c] \in \widehat{I}_{\text{control}} \). If \( b > 0 \), the induction assumption gives \( [\text{ww} \mapsto 0, \text{ar} \mapsto b - 1, \text{aw} \mapsto c] \in \widehat{I}_{\text{control}} \). Applying sequential consistency to some states \( v, v' \) with \( v(p_{\text{read}_A}) = \text{start read}_A \) and \( v' \) to \( [\text{ww} \mapsto 0, \text{ar} \mapsto b - 1, \text{aw} \mapsto c] \in M_{\text{start read}_A reader} \). Applying sequential consistency once again to
Analogously we get \([ww \to 0, ar \to b, aw \to c] \in M_{\text{startreadC.reader}}\). Applying sequential consistency to the transition terminating the critical section, we obtain \([ww \to 0, ar \to b, aw \to c] \in I_{\text{control}}\).

Step 3. Now we will prove by induction on \(a\) that for all \(a, b \geq 0, c \in \{0, 1\}\) the map \([ww \to a, ar \to b, aw \to c]\) is in \(I_{\text{control}}\). Notice that for \(a = 0\) we have just proven \([ww \to 0, ar \to b, aw \to c] \in I_{\text{control}}\). For \(a > 0\), the induction assumption states that \([ww \to a - 1, ar \to b, aw \to c] \in I_{\text{control}}\). Sequential consistency, applied to any pair of states \(v, v'\) with \(v(pc_{\text{reader}}) = \text{askwriteA}\) and \(v'_{\text{writer}}\), gives \([ww \to a - 1, ar \to b, aw \to c] \in M_{\text{askwriteA.writer}}\). Applying sequential consistency once again gives \([ww \to a, ar \to b, aw \to c] \in M_{\text{askwriteC.writer}}\), and applying it again gives \([ww \to a, ar \to b, aw \to c] \in I_{\text{control}}\).

We have shown that \(I_{\text{control}} \subseteq I_{\text{control}}\).

From fact 1 we get \(M_{\text{startreadA.reader}} \subseteq M_{\text{startreadA.reader}}, M_{\text{finishreadA.reader}} \subseteq M_{\text{finishreadA.reader}}, M_{\text{read.reader}} \subseteq M_{\text{read.reader}}\), (1 \( \leq i \leq n\) and \(M_{\text{askwriteA.writer}} \subseteq M_{\text{askwriteA.writer}}, M_{\text{startwriteA.writer}} \subseteq M_{\text{startwriteA.writer}}, M_{\text{writer.writer}} \subseteq M_{\text{writer.writer}}, M_{\text{finishwriteD.writer}} \subseteq M_{\text{finishwriteD.writer}}, (1 \leq j \leq m)\).

Fix some \(i \in \mathbb{N}\) and states \(v, v'\) such that \(v(pc_{\text{reader}}) = \text{startreadA}, v(ww) = 0, v(ar) \geq 0\) and \(v(aw) \leq 1\). Then \(v'_{\text{LocalData\_reader}} = v'_{\text{LocalData\_reader}}\{\text{ProofVar}(\text{as}(\text{startreadA}))\} = \emptyset \in M_{\text{startreadA.reader}}\) and \(v'_{\text{ProofVar(control)}} \in I_{\text{control}}\). By sequential consistency, \(v'_{\text{LocalData\_reader}} = v'_{\text{LocalData\_reader}}\{\text{ProofVar}(\text{as}(\text{startreadA}))\} = v'_{\text{control}} \in M_{\text{startreadA.reader}}\). Thus for any \(b \geq 0\) and \(c \in \{0, 1\}\) we have \([ww \to 0, ar \to b, aw \to c] \in M_{\text{startreadA.reader}}\). In particular, \(M_{\text{startreadA.reader}} \subseteq M_{\text{startreadA.reader}}\). Applying sequential consistency to \(v'\) and \(v''\) with \(v'_{\text{reader}} = \text{startreadB}, v''(ww) = 0\) and \(v'(ar) \geq 0\) and \(v'(aw) \in \{0, 1\}\), we obtain \(M_{\text{startreadC.reader}} \subseteq M_{\text{startreadC.reader}}\).

Analogously we get \(M_{\text{finishreadD.reader}} \subseteq M_{\text{finishreadD.reader}}, M_{\text{finishreadC.reader}} \subseteq M_{\text{finishreadC.reader}}, (1 \leq i \leq n)\) and \(M_{\text{askwriteB.writer}} \subseteq M_{\text{askwriteB.writer}}, M_{\text{askwriteC.writer}} \subseteq M_{\text{askwriteC.writer}}\), \(M_{\text{startwriteC.writer}} \subseteq M_{\text{startwriteC.writer}}, M_{\text{finishwriteB.writer}} \subseteq M_{\text{finishwriteB.writer}}, M_{\text{finishwriteC.writer}} \subseteq M_{\text{finishwriteC.writer}}\), \(1 \leq j \leq m\). So \(P\) is really the smallest Owicki-Gries-core proof.
Now we will show that $\gamma_{OG}(P)$ equals

$$\{v \in ConsState \mid v(ww), v(ar) \in \mathbb{N}_0 \land v(aw) \in \{0, 1\}$$

$$\land \ \forall i \in \{1, \ldots, n\} : \ (v(pc_{reader_i}) \in \{x\text{read}, \text{read} \mid x \in \{\text{start}, \text{finish}\}$$

$$\land y \in \{A,B,C\})$$

$$\land (v(pc_{reader_i}) = \text{startreadB} \Rightarrow v(ww) = 0)$$

$$\land (v(pc_{reader_i}) = \text{startreadC} \Rightarrow v(ww) = 0 < v(ar))$$

$$\land \ \forall j \in \{1, \ldots, m\} : \ (v(pc_{writer_j}) \in \{x\text{write}, \text{write} \mid x \in \{\text{ask}, \text{start}, \text{finish}\}$$

$$\land y \in \{A,B,C\})$$

$$\land (v(pc_{writer_j}) = \text{askwriteC} \Rightarrow v(ww) > 0)$$

$$\land (v(pc_{writer_j}) = \text{startwriteB} \Rightarrow v(ar) = v(aw) = 0)$$

$$\land (v(pc_{writer_j}) = \text{startwriteC} \Rightarrow v(ar) = 0 < v(aw))$$

$$\land (v(pc_{writer_j}) = \text{finishwriteC} \Rightarrow v(aw) = 0) \}.$$

\[\subseteq\]: Since there are no local data variables, the defining condition of $\gamma_{OG}(P)$ restricts the variables of control at least once: either by the resource invariant, or by the annotation of a control flow location in a critical region. Since both the resource invariant as well as the annotations of all control flow locations inside the critical regions allow only values 0 and 1 of aw, we have $\pi_{aw}(\gamma_{OG}(P)) \subseteq \{0, 1\}$. Some $\mathcal{M}_c$ are empty, restricting the program counters of the readers and writers. If the variables $ww, ar$ are restricted beyond being nonnegative, then the restriction comes from the nonempty annotations of the control flow points.

\[\supseteq\]: Take a state $v$ from the right hand side. It satisfies the resource invariant in any case. If control is available in $v$, then no control flow annotation imposes additional restrictions on $v$, so $v$ is in the left hand side. If a state’s location is in a critical section, then the location is unique. The annotation of that location is satisfied either because the annotation is exactly the resource invariant. Or the annotation is satisfied by a condition of the right hand side.

\[\square\]

Extension of Example 2. The syntactic structure of Upper is given by

- $\mathcal{Tid} = \{1, 2\}$;
- $\mathcal{PL} = \{A,B,C,\ldots, V, W\}$;
- $\mathcal{Val} = \mathcal{PL} \cup \{0, 1\}$;
- $\mathcal{Res} = \{r, r'\}$ where $r = \{u, z\}, r' = \{x, y\}$;
- $\mathcal{Local}_1 = \{1.x, pc_1\}, \mathcal{Local}_2 = \{y, z, pc_2\}$;
- $\mathcal{ProofVar}(r) = \{u, z\} = r, \mathcal{ProofVar}(r') = \{x, y\} = r'$;
- $\mathcal{rsc} : \mathcal{PL} \rightarrow 2^\{\mathcal{Res}\}$ given by

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathcal{rsc}(p)$</td>
<td>$\emptyset$</td>
<td>${r}$</td>
<td>${r'}$</td>
<td>${r, r'}$</td>
</tr>
</tbody>
</table>

25
We have
\[
\text{init} = \{ \begin{align*}
|u| & \mapsto 1, z \mapsto 0, x \mapsto 0, y \mapsto 0, l \mapsto 0, pc_1 \mapsto A, pc_2 \mapsto 0, \\
|u| & \mapsto 0, z \mapsto 1, x \mapsto 1, y \mapsto 1, l \mapsto 1, pc_1 \mapsto A, pc_2 \mapsto 0
\end{align*} \}.
\]

Let \( P = (\{ r \mapsto I_r, r' \mapsto I_{r'} \}, (M_{r,p})_{p \in PL \times Td}) \), where
\[
I_r = \{ \begin{align*}
|u| & \mapsto 0, z \mapsto 1, [u \mapsto 1, z \mapsto 0], \\
|u| & \mapsto 1, z \mapsto 1
\end{align*} \},
\]
\[
I_{r'} = \{ \begin{align*}
[x \mapsto 0, y \mapsto 0, [x \mapsto 0, y \mapsto 1, [x \mapsto 1, y \mapsto 1]]
\end{align*} \},
\]
\[
M_{r,1} = \{ \begin{align*}
|u| & \mapsto 0, z \mapsto 1, x \mapsto 0, y \mapsto 0, l \mapsto 0, [u \mapsto 0, z \mapsto 1, x \mapsto 0, y \mapsto 0, l \mapsto 0, [u \mapsto 1, z \mapsto 0, x \mapsto 1, y \mapsto 1, l \mapsto 1]], \\
|u| & \mapsto 1, z \mapsto 0, x \mapsto 0, y \mapsto 1, l \mapsto 1
\end{align*} \},
\]
\[
M_{r,2} = \{ \begin{align*}
|u| & \mapsto 0, z \mapsto 1, x \mapsto 0, l \mapsto 0, [u \mapsto 1, z \mapsto 0, x \mapsto 0, l \mapsto 1] \}
\end{align*} \},
\]
\[
M_{r,3} = \emptyset \text{ for } (x,t) \in (PL \times Td) \setminus \{(A, 1), (B, 1), (C, 1), (D, 1), (E, 1), (0, 2)\}.
\]

Notice that the two initial states satisfy annotations of locations \( A \) and \( 0 \) as well as the resource invariants. Thus the program annotation proves the initial state is sequentially consistent. Thus \( P \) is an Owicki-Gries-core proof.

Now we’ll show that \( P \) is smaller than or equal to any Owicki-Gries-core proof \( (\{ r \mapsto I_r, r' \mapsto I_{r'} \}, (M_{r,p})_{p \in PL \times Td}) \). From the initial condition we get \([u \mapsto 0, z \mapsto 1, [u \mapsto 1, z \mapsto 0]] \in I_r \). So \( I_r \subseteq I_r \). The initial condition also implies \([x \mapsto 0, l \mapsto 0, [x \mapsto 1, l \mapsto 1] \in M_{k,1} \), so \( M_{k,1} \subseteq M_{k,1} \). Again from the initial condition we get \([y \mapsto 0, z \mapsto 0, [y \mapsto 1, z \mapsto 1] \in M_{k,2} \), so \( M_{k,2} \subseteq M_{k,2} \). At last the initial condition gives \([x \mapsto 0, y \mapsto 0, [x \mapsto 1, y \mapsto 1] \in I_r \). Now let
\[
A^u = [u \mapsto 1, z \mapsto 0, x \mapsto 1, y \mapsto 1, l \mapsto 1, pc_1 \mapsto A, pc_2 \mapsto 0]
\]
and
\[
A^v = [u \mapsto 1, z \mapsto 0, x \mapsto 1, y \mapsto 1, l \mapsto 1, pc_1 \mapsto B, pc_2 \mapsto 0].
\]
Notice that \( rsc(A) = \emptyset, rsc(B) = \{ r \} \), so
\[
A^u_{LocalDataVar rsc(A)} = [x \mapsto 1, l \mapsto 1] \in \hat{M}_{k,1}
\]
and
\[
A^u_{\text{ProofVar}(rsc(A))} = [u \mapsto 1, z \mapsto 0] \in I_r.
\]
Since \( v^u(u) = 1 = v^u(l) \), we have \( v^u \rightarrow v^u \). By sequential consistency,
\[
A^v_{LocalDataVar rsc(B)} \in \hat{M}_{k,1}, \text{ i.e., } [u \mapsto 1, z \mapsto 0, x \mapsto 1, l \mapsto 1] \in \hat{M}_{k,1}.
\]
Let
\[
v^c = [u \mapsto 1, z \mapsto 0, x \mapsto 1, y \mapsto 1, l \mapsto 1, pc_1 \mapsto C, pc_2 \mapsto 0].
\]
Since \( v^u_{\text{ProofVar}(rsc(B))} = [x \mapsto 1, y \mapsto 1] \in I_r \) and \( v^u \rightarrow v^u \), we obtain from the sequential consistency condition that \( v^u_{LocalDataVar rsc(B)} \in \hat{M}_{k,1} \).

Let
\[
v^p = [u \mapsto 1, z \mapsto 0, x \mapsto 0, y \mapsto 0, l \mapsto 1, pc_1 \mapsto D, pc_2 \mapsto 0].
\]
Since \( v^c \rightarrow v^p \), sequential consistency gives \( v^p_{LocalDataVar rsc(B)} \in \hat{M}_{k,1} \).

Let
\[
v^p = [u \mapsto 1, z \mapsto 0, x \mapsto 0, y \mapsto 0, l \mapsto 1, pc_1 \mapsto E, pc_2 \mapsto 0].
\]
From \( v^c \rightarrow v^p \), sequential consistency and \( r' \in rsc(D) \setminus rsc(E) \) we get
\[
v^p_{LocalDataVar rsc(B)} \in \hat{M}_{k,1} \text{ and } I_r \supseteq v^p_{\text{ProofVar}(r')} = [x \mapsto 0, y \mapsto 1].
\]
Thus \( I_{r'} \subseteq I_r \).

Now let
\[
v^u = [u \mapsto 0, z \mapsto 1, x \mapsto 0, y \mapsto 1, l \mapsto 0, pc_1 \mapsto A, pc_2 \mapsto 0]
\]
and
\[
v^v = [u \mapsto 0, z \mapsto 1, x \mapsto 0, y \mapsto 1, l \mapsto 0, pc_1 \mapsto B, pc_2 \mapsto 0].
\]
Since $\varphi(u) = 0 = \varphi(l)$, we have $\varphi \to_1 \varphi$. Since additionally $\varphi_1^{\text{LocalData}} \sqcup \varphi_1^{\text{ProofVar}(\text{rsc}(k))} = [x \mapsto 0, l \mapsto 0] \in M_{k, 1}$, $\text{rsc}(\varphi) \setminus \text{rsc}(\varphi_1) = \{r\}$ and $\varphi_1^{\text{ProofVar}(r)} = [u \mapsto 0, z \mapsto 1] \in \tilde{L}$, we have $M_{k, 1} \supseteq \varphi_1 |_{\text{LocalData}} \sqcup \varphi_1 |_{\text{ProofVar}(\text{rsc}(k))} = [u \mapsto 0, z \mapsto 1, x \mapsto 0, l \mapsto 0]$.

Since $[u \mapsto 1, z \mapsto 0, x \mapsto 1, l \mapsto 0]$, $[u \mapsto 0, z \mapsto 1, x \mapsto 0, l \mapsto 0] \in M_{k, 1}$, we have $M_{k, 1} \subseteq M_{k, 1}$.

From $[u \mapsto 0, z \mapsto 1, x \mapsto 0, l \mapsto 0]$, $[u \mapsto 1, z \mapsto 0, x \mapsto 1, l \mapsto 1] \in M_{k, 1}$, $[x \mapsto 0, y \mapsto 0]$, $[x \mapsto 0, y \mapsto 1], [x \mapsto 1, y \mapsto 1] \in \tilde{L}$, we get $[u \mapsto 0, z \mapsto 1, x \mapsto 0, y \mapsto 0, l \mapsto 0]$, $[u \mapsto 0, z \mapsto 1, x \mapsto 0, y \mapsto 1, l \mapsto 0] \in M_{k, 1}$, Thus, $M_{k, 1} \subseteq M_{k, 1}$.

Applying sequential consistency with respect to $x := 0$ we get $[u \mapsto 0, z \mapsto 1, x \mapsto 0, y \mapsto 0, l \mapsto 0]$, $[u \mapsto 0, z \mapsto 1, x \mapsto 0, y \mapsto 1, l \mapsto 0]$, $[u \mapsto 1, z \mapsto 0, x \mapsto 0, y \mapsto 1, l \mapsto 1] \in M_{k, 1}$, i.e., $M_{k, 1} \subseteq M_{k, 1}$.

Applying sequential consistency to $[u \mapsto 0, z \mapsto 1, x \mapsto 0, y \mapsto 0, l \mapsto 0]$, $[u \mapsto 1, z \mapsto 0, x \mapsto 0, y \mapsto 1, l \mapsto 1] \in M_{k, 1}$ we get $[u \mapsto 0, z \mapsto 1, x \mapsto 0, y \mapsto 0, l \mapsto 0]$, $[u \mapsto 1, z \mapsto 0, x \mapsto 0, y \mapsto 1, l \mapsto 1] \in M_{k, 1}$, i.e., $M_{k, 1} \subseteq M_{k, 1}$.

We have shown that $P$ is the smallest Owicki-Gries-core proof. It denotes the following states (column = state):

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>$u$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$z$</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$x$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$y$</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$l$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$pc_1$</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td>D</td>
<td>E</td>
</tr>
<tr>
<td>$pc_2$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

\[ \square \]

**Extension of Example 3.** A syntactic structure $(Tid, PL, Val, Res, \{Local, pc\}_{t \in Tid}, \text{ProofVar}, \text{rsc})$ belongs to the class $\text{StrSimple}$ iff $|Res| \leq 1$, $(\forall t \in Tid : \text{Local} \cap \{t\} \neq \emptyset)$ and $(\forall r \in Res : \text{ProofVar}(r) \neq r \neq \emptyset)$. An RPL transition system $(\text{init}, (-\rightarrow))_{t \in Tid}$ belongs to the class $\text{Simple}$ iff it obeys a syntactic structure from $\text{StrSimple}$. All programs from the family Readers-Writers are in Simple.

\[ \square \]

**Extension of Example 4.** A syntactic structure $(Tid, PL, Val, Res, \{Local, pc\}_{t \in Tid}, \text{ProofVar}, \text{rsc})$ belongs to the class $\text{StrSepThreads}$ iff $Res = \emptyset$ and $Tid$ is finite. An RPL transition system $(\text{init}, (-\rightarrow))_{t \in Tid}$ belongs to the class $\text{SepThreads}$ iff it obeys a syntactic structure from $\text{StrSepThreads}$ and $\forall t \in Tid : (\exists \bar{v} \in \text{ConsState} : (\forall v \in ConsState : \bar{v} \Rightarrow v \in \text{init}) \Rightarrow v \sim_{\text{Local}} \bar{v}) \Rightarrow \bar{v} \Rightarrow v \in \text{init}$.

Notice that $\text{StrSepThreads} \subseteq \text{StrSimple}$ and $\text{SepThreads} \subseteq \text{Simple}$.

We will show later, using the lower bound, that the smallest Owicki-Gries-core proof of an RPL transition system from $\text{SepThreads}$ denotes the strongest invariant.

\[ ^5 \text{For infinite } Tid \text{ only those states are reachable that have finitely many non-initial components, but the Owicki-Gries-core proof denotes states that may have arbitrary many non-initial components. Thus we study here the finite-threaded case only.} \]
C  Owicki-Gries core as abstract interpretation

Within the section C, fix a syntactic structure and an RPL transition system obeying it as in section A. Let

\[ \text{next}^#_{OG} : \mathcal{P}A \rightarrow \mathcal{P}A, \]
\[ (I, M) \mapsto \{ \{v'\}_{\text{ProofVar}(r)} | \exists t \in \text{Tid}, v \rightarrow_t v' \land \]
\[ v \text{LocalData}_L \cup \{v'_{\text{LocalVar}}(rsc(v(pc_t)))\} \in M_{v(pc_t) \cdot t} \land \]
\[ r \in \text{rsc}(v(pc_t)) \} \} \}_{r \in \text{Res}}, \]
\[ \{ \{v'\}_{\text{LocalData}_L \cup \{v'_{\text{LocalVar}}(rsc(p))\}} | \exists v \rightarrow v' \land \]
\[ v'_{\text{LocalVar}}(rsc(v(pc_t))) \in M_{v(pc_t) \cdot t} \land \]
\[ v' \in \text{rsc}(p) \} \}_{p \in \text{PL}, t \in \text{Tid}}, \]
\[ I_{\text{init}} = \{ \{v\}_{\text{ProofVar}(r)} | v \in \text{init} \}_{r \in \text{Res}} \]
\[ M_{\text{init}} = \{ \{v\}_{\text{LocalData}_L} | v \in \text{init} \land v(pc_t) = p \}_{p \in \text{PL}, t \in \text{Tid}}. \]

Let the sound Owicki-Gries-core abstract successor map be

\[ \text{post}^#_{OG} : \mathcal{P}A \rightarrow \mathcal{P}A, \]
\[ (I, M) \mapsto (I, M) \cup \text{next}^#_{OG}(I, M), \]

and the Owicki-Gries-core abstract transformer be

\[ F^#_{OG} : \mathcal{P}A \rightarrow \mathcal{P}A, \]
\[ (I, M) \mapsto (I, M) \cup \text{next}^#_{OG}(I, M). \]

Lemma 28. The map \text{next}^#_{OG} is monotone.

Proof. Let \((I, M) \subseteq (I, M')\) be program annotations, \text{next}^#_{OG}(I, M) = (I', M') \quad \text{next}^#_{OG}(I, \tilde{M}) = (\tilde{I}', \tilde{M}')

\[ \forall r \in \text{Res} : I'_r \subseteq \tilde{I}'_r. \] Let \(r \in \text{Res}.\) Let \(w \in I'_r.\) Then there is a thread \(t \in \text{Tid}\) and some transition \(v \rightarrow_t v'\) such that \(v'_{\text{LocalData}_L \cup \{v'_{\text{LocalVar}}(rsc(v(pc_t)))\}} \in M_{v(pc_t) \cdot t} \land r \in \text{rsc}(v(pc_t)) \}\]
\[ v'_{\text{LocalVar}}(rsc(v(pc_t))) \quad \text{and} \quad v'_{\text{ProofVar}(r)} = w. \] Then \(\tilde{M}_{v(pc_t) \cdot t} \exists v'_{\text{LocalData}_L \cup \{v'_{\text{LocalVar}}(rsc(v(pc_t)))\}}.\]
\[ \text{So } w \in \tilde{I}'_r. \]

\[ \forall t \in \text{Tid}, p \in \text{PL} : M'_{p,t} \subseteq \tilde{M}'_{p,t}. \]

\[ \text{Let } t \in \text{Tid}, p \in \text{PL}. \] Let \(w \in M'_{p,t}. \) Then there is some transition \(v \rightarrow_t v'\) such that \(v'_{\text{LocalData}_L \cup \{v'_{\text{LocalVar}}(rsc(v(pc_t)))\}} \in M_{v(pc_t) \cdot t} \land r \in \text{rsc}(v(pc_t)) \}\]
\[ v'_{\text{LocalVar}}(rsc(v(pc_t))) \quad \text{and} \quad v'_{\text{ProofVar}(r)} = w. \] Then \(\tilde{M}_{v(pc_t) \cdot t} \exists v'_{\text{LocalData}_L \cup \{v'_{\text{LocalVar}}(rsc(v(pc_t)))\}}. \]
\[ \text{So } w \in \tilde{M}'_{p,t}. \]

Corollary 29. The Owicki-Gries-core abstract transformer \(F^#_{OG}\) is monotone.

Corollary 29 implies that the Owicki-Gries-core abstract transformer has a least fixpoint, which follows from a well-known fixpoint theorem6.

A postfix point of a map \(f : X \rightarrow X\) on a poset \((X, \leq)\) is any \(x \in X\) such that \(f(x) \leq x.\) Let \(\text{postfp}(f)\) be the set of postfix points of \(f.\)

\[ \text{Known today as Tarski’s fixpoint theorem (Thm. 1 in [28]). This existence of the least fixpoint, however, was also mentioned independently, e.g., Exercise 5 in §4 of Chapter IV of [2] in year 1948. See also [3], Ch. V, §3, p. 115.} \]
Theorem 30. Every Owicki-Gries-core proof is a postfix point of the Owicki-Gries-core abstract transformer and vice versa. Formally:

$$\mathcal{O} = \text{postfp}(F_{OG}^\#).$$

Proof. "\(\subseteq\)". Let \((I, M) \in \mathcal{O}\). We will show that \((I', M') := F_{OG}^\#(I, M)\) is less than or equal to \((I, M)\). Let \((I, M) = \text{next}_\mathcal{O}(I, M)\).

\(\forall r \in \text{Res} : I'_r \subseteq I'_r\) : Let \(r \in \text{Res} \). Let \(w \in I'_r\). Then \(w \in I'_r \cup I_r \cup I'_r\).

Case \(w \in I'_r\). Then there is some \(v \in \text{init}\) such that \(v|_{\text{ProofVar}(r)} = w\). By the initial condition, \(v \in \mathcal{Y}_\mathcal{O}(I, M)\). Since every resource is available in an initial state, \(r \in \text{Res} \setminus \text{rsc}(v(PC\text{Var}))\). Thus \(v|_{\text{ProofVar}(r)} \in I_r\).

Case \(w \in I_r\). Then we don’t have to prove anything more.

Case \(w \in I'_r\). Then there is \(t \in \text{Tid}, (v, v') \in t\) such that \(v|_{\text{LocalDataVar}} \cup \text{res}(v|_{\text{pc}_r})\) \(\in M_{\gamma}(pc_r), r \in \text{rsc}(v|_{\text{pc}_r}) \) and \(w = v|_{\text{ProofVar}(r)}\). By (5) we have \(\text{rsc}(v|_{\text{pc}_r}) \supseteq \text{rsc}(v|_{\text{pc}_r})\). Sequential consistency implies \(v|_{\text{ProofVar}(r)} \in I_r\).

In all cases \(w \in I_r\). So \(I'_r \subseteq I_r\).

\(\forall t \in \text{Tid}, p \in \text{PL} : M'_{p,t} \subseteq M_{p,t}\). Let \(t \in \text{Tid}, p \in \text{PL}\). Let \(w \in M'_{p,t}\). Then \(w \in M_{p,t} \cup M_{p,t} \cup M_{p,t}\).

Case \(w \in M_{p,t}\). Then there is some \(v \in \text{init}\) such that \(v|_{\text{pc}_r} = p\) and \(w = v|_{\text{LocalDataVar}}\). By the initial condition, \(v \in \mathcal{Y}_\mathcal{O}(I, M)\). From definition of \(\mathcal{Y}_\mathcal{O}\) and \(\text{rsc}(v|_{\text{pc}_r}) = [v \in \text{init}]\) we get \(v|_{\text{LocalDataVar}} \in M_{p,t}\).

Case \(w \in M_{p,t}\). Then nothing more has to be proven.

Case \(w \in M_{p,t}\). Then there is \(t \in \text{Tid}, (v, v') \in t\) such that \(v|_{\text{LocalDataVar}} \cup \text{res}(v|_{\text{pc}_r})\) \(\in M_{pc_r}, r \in \text{rsc}(v|_{\text{pc}_r}) \) and \(w = v|_{\text{ProofVar}(r)}\). Then \(v|_{\text{LocalDataVar}} \cup \text{res}(v|_{\text{pc}_r}) \in M_{p,t}\) by sequential consistency.

In any case \(w \in M_{p,t}\). So \(M'_{p,t} \subseteq M_{p,t}\).

\(\supseteq\) : Let \((I, M) \in \text{postfp}(F_{OG}^\#), \) i.e., for \((I', M') = F_{OG}^\#(I, M)\) we have \((I', M') \subseteq (I, M)\).

We’ll show that \((I, M)\) is an Owicki-Gries-core proof.

Sequential consistency: Let \(t \in \text{Tid}, (v, v') \in t\), \(p = v|_{\text{pc}_r}, p' = v'|_{\text{pc}_r}, R = \text{rsc}(p), R' = \text{rsc}(p')\) \(\in M_{p,t}\) and \(\forall r \in R' \setminus R : v|_{\text{ProofVar}(r)} \in I_r\). By definition of \(\text{next}_\mathcal{O}\) we obtain \(v|_{\text{LocalDataVar}} \cup \text{res}(v|_{\text{pc}_r})\) \(\in M'_{p,t} \subseteq M_{p,t}\). If any \(r \in R' \setminus R'\) is given, the definition of \(\text{next}_\mathcal{O}\) implies \(v|_{\text{ProofVar}(r)} \in I'_r \subseteq I_r\).

Initial condition: Let \(v \in \text{init}\).

Let \(r \in \text{Res} \setminus \text{rsc}(v(PC\text{Var}))\). Then \(v|_{\text{ProofVar}(r)} \in I'_r \subseteq I'_r \subseteq I_r\).

Now let \(t \in \text{Tid}\). Then \(v|_{\text{LocalDataVar}} \in M_{\text{init}}\). Since initial states don’t have any busy resources, \(v|_{\text{LocalDataVar}} \cup \text{res}(v|_{\text{pc}_r})\) \(\in M_{\text{pc}_r,M_{\text{pc}_r,t}} \subseteq M_{\text{pc}_r,M_{\text{pc}_r,t}}\). We have shown \(v \in \mathcal{Y}_\mathcal{O}(I, M)\). Thus \(\text{init} \subseteq \mathcal{Y}_\mathcal{O}(I, M)\).

\[\blacksquare\]

Restatement of Theorem 5. The smallest Owicki-Gries-core proof is the least fixpoint of the Owicki-Gries-core abstract transformer, formally:

\[\text{inf}(\mathcal{O}) = \text{lfp}(F_{OG}^\#).\]
Proof. $\inf(\mathcal{D}) = [\text{Thm. 30}] \inf(postp(F^b_{\text{OG}})) = [\text{Tarski’s fixpoint theorem}] \lfloor p(F^b_{\text{OG}})\rfloor$. 

**Proposition 31.** The map $\text{post}^b_{\text{OG}}$ is sound with respect to the concrete successor map $\text{post}$. Formally:

$$\forall P \in \mathcal{P}A: \text{post} \circ \gamma_{\text{OG}}(P) \subseteq \gamma_{\text{OG}} \circ \text{post}^b_{\text{OG}}(P).$$

Proof. Let $(I, M) \in \mathcal{P}A$. Let $v' \in \text{post}(\gamma_{\text{OG}}(I, M))$. Let $(I', M') = \text{next}^b_{\text{OG}}(I, M)$ and $(I, M) = \text{post}^b_{\text{OG}}(I, M)$. Then $(I, M) = (I, M) \cup (I', M')$. By definition of $\text{post}$ there is some $t \in \text{Tid}$ and some $v \in \gamma_{\text{OG}}(I, M)$ such that $v \rightarrow_t v'$. By definition of $\gamma_{\text{OG}}$ we have $v|_{\text{LocalData}} \cup v|_{\text{ProofVar}} \subseteq v|_{\text{LocalData}} \cup v|_{\text{ProofVar}}$. To show that $v'$ is in $\gamma_{\text{OG}}(\hat{I}, \hat{M})$ we have to prove the following two claims.

1. $\forall r \in \text{Res} \setminus \text{Rsc}(v|_{\text{PCVar}}): v'|_{\text{ProofVar}(r)} \in \hat{I}$.
2. Let $r \in \text{Res} \setminus \text{Rsc}(v|_{\text{PCVar}})$. The definition of $\gamma_{\text{OG}}$ implies that $\nu_{\text{ProofVar}(r)} = \nu_{\text{ProofVar}(r)}$. Notice that $r \notin \text{Rsc}(v|_{\text{PCVar}}) \cap \text{Rsc}(v|_{\text{PCVar}})$. Thus for all $x \in \text{ProofVar}(r)$ we have $x = \nu_{\text{ProofVar}(r)}(x)$. So $\nu_{\text{ProofVar}(r)} = \nu_{\text{ProofVar}(r)}$.

In both cases $v'|_{\text{ProofVar}(r)} \in \hat{I}$.

**Remark 32.** A reader might wonder why we have not taken the map $\mathcal{P}A \rightarrow \mathcal{P}A$, $(I, M) \rightarrow (\text{next}^b_{\text{OG}}(I, M), M')$ as the abstract transformer. It is also monotone and the set of its postfix points is equal to the set of Owicki-Gries-core proofs. However, $\text{next}^b_{\text{OG}}$ is in general not a sound approximation of $\text{post}$ under $(\alpha_{\text{OG}}, \gamma_{\text{OG}})$. 

**D. Upper bound on precision**

Within the current section D, fix a syntactic structure $\{\text{Tid}, PL, \text{Val}, \text{Res}, (\text{Local}_i, \text{pc}_i)_{i \in \text{Tid}}, \text{ProofVar}, \text{rsc}\}$, let $\text{ConsState}$ be the set of consistent states, $D = \mathcal{P}(\text{ConsState})$ and $(PA, \sqsubseteq)$ the lattice of program annotations.
Let

$$\alpha_{OG} : D \to PA,$$

$$S \mapsto ((\{v \in \text{ProofVar}(r) \mid v \in S \land r \not\in \bigcup_{p \in PL} \text{Res}(v(\text{PCVar}(p))))\}_{r \in \text{Res}},$$

$$((\{v \in \text{LocalDataVar}, \text{ProofVar}(\text{rcx}(p)) \mid v \in S \land p = v(p_c)\}_{p \in \text{PL}})).$$

A pair of adjoint maps\(^7\) between two posets $$(X, \leq)$$, $$(Y, \preceq)$$ is a pair of maps $$(\alpha, \gamma)$$ such that $\alpha : X \to Y$, $\gamma : Y \to X$ and

$$\forall x \in X, y \in Y : \alpha(x) \preceq y \iff x \leq \gamma(y).$$

**Proposition 33.** $$(\alpha_{OG}, \gamma_{OG})$$ is a pair of adjoint maps between $$(D, \subseteq)$$ and $$(PA, \sqsubseteq)$$.

**Proof.** Let $S \in D$, $\alpha_{OG}(S) = (I, M)$, $T = (J, N) \in PA$. We will show that $\alpha_{OG}(S) \subseteq T$ if and only if $S \subseteq \gamma_{OG}(T)$.

“only if”: Let $v \in S$. By definition of $D$ we get $v \in \text{ConstState}$. Let $r \in \text{Res} \setminus \bigcup \text{Res}(v(\text{PCVar})).$

By definition of $\alpha_{OG}$ we get $v|_{\text{ProofVar}(r)} \in I_r$. By assumption, $I_r \subseteq J_r$ so $v|_{\text{ProofVar}(r)} \in J_r$.

Now let $t \in \text{Tid}$ and $p = v(p_c)$. By definition of $\alpha_{OG}$ we get $v|_{\text{LocalDataVar}, \text{ProofVar}(\text{rcx}(p))} \in M_{p,t}$. By assumption, $N_{p,t} \supseteq M_{p,t}$. Thus $N_{p(c), t} \supseteq v|_{\text{LocalDataVar}, \text{ProofVar}(\text{rcx}(v(p_c)))}$. Combining, we obtain $v \in \gamma_{OG}(T)$.

“if”: Let $r \in \text{Res}$. Let $u \in I_r$. By definition of $\alpha_{OG}$ there is $v \in S$ such that $r \not\in \bigcup \text{Res}(v(\text{PCVar}))$ and $u = v|_{\text{ProofVar}(r)}$. By assumption, $v \in \gamma_{OG}(T)$. By definition of $\gamma_{OG}$ we have $u \in J_r$. Thus $I_r \subseteq J_r$.

Let $t \in \text{Tid}$ and $p \in \text{PL}$. Let $u \in M_{p,t}$. By definition of $\alpha_{OG}$ there is some $v \in S$ such that $p = v(p_c)$ and $v|_{\text{LocalDataVar}, \text{ProofVar}(\text{rcx}(p))} = u$. By assumption, $v \in \gamma_{OG}(T)$.

By definition of $\gamma_{OG}$ we get $u \in N_{p,t}$. Thus $M_{p,t} \subseteq N_{p,t}$.

Combining, we obtain $\alpha_{OG}(S) \subseteq T$.

Let $\rho = \gamma_{OG} \circ \alpha_{OG}$.

Then for $Q \in D$ we have $\rho(Q) =$

$$\left\{ v \in \text{ConstState} \mid \forall r \in \text{Res} \setminus \text{Res}(v(\text{PCVar})) \exists \tilde{v} \in Q : \left( r \not\in \bigcup \text{Res}(v(\text{PCVar})) \land \langle v \sim_{\text{ProofVar}(r)} \tilde{v} \rangle \right) \right\}.$$

A closure (sometimes called an upper closure operator) on a poset $$(X, \leq)$$ is a map $\rho : X \to X$ which is monotone, extensive and idempotent. (For an introduction to closures see [31].)

**Proposition 34.** $\rho : D \to D$ is a closure operator.

---

\(^7\) As of year 2011, it is also called a (monotone) Galois connection. The definition of a Galois connection is changing over time; see, e.g., § 6 in Chapter IV of [2], also § 8 in Chapter V of [3], for a more antique definition where the maps $\alpha$ and $\gamma$ are antitone.
Proof. By a standard result (exercise for the reader, see also [9], Corollary 5.3.0.5), applying the right adjoint after the left adjoint gives a closure operator.

**Restatement of Theorem 10.** Abstract interpretation with $\rho$ proves the strongest Owicki-Gries-provable property.

Formally, let $T = (\text{init}, \ldots)$ be an RPL transition system that obeys the given syntactic structure and has successor operator $\text{post}$ and let $\mathcal{D}$ be the lattice of Owicki-Gries-core proofs of $T$; then

$$\text{lfp}(\lambda x. \rho(\text{init} \cup \text{post}(x))) \subseteq \gamma_{\text{OG}}(\inf \mathcal{D}).$$

**Proof.** Let $P = \inf \mathcal{D}$. By Prop. 27 we have

$$\text{init} \cup \text{post}(\gamma_{\text{OG}}(P)) \subseteq \gamma_{\text{OG}}(P).$$

Since $(\alpha_{\text{OG}}, \gamma_{\text{OG}})$ is a pair of adjoint maps, we have

$$\alpha_{\text{OG}}(\text{init} \cup \text{post}(\gamma_{\text{OG}}(P))) \subseteq P.$$ Right adjoints are monotone, so

$$\gamma_{\text{OG}}(\alpha_{\text{OG}}(\text{init} \cup \text{post}(\gamma_{\text{OG}}(P)))) \subseteq \gamma_{\text{OG}}(P),$$

otherwise stated

$$\rho(\text{init} \cup \text{post}(\gamma_{\text{OG}}(P))) \subseteq \gamma_{\text{OG}}(P).$$

Let $F = \lambda x. \rho(\text{init} \cup \text{post}(x))$, then $\gamma_{\text{OG}}(P) \in \text{postfp}(F)$. Since the least fixpoint of a monotone map is the infimum of its postfix points, $\text{lfp}(F) \subseteq \gamma_{\text{OG}}(P)$. Apply Corollary 26.

In particular, abstract interpretation with $\rho$ allows proving at least as many properties as the core of the Owicki-Gries method.

**Extension of Example 11.** We will see later in Example 19 that $\text{lfp}(\lambda x. \rho(\text{init} \cup \text{post}(x))) = \gamma_{\text{OG}}(I, M)$. So, for Readers-Writers, the Owicki-Gries-core proof method and abstract interpretation with $\rho$ are equally strong. □

**Extension of Example 12.** Notice that $\rho(\text{init} \cup \text{post}(\text{init})) = \rho(\text{init} \cup \emptyset) = \rho(\text{init}) \subseteq \text{init}$. Since init is the set of reachable states, $\text{lfp}(\lambda x. \rho(\text{init} \cup \text{post}(x))) = \text{init}$. This is for the RPL transition system Upper abstract interpretation under $\rho$ can prove strictly stronger properties than the core of the Owicki-Gries method. □

**Extension of Example 13.** For the programs of the class Simple we will show later in Example 22 that $\text{lfp}(\lambda x. \rho(\text{init} \cup \text{post}(x))) = \gamma_{\text{OG}}(\inf \mathcal{D})$.

**Extension of Example 14.** For the RPL transition systems in the class SepThreads we will show later that the abstract interpretation using the lower bound produces exactly the set of reachable states. Thus abstract interpretation using the upper bound $\rho$ will also produce the set of reachable states. □
E  Lower bound on precision

For a set $X$ of sets, let

$$\text{Part}(X) = \{ Y \mid \exists T \subseteq X : Y = (\bigcap T) \cap (\bigcap_{Z \in X \setminus T} ((\bigcup X) \setminus Z)) \neq \emptyset \}$$

be the partition of $X$, where $\bigcap \emptyset = \bigcup X$ by convention. The elements of a partition are called blocks.

**Lemma 35.** Let $X$ be a set of sets. Then:
1. $\bigcup \text{Part}(X) = \bigcup X$;
2. for all different $s_1, s_2 \in \text{Part}(X)$ we have $s_1 \cap s_2 = \emptyset$;
3. if $s \in \text{Part}(X)$ and $S \in X$, then either $s \cap S = \emptyset$ or $s \subseteq S$;
4. if $X$ is finite, so is $\text{Part}(X)$.

**Proof.** 1. “$\subseteq$”: Intersection of subsets of $\bigcup X$ produces a subset of $\bigcup X$.
   \[ x \in \bigcup X \Rightarrow T = \{ S \in X \mid x \in S \}. \]
   Then for all $Z \subseteq X \setminus T$ we have $x \notin Z$. So $x \in (\bigcap T) \cap (\bigcap_{Z \in X \setminus T} ((\bigcup X) \setminus Z))$.

2. Let $T_1, T_2 \subseteq X$ be such that for $s_1 = (\bigcap T_1) \cap (\bigcap_{Z \in X \setminus T_1} ((\bigcup X) \setminus Z)) \neq \emptyset$ and $s_2 = (\bigcap T_2) \cap (\bigcap_{Z \in X \setminus T_2} ((\bigcup X) \setminus Z)) \neq \emptyset$ we have $s_1 \neq s_2$. Assume for the purpose of contradiction that there is some $y$ in $s_1 \cap s_2$. Since $s_1 \neq s_2$, there is some $x$ in $(s_1 \setminus s_2) \cup (s_2 \setminus s_1)$. Without loss of generality let $x \in s_1 \setminus s_2$, the other case is symmetrical. Then $x \in (\bigcup X) \setminus s_2$, so there are two cases.
   - Case $\exists S \subseteq T_1 : x \notin S$. Take such $S$. Then $S \notin T_1$, thus $S \subseteq X \setminus T_1$, so $y \in (\bigcup X) \setminus S$. Since $S \in T_2$, we have $y \in S$. Contradiction!
   - Case $\exists Z \subseteq X \setminus T_2 : x \notin (\bigcup X) \setminus Z$. Then $Z \subseteq X \setminus T_1$ (otherwise $x$ were not in $s_1$). So $Z \subseteq T_1$. So $x \in Z$. But $y \in s_2$, so $y \in (\bigcup X) \setminus Z$. Contradiction!

3. Let $s \in \text{Part}(X)$ and $S \subseteq X$. Assume for the purpose of contradiction that $s \cap S$ contains some element, say, $x$, but $s \setminus S$ also contains some element, say, $y$. There is some $T \subseteq X$ such that $s = (\bigcap T) \cap (\bigcap_{Z \in X \setminus T} ((\bigcup X) \setminus Z))$. So $y \in \bigcap T$. If $S \subseteq T$, we get $y \notin T$, a contradiction. If $S \notin T$, then $S \subseteq X \setminus T$, so $x \in s \subseteq (\bigcup X) \setminus S$ implies $x \notin S$, also a contradiction.

4. If $X$ is finite, $|\text{Part}(X)| \leq 2^{|X|}$.

For the rest of section E, fix a syntactic structure $(\text{Tid}, \text{PL}, \text{Val}, \text{Res}, (\text{Local}, p_{\text{c}})_{t \in \text{Tid}})$, ProofVar, rsc, let ConsState be the set of consistent states and $D = \exists (\text{ConsState})$. Let

$$RL = \text{Res} \cup \{ \text{Local} \mid t \in \text{Tid} \} \quad \text{and} \quad \widetilde{RL} = \text{Part}(RL).$$

Let

$$\rho : D \rightarrow D,
\begin{align*}
Q & \mapsto \\
\forall s \in \widetilde{RL}, r \in \text{Res} : s \subseteq r & \Rightarrow \\
(r \notin \bigcup \text{rsc}(v(\text{PCVar}))) & \Rightarrow \exists \tilde{v} \in Q : v \sim_\gamma \tilde{v} \land r \notin \bigcup \text{rsc}(\tilde{v}(\text{PCVar})).
\end{align*}$$

Let

$$\forall t \in \text{Tid} : r \in \text{rsc}(v(p_{\text{c}})) & \Rightarrow \exists \tilde{v} \in Q : v \sim_\gamma (\text{Local} \setminus \text{Res} \setminus \tilde{v}).$$
Proof. Monotonicity. Let \( \rho \): \( D \rightarrow D \). 

\[ \forall v \in \text{ConsState} \mid \exists s \in R\bar{L} \exists \bar{v} \in Q : v \sim_s \bar{v} \]. 

Note that neither \( \bar{\rho} \) nor \( \rho_c \) depend on the map \( \text{ProofVar} \). Thus for syntactic structures that differ only in the map \( \text{ProofVar} \) we have the same \( \bar{\rho} \) and the same \( \rho_c \).

**Proposition 36.** \( \bar{\rho} \) is a closure operator on \( (D, \subseteq) \).

**Proof.**

- **Idempotence.** Let \( Q \subseteq Q' \subseteq \text{ConsState} \).
  - Let \( v \in \bar{\rho}(Q) \).
    - Assume for a moment that \( r \notin \bigcup \text{rsc}(\bar{v}(\text{PCVar})) \). Take \( \bar{v} := v \).
    - Let \( t \in \text{Tid} \) and \( r \in \text{rsc}(v(pc_i)) \). Then \( \bar{v} \in Q \) such that \( v \sim_{(\text{Local} \cup \text{Res}) \cup \text{It}} \bar{v} \). Notice that \( \bar{v} \in Q' \).

- **Extensivity.** Let \( Q \subseteq D \). Let \( v \in Q \).
  - Let \( s \in R\bar{L}, r \in \text{Res}, s \subseteq r \).
    - Assume for a moment that \( r \notin \bigcup \text{rsc}(v(\text{PCVar})) \). Take \( \bar{v} := v \).
    - Let \( t \in \text{Tid} \) and \( r \in \text{rsc}(v(pc_i)) \). Take \( \bar{v} := v \).
    - Let \( t \in \text{Tid} \). Take \( \bar{v} := v \).

Thus \( v \in \bar{\rho}(Q) \). We have shown that \( Q \subseteq \bar{\rho}(Q) \).

**Extensivity.** Let \( Q \subseteq D \). Let \( v \in \bar{\rho}(\bar{\rho}(Q)) \). We’ll show that \( v \in \bar{\rho}(Q) \).

- Let \( s \in R\bar{L}, r \in \text{Res}, s \subseteq r \).
  - Assume for a moment that \( r \notin \bigcup \text{rsc}(v(\text{PCVar})) \).
    - Let \( t \in \text{Tid} \) such that \( r \in \text{rsc}(v(pc)) \). Then \( \bar{v} \in Q \) such that \( v \sim_{(\text{Local} \cup \text{Res}) \cup \text{It}} \bar{v} \). Then \( \bar{v} \in Q \) such that \( v \sim_{(\text{Local} \cup \text{Res}) \cup \text{It}} \bar{v} \). Notice that \( v \sim_{(\text{Local} \cup \text{Res}) \cup \text{It}} \bar{v} \).

Thus \( v \in \bar{\rho}(Q) \). We have shown that \( \bar{\rho}(\bar{\rho}(Q)) \subseteq \bar{\rho}(Q) \). The opposite inclusion follows from extensivity.

**Proposition 37.** \( \rho_c \) is a closure operator on \( (D, \subseteq) \)

**Proof.** We will show the three properties of a closure operator.

- **Monotonicity.** Let \( Q \subseteq Q' \) be sets of consistent states and \( v \in \rho_c(Q) \). Then \( v \in \text{ConsState} \) and for each block \( s \in R\bar{L} \) there is a state \( \bar{v} \in Q \) such that \( v \sim_s \bar{v} \). Notice that such \( \bar{v} \) are also in \( Q' \). We have shown \( \rho_c(Q) \subseteq \rho_c(Q') \).

- **Extensivity.** Let \( Q \subseteq D \). Let \( v \in Q \). Let \( s \in R\bar{L} \). Certainly \( v \sim_s v \). Thus \( v \in \rho_c(Q) \).

We have shown \( Q \subseteq \rho_c(Q) \).

- **Idempotence.** Let \( Q \subseteq D \). Let \( v \in \rho_c(\rho_c(Q)) \). Let \( s \in R\bar{L} \). Then there is some \( \bar{v} \in \rho_c(Q) \) such that \( v \sim_s \bar{v} \). Then there is some \( \bar{v} \in Q \) such that \( \bar{v} \sim_s \bar{v} \). Thus \( v \in \rho_c(Q) \). We have shown \( \rho_c(\rho_c(Q)) \subseteq \rho_c(Q) \). The opposite inclusion follows from extensivity.
Proposition 38. For all \( Q \in D \) we have \( \breve{\rho}(Q) \subseteq \rho_c(Q) \).

Proof. Let \( Q \in D \). Let \( v \in \breve{\rho}(Q) \). Let \( s \in RL \). By part 3 of Lemma 35 we have two cases. Case there is \( r \in Res \) such that \( s \subseteq r \). There are two subcases.

Case \( r \) is available in \( v \). Then there is some \( \hat{v} \in Q \) such that \( v \sim_s \hat{v} \). Let \( \hat{v} := \hat{v} \).

Case \( r \in rsc(v(pc_\ell)) \) for some \( t \in Tid \). Then there is \( \hat{v} \in Q \) such that \( v \sim_{\text{Local}\cup \text{Res}:i,s} \hat{v} \). Let \( \hat{v} := \hat{v} \).

Case \( s \cap \text{Res} = \emptyset \). Since \( s \neq \emptyset \), there is some \( t \in Tid \) such that \( s \subseteq \text{Local}_t \cup \text{Res} \). There is \( \hat{v} \in Q \) such that \( v \sim_{\text{Local}_t \cup \text{Res} v} \hat{v} \). Let \( \hat{v} := \hat{v} \).

In any case there is \( \hat{v} \in Q \) such that \( v \sim_s \hat{v} \).

For the purpose of the proof let \( T = (\text{init}, (\rightarrow)_i)_{i \in Tid} \) be an RPL transition system that obeys the given syntactic structure and has successor operator \( \text{post} \). Let \( F = \lambda x \in D. \breve{\rho}(\text{init} \cup \text{post}(x)) \), let \( \mu \in \text{Ord} \) have cardinality greater than the cardinality of \( D \) and let \( (Y^{(i)})_{i \in \mu} \) be the \( \mu \)-termed upper iteration sequence for \( F \) starting with \( 0 \in D : \)

\[
Y^{(0)} = \emptyset, \quad Y^{(\sigma + 1)} = F\left( Y^{(\sigma)} \right) \text{ for } \sigma + 1 \in \mu, \quad Y^{(a\sigma)} = \bigcup_{\sigma \in a\sigma} Y^{(\sigma)} \text{ for } a\sigma \in \mu.
\]

Let \( Q = \text{lfp}(F) \). The sequence \( (Y^{(i)})_{i \in \mu} \) is monotonically increasing, and its limit is \( Q \).

Lemma 39. Let \( t \neq \hat{t} \) in \( Tid \). Then

1. \( \forall \tau \in Tid, (v, v') \in \rightarrow_{\tau} : v \sim_{\text{Local}_t \cup \text{Local}_\hat{t}} v' \lor v \sim_{\text{Local}_t \cup \text{Local}_\hat{t} \cup \text{Res}} v' \);
2. \( \text{Local}_t \cap \text{Local}_\hat{t} = \bigcap_{i \in Tid} \text{Local}_i \).

Proof. 1. Let \( \tau \in Tid \), \( v \rightarrow_{\tau} v' \). Then \( \tau \neq t \) or \( \tau \neq \hat{t} \). From (1) we get \( v \sim_{\text{Local}_t} v' \) or \( v \sim_{\text{Local}_\hat{t}} v' \). In any case \( v \sim_{\text{Local}_t \cup \text{Local}_\hat{t}} v' \). In particular, \( v \sim_{\text{Local}_t \cup \text{Local}_\hat{t}} v' \).

2. “\( \subseteq \)”: Let \( x \in \text{Local}_t \cap \text{Local}_\hat{t} \) and \( i \in Tid \). We are going to show that \( x \in \text{Local}_i \).

First, the definition of the syntactic structure implies \( x \notin PCV \). Thus, \( x \in \text{Data} \).

Next, consider arbitrary \( \tau \in Tid \setminus \{ \hat{t} \} \) and \( (v, v') \in \rightarrow_{\tau} \). As shown above, \( v \sim_{\text{Local}_t \cup \text{Local}_\hat{t}} v' \), so \( v(x) = v'(x) \). We have shown \( \forall \tau \in Tid \setminus \{ \hat{t} \}, (v, v') \in \rightarrow_{\tau} : v(x) = v'(x) \).

By definition of RPL, \( x \in \text{Local}_i \).

“\( \supseteq \)”: Follows from \( \text{Local}_i \supseteq \bigcap_{i \in Tid} \text{Local}_i \) and \( \text{Local}_i \supseteq \bigcap_{i \in Tid} \text{Local}_j \).

Lemma 40. Let \( s \in RL \), \( t \neq \hat{t} \) in \( Tid \) such that \( s \subseteq \text{Local}_t \cap \text{Local}_\hat{t} \cup \text{Res} \).

Then \( \forall \sigma \in \mu, v \in Y^{(\sigma)} \exists w \in \text{init} : v \sim_s w \).

Proof. By transfinite induction. Let \( \sigma \in \mu \) and \( \forall \hat{\sigma} \in \sigma \forall v \in Y^{(\hat{\sigma})} \exists w \in \text{init} : v \sim_s w \). Let \( v \in Y^{(\sigma)} \). Then \( \sigma > 0 \). There are two cases.

Case \( \sigma = \hat{\sigma} + 1 \) for some \( \hat{\sigma} \in \mu \). There is some \( r \in \text{Res} \) such that \( s \subseteq r \). There are two cases.

Case \( r \in rsc(v(pc_\ell)) \) for some \( t \in Tid \). By definition of \( \breve{\rho} \) there is \( \breve{v} \in \text{init} \cup \text{post}(Y^{(\sigma)}) \) such that \( v \sim_{\text{Local}_t \cup \text{Res},i,s} \breve{v} \). In particular, \( v \sim_s \breve{v} \) and \( v(pc_\ell) = \breve{v}(pc_\ell) \). Thus \( r \in rsc(\breve{v}(pc_\ell)) \). Since in initial states all resources are available, \( \breve{v} \notin \text{init} \). So there is some \( z \in Y^{(\sigma)} \) such that \( \breve{v} \in \text{post}(\{z\}) \). Part 1 of Lemma 39 implies \( \breve{v} \sim_s z \). so \( v \sim_s z \).
Proof. \( \sigma \) Case

Let \( \sigma \) be a limit ordinal. Then there is \( \exists w \in \text{init} \) such that \( \forall v \in Y(\sigma) \). Apply the induction hypothesis.

Lemma 41. Let \( t \neq \bar{t} \in \text{Tid} \). Then \( \forall \sigma \in \mu, v \in Y(\sigma) \exists w \in \text{init} : v \sim_{(\text{Local} \setminus \text{Local}_{\bar{t}})} w. \)

Proof. Let \( C = (\text{Local} \cap \text{Local}_{\bar{t}}) \setminus \text{Res} \). We'll use transfinite induction. Let \( \sigma \in \mu \) and \( \forall \sigma \in \sigma \forall v \in Y(\sigma) \exists w \in \text{init} : v \sim_{C} w. \) Let \( v \in Y(\sigma) \). Then \( \sigma > 0 \).

Case \( \sigma = \bar{\sigma} + 1 \) for some \( \bar{\sigma} \in \mu \). By definition of \( Y(\sigma+1) \) there is \( \bar{v} \in \text{init} \setminus \text{post}(Y(\sigma)) \) such that \( v \sim_{\text{Local} \setminus \text{Local}_{\bar{t}}} \bar{v} \). Then \( v \sim_{C} \bar{v} \). If \( \bar{v} \in \text{init} \), let \( w := \bar{v} \). Otherwise there is \( \exists z \in Y(\sigma) \) such that \( \bar{v} \in \text{post}(\{z\}) \). Part 1 of Lemma 39 implies that \( \bar{v} \sim_{C} z \), so \( v \sim_{C} z \).

Applying the induction hypothesis to \( \bar{\sigma} \) and \( z \) we obtain some \( w \in \text{init} \) such that \( z \sim_{C} w \), so \( v \sim_{C} w \).

Case \( \sigma \) is a limit ordinal. Then there is \( \exists w \in \text{init} \) such that \( v \in Y(\sigma) \). Apply the induction hypothesis.

Lemma 42. Let \( s \in \bar{RL}, t \in \text{Tid} \), \( r \in \text{Res}, s \subseteq r \cap \text{Local}_{\bar{t}} \), and \( \forall \bar{t} \in \text{Tid} \setminus \{t\} : s \cap \text{Local}_{\bar{t}} = \emptyset \). Then \( \forall \sigma \in \mu, v \in Y(\sigma) : r \notin \text{rsc}(v(pc_{t})) \Rightarrow \exists w \in Y(\sigma) : v \sim_{\text{Local} \setminus \text{Res}} w \land r \text{ is available in } w. \)

Proof. We'll use transfinite induction. Let \( \sigma \in \mu \) and \( \forall \sigma \in \sigma \forall v \in Y(\sigma) : r \notin \text{rsc}(v(pc_{t})) \Rightarrow \exists w \in Y(\sigma) : v \sim_{\text{Local} \setminus \text{Res}} w \land r \text{ is available in } w. \) Let \( v \in Y(\sigma) \) such that \( r \notin \text{rsc}(v(pc_{t})) \). Then \( \sigma > 0 \).

Case \( \sigma = \bar{\sigma} + 1 \) for some \( \bar{\sigma} \in \mu \). If \( r \) is available in \( v \), take \( w := v \). Otherwise there is some \( \bar{t} \in \text{Tid} \setminus \{t\} \) such that \( r \in \text{rsc}(v(pc_{\bar{t}})) \). By definition of \( \rho \) there is \( y \in \text{init} \setminus \text{post}(Y(\sigma)) \) such that \( v \sim_{\text{Local} \setminus \text{Local}_{\bar{t}}} y. \) Then \( v(pc_{\bar{t}}) = y(pc_{\bar{t}}) \) and \( v \sim_{\text{Local} \setminus \text{Local}_{\bar{t}}} \).

Case \( \tau \neq \bar{t} \). From (1) we obtain \( \text{rsc}(z(pc_{\bar{t}})) = \text{rsc}(z(pc_{\bar{t}})) \), thus \( r \in \text{rsc}(z(pc_{\bar{t}})). \)

From \( z \in \text{Cons} \text{State} \) we get \( r \notin \text{rsc}(z(pc_{\bar{t}})) \). Thus \( r \in \text{Res}(\text{rsc}(y(pc_{\bar{t}})) \cup \text{rsc}(z(pc_{\bar{t}}))) \).

From (2) we get \( z \sim_{\bar{t}} y, z \sim_{\bar{t}} y, z \sim_{\bar{t}} y. \) Apply the induction hypothesis to \( \bar{\sigma} \) and \( z \).

Case \( \tau = \bar{t} \). From (1) we obtain \( z \sim_{\text{Local}, y, z \sim_{\bar{t}} y, z \sim_{\bar{t}} y, \text{Also } (z(pc_{\bar{t}})) = y(pc_{\bar{t}}), \) thus \( r \notin \text{rsc}(z(pc_{\bar{t}})) \). Apply the induction hypothesis to \( \bar{\sigma} \) and \( z \).

Case \( \sigma \) is a limit ordinal. Then there is \( \sigma \in \sigma \) such that \( v \in Y(\sigma) \). Apply the induction hypothesis to \( \bar{\sigma} \) and \( v \).

Lemma 43. Let \( t \in \text{Tid}, v \in Q, r \in \text{Res} \setminus \text{rsc}(v(pc_{t})) \), \( s \in \bar{RL}, s \subseteq r \cap \text{Local}_{\bar{t}} \).

Then \( \exists w \in Q : v \sim_{s \cap \text{Local}_{\bar{t}}} w \land r \text{ is available in } w. \)

Proof. There is some \( \sigma \in \mu \) such that \( v \in Y(\sigma) \).

Case there is \( \bar{t} \in \text{Tid} \setminus \{t\} \) such that \( s \subseteq \text{Local}_{\bar{t}} \). By Lemma 40 there is some \( w \in \text{init} \subseteq Q \) such that \( v \sim_{s \cap \text{Local}_{\bar{t}}} w \).

Notice that all resources are available in \( w \).

Case \( \forall \bar{t} \in \text{Tid} \setminus \{t\} : s \cap \text{Local}_{\bar{t}} = \emptyset \). Lemma 42 provides a suitable \( w \in Y(\sigma) \subseteq Q \).
Lemma 44. Let $t \in Tid$, $v \in Q$, $r \in Res \setminus \text{rsc}(v(pc_3))$. Then there is $w \in Q$ such that $r$ is available in $w$ and $w \sim_{\text{Local}_t \cup \text{rsc}(w(pc_3))} v$.

Proof. If $r$ is available in $w$, take $w := v$. Otherwise there is $\tilde{t} \in Tid \setminus \{t\}$ such that $r \in \text{rsc}(v(pc_3))$. Lemma 41 implies the existence of some $u \in \text{init}$ such that $u \sim_{\text{Local}_t \cup \text{Local}_\tilde{t} \cup \text{Res}_v}$. Let

$$w : \text{Val} \rightarrow \text{Val}, \quad x \mapsto \begin{cases} u(x), & \text{if } x \in (\text{Local}_t \cup \text{Res}) \cup ((\bigcup \text{rsc}(v(pc_3))) \setminus \text{Local}_t), \\ v(x), & \text{otherwise.} \end{cases}$$

We’ll show:

"$\sim rsc(v(pc_3)) \cup \text{rsc}(w(\text{PCVar})) = \emptyset$": $\text{rsc}(v(pc_3)) \cap \text{rsc}(w(\text{PCVar})) = \emptyset \cap (\text{rsc}(w(pc_3)) \cup \bigcup_{\tilde{t} \in Tid \setminus \{t\}} \text{rsc}(w(pc_3))) = \emptyset$ [since $v \in Cons\text{State}$].

"$w \sim_{\text{Local}_t \cup \text{rsc}(w(pc_3))} v$": Let $x \in \text{Local}_t \cup \text{rsc}(w(pc_3))$. There are two cases.

Case $x \in (\text{Local}_t \cup \text{Res}) \cup ((\bigcup \text{rsc}(v(pc_3))) \setminus \text{Local}_t)$. Then $w(x) = u(x)$.

Case $x \in \text{Local}_t \cup \text{Res}$. Then $w(x) = v(x)$, so $w(x) = v(x)$.

By the already proven, $\tilde{t} \notin \bigcup \text{rsc}(w(\text{PCVar}))$, so $w \notin \bigcup \text{rsc}(w(pc_3))$. Also $x \notin \text{Local}_t$. Thus $x \notin \text{Local}_t \cup \text{rsc}(w(pc_3))$, a contradiction.

Case $x \notin (\text{Local}_t \cup \text{Res}) \cup ((\bigcup \text{rsc}(v(pc_3))) \setminus \text{Local}_t)$. Then $w(x) = v(x)$.

"$w \in Q$": We’ll show first that $w$ is in $\rho(Q)$ as follows.

Initially, we’ll show that $w$ is a consistent state.

For all $\tilde{t} \in Tid$ we have $w(pc_3) \in \{u(pc_3), v(pc_3)\} \subseteq PL$ and $\text{rsc}(u(pc_3)) = \emptyset \subseteq \text{rsc}(v(pc_3))$. Thus for $t_1 \neq t_2$ in Tid we have $\text{rsc}(w(pc_3)) \cap \text{rsc}(w(pc_3)) \subseteq \text{rsc}(v(pc_3)) \cap \text{rsc}(\text{rsc}(v(pc_3))) = \emptyset$. Thus $w \in Cons\text{State}$.

Next, let $s \in RL$ and $\tilde{r} \in Res$ such that $s \subseteq \tilde{r}$. We will show that

"$(\hat{\tilde{r}} \notin \bigcup \text{rsc}(w(\text{PCVar})) \Rightarrow \exists \hat{\tilde{r}} \in Q : w \sim_{\text{Res}_\hat{\tilde{r}}} \tilde{r}) \land (\forall \tilde{t} \in Tid : \hat{\tilde{r}} \notin \text{rsc}(w(pc_3)) \rightarrow \exists \hat{\tilde{r}} \in Q : w \sim_{\text{Local}_t \cup \text{Res}_\hat{\tilde{r}}}}$".

Notice that $s \cap (\text{Local}_t \cup \text{Res}) = \emptyset$.

- Assume for a moment that $\tilde{r} \notin \bigcup \text{rsc}(w(\text{PCVar}))$. We distinguish two cases.

Case $\tilde{r} \in rsc(v(pc_3))$. By part 3 of Lemma 35 one of the following cases holds.

Case $s \subseteq \text{Local}_t$. Then $s \cap \{ \text{rsc}(v(pc_3)) \} \setminus \text{Local}_t = \emptyset$, so $w \sim_s v$. From $v \in Cons\text{State}$ we get $\tilde{r} \notin rsc(v(pc_3))$. By Lemma 43 there is $\hat{w} \in Q$ such that $v \sim_s \hat{w}$ and $\tilde{r}$ is available in $\hat{w}$. Then $w \sim_s \hat{w}$.

Case $s \cap \text{Local}_t = \emptyset$. Then $w \sim_s u$. Take $u := v$.

Case $\tilde{r} \notin rsc(v(pc_3))$. Then $w \sim_s v$. From $\tilde{r} \notin \bigcup\text{rsc}(w(pc_3)) \cup \bigcup_{\tilde{t} \in Tid \setminus \{t\}} \text{rsc}(v(pc_3))$ we get that $\tilde{r}$ is available in $v$. Take $u := v$.

- Let $\tilde{t} \in Tid$ such that $\tilde{r} \in \text{rsc}(w(pc_3))$. From $\tilde{r} \notin \emptyset = \text{rsc}(w(pc_3))$ we get $\tilde{t} \neq t$, so $\tilde{r} \in \text{rsc}(v(pc_3))$. From consistency of $v$ we get $\tilde{r} \notin \text{rsc}(v(pc_3))$. Thus $s \cap rsc(v(pc_3)) = \emptyset$. So $s \cap (\text{Local}_t \cup \text{Res}) \cup \{ \text{rsc}(v(pc_3)) \} \setminus \text{Local}_t = \emptyset$, thus $w \sim_s v$. Now let $x \in \text{Local}_t \cup \text{Res}$. Then $x \notin (\bigcup \text{rsc}(v(pc_3))) \setminus \text{Local}_t$.\]
Restatement of Lemma 17. Let \( t \in Tid, \forall v, v' \in P_{CVar} \) with \( r = rsc(v(pc)) \), \( r' = rsc(v'(pc)) \), \( r \in R' \setminus R, \hat{v}, \check{v} \in Q \). Then there is \( v' \in Q \) such that \( w \sim (Local \cup Local') \backslash \{v\} \). Let \( w : \forall v \rightarrow Val, x \mapsto \begin{cases} \check{v}(x), & \text{if } x \in r, \\ \hat{v}(x), & \text{if } x \notin r. \end{cases} \)

We claim:

\[ "r" \text{ is available in } w": \text{ Follows from } rsc(w(\{PCVar\})) = rsc(\{v(\{PCVar\})\}). \]
\[ "w \sim (Local \cup Local') \backslash \{v\}": \text{ From (5) we obtain } Local \cup Local' = Local \cup Local'. \text{ Then } w \sim (Local \cup Local') \backslash \{v\} \sim (Local \cup Local') \backslash \{v\}. \]
\[ "w \in Q": \text{ First, we'll show that } w \in \hat{\rho}(Q). \]

Initially, we'll show that \( w \in \hat{\rho}(Q) \). For all \( t \in Tid \), we have \( w(pc) = \hat{v}(pc) \in PL \). So for \( t_1 \neq t_2 \), \( w(\hat{v}(pc)) = rsc(\{PCVar\}) \cap rsc(\{v(\{PCVar\})\}) = [since \check{v} \in ConsState] \emptyset. \)

Next, let \( s \in RL, \check{v} \in Res, s \subseteq \check{v} \). We have to show two statements.

\[ "\check{v} \notin rsc(w(\{PCVar\})) \Rightarrow \exists \hat{v} \in Q : w \sim (Local \cup Local') \backslash \{v\}": \text{ Assume for a moment that } \check{v} \text{ is available in } w. \text{ We distinguish two cases.} \]

Case \( \check{v} = r. \text{ Notice that } w \sim r. \check{v} \text{ and } \check{v} \text{ is available in } \check{v}. \text{ Take } \hat{w} := \emptyset. \]

Case \( \check{v} \neq r. \text{ Then } \check{v} \cap r = \emptyset. \text{ Thus, } w \sim \check{v}. \check{v} \text{. Since } rsc(w(\{PCVar\})) = rsc(\{v(\{PCVar\})\}), \text{ we obtain that } \check{v} \text{ is available in } \check{v}. \text{ Take } \hat{w} := \check{v}. \]

At last, we'll show

\[ "\forall \check{v} \in Tid \exists \hat{v} \in Q : w \sim (Local \cup Local') \backslash \{v\}": \text{ Let } \hat{v} \in Tid \text{ be given. Then } w \sim (Local \cup Local') \backslash \{v\}. \text{ Take } \hat{w} := \hat{v}. \]

We have shown \( w \in \hat{\rho}(Q) \). From \( \hat{\rho}(Q) = Q \) we obtain \( w \in Q \).
By (4) and Remark 23 there is \( w' \) such that \( w \rightarrow_r w' \) and \( w' \sim_{\text{Local} \cup \bigcup R} v' \). Notice that \( w' \in \text{post}(Q) \subseteq Q \). \hfill \blacksquare

Let \( \mathcal{O} \) be the lattice of Owicki-Gries-core proofs of \( T \).

**Restatement of Theorem 18.** The strongest property provable by abstract interpretation with \( \rho \) is provable by the Owicki-Gries core. Formally:

\[
\gamma_{OG} \left( \inf \mathcal{O} \right) \subseteq \text{lpf} \left( \lambda x. \rho (\text{init} \cup \text{post}(x)) \right).
\]

**Proof.** For each \( r \in \text{Res} \) let

\[
I_r = \{ u \in (\text{ProofVar}(r) \rightarrow \text{Val}) \mid \exists \hat{v} \in Q : u \sim_r \hat{v} \land r \text{ is available in } \hat{v} \},
\]

and for all \( t \in \text{Tid} \), \( p \in \text{PL} \) let

\[
M_{p,t} = \{ u \in (\bigcup \text{LocalDataVar} \cup \bigcup \text{ProofVar}(\text{rsc}(p))) \rightarrow \text{Val}) \mid \exists \hat{v} \in Q : u \sim_{\text{LocalDataVar} \cup \text{LocalVar}(p)} \hat{v} \land \hat{v}(pc_r) = p \}.
\]

Let \( P = (I_r)_{r \in \text{Res}}, (M_{p,t})_{p \in \text{PL}, t \in \text{Tid}} \). We'll show that \( P \) is an Owicki-Gries-core proof that denotes a subset of \( Q \) by proving the following three properties.

**Sequential consistency.** Let \( t \in \text{Tid}, (v, v') \sim_r \rightarrow_r, p = v(pc_r), p' = v'(pc_r), R = \text{rsc}(p), R' = \text{rsc}(p'), v_{\text{LocalDataVar}}(R, \text{ProofVar}(R)) \subseteq M_{p,t} \text{ and } \forall r \in R' \setminus R : v_{\text{ProofVar}(r)} \in I_r \). Then there is \( \hat{v} \in Q \) such that \( \hat{v} \sim_{\text{LocalDataVar} \cup \text{LocalVar}(p')} v' \) and \( \hat{v}(pc_r) = p \). Then \( \hat{v}(pc_r) = v(pc_r) \).

Thus \( \hat{v} \sim_{\text{LocalDataVar} \cup \text{LocalVar}(p')} v' \) by (5) there are two cases.

Case \( R' \subseteq R \). Then \( \hat{v} \sim_{\text{LocalDataVar} \cup \text{LocalVar}(p')} v' \). From (4) and Remark 23 we obtain some \( \hat{v}' \in \text{ConsState} \) such that \( (v', \hat{v}') \sim_{\rightarrow_r} \land \hat{v}' \sim_{\text{LocalDataVar} \cup \text{LocalVar}(p')} v' \). Then \( \hat{v}' \in \text{post}(Q) \subseteq Q \). Also \( \hat{v}'(pc_r) = \hat{v}(pc_r) = p' \) and \( \hat{v}' \sim_{\text{LocalDataVar} \cup \text{LocalVar}(p')} v' \). Therefore, \( v' \sim_{\text{LocalDataVar} \cup \text{LocalVar}(p')} v' \) holds.

Now take any \( r \in R \setminus R' \) (by (5) there is one or none). Note that \( r \in \text{rsc}(v'(pc_r)) \).

Since \( \hat{v} \in \text{ConsState} \), we obtain that \( r \notin \bigcup_{t \in \text{Tid}(r)} \text{rsc}(v(pc_r)) = \{ \text{using (1)} \}
\[
\bigcup_{t \in \text{Tid}(r)} \text{rsc}(v'(pc_r)). \]Moreover, \( r \notin \text{rsc}(v'(pc_r)) \). Thus, \( r \) is available in \( v' \). We have \( v' \sim_r [\text{by (3)}] v' \sim_r [\text{since } r \in \text{R}] v' \sim_r [\text{by (3)}] v' \). Therefore, \( v' \sim_{\text{ProofVar}(r)} \in I_r \).

Case \( R' = R \setminus \{ r \} \) for some \( r \in \text{Res} \). From assumption \( v_{\text{ProofVar}(r)} \in I_r \), we obtain some \( \hat{v} \in Q \) such that \( v \sim_r \hat{v} \land r \) is available in \( \hat{v} \). By Lemma 17 there is \( w' \in Q \) such that \( v \sim_r w' \) and \( w' \sim_{\text{LocalDataVar} \cup \text{LocalVar}(p')} v' \). From \( w' \in Q, w'(pc_r) = p' \) and \( w' \sim_{\text{LocalDataVar} \cup \text{LocalVar}(p')} v' \) we obtain \( \hat{v} \sim_{\text{LocalDataVar} \cup \text{LocalVar}(p')} v' \) holds.

Initial condition. Let \( v \in \text{init} \). Then \( v \in \text{ConsState} \), all resources are available in \( v \) and \( v \in Q \). Thus for any \( r \in \text{Res} \) we have \( v_{\text{ProofVar}(r)} \in I_r \). Now let \( t \in \text{Tid} \). By definition of \( M_{v(pc_r), t} \) we obtain \( v_{\text{LocalDataVar} \cup \text{LocalVar}(v_{\text{ProofVar}(r)}(pc_r))} \subseteq M_{v(pc_r), t} \). So \( v \in \gamma_{OG}(P) \).

We've shown \( \text{init} \subseteq \gamma_{OG}(P) \).

Safe condition. Let \( v \in \gamma_{OG}(P) \). Then \( v \in \text{ConsState} \).

Let \( s \in \mathbb{RL}, r \in \text{Res}, s \subseteq r \). We'll show two statements. \(" r \notin \bigcup \text{rsc}(v(\text{PCVar})) \Rightarrow \exists \hat{v} \in Q : v \sim_r \hat{v} \land r \notin \bigcup \text{rsc}(v(\text{PCVar}))\): Assume for a moment that \( r \notin \bigcup \text{rsc}(v(\text{PCVar})) \). The definition of \( \gamma_{OG} \) implies that \( v_{\text{ProofVar}(r)} \in I_r \). So there is \( \hat{v} \in Q \) such that \( v \sim_r \hat{v} \) and \( r \) is available in \( \hat{v} \). Then \( v \sim_r \hat{v} \).
“∀t ∈ Tid : r ∈ rsc(ν(pc_1)) ⇒ ∃v ∈ Q: v ∼ Local(\cup \text{Res}) \cup F”:\ Let t ∈ Tid and r ∈ rsc(ν(pc_1)). Then v|_{LocalData∪\cup \text{ProofVar}(rsc(ν(pc_1)))} ∈ \{definition of γOG(M_r(\text{pc}_1)), rsc\}. Then there is \bar{v} ∈ Q such that \bar{v} ∼ LocalData∪\cup \text{ProofVar}(rsc(ν(pc_1))) v and \bar{v}(pc_1) = ν(pc_1). Thus \bar{v} ∼ Local\setminus\cup \text{Res} v and \bar{v} ∼ L ρ. Take \bar{v} := \bar{v}.

Now we’ll show that “∀ t ∈ Tid \exists v ∈ Q: v ∼ Local\setminus\cup \text{Res} v”: Let t ∈ Tid. The definition of γOG(P) implies v|_{LocalData∪\cup \text{ProofVar}(rsc(ν(pc_1)))} ∈ M_r(\text{pc}_1), t. So there is \bar{v} ∈ Q such that \bar{v}(pc_1) = ν(pc_1) and \bar{v} ∼ LocalData∪\cup \text{ProofVar}(rsc(ν(pc_1))) v. Then \bar{v} ∼ Local\setminus\cup \text{Res} v.

We’ve shown that v ∈ \bar{ρ}(Q) ⊆ [since Q is in the image of \bar{ρ} by definition, it is a fixpoint of \bar{ρ}] Q. Thus γOG(P) ⊆ Q.

Thus any property provable by abstract interpretation with \bar{ρ} has an Owicki-Gries-core proof.

**Corollary 45.** Let lfp(λx. ρ_ρ(init ∪ post(x))) ⊆ safe ∈ D. Then safe has an Owicki-Gries-core proof.

**Proof.** Let S = lfp(λx. ρ_ρ(init ∪ post(x))), S ⊆ safe ∈ D. From Prop. 38 we get \bar{ρ}(init ∪ post(S)) ⊆ \bar{ρ}_ρ(init ∪ post(S)) = S, so S is a postfix point of λx. \bar{ρ}(init ∪ post(x)) which is by Tarski’s fixpoint theorem greater than or equal to its least fixpoint. Thus lfp(λx. \bar{ρ}(init ∪ post(x))) ⊆ S ⊆ safe. Apply Thm. 18.

**Proposition 46.** Fix a syntactic structure (Tid, PL, Val, Res, (Local_1, pc_1), ∈ Tid, ProofVar, rsc) from StrSimple and let ConsState be the set of consistent states of this syntactic structure and D its powerset. Let \bar{ρ} and \bar{ρ}_ρ be defined for StrSimple as in Sections D and E, respectively. Then the following statements hold.

1. ρ = \bar{ρ}.
2. For all RPL transitions systems (init, (−r_i) ∈ Tid) from Simple that have successor map post and the set of Owicki-Gries-core proofs \bar{Ω} we have γOG(inf(\bar{Ω})) = lfp(λx. ρ(init ∪ post(x))) = lfp(λx. \bar{ρ}(init ∪ post(x))).

**Proof.** 1. Let Q ∈ D. Since [Res] ≤ 1, we distinguish two cases.

Case Res = ∅. Then

\bar{ρ}(Q) = \{v ∈ ConsState | ∀ t ∈ Tid ∃ \bar{v} ∈ Q: v ∼ Local, \bar{v}\} = \bar{ρ}(Q).

Case Res = \{r\}. Then r ≠ ∅. Then \bar{ρ}(Q) =

\{v ∈ ConsState \mid \left( r \notin \cup \text{rsc}(v(\text{PCVar})) \Rightarrow \exists \bar{v} ∈ Q: \left( r \notin \cup \text{rsc}(\bar{v}(\text{PCVar})) \wedge v ∼ Local, \bar{v} \right) \right) \}

[since r ≠ ∅ and is disjoint from all Local_i (t ∈ Tid), we have r ∈ RL] = \bar{ρ}(Q).
2. Let \((init, (\rightarrow_i)_{i \in \mathbb{N}})\) be an RPL transition system from Simple that obeys the fixed syntactic structure and has a set of Owicki-Gries-core proofs \(\mathcal{O}\) and successor map \(post\). Then \(lfp(\lambda x. \rho(init \cup post(x))) \subseteq [\text{Thm. 10}] \cap \mathcal{O}(\inf D) \subseteq [\text{Thm. 18}]\ \ lfp(\lambda x. \rho(init \cup post(x))) \subseteq \{\text{part 1 of this Lemma}\} lfp(\lambda x. \rho(init \cup post(x))).

**Extension of Example 19.** Consider the RPL transition system Readers-Writers from Example 1.

Notice that \(|Res| = 1\). Moreover, \(\forall t \in \text{Tid}: \text{Local} \cap \text{control} = \{pc_1\} \cap \{ww, ar, aw\} = \emptyset\) and \(\text{ProofNar} (\text{control}) = \text{control}\). Thus Readers-Writers belongs to Simple and its syntactic structure belongs to StrSimple. By Prop. 46, part 2, the strongest Owicki-Gries-core-provable property is equal to \(lfp(\lambda x. \rho(init \cup post(x))) = lfp(\lambda x. \rho(init \cup post(x))).\)

**Extension of Example 20.** For the RPL transition system Upper from Example 2 we have \(RL = \{r, r', \text{Local}_1, \text{Local}_2\} = \{\{u, z\}, \{x, y\}, \{x, l, pc_1\}, \{y, z, pc_2\}\}, \text{RL} = \{\{u\}, \{z\}, \{x\}, \{y\}, \{l, pc_1\}, \{pc_2\}\}.\) Let

\[
C = \{v \in \text{ConsState} \mid v(u), v(z), v(x), v(y), v(l) \in \{0, 1\} \land v(pc_2) = 0\}.
\]

The upper iteration sequence \((X^{(i)})_{i \in \omega}\) for \(\lambda x. \rho(init \cup post(x))\) starting from \(\emptyset \in D\) is below.

\[
X^{(0)} = \emptyset,
\]

\[
X^{(1)} = \rho(init) = \{v \in C \mid v(pc_1) = A\},
\]

\[
post(X^{(1)}) = \{v \in C \mid v(pc_1) = B \land v(l) = v(u)\},
\]

\[
X^{(2)} = \rho(init \cup post(X^{(1)})) = \{v \in C \mid v(pc_1) = A \lor (v(pc_1) = B \land v(u) = v(l))\},
\]

\[
post(X^{(2)}) = \{v \in C \mid v(pc_1) \in \{B, C\} \land v(u) = v(l)\},
\]

\[
X^{(3)} = \rho(init \cup post(X^{(2)})) = \{v \in C \mid v(pc_1) = A \lor (v(pc_1) \in \{B, C\} \land v(u) = v(l))\},
\]

\[
post(X^{(3)}) = \{v \in C \mid (v(pc_1) \in \{B, C\} \land v(u) = v(l)) \lor (v(pc_1) = D \land v(u) = v(l) \land v(x) = 0)\},
\]

\[
X^{(4)} = \rho(init \cup post(X^{(3)})) = \{v \in C \mid v(pc_1) = A \lor (v(pc_1) \in \{B, C\} \land v(u) = v(l)) \lor (v(pc_1) = D \land v(u) = v(l) \land v(x) = 0)\},
\]

\[
post(X^{(4)}) = \{v \in C \mid (v(pc_1) \in \{B, C\} \land v(u) = v(l)) \lor (v(pc_1) \in \{B, E\} \land v(u) = v(l) \land v(x) = 0)\},
\]

\[
X^{(5)} = \rho(init \cup post(X^{(4)})) = \{v \in C \mid v(pc_1) = A \lor (v(pc_1) \in \{B, C, E\} \land v(u) = v(l)) \lor (v(pc_1) = D \land v(u) = v(l) \land v(x) = 0)\},
\]

\[
post(X^{(5)}) = \{v \in C \mid (v(pc_1) \in \{B, C\} \land v(u) = v(l)) \lor (v(pc_1) \in \{B, E\} \land v(u) = v(l) \land v(x) = 0)\} \subseteq X^{(5)}, \text{ so}
\]

\[
X^{(6)} = \rho(init \cup post(X^{(5)})) \leq \rho(init \cup X^{(5)}) = \rho(X^{5}) = X^{(5)}.
\]
Thus
\[
\text{ifp}(\lambda x. \hat{\varphi}(\text{init} \cup \text{post}(x))) = \begin{cases} 
  v \in C & v(pc_1) = A \\
  v(pc_1) \in \{B, C, E\} \land v(u) = v(l) \\
  v(pc_1) = D \land v(u) = v(l) \land v(x) = 0 
\end{cases}
\]
is strictly weaker than the strongest Owicki-Gries-core-provable property, e.g., containing the state \([u \rightarrow 0, z \rightarrow 0, x \rightarrow 0, y \rightarrow 0, l \rightarrow 0, pc_1 \rightarrow k, pc_2 \rightarrow 0] \notin \gamma_{\mathsf{OG}}(\text{init})\].

**Extension of Example 22.** Fix an RPL transition system from SepThreads. For all \(S \subseteq \text{ConsState}\) we have
\[
\hat{\varphi}(S) = \{v \in \text{ConsState} \mid \forall t \in \text{Tid} \exists \exists_{\text{Local}} v : v \sim v\} = \hat{\varphi}(S).
\]
Within this example, let \(F := \lambda x. \text{init} \cup \text{post}(x)\) and \(Q := \text{ifp}(F)\). Notice that \(\text{post}\) is a join-morphism, so is \(F\). By Kleene’s fixpoint theorem \(Q = \bigcup_{n \in \mathbb{N}} F^n(\emptyset)\). Let \(v \in \hat{\varphi}(Q)\). Then there is a map \(m : \text{Tid} \rightarrow \mathbb{N}\) such that \(\forall t \in \text{Tid} \exists \exists_{\text{Local}} v : v \sim v\). Since \(\text{Tid}\) is finite and the sequence \((F^n(\emptyset))_{n \in \mathbb{N}}\) is monotonically increasing, \(\forall t \in \text{Tid} \exists \exists_{\text{Local}} v : v \sim v\). Thus \(v \in \hat{\varphi}(F^{\text{max}(\text{Tid})}(\emptyset))\).

We have shown that \(\hat{\varphi}(Q) \subseteq \bigcup_{n \in \mathbb{N}} \hat{\varphi}(F^n(\emptyset))\). Now we are going to show by induction that for each \(i \in \mathbb{N}\) the set \(\hat{\varphi}(F^i(\emptyset))\) is a subset of \(Q\).

**Case i = 0.**
Then \(\hat{\varphi}(F^0(\emptyset)) = \hat{\varphi}(\text{init}) \subseteq \text{def. of SepThreads} \text{init} \subseteq Q\).

**Case i > 1.** Let \(v \in \hat{\varphi}(F^i(\emptyset))\), i.e., \(v \in \hat{\varphi}(\text{init} \cup \text{post}(F^{i-1}(\emptyset)))\). Let \(I = \{t \in \text{Tid} \mid \exists \exists_{\text{Local}} v \sim v\}\). Then for all \(t \in \text{Tid} \setminus I\) there is \(\exists_{\text{Local}} v \sim v\). Thus there are maps \(f, f' : \text{ConsState} \rightarrow \text{ConsState}\) such that \(\forall t \in K : f(t) \in F^{i-1}(\emptyset) \land f(t) \sim f'(t) \land f'(t) \sim \exists_{\text{Local}} v\), where \(K = \text{Tid} \setminus (I \cup J)\). Let \(\varphi = \bigcup_{j \in \mathbb{N}} (\text{Local}_{t_j} \setminus \text{Local}_{t_i})\). There is a map \(h : (\varphi \setminus C) \rightarrow \text{Tid}\) such that \(\forall x \in \varphi \setminus C : x \in \text{Local}_{h(x)}\). Such a map \(h\) is unique. Let \(n = |K|\), and fix some enumeration \(\tau_1, \ldots, \tau_n\) of \(K\). For each \(k \in \mathbb{N}\) let
\[
w^{(k)} : \varphi \rightarrow \text{Val}, x \mapsto \begin{cases} 
  v(x), & \text{if } x \in C \cup \bigcup_{j \in \mathbb{N}} \text{Local}_{t_j} \cup \bigcup_{j=1}^k \text{Local}_{t_j}, \\
  f(h(x))(x), & \text{if } x \in \bigcup_{k+1}^n \text{Local}_{t_j} \setminus C.
\end{cases}
\]
To show that each \(w^{(k)}\) is well-defined (0 ≤ k ≤ n), notice that

- \(\varphi \subseteq C \cup \bigcup_{j \in \mathbb{N}} \text{Local}_{t_j} \cup \bigcup_{j=1}^k \text{Local}_{t_j} \cup \bigcup_{j=k+1}^n \text{Local}_{t_j} \setminus C\);
- \((I \cup J) \cap K = \emptyset\) and the definition of \(C\) imply that for \(a \in I \cup J \cup \{\tau_j \mid 1 \leq j \leq k\}\) and \(b \in \{\tau_j \mid k < j \leq n\}\) we have \(\text{Local}_{a} \cap (\text{Local}_{b} \setminus C) = \emptyset\).
Now we’ll show by induction that for all \( k \in \mathbb{N}_0 \cap [0,n] \) we have \( w^{(k)} \in Q \).

Case \( k = 0 \). First, we’ll show that \( w^{(0)} \) is in \( \hat{\rho}(F^{i-1}(\emptyset)) \). Let \( t \in \text{Trd} \).

Case \( t \in I \). Then \( w^{(0)} \sim^{\text{Local}_t} v \). By definition of \( I \), there is some \( \tilde{v} \in \text{init} \) such that \( v \sim^{\text{Local}_t} \tilde{v} \). Then \( w^{(0)} \sim^{\text{Local}_t} \tilde{v} \). From \( i-1 \geq 1 \) we get \( F^{i-1}(\emptyset) \supseteq \text{init} \).

Case \( t \in J \). Then \( w^{(0)} \sim^{\text{Local}_t} v \). By definition of \( J \), there is some \( \tilde{v} \in F^{i-1}(\emptyset) \) such that \( v \sim^{\text{Local}_t} \tilde{v} \). Then \( w^{(0)} \sim^{\text{Local}_t} \tilde{v} \).

Case \( t \in K \). Let \( x \in \text{Local}_t \). There is some \( j \in \mathbb{N}^+ \cap [1,n] \) such that \( t = \tau_j \); then \( x \in \text{Local}_{\tau_j} \).

Case \( x \in C \). Then \( w^{(0)}(x) = v(x) = f'(\tau_j)(x) = [\text{part 1 of Lemma 39}] \) and \( x \in C \). Notice that \( f(\tau_j)(x) = f(t)(x) \).

Case \( x \notin C \). Then \( f(\tau_j)(x) = w^{(k-1)}(x) \).

We have shown that \( w^{(0)}(x) = f(t)(x) \) for all \( x \in \text{Local}_t \). Thus \( w^{(0)} \sim^{\text{Local}_t} f(t) \). Notice that \( f(t) \in F^{i-1}(\emptyset) \).

Thus \( w^{(0)} \in \hat{\rho}(F^{i-1}(\emptyset)) \). By induction hypothesis, \( \hat{\rho}(F^{i-1}(\emptyset)) \subseteq Q \). Thus \( w^{(0)} \in Q \).

Case \( k \geq 1 \). We are going to show two auxiliary statements.

1. We’ll show now that \( w^{(k-1)} \sim^{\text{Local}_t} w^{(k-1)} \): Let \( x \in \text{Local}_{\tau_k} \).

Case \( x \in C \). Then \( f(\tau_j)(x) = [\text{part 1 of Lemma 39}] \) and \( x \in C \). Notice that \( h(x) = \tau_k \). Then \( f(\tau_j)(x) = w^{(k-1)}(x) \).

2. \( w^{(k-1)} \rightarrow_{\tau_k} w^{(k)} \): From (4) and \( f(\tau_j) \rightarrow_{\tau_k} f'(\tau_j) \) we obtain some \( w' \) such that \( w^{(k-1)} \rightarrow_{\tau_k} w' \) and \( w' \sim^{\text{Local}_t} f'(\tau_j) \). We’ll show now that \( w' \) is equal to \( w^{(k)} \).

So let \( x \in \text{Var} \) be arbitrary.

Case \( x \in C \cup \bigcup_{\tau \in I \cup J} \text{Local}_t \). If \( x \in C \), part 1 of Lemma 39 implies \( w'(x) = w^{(k-1)}(x) \). If \( x \in \text{Local}_t \) for some \( t \in I \cup J \), then \( t \neq \tau_k \), so (1) implies \( w'(x) = w^{(k-1)}(x) \). In both cases \( w'(x) = w^{(k-1)}(x) = v(x) = w^{(k)}(x) \).

Case \( x \in \text{Local}_{\tau_k} \). Then \( w'(x) = f'(\tau_k)(x) = v(x) = w^{(k)}(x) \).

Case \( x \in \text{Local}_{\tau_j} \) for some \( j \neq k \). Then \( w'(x) = [\text{by (1)}] w^{(k-1)}(x) \). If \( j < k \), then \( w^{(k-1)}(x) = [\text{since } j < k-1] v(x) = [\text{since } j < k] k^{(k)}(x) \).

If \( j > k \), then \( w^{(k-1)}(x) = [\text{since } j > k \text{ for some } h(x)](x) = [\text{since } j > k + 1] k^{(k)}(x) \).

Since \( x \) was arbitrary, \( w' = w^{(k)} \). Thus, \( w^{(k-1)} \rightarrow_{\tau_k} w^{(k)} \).

By induction hypothesis, \( w^{(k-1)} \in Q \). Then, \( w^{(k)} \in \text{post}(\{w^{(k-1)}\}) \subseteq \text{post}(Q) \subseteq Q \).

In particular, \( v = w^{(n)} \in Q \).

We have proven by induction that \( \forall i \in \mathbb{N}_0: \hat{\rho}(F^i(\emptyset)) \subseteq Q \). Thus \( \hat{\rho}(Q) \subseteq Q \). So \( \hat{\rho}(F(Q)) = \hat{\rho}(Q) \), i.e., \( Q \) is a fixpoint of \( \hat{\rho} \circ F \). Since \( Q = \text{lfp}(F) \subseteq \text{lfp}(\hat{\rho} \circ F) \subseteq Q \).

\[ \text{lfp}(\lambda x. \hat{\rho}(\text{init} \cup \text{post}(x))) = \text{lfp}(\hat{\rho} \circ \text{init} \cup \text{post}(x)). \]
By Theorems 10 and 18 we also get
\[ \text{lfp}(\lambda x. \rho(\text{init} \cup \text{post}(x))) = \gamma_{\mathcal{I}}(\inf \Omega) = \text{lfp}(\lambda x. \rho(\text{init} \cup \text{post}(x))). \]

\[ \square \]

**F Absence of equivalent semantic characterization in abstract interpretation**

Given a complete lattice \( D \), a *semantic transformation* over \( D \) is a map \( F^\# \in (D \to D) \to D \to D \) such that

- for all join morphisms \( \tau \in D \to D \), the map \( F^\#_\tau : D \to D \) is monotone and
- for all join morphisms \( \tau_1, \tau_2 \in D \to D \) we have

\[ \text{lfp}(\tau_1) = \text{lfp}(\tau_2) \Rightarrow \text{lfp}(F^\#_\tau_1) = \text{lfp}(F^\#_\tau_2). \]

**Lemma 47.** Let \((D, \subseteq)\) be a complete lattice and \( f : (D \times D) \to D \) be any map that is monotone in the second component. Then

\[ F^\# : (D \to D) \to (D \to D), \quad \tau \mapsto \lambda x. f \left( \begin{cases} \text{lfp}(\tau), & \text{if } \tau \text{ is monotone} \\ \sup D, & \text{otherwise} \end{cases} \right) \]

is a semantic transformation.

**Proof.** For all join morphisms \( \tau \in D \to D \) and all elements \( x \subseteq y \) of \( D \) we have \( F^\#_\tau(x) = f(\text{lfp}(\tau), x) \subseteq f(\text{lfp}(\tau), y) = F^\#_\tau(y) \).

Now take two join morphisms \( \tau_1, \tau_2 \in D \to D \) such that \( \text{lfp}(\tau_1) = \text{lfp}(\tau_2) \). Then \( \text{lfp}(F^\#_\tau_1) = \text{lfp}(\lambda x. f(\text{lfp}(\tau_1), x)) = \text{lfp}(\lambda x. f(\text{lfp}(\tau_2), x)) = \text{lfp}(F^\#_\tau_2). \) \( \square \)

**Example 48.** Given a complete lattice \( D \), the following maps are semantic transformations (where infimum over the empty set is the top of \( D \)):

- \( \lambda \tau \in D \to D. \lambda x \in D. \sup(D); \)
- \( \lambda \tau \in D \to D. \lambda x \in D. \inf\{y \in D \mid \tau(y) = y\}; \)
- \( \lambda \tau \in D \to D. \lambda x \in D. \sup\{\inf\{y \in D \mid \tau(y) = y\}\}, x\). \( \square \)

Given a syntactic structure \((\text{Tid}, \text{PL}, \text{Val}, \text{Res}, (\text{Local}, \rho_c), rsc)\) and \((\text{ProofVar}, rsc)\), let

\[ \text{Trace} = \text{ConsState}^*, \quad \tilde{D} = \mathcal{P}(\text{Trace}) \quad \text{and} \quad \tilde{\alpha} : \tilde{D} \to D, \quad T \mapsto \bigcup_{\delta \in T} \pi_2(\delta), \]

where a trace is viewed as a finite word, i.e., a map from \( \mathbb{N}_n \) for some natural \( n \in \mathbb{N}^+ \) to consistent states, and where \( \pi_2(\delta) = \{ y \mid \exists x \in \delta : (x, y) \in \delta \} \) is the set of states occurring in the trace \( \delta \).

Given a program \((\text{init}, (\to_t), r)\) that obeys the above syntactic structure, its set of **initial traces** is \( \text{init} = \{(1, v) \mid v \in \text{init}\} \) and its **trace extension operator** is

\[ \tilde{\text{post}} : \tilde{D} \to \tilde{D}, \quad T \mapsto \{ \delta v' \mid \delta v \in T \land \exists t : (v, v') \in \to_t \}. \]

44
Restatement of Theorem 6. There is a syntactic structure
(Tid, PL, Val, Res, (Local, pc) ∈ Tid, ProofVar, rsc)
such that for ConsState, D, D, α defined as above, all the following statements hold:
1. There is no semantic transformation $F^#$ over D such that for any RPL transition
system (init, . . . ) that obeys the syntactic structure, has successor map post and the
least Owicki-Gries-core proof P, we have
$$\gamma_{OG}(P) = \text{lfp}(F^#_{\lambda x. \text{init} \cup \text{post}(x)}).$$
2. There is no monotone operator $\rho : D \rightarrow D$ such that for any RPL transition
system (init, . . . ) that obeys the syntactic structure, has successor map post and the
least Owicki-Gries-core proof P, we have
$$\gamma_{OG}(P) = \text{lfp}(\lambda x. \rho(\text{init} \cup \text{post}(x))).$$
3. There is no monotone operator $\tilde{\rho} : \tilde{D} \rightarrow \tilde{D}$ such that for any RPL transition
system that obeys the syntactic structure, has a set of initial traces init, has a trace extension
operator post and has the least Owicki-Gries-core proof P, we have
$$\gamma_{OG}(P) = \tilde{\alpha}(\text{lfp}(\lambda x. \tilde{\rho}(\text{init} \cup \text{post}(x)))).$$

Proof. Consider the syntactic structure S given by
- Tid = \{1, 2\};
- PL = \{A, B, C, . . . , V, W\};
- Val = PL ∪ \{0, 1\};
- Res = \{r, r’\} where r = \{u, z\}, r’ = \{x, y\};
- Local₁ = \{l, x, pc₁\}, Local₂ = \{y, z, pc₂\};
- ProofVar(r) = r and ProofVar(r’) = r’.
- rsc : PL → \powerset(Res) given by

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>rsc(p)</td>
<td>{r}</td>
<td>{r’}</td>
<td>{r, r’}</td>
</tr>
</tbody>
</table>

The distribution of variables into different sets is given in Figure 4.

![Distribution of variables of program UpperA.](image)

Fig. 4: Distribution of variables of program UpperA.

Let D be the powerset of the set of consistent states defined by S as stated in the theorem.
The RPL transition system UpperA defined by Fig. 5 obeys S. It differs from Upper
only at location A.
We are going to show an Owicki-Gries-core proof of property \textit{init} for \textit{UpperA}. Let 
\[ I_r = \{ [u \mapsto 0, z \mapsto 1], [u \mapsto 1, z \mapsto 0] \}, \ I_r' = \{ [x \mapsto 0, y \mapsto 0], [x \mapsto 1, y \mapsto 1] \}, \]
\[ M_{A,1} = \{ [x \mapsto 0, l \mapsto 0], [x \mapsto 1, l \mapsto 1] \}, \]
\[ M_{0,2} = \{ [y \mapsto 0, z \mapsto 0], [y \mapsto 1, z \mapsto 1] \} \text{ and} \]
\[ M_{x,l} = \emptyset \text{ for } (x,t) \in (\text{PL} \times \text{Tid}) \setminus \{(A,1),(0,2)\}. \]

Let \( P_{\text{UpperA}} = ([r \mapsto I_r, r' \mapsto I_r'], (M_{x,t})_{x \in \text{PL}, t \in \text{Tid}}) \). Now we will show that \( P_{\text{UpperA}} \) is an Owicki-Gries-core proof denoting \textit{init}.

By definition, \( P_{\text{UpperA}} \in \)
\[ (\Psi(\text{ProofVar}(r) \rightarrow \text{Val}) \times \Psi(\text{ProofVar}(r') \rightarrow \text{Val})) \times \]
\[ (\Psi(\text{LocalDataVar}_1 \rightarrow \text{Val}) \times \Psi(\text{LocalDataVar}_2 \rightarrow \text{Val}) \times \]
\[ \Psi((\text{LocalDataVar}_1 \cup \text{ProofVar}(r)) \rightarrow \text{Val}) \times \]
\[ \ldots, \]

where the components are indexed by \( r, r' \) in the first line and \((A,1), (0,2), (8,1) \) and so on in the remainder. Thus \( P_{\text{UpperA}} \in PA \). We will show:

- Sequential consistency. Let \( t \in \text{Tid} \), \( (v,v') \in \rightarrow_t \), \( R = \text{rsc}(v(pc_1)), R' = \text{rsc}(v'(pc_2)) \), as well as \( \forall \text{LocalDataVar}_1 : \exists (\text{LocalDataVar}_1 \cup \text{ProofVar}(R)) \in M_{(pc_1),t} \) and \( \forall r \in R' \setminus R : \forall \text{ProofVar}(r) \in I_r \).
  - Case \( v(pc_1) \notin \{A,0\} \). Then thread \( r \) can’t proceed from \( v \), a contradiction.
  - Case \( v(pc_1) \in \{A,0\} \). Then \( v \in \text{LocalDataVar}_1 \cup \text{ProofVar}(R) \in \emptyset \), a contradiction.

- Initial condition. We have
\[ \gamma(OG(P_{\text{UpperA}})) = \{ [u \mapsto 1, z \mapsto 0, x \mapsto 0, y \mapsto 0, l \mapsto 0, pc_1 \mapsto A, pc_2 \mapsto 0], \]
\[ [u \mapsto 0, z \mapsto 1, x \mapsto 1, y \mapsto 1, l \mapsto 1, pc_1 \mapsto A, pc_2 \mapsto 0] \} \].

Notice that \( init \subseteq \gamma(OG(P_{\text{UpperA}})) \).

Since \( \gamma(OG(P_{\text{UpperA}})) \subseteq init \), \( P_{\text{UpperA}} \) is an Owicki-Gries-core proof of property \textit{init} for the program \textit{UpperA}. 

Fig. 5: Program UpperA.
The RPL transition system Upper from Example 2 also obeys $S$ and has the same initial states as UpperA, but, as stated in the example, has no Owicki-Gries-core proof of $init$.

Now we’ll show the claims of the theorem.

Let $postU$ be the successor map of Upper and $postUA$ the successor map of UpperA. Notice that $postU(init) = postUA(init)$, since the values of program variables $l$ and $u$ are different in each state of $init$. Moreover, $init$ is exactly the set of reachable states of both Upper and UpperA. In particular, $init$ is the strongest Owicki-Gries-core-provable property of UpperA.

1. Assume for the purpose of contradiction that a monotone operator $\rho : D \rightarrow D$ exists such that for any RPL transition system $T = (init, \ldots)$ that obeys $S$ and has successor map $post$ we have

$$\gamma_{OG}(\text{the smallest Owicki-Gries-core proof of } T) = \text{lfp}(F_{\lambda x.\text{init} \cup post(x)}^\#).$$

Notice that $\lambda x.\text{init} \cup postU(x)$ and $\lambda x.\text{init} \cup postUA(x)$ are join-morphisms on the same lattice and their least fixpoints coincide. By the assumption, for UpperA with successor map $postUA$, the strongest Owicki-Gries-core-provable property is $\text{lfp}(F_{\lambda x.\text{init} \cup postUA(x)}^\#)$. Thus, $init = \text{lfp}(F_{\lambda x.\text{init} \cup postUA(x)}^\#)$, which is also the strongest Owicki-Gries-core-provable property of Upper. Contradiction!

2. Assume for the purpose of contradiction that a monotone operator $\rho : D \rightarrow D$ exists such that for any RPL transition system $T = (init, \ldots)$ that obeys $S$ and has successor map $post$ we have

$$\gamma_{OG}(\text{the smallest Owicki-Gries-core proof of } T) = \text{lfp}(\lambda x.\rho(\text{init} \cup post(x))).$$

Then for UpperA with initial states $init$ and successor map $postUA$ we have $\text{lfp}(\lambda x.\rho(\text{init} \cup postUA(x))) = init$. So $\rho(\text{init} \cup postUA(init)) = init$. Since $postUA(init) = postU(init)$, we get $\rho(init \cup postU(init)) = init$. Then $\text{lfp}(\lambda x.\rho(\text{init} \cup postU(x))) \subseteq init$. Applying the assumption to Upper, we get an Owicki-Gries-core proof $P$ of Upper such that $\gamma_{OG}(P) \subseteq init$. But Upper has no Owicki-Gries-core proof of $init$. Contradiction!

3. Assume for the purpose of contradiction that a monotone operator $\tilde{\rho} : \tilde{D} \rightarrow \tilde{D}$ exists such that for any RPL transition system $T = (init, \ldots)$ that obeys $S$ and has $init$ as a set of initial traces and the trace extension operator $post$ we have

$$\gamma_{OG}(\text{the smallest Owicki-Gries-core proof of } T) = \tilde{\alpha}(\text{lfp}(\lambda x.\tilde{\rho}(\text{init} \cup post(x)))).$$

Then for UpperA with the set of initial traces $init$ and the trace extension operator $\tilde{\text{postUA}}$ we have $\tilde{\text{init}} = \tilde{\alpha}(\text{lfp}(\lambda x.\tilde{\rho}(\tilde{\text{init}} \cup postUA(x))))$. From definition of $\tilde{\alpha}$ we get $\text{lfp}(\lambda x.\tilde{\rho}(\tilde{\text{init}} \cup postUA(x))) \subseteq \text{init}^\#$. Consider the upper fixpoint iteration sequence $(X^\prime)_{\mu}$ for $\lambda x.\tilde{\rho}(\tilde{\text{init}} \cup postUA(x))$ that starts with $X^0 = \emptyset$ and where $\mu > |\tilde{D}|$ is some ordinal. This sequence is monotonically increasing and its limit is a subset of $\text{init}^\#$. Since $\text{postU}(\text{init}^\#) = \emptyset = postUA(\emptyset)$, we have $\tilde{\rho}(\text{init} \cup postU(\text{init}^\#)) = \tilde{\rho}(\tilde{\text{init}} \cup postUA(X^0)) = X^1 \subseteq \text{init}^\#$. So $\text{init}^\# \in \text{postfp}(\lambda x.\tilde{\rho}(\tilde{\text{init}} \cup postUA(x)))$. Thus,
\[ \text{lfp}(\lambda x. \tilde{\rho}(\text{init} \cup \text{postU}(x))) \subseteq \text{init}^*, \text{so } \tilde{\alpha}(\text{lfp}(\lambda x. \tilde{\rho}(\text{init} \cup \text{postU}(x)))) \subseteq \text{init}. \]

By assumption, the smallest Owicki-Gries-core proof of Upper denotes a subset of init. But Upper has no Owicki-Gries-core proof of init. Contradiction! \[ \blacksquare \]

**Remark 49.** The proof relied on the statements assume false to denote blocking. Strictly speaking, Owicki’s RPL does not have an assume statement. A purist may emulate it by while true do begin end or by with \( r' \) when false do endwith for an empty fresh resource \( r' \).

It is also possible to rewrite Upper and UpperA into nonblocking terminating programs using if-then-else statements.

Moreover, the programs of the proof depend on realizability of the overlap of resources and locals, but require a relatively small number (five) of data variables.

As a consequence, Thm. 6 holds even for the restricted class of programs that are written strictly in the original Owicki’s syntax, in which every execution terminates with threads at their final locations, and that use at most five data variables. \[ \square \]

## G Improving precision

Now we will show a method, called Relaxed Frontier Search [21], that allows improving precision of many abstract interpretations, in particular, of the Owicki-Gries core. First we will show the general case and then specialize it to the Owicki-Gries core.

### G.1 Relaxed Frontier Search - in general

Now we will show relaxed frontier search for a large class of abstract transfer functions.

Within Section G.1, let \((D, \subseteq)\) be a complete lattice of sets, \((D^\#, \subseteq)\) a complete lattice, \((\alpha, \gamma)\) a pair of adjoint maps, init \(\in D\), post : \(D \rightarrow D\) a complete join morphism and post^# : \(D^\# \rightarrow D^\#\) a monotonic operator such that \(\forall Y \in D^\# : \alpha \text{post}^Y \subseteq \text{post}^# Y\).

Intuitively, \(D\) is the powerset of program states, init is the set of initial states, post maps a set of states to the set of their direct successors, \(D^\#\) is an abstract lattice used for analysis and post^# is an abstract transformer.

The relaxed frontier search sequence is the sequence \((T^{(i)})_{i \in \mathbb{N}_0}\) of elements of \(D^\#\) defined recursively by

\[ T^{(0)} = \alpha \text{init}, \]

\[ T^{(i+1)} = \begin{cases} \text{post}^# T^{(i)}, & \text{if } \text{post}^# T^{(i)} \not\subseteq \bigcup_{j=0}^i T^{(j)}, \\ T^{(i)} \cup \text{post}^# T^{(i)}, & \text{if } \text{post}^# T^{(i)} \subseteq \bigcup_{j=0}^i T^{(j)}. \end{cases} \]

Let \(k = \min\{i \mid T^{(i+1)} \subseteq T^{(i)}\} \in \mathbb{N}_0 \cup \\{\infty\}\) (where \(\infty = \min \emptyset\)).

The height of a partial order is the supremum over cardinalities of its chains.

The above (in general non-monotone) sequence is the basis of our algorithm, which needs only elements of the sequence up to position \(k\). First we prove that \(k\) is well-defined, and is asymptotically at most quadratic in the height of \(\subseteq\).

**Proposition 50.** If the height \(h\) of \((D^\#, \subseteq)\) is finite, then \(k \leq h(h - 1)\).
Proof. Let \( h \) be finite. The elements of the monotone sequence \( \bigcup_{k=0}^{h} T^{(i)} \) build a chain, so this sequence stabilizes for some \( k' \geq 0 \), i.e., \( T^{(j)} \subseteq \bigcup_{k=0}^{k'} T^{(i)} \) for all \( j \geq k' \). Take the smallest such \( k' \). For all \( j \geq k' \) we have \( T^{(j+1)} \subseteq post^b T^{(j)} \) and thus \( post^b T^{(j)} \subseteq \bigcup_{k=0}^{k'} T^{(i)} \). By definition of the algorithm, the sequence \( (T^{(j)})_{j \geq k'} \) is monotonically increasing. The domain has finite height, so there is a \( k \geq k' \) with \( T^{(k+1)} = T^{(k)} \). Take the smallest such \( k \).

Now we derive the number of iteration steps. There are two cases

Case \( post^b T^{(0)} \subseteq T^{(0)} \). Then \( post^b T^{(0)} \subseteq \bigcup_{i=0}^{0} T^{(j)} \), so \( T^{(1)} = T^{(0)} \). Then \( k = 0 \leq h(h - 1) \).

Case \( post^b T^{(0)} \not\subseteq T^{(0)} \). Then \( post^b T^{(0)} \not\subseteq \bigcup_{i=0}^{0} T^{(j)} \), so \( T^{(1)} = post^b T^{(0)} \not\subseteq T^{(0)} \). Therefore \( \bigcup_{j=0}^{b} T^{(j)} \neq \bigcup_{j=0}^{h} T^{(i)} \) (otherwise \( T^{(1)} \) were less than or equal to \( T^{(0)} \)).

Since \( \{ \bigcup_{j=0}^{b} T^{(j)} \mid j \in \mathbb{N}_0 \} \) is a chain, there are at most \( h - 1 \) indices \( j > 0 \) such that \( \bigcup_{j=0}^{j-1} T^{(j)} \neq \bigcup_{j=0}^{b} T^{(j)} \), the smallest such index is \( 1 \). Consider any two such “neighbor” indices \( a < b \) with \( \bigcup_{i=0}^{0} T^{(i)} \neq \bigcup_{i=0}^{a} T^{(i)} \) and \( \bigcup_{i=0}^{0} T^{(i)} \neq \bigcup_{i=0}^{b-1} T^{(i)} \) and \( 0 < a \)

so that for all \( c \) with \( a < c < b \) we have \( \bigcup_{i=0}^{c-1} T^{(i)} = \bigcup_{i=0}^{c} T^{(i)} \).

The sequence \( (T^{(i)})_{a \leq c \leq b} \) is increasing by the definition of the relaxed frontier sequence. The increase is strict, i.e., \( T^{(c-1)} \neq T^{(c)} \) for \( a < c < b \) (since otherwise the sequence \( (T^{(i)})_{i \geq c} \) were constant for some \( c < b \), contradicting the choice of \( b \)).

The maximal chain length gives \( b - a \leq h \) and finally \( k - k' < h \). The number of such neighbor pairs \( (a, b) \) as above is at most \( h - 2 \), the last such \( b \) is \( k' \), the first such \( a \) is \( 1 \). Thus \( k' - 1 \leq h(h - 2) \). Thus \( k' \leq h^2 - 2h + 1 \) and \( k \leq k' + h - 1 \leq h^2 - h \).

\[ \blacksquare \]

Proposition 51. The set \( \bigcup_{i \in \mathbb{N}_0} \gamma T^{(i)} \) is an inductive invariant. Formally:

\[ init \cup post \left( \bigcup_{i \in \mathbb{N}_0} \gamma T^{(i)} \right) \subseteq \bigcup_{i \in \mathbb{N}_0} \gamma T^{(i)} \]

Proof. By extensivity of \( \gamma \alpha \) we obtain \( init \subseteq \gamma \alpha init = \gamma T^{(0)} \). Moreover

\[ post \left( \bigcup_{i \in \mathbb{N}_0} \gamma T^{(i)} \right) = \bigcup_{i \in \mathbb{N}_0} post^\alpha T^{(i)} \subseteq [\text{by definition of a pair of adjoint maps}] \]

\[ \subseteq \bigcup_{i \in \mathbb{N}_0} \gamma post^\alpha T^{(i)} \subseteq \bigcup_{i \in \mathbb{N}_0} \gamma T^{(i+1)} \subseteq \bigcup_{i \in \mathbb{N}_0} \gamma T^{(i)} \].

\[ \blacksquare \]

49
Proposition 52. If $k < \infty$, then $\bigcup_{i=0}^{k} \gamma T^{(i)}$ is an inductive invariant. Formally:

$$k < \infty \Rightarrow \text{init} \cup \text{post} \left( \bigcup_{i=0}^{k} \gamma T^{(i)} \right) \subseteq \bigcup_{i=0}^{k} \gamma T^{(i)}.$$  

Proof. By definition of $k$ we have $T^{(k+1)} \sqsubseteq T^{(k)}$. If for some $j > k$ we have $T^{(j)} \sqsubseteq T^{(k)}$, then $T^{(j+1)} \sqsubseteq T^{(j)} \cup \text{post} \left( T^{(j)} \right) \subseteq \left[ \text{by assumption and monotonicity of post} \right] T^{(k)} \cup \text{post} \left( T^{(k)} \right) \sqsubseteq T^{(k)} \sqsubseteq T^{(k+1)} \sqsubseteq \left[ \text{by definition of } k \right] T^{(k)}$. By induction $T^{(j)} \sqsubseteq T^{(k)}$ for all $j \geq k$. Thus $\gamma T^{(j)} \subseteq \gamma T^{(k)}$ for all $j \geq k$, implying $\bigcup_{i=0}^{k} \gamma T^{(i)} = \bigcup_{i=0}^{k} \gamma T^{(i)}$. \hfill \qed

As a corollary, if $(D^A, \sqsubseteq)$ has a finite height, $\bigcup_{i=0}^{k} \gamma T^{(i)}$ is an inductive invariant.

G.2 Relaxed Frontier Search - specialized for the Owicki-Gries core

Now we are going to specialize relaxed frontier search from Section G.1 to the Owicki-Gries core\(^8\).

Let $(\text{Tid}, \text{Pl}, \text{Val}, \text{Res}, (\text{Local}, \text{pc}_i)_{i \in \text{Tid}}, \text{ProofVar}, \text{rsc})$ be an arbitrary but fixed syntactic structure, $D$ the powerset of consistent states, $D^A$ the set of program annotations equipped with componentwise order, $(\text{init}, (-, \tau)_{i \in \text{Tid}})$ an RPL program that obeys the syntactic structure, $\text{post}$ its successor map, $\mathcal{O}$ the lattice of Owicki-Gries-core proofs, and

$$p_{\mathcal{O}}^A : \text{PA} \rightarrow \text{PA}, \quad (I, M) \mapsto$$

\[
\left\{ \begin{array}{ll}
  u \in \text{ProofVar}(r) \rightarrow \text{Val} & \exists t \in \text{Tid}, (v, v') \in \rightarrow_t : r \not\in \text{rsc}(v'(pc)) \land \\
  \quad & (r \not\in \text{rsc}(v(pc)) \land u \in I_t) \lor \\
  & (r \in \text{rsc}(v(pc)) \land u = v_{\text{ProofVar}(r)}) \end{array} \right\}_{r \in \text{Res}}
\]

\[
\left\{ \begin{array}{ll}
  u \in (\text{LocalDataVar} \cup \text{ProofVar}(\text{rsc}(p))) \rightarrow \text{Val} & \exists t \in \text{Tid}, (v, v') \in \rightarrow_t : u \in M_{pc_t} \land \\
  & \forall v_{\text{LocalDataVar} \cup \text{ProofVar}(\text{rsc}(pc))} \in M_{pc_t} : (rsc(v'(pc)) \cup \text{rsc}(v(pc)) \cap \text{rsc}(p) = \emptyset) \lor \\
  & (v, v') \in \rightarrow_t : v'(pc) = p \land \\
  & u = v_{\text{LocalDataVar} \cup \text{ProofVar}(\text{rsc}(pc))} \land \\
  & \forall t \in \text{Tid}, (v, v') \in \rightarrow_t : \text{rsc}(v'(pc)) : v_{\text{ProofVar}(r)} \in I_t \\
  \end{array} \right\}_{p \in \text{Pl}, t \in \text{Tid}}
\]

We call $p_{\mathcal{O}}^A$ the improved Owicki-Gries-core abstract successor map. As before in Section C, let

$$I_{\text{init}} = \{ (v_{\text{ProofVar}(r)} | v \in \text{init} ) \}_{r \in \text{Res}},$$

$$M_{\text{init}} = \{ (v_{\text{LocalDataVar}}, v \in \text{init} \land v(pc) = p ) \}_{p \in \text{Pl}, t \in \text{Tid}}.$$  

\(^8\) Using $\text{post}^A_{\mathcal{O}}$ would not give us more precision: the generated inductive invariant would be equal to $\gamma_{\mathcal{O}}(\text{fp}(p_{\mathcal{O}}^A))$. We cannot use $\text{next}_{\mathcal{O}}^A$, as it does not overapproximate $\alpha_{\mathcal{O}} \circ \text{post} \circ \gamma_{\mathcal{O}}$ in general. We are going to suggest an operator in between: it will overapproximate $\alpha_{\mathcal{O}} \circ \text{post} \circ \gamma_{\mathcal{O}}$ and underapproximate $\text{post}^A_{\mathcal{O}}$, allowing more precision in the relaxed frontier search.
and the improved Owicki-Gries-core abstract transformer be

\[ G_{OG}^\# : PA \to PA, \]

\[ (I, M) \mapsto (I^{init}, M^{init}) \cup p_{OG}(I, M). \]

**Proposition 53.** \( p_{OG}^\# \) is monotone.

**Proof.** Let \((I, M) \subseteq (\hat{I}, \hat{M})\) be program annotations, \( p_{OG}^\#(I, M) = (I', M') \), \( p_{OG}^\#(\hat{I}, \hat{M}) = (\hat{I}', \hat{M}') \).

```
\forall r \in Res : I' \subseteq \hat{I}'.
```

Let \( r \in Res \). Let \( w \in I' \). Then there is a thread \( t \in Tid \) and some transition \( v \to v' \) such that \( v|_{LocalDat\hat{ar}(\hat{I})} \subseteq M_{v(pc_1), t} \), which is a subset of \( M_{v(pc_1), t} \), \( r \not\in rsc(v'(pc_1)) \), and either \( r \not\in rsc(v(pc_1)) \land w \in I' \), which is a subset of \( I' \), or \( r \not\in rsc(v'(pc_1)) \land w \in I' \). Then \( v|_{LocalDat\hat{ar}(\hat{I})} \subseteq M_{v(pc_1), t} \); also either \( r \not\in rsc(v'(pc_1)) \land w \in I' \), or \( r \not\in rsc(v(pc_1)) \land w \in I' \).

Thus \( w \in I' \).

```
\forall t \in Tid, p \in PL : M_{p,t} \subseteq \hat{M}_{p,t}.
```

Let \( t \in Tid \), \( p \in PL \). Let \( w \in M_{p,t} \). There are two cases.

- Either there is \( t \in Tid \setminus \{t\} \) and \( v, v' \in \to_t \) such that \( v|_{LocalDat\hat{ar}(\hat{I})} \subseteq M_{v(pc_1), t} \) \( w \in M_{p,t} \) and \( \emptyset = rsc(p) \cap rsc(v'(pc_1)) \cup rsc(v(pc_1)) \). Notice that \( M_{p,t} \subseteq M_{p,t} \) and \( M_{v(pc_1), t} \subseteq M_{v(pc_1), t} \). Thus \( v|_{LocalDat\hat{ar}(\hat{I})} \subseteq M_{v(pc_1), t} \) and \( w \in M_{p,t} \). So \( w \in \hat{M}_{p,t} \).

- Or there is a transition \( v \to_v v' \) of the same thread \( t \) such that \( v'(pc_1) = p, w = v'(pc_1) \), \( v' \subseteq \to_t(v'(pc_1)) \), \( v|_{LocalDat\hat{ar}(\hat{I})} \subseteq M_{v(pc_1), t} \) and \( \forall r \in rsc(p) \setminus rsc(v'(pc_1)) : v|_{\text{ProofVar}(r)} \in I' \). Notice that \( M_{v(pc_1), t} \subseteq M_{v(pc_1), t} \) and for all \( r \in Res \) we have \( I' \subseteq I' \). Then \( M_{v(pc_1), t} \supseteq v|_{LocalDat\hat{ar}(\hat{I})} \subseteq M_{v(pc_1), t} \) and \( \forall r \in rsc(p) \setminus rsc(v'(pc_1)) : v|_{\text{ProofVar}(r)} \in I' \). Then \( w \in M_{p,t} \).

Thus the improved Owicki-Gries-core abstract transformer is also monotone.

**Proposition 54.** The set of Owicki-Gries-core proofs coincides with the set of postfix points of the improved Owicki-Gries-core abstract transformer. Formally:

\[ \mathcal{O} = \text{postfp}(G_{OG}^\#). \]

**Proof.** Let \((I, M) \in \mathcal{O} \) and \((\hat{I}, \hat{M}) = p_{OG}(I, M)\). We will show that \((I', M') := G_{OG}^\#(I, M)\) is less than or equal to \((I, M)\).

```
\forall r \in Res : I' \subseteq I'.
```

Let \( r \in Res \). Let \( w \in I' \).

If \( w \in I^{init} \), there is some \( v \in \text{init} \) such that \( v|_{\text{ProofVar}(r)} = w \). By the initial condition, \( v \in \gamma_{OG}(I, M) \). Since every resource is available in an initial state, \( r \in Res \setminus rsc(v(PCVar)) \). Thus \( v|_{\text{ProofVar}(r)} \in I' \).

Otherwise \( w \in \hat{I} \). So there is some \( t \in Tid \) and some transition \( v \to v' \) such that \( v|_{LocalDat\hat{ar}(\hat{I})} \subseteq M_{v(pc_1), t} \), \( r \not\in rsc(v'(pc_1)) \), and either \( r \not\in rsc(v(pc_1)) \land w \in I' \), or \( r \not\in rsc(v'(pc_1)) \land w \in I' \). Assume for the purpose of contradiction that \( w \not\in I' \). Then \( r \in rsc(v(pc_1)) \lor rsc(v'(pc_1)) \land w = v|_{\text{ProofVar}(r)} \). By (5) we have \( rsc(v(pc_1)) \supseteq rsc(v'(pc_1)) \). Sequential consistency implies \( v|_{\text{ProofVar}(r)} \in I' \). Contradiction!

We have shown that in both cases \( w \in I' \). So \( I' \subseteq I' \).
"∀ t ∈ Tid, p ∈ PL : M^p,t ⊆ M_p,t": Let t ∈ Tid, p ∈ PL. Let w ∈ M^p,t.

If w ∈ M^p,t, there is some v ∈ init such that v(p_c) = p and w = w|_{LocalDataVar}.

By the initial condition, v ∈ OG(I, M). From definition of OG and rsc(v(p_c)) = {v ∈ init}. We get w|_{LocalDataVar} ∈ M^p,t.

Otherwise w ∈ M^p,t. Assume for the purpose of contradiction that w /∈ M_p,t. By definition of p OG there is a transition v →, v′ such that w = v|_{LocalDataVar} |\cup| ProofVar(rsc(p)):

v|_{LocalDataVar} |\cup| ProofVar(rsc(v(p_c))) ∈ M^p(t), v′(p_c) = p and ∀ r ∈ rsc(p) \cup rsc(v(p_c)):

v|_{ProofVar(r)} ∈ I. From sequential consistency we get v|_{LocalDataVar} |\cup| ProofVar(rsc(p)) ∈ M_p,t. Contradiction!

In both cases w ∈ M_p,t. So M^p,t ⊆ M_p,t.

"⊆": Let (I, M) ∈ postfp(G^w_{OG}), i.e., for (I′, M′) = G^w_{OG}(I, M) we have (I′, M′) ⊆ (I, M).

We’ll show that (I, M) is an Owicki-Gries-core proof.

Sequential consistency: Let t ∈ Tid, (v, v′) →, p = v(p_c), p′ = v′(p_c), R = rsc(p), R′ = rsc(p′), v|_{LocalDataVar} |\cup| ProofVar(rsc(p)) ∈ M_p,t and ∀ r ∈ R \setminus R :

v|_{ProofVar(r)} ∈ I. By definition of p OG we obtain v|_{LocalDataVar} |\cup| ProofVar(rsc(p)) ∈ M_p,t. If any r ∈ R \setminus R is given, the definition of p OG implies v|_{ProofVar(r)} = [by (3)] v|_{ProofVar(r)} ∈ I′. Initial condition: Let v ∈ init.

Let r ∈ Res \setminus rsc(v(PCVar)). Then v|_{ProofVar(r)} ∈ I^{init}_{rsc} \subseteq I′ \subseteq I.

Now let t ∈ Tid. Then v|_{LocalDataVar} ∈ M^{init}_{v(p_c)t}. Since initial states don’t have any busy resources, v|_{LocalDataVar} |\cup| ProofVar(rsc(v(p_c))) ∈ M^{init}_{v(p_c)t} ⊆ M^{init}_{v(p_c)t} ⊆ M^p_{v(p_c)t}.

We have shown v ∈ OG(I,M). Thus init ⊆ OG(I,M).

Corollary 55. The smallest Owicki-Gries-core proof is the least fixpoint of the improved Owicki-Gries-core abstract transformer, formally:

\text{lfp}(G^w_{OG}) = \text{inf} \mathcal{D}.

Proof. inf \mathcal{D} = [Prop. 54] inf(postfp(G^w_{OG})) = [Tarski’s fixpoint theorem] lfp(G^w_{OG}).

Proposition 56. The map p OG overapproximates the best abstract successor map with respect to the pair of adjoint maps (α OG, OG). Formally:

∀ P ∈ PA : α OG \circ post \circ OG(P) ⊆ p^w_{OG}(P).

Proof. Let P = (I, M) ∈ PA, (I^R, M^R) = α OG \circ post \circ OG(P), (I^R, M^R) = p^w_{OG}(P). We have to show two facts.

"∀ r ∈ Res : I^R_r ⊆ I^R_r": Let r ∈ Res. Let w ∈ I^R_r. Then there is t ∈ Tid, (v, v′) →, such that v ∈ OG(P), r is available in v′ and v′|_{ProofVar(r)} = w. By definition of OG we have v|_{LocalDataVar} |\cup| ProofVar(rsc(v(p_c))) ∈ M^p_{v(p_c)t}. There are two cases.

Case r ∈ rsc(v(p_c)). Then rsc(v(p_c)) \neq rsc(v′(p_c)). From (3) we conclude v|_{ProofVar(r)} = v|_{ProofVar(r)}. By definition of p OG we get w ∈ I^R_r.

Case r ∉ rsc(v(p_c)). Then r ∉ rsc(v(p_c)) ∪ rsc(v′(p_c)). In particular, r ∉ rsc(v(p_c)) ∩ rsc(v′(p_c)). If x ∈ ProofVar(r), we have v(x) = v′(x) by definition of ProofVar.

Thus w = v|_{ProofVar(r)}. Since r is available in v′, it is also available in v, since

52
resources of threads other than \( t \) don’t change in the transition. By definition of \( \gamma_\text{OG} \) we get \( v|_{\text{ProofVar}(t)} \in I_r \), thus \( w \in I_r \). By definition of \( p^\#_\text{OG} \) we have \( w \in I^R_r \).

We have shown \( I^L_r \subseteq I^R_r \).

Let \( p \in \text{PL} \), \( t \in \text{Tid} \), \( M^L_{p,j} \subseteq M^R_{p,j} \). Then there is some \( \hat{i} \in \text{Tid} \), \( (v,v') \rightarrow t \) such that \( w = v|_{\text{LocalDataVar} \cup \text{ProofVar}(rsc(p))} \), \( v \in \gamma_\text{OG}(P) \) and \( v'(p_c) = p \). There are two cases.

Case \( t \neq \hat{i} \). By (1) we have \( v \sim_{\text{Local}} v' \). Take any \( r \in \text{rsc}(p) \); then \( r \notin \text{rsc}(v'(p_c)) \); thus \( v \sim_{\text{ProofVar}(r)} v' \). So \( v|_{\text{LocalDataVar} \cup \text{ProofVar}(rsc(p))} = w \). From definition of \( \gamma_{\text{OG}} \) we get \( v|_{\text{LocalDataVar} \cup \text{ProofVar}(rsc(v(p_c)))} \in M^L_{p,j} \), and \( v|_{\text{LocalDataVar} \cup \text{ProofVar}(rsc(v(p_c)))} \in M^L_{\hat{i},j} \). Notice that \( v(p_c) = p \). Thus \( w \in M^R_{p,j} \) and from definition of consistent states we get \( \text{rsc}(p) \cap \text{rsc}(v(p_c)) = \emptyset \). Thus \( \text{rsc}(p) \cap (\text{rsc}(v(p_c)) \cup \text{rsc}(v'(p_c))) = \emptyset \). By definition of \( p^\#_{\text{OG}} \) we get \( w \in M^R_{p,j} \).

Case \( t = \hat{i} \). By definition of \( \gamma_{\text{OG}} \) we get \( v|_{\text{LocalDataVar} \cup \text{ProofVar}(rsc(v(p_c)))} \in M^L_{\hat{i},j} \).

Consider an arbitrary \( r \in \text{rsc}(p) \setminus \text{rsc}(v(p_c)) \) (there may be none). From \( v' \in \text{ConsState} \) and (1) we get \( r \in \bigcup_{t \in \text{Tid} \setminus t} \text{rsc}(v(p_c)) \). Thus \( r \) is available in \( v \).

By definition of \( \gamma_{\text{OG}} \) we get \( v|_{\text{LocalDataVar} \cup \text{ProofVar}(rsc(p))} \) (there may be none). From \( v' \in \text{ConsState} \) and (1) we get \( r \in \bigcup_{t \in \text{Tid} \setminus t} \text{rsc}(v(p_c)) \). Thus \( r \) is available in \( v \).

By definition of \( \gamma_{\text{OG}} \) we get \( v|_{\text{LocalDataVar} \cup \text{ProofVar}(rsc(v(p_c)))} \in M^L_{\hat{i},j} \). Thus \( w \in M^R_{p,j} \).

We have shown \( M^L_{p,j} \subseteq M^R_{p,j} \).

The last proposition allows using \( p^\#_{\text{OG}} \) in the relaxed frontier search.

G.3 Examples

Example 57. Consider the program Upper from Example 2. Let \((T^{(i)})_{i \in \mathbb{N}_0}\) be the relaxed frontier search sequence for Upper. Then:

\[
T^{(0)} = \alpha_{\text{OG}}(\text{init}) = \left[ \begin{array}{c}
\{ r \mapsto \{(u \mapsto 0, z \mapsto 1), (u \mapsto 1, z \mapsto 0)\}, \\
\{ r' \mapsto \{(x \mapsto 0, y \mapsto 0), (x \mapsto 1, y \mapsto 1)\}, \\
\{ (A, 1) \mapsto \{(x \mapsto 0, l \mapsto 0), (x \mapsto 1, l \mapsto 1)\}, \\
\{ (0, 2) \mapsto \{(y \mapsto 0, z \mapsto 0), (y \mapsto 1, z \mapsto 1)\}, \\
(\text{everything else}) \mapsto \emptyset
\end{array} \right],
\]

\[
0 \preceq \bigcup_{j=0}^{\infty} T^{(j)}, \text{ so } T^{(1)} = p^\#_{\text{OG}}(T^{(0)}),
\]

\[
p^\#_{\text{OG}}(T^{(1)}) = \left[ \begin{array}{c}
\{ r \mapsto \emptyset, r' \mapsto \emptyset\}, \\
\{ (C, 1) \mapsto \{(u \mapsto 0, z \mapsto 1, x \mapsto 0, y \mapsto 0, l \mapsto 0)\}, \\
\{ (u \mapsto 1, z \mapsto 0, x \mapsto 1, y \mapsto 1, l \mapsto 1)\}, \\
\{ (0, 2) \mapsto \{(y \mapsto 0, z \mapsto 0), (y \mapsto 1, z \mapsto 1)\}, \\
(\text{everything else}) \mapsto \emptyset
\end{array} \right]
\]

53
From $T \cup \{0\} \cup \{0\}$, so $T^{(2)} = p_{OG}(T^{(1)})$,

$$p_{OG}(T^{(2)}) = \begin{pmatrix}
[r \mapsto 0, r' \mapsto 0], \\
(D, 1) \mapsto \begin{cases}
[u \mapsto 0, z \mapsto 1, x \mapsto 0, y \mapsto 0, l \mapsto 0], \\
[u \mapsto 1, z \mapsto 0, x \mapsto 0, y \mapsto 1, l \mapsto 1]
\end{cases}, \\
(0, 2) \mapsto \begin{cases}
y \mapsto 0, z \mapsto 0, [y \mapsto 1, z \mapsto 1]
\end{cases}, \\
\text{(everything else)} \mapsto \emptyset
\end{pmatrix}$$

$$\bigvee_{j=0}^{2} T^{(j)} = p_{OG}(T^{(2)})$$

$$p_{OG}(T^{(3)}) = \begin{pmatrix}
[r \mapsto 0, r' \mapsto 0], \\
(E, 1) \mapsto \begin{cases}
[u \mapsto 0, z \mapsto 1, x \mapsto 0, l \mapsto 0], \\
[u \mapsto 1, z \mapsto 0, x \mapsto 0, l \mapsto 1]
\end{cases}, \\
(0, 2) \mapsto \begin{cases}
y \mapsto 0, z \mapsto 0, [y \mapsto 1, z \mapsto 1]
\end{cases}, \\
\text{(everything else)} \mapsto \emptyset
\end{pmatrix}$$

$$\bigvee_{j=0}^{3} T^{(j)} = p_{OG}(T^{(3)})$$

$$p_{OG}(T^{(4)}) = \left( [r \mapsto 0, r' \mapsto 0] \right) \in \bigcup_{j=0}^{4} T^{(j)}$$

$$T^{(5)} = T^{(4)} \cup p_{OG}(T^{(4)}) = T^{(4)}$$

From $T^{(5)} \subseteq T^{(4)}$ we get $k = 4$. By Prop. 52, the generated inductive invariant is

$$\bigcup_{j=0}^{k} \gamma_{OG}(T^{(j)}) = \begin{pmatrix}
[u \mapsto 0, z \mapsto 1, x \mapsto 1, y \mapsto 1, l \mapsto 1, pc_1 \mapsto A, pc_2 \mapsto 0], \\
[u \mapsto 1, z \mapsto 0, x \mapsto 0, y \mapsto 0, l \mapsto 0, pc_1 \mapsto A, pc_2 \mapsto 0], \\
[u \mapsto 0, z \mapsto 1, x \mapsto 0, y \mapsto 1, l \mapsto 0, pc_1 \mapsto A, pc_2 \mapsto 0], \\
[u \mapsto 1, z \mapsto 0, x \mapsto 0, y \mapsto 0, l \mapsto 1, pc_1 \mapsto E, pc_2 \mapsto 0],
\end{pmatrix}.$$

Notice that $\bigcup_{j=0}^{k} \gamma_{OG}(T^{(j)})$ is strictly stronger than $\gamma_{OG}(\inf \Theta)$, e.g., $[u \mapsto 0, z \mapsto 1, x \mapsto 0, y \mapsto 1, l \mapsto 0, pc_1 \mapsto A, pc_2 \mapsto 0] \in \gamma_{OG}(\inf \Theta) \setminus \left( \bigcup_{j=0}^{k} \gamma_{OG}(T^{(j)}) \right)$. \hfill \Box

**H Comparison to modular methods for general programs**

Modular methods for general programs are variants of the original Owicki method [25], rely-guarantee reasoning [17], thread-modular model-checking [14], local proofs [7] and multithreaded Cartesian abstraction [20, 22]. We are going to compare the Owicki-Gries core with multithreaded Cartesian abstraction. We will show that the methods for programs with and without resources, when treated without auxiliary variables, have similar but incomparable precision.

Fix a syntactic structure and an RPL transition system obeying this syntactic structure.

54
Let us consider, for instance, the variant of multithreaded Cartesian approximation on the powerset of states that describes the core of Owicki-Gries for general multithreaded programs exactly:

\[ S \mapsto \{ \tilde{v} \mid \forall t \in Tid \exists v \in S : \tilde{v} \sim_{\{pc_t\} \cup \text{DataVar}} v \}. \]

This approximation is not directly usable for RPL, since its values are not necessarily subsets of \( \text{ConsState} \). But a similar mapping on the powerset of consistent states \( D = \mathcal{P}(\text{ConsState}) \), namely

\[ \rho_{\text{OG,mc}} : D \rightarrow D, S \mapsto \{ v \in \text{ConsState} \mid \forall t \in Tid \exists \tilde{v} \in S : v \sim_{\{pc_t\} \cup \text{DataVar}} \tilde{v} \}, \]

is usable for RPL.

**Proposition 58.** \( \rho_{\text{OG,mc}} : D \rightarrow D \) is a closure operator on \( D \).

**Proof.** We will prove the defining properties of a closure.

**Monotonicity.** Let \( Q \subseteq Q' \) be sets of consistent states and \( v \in \rho_{\text{OG,mc}}(Q) \). Let \( t \in Tid \).

Then there is some \( \tilde{v} \in Q \) such that \( v \sim_{\{pc_t\} \cup \text{DataVar}} \tilde{v} \). Notice that \( \tilde{v} \in Q' \). Thus \( v \in \rho_{\text{OG,mc}}(Q') \). We have shown \( \rho_{\text{OG,mc}}(Q) \subseteq \rho_{\text{OG,mc}}(Q') \).

**Extensivity.** Let \( Q \in D \). Let \( v \in Q \). Certainly \( \forall t \in Tid : v \sim_{\{pc_t\} \cup \text{DataVar}} v \). Thus \( v \in \rho_{\text{OG,mc}}(Q) \). We have shown \( Q \subseteq \rho_{\text{OG,mc}}(Q) \).

**Idempotence.** Let \( Q \in D \). Let \( v \in \rho_{\text{OG,mc}}(\rho_{\text{OG,mc}}(Q)) \). Let \( t \in Tid \). Then there is some \( \tilde{v} \in \rho_{\text{OG,mc}}(Q) \) such that \( v \sim_{\{pc_t\} \cup \text{DataVar}} \tilde{v} \). Then there is some \( \tilde{\tilde{v}} \in Q \) such that \( \tilde{v} \sim_{\{pc_t\} \cup \text{DataVar}} \tilde{\tilde{v}} \). Now \( v \sim_{\{pc_t\} \cup \text{DataVar}} \tilde{\tilde{v}} \). Thus \( v \in \rho_{\text{OG,mc}}(Q) \). We have shown \( \rho_{\text{OG,mc}}(\rho_{\text{OG,mc}}(Q)) \subseteq \rho_{\text{OG,mc}}(Q) \).

Theoretically, other equivalent proof methods (rely-guarantee reasoning, thread-modular model-checking or local proofs) could be adapted to RPL. However, to the best of our knowledge, such adaptations have not been cleanly formulated so far. In their original formulation, they are also not exactly equivalent, e.g., the “locals” of threads in thread-modular reasoning have to be disjoint, the “locals” of threads in RPL may overlap, the “locals” of threads in Owicki-Gries for general multithreaded programs consist only of the program counters.

The question, whether the straightforward adaptation of thread-modular model checking is equivalent to abstract interpretation with \( \rho_{\text{OG,mc}} \), is not so easy for RPL. However, at least one direction holds: following the proof of Thm. 1.7.2 in [20], we relatively easily obtain that abstract interpretation with \( \rho_{\text{OG,mc}} \) always proves properties at least as strong as those provable by thread-modular model checking.

We are going to proceed with comparison of the Owicki-Gries core with abstract interpretation under the closure \( \rho_{\text{OG,mc}} \).

**Example 59 (Readers-Writers).** For the program Readers-Writers, let \( F = \lambda x. \rho_{\text{OG,mc}}(\text{init} \cup \text{post}(x)) \) and \( Q = \text{lfp}(F) \). We will show that \( Q \) equals the strongest Owicki-Gries-core-
provably property

\{ v \in \text{ConsState} \mid v(ww), v(ar) \in \mathbb{N}_0 \land v(aw) \in \{0,1\} \}
\land \forall i \in \mathbb{N}_m :
\{ v(pc_{\text{reader}}) \in \{ \text{ready, read} \mid x \in \{ \text{start, finish} \} \land y \in \{ A, B, C \} \} \}
\land (v(pc_{\text{reader}}) = \text{startread}B \Rightarrow v(ww) = 0)
\land (v(pc_{\text{reader}}) = \text{startread}C \Rightarrow v(ww) = 0 < v(ar))
\land \forall j \in \mathbb{N}_n :
\{ v(pc_{\text{reader}}) \in \{ \text{write, write} \mid x \in \{ \text{ask, start, finish} \} \land y \in \{ A, B, C \} \} \}
\land (v(pc_{\text{writer}}) = \text{askwrite}C \Rightarrow v(ww) > 0)
\land (v(pc_{\text{writer}}) = \text{startwrite}B \Rightarrow v(ar) = v(aw) = 0)
\land (v(pc_{\text{writer}}) = \text{startwrite}C \Rightarrow v(ar) = 0 < v(aw))
\land (v(pc_{\text{writer}}) = \text{finishwrite}C \Rightarrow v(aw) = 0) \}.

\subseteq: First we show the right hand side (RHS) is closed under \( \rho_{OG.mc} \). Let \( v \in \rho_{OG.mc}(RHS) \).
By definition of \( \rho_{OG.mc} \) there is some \( w \in RHS \) such that \( v \sim_{\{ pc_{\text{reader}}, \text{ww, ar, aw} \}} w \).
Then \( v(ww), v(ar) \in \mathbb{N}_0 \) and \( v(aw) \in \{0,1\} \).
Let \( i \in \mathbb{N}_m \). Then there is \( w \in RHS \) such that \( v \sim_{\{ pc_{\text{reader}}, \text{ww, ar, aw} \}} w \).
Then \( v(pc_{\text{reader}}) \in \{ \text{startread}A, \text{startread}B, \text{startread}C, \text{read}, \text{finishread}A, \text{finishread}B, \text{finishread}C \} \).
If \( v(pc_{\text{reader}}) = \text{startread}B \), then \( w(pc_{\text{reader}}) = \text{startread}B \), so \( w(ww) = 0 \) by definition of RHS, so \( v(ww) = 0 \). If \( v(pc_{\text{reader}}) = \text{startread}C \), then \( w(pc_{\text{reader}}) = \text{startread}C \), so \( w(ww) = 0 < w(ar) \) by definition of RHS, so \( v(ww) = 0 < v(ar) \).
Let \( j \in \mathbb{N}_n \). Then there is \( w \in RHS \) such that \( v \sim_{\{ pc_{\text{writer}}, \text{ww, ar, aw} \}} w \).
Then \( v(pc_{\text{writer}}) \in \{ \text{askwrite}A, \text{askwrite}B, \text{askwrite}C, \text{startwrite}A, \text{startwrite}B, \text{startwrite}C, \text{write}, \text{finishwrite}A, \text{finishwrite}B, \text{finishwrite}C \} \).
If \( v(pc_{\text{writer}}) = \text{askwrite}C \), then \( w(pc_{\text{writer}}) = \text{askwrite}C \), so \( w(ww) > 0 \), so \( v(ww) > 0 \). If \( v(pc_{\text{writer}}) = \text{startwrite}B \), then \( w(pc_{\text{writer}}) = \text{startwrite}B \), so \( w(ar) = w(aw) = 0 \), so \( v(ar) = v(aw) = 0 \). If \( v(pc_{\text{writer}}) = \text{startwrite}C \), then \( w(pc_{\text{writer}}) = \text{startwrite}C \), so \( w(ar) = 0 < w(aw) \), so \( v(ar) = 0 < v(aw) \). If \( v(pc_{\text{writer}}) = \text{finishwrite}C \), then \( w(pc_{\text{writer}}) = \text{finishwrite}C \), so \( w(aw) = 0 \), so \( v(aw) = 0 \).
Thus \( v \in RHS \). Since \( v \) was arbitrary, \( \rho_{OG.mc}(RHS) \subseteq RHS \). Notice that \( \text{init} \cup \text{post}(RHS) \subseteq RHS \), thus \( \rho_{OG.mc}(\text{init} \cup \text{post}(RHS)) \subseteq RHS \), so RHS is a postfix point of \( F \), so \( Q \subseteq RHS \).

\supseteq: Let
\begin{align*}
\text{CritR} &= \{ \text{read}, \text{xread} \mid x \in \{ \text{start, finish} \}, y \in \{ B, C \} \}, \\
\text{CritW} &= \{ \text{write} \mid x \in \{ \text{ask, start, finish} \}, y \in \{ B, C \} \}, \\
\text{NonCritR} &= \{ \text{read}, \text{xread} \mid x \in \{ \text{start, finish} \} \}, \\
\text{NonCritW} &= \{ \text{write}, \text{xwrite} \mid x \in \{ \text{ask, start, finish} \} \}.
\end{align*}
(I) First we will show that for all \( a, b \in \mathbb{N}_0, c \in \{0, 1\} \), the state \( v \) with \((\forall i \in \mathbb{N}_n : v(pc_{\text{reader}}) = \text{startreadA}) \land (\forall j \in \mathbb{N}_n : v(pc_{\text{writer}}) = \text{askwriteA}) \land v(\text{ww}) = a \land v(ar) = b \land v(aw) = c \) is in \( Q \).

We will do that in 3 steps.

Step 1. We’ll show this claim for \( a = b = 0 \). If \( c = 0 \), notice that such a state is in \( \text{init} \subseteq Q \). Otherwise \( c = 1 \). Take the initial state, make 3 steps of \text{writer}_1, resulting in a state \( v_1 \in Q \) with \( v_1(pc_{\text{writer}}) = \text{startwriteA} \), all other writers are at \text{askwriteA}, all readers are at \text{startreadA}, \( v_1(\text{ww}) = 1, v_1(ar) = 0, v_1(aw) = 0 \). Making 3 steps of \text{writer}_2 from the initial state results in a state \( v_2 \in Q \) with \( v_2(pc_{\text{writer}}) = \text{startwriteA} \), all other writers are at \text{askwriteA}, all readers are at \text{startreadA}, \( v_2(\text{ww}) = 1, v_2(ar) = 0, v_2(aw) = 0 \). Consider the state \( v_3 \) such that \( v_3(pc_{\text{writer}}) = v_3(pc_{\text{reader}}) = \text{startreadA} \land v_3(\text{ww}) = 1 \land v_3(ar) = v_3(aw) = 0 \). By definition of \( \rho_{\text{OG,mc} \cdot} \cdot v_3 \in Q \). Making seven steps of \text{writer}_1 from \( v_3 \) results in a state \( v_4 \in Q \) such that \((\forall i \in \mathbb{N}_n : v_4(pc_{\text{reader}}) = \text{startreadA}) \land v_4(pc_{\text{writer}}) = \text{startwriteA} \land (\forall j \in \mathbb{N}_n \setminus \{2\} : v_4(pc_{\text{writer}}) = \text{askwriteA}) \land v_4(\text{ww}) = v_4(ar) = v_4(aw) = 0 \). Making three steps of \text{writer}_2 from \( v_4 \) results in a state \( v_5 \in Q \) such that \((\forall i \in \mathbb{N}_n : v_5(pc_{\text{reader}}) = \text{startreadA}) \land v_5(pc_{\text{writer}}) = \text{write} \land (\forall j \in \mathbb{N}_n \setminus \{2\} : v_5(pc_{\text{writer}}) = \text{askwriteA}) \land v_5(\text{ww}) = v_5(ar) = v_5(aw) = 0 \land v_5(aw) = 1 \). Analogously, starting from \( v_3 \), making seven steps of \text{writer}_2 and three steps of \text{writer}_1 results in a state \( v_6 \in Q \) such that \((\forall i \in \mathbb{N}_n : v_6(pc_{\text{reader}}) = \text{startreadA}) \land v_6(pc_{\text{writer}}) = \text{write} \land (\forall j \in \mathbb{N}_n \setminus \{1\} : v_6(pc_{\text{writer}}) = \text{askwriteA}) \land v_6(\text{ww}) = v_6(ar) = 0 \land v_6(aw) = 1 \). By definition of \( \rho_{\text{OG,mc} \cdot} \cdot \) there is some \( v_7 \in Q \) such that \((\forall i \in \mathbb{N}_n : v_7(pc_{\text{reader}}) = \text{startreadA}) \land (\forall j \in \mathbb{N}_n : v_7(pc_{\text{writer}}) = \text{askwriteA}) \land v_7(\text{ww}) = v_7(ar) = 0 \land v_7(aw) = 1 \). Then \( v_7 \) satisfies the stated conditions for \( v \).

Step 2. Now we will show that for all \( b \in \mathbb{N}_0, c \in \{0, 1\} \), the state \( v \) with \((\forall i \in \mathbb{N}_n : v(pc_{\text{reader}}) = \text{startreadA}) \land (\forall j \in \mathbb{N}_n : v(pc_{\text{writer}}) = \text{askwriteA}) \land v(\text{ww}) = 0 \land v(ar) = b \land v(aw) = c \) is in \( Q \).

For \( b = 0 \) the claim has been shown in step 1. Now assume that \( b > 0 \) and the claim has been proven for \( b - 1 \). Let \( c \in \{0, 1\} \). By induction assumption there is a state \( v_1 \in Q \) in which each thread sits at its initial location and \( v_1(\text{ww}) = 0 \land v_1(ar) = b - 1 \land v_1(aw) = c \). Making three steps of \text{reader}_1 from \( v_1 \) results in a state \( v_2 \in Q \) such that \( v_2(pc_{\text{reader}}) = \text{read} \land (\forall i \in \mathbb{N}_n \setminus \{1\} : v_2(pc_{\text{reader}}) = \text{startreadA}) \land (\forall j \in \mathbb{N}_n : v_2(pc_{\text{writer}}) = \text{askwriteA}) \land v_2(\text{ww}) = 0 \land v_2(aw) = b \land v_2(aw) = c \). Making three steps of \text{reader}_2 from \( v_1 \), we get a state \( v_3 \) such that \( v_3(pc_{\text{reader}}) = \text{read} \land (\forall i \in \mathbb{N}_n \setminus \{2\} : v_3(pc_{\text{reader}}) = \text{startreadA}) \land (\forall j \in \mathbb{N}_n : v_3(pc_{\text{writer}}) = \text{askwriteA}) \land v_3(\text{ww}) = 0 \land v_3(ar) = b \land v_3(aw) = c \). Since \( Q \) is a fixpoint of \( \rho_{\text{OG,mc} \cdot} \cdot \) the state \( v \)
in which all threads are at their initial locations, \( v(ww) = 0 \land v(ar) = b \land v(aw) = c \) is in \( Q \).

Step 3. Now we will show that for all \( a \in \mathbb{N}_0, b \in \mathbb{N}_0, c \in \{0,1\} \), the state \( v \) with \((\forall i \in \mathbb{N}_n : v(pc_{\text{reader}}) = \text{startreadA}) \land (\forall j \in \mathbb{N}_m : v(pc_{\text{writer}}) = \text{askwriteA}) \land v(ww) = a \land v(ar) = b \land v(aw) = c \) is in \( Q \).

For \( a = 0 \) the claim has been shown in step 2. Now assume that \( a > 0 \) and the claim has been proven for \( a - 1 \). Let \( b \in \mathbb{N}_0, c \in \{0,1\} \). By induction assumption there is a state \( v_1 \in Q \) in which each threads sits at its initial location, \( v(ww) = a - 1 \land v(ar) = b \land v(aw) = c \). Making three steps of \( \text{writer}_1 \) from \( v_1 \) results in a state \( v_2 \in Q \) such that \( v_2(pc_{\text{writer}}) = \text{startwriteA}, v_2(ww) = a \land v(ww) = b \land v(aw) = c \). Making three steps of \( \text{writer}_2 \) from \( v_1 \) results in a state \( v_3 \in Q \) such that \( v_3(pc_{\text{writer}}) = \text{startwriteA}, v_3(ww) = a \land v(ww) = b \land v(aw) = c \). From \( v_2 \in Q, v_3 \in Q \) and the definition of \( p_{\text{OG,mc}} \) we obtain that the state \( v \) such that all threads in \( v \) are at their initial locations, \( v(ww) = a \land v(ar) = b \land v(aw) = c \) is in \( Q \). We’ll use induction on \( a \).

Case \( a = 0 \). Let \( b \in \mathbb{N}, c \in \{0,1\}, i \in \mathbb{N}_n \). From (I) we already know that there is some \( v_1 \in Q \) in which all threads are at their initial locations, \( v(ww) = 0 \land v(ww) = b \land v(ar) = c \). Making three steps by thread \( \text{reader}_i \) results in a state \( v_2 \in Q \) such that \( v_2(pc_{\text{reader}}) = \text{read}, v_2(ww) = 0 \land v(ww) = b \land v(ww) = c \). Since \( n \geq 2 \), there is some \( k \in \mathbb{N}_n \setminus \{i\} \). Making three steps from \( v_1 \) by thread \( \text{reader}_k \) results in a state \( v_3 \in Q \) such that \( v_3(pc_{\text{reader}}) = \text{read}, v_3(ww) = 0 \land v(ww) = b \land v(ww) = c \). Combining \( v_2 \in Q, v_3 \in Q \) and using the definition of \( p_{\text{OG,mc}} \) we obtain \( v_4 \in Q \) such that \( v_4(pc_{\text{reader}}) = \text{read} \land v_4(pc_{\text{reader}}) = \text{read} \land v_4(ww) = 0 \land v(ar) = b + 1 \land v(aw) = c \). Making four steps from \( v_4 \) by thread \( \text{reader}_k \) results in the state \( v \) such that \( v(pc_{\text{reader}}) = \text{read} \land v(ww) = 0 \land v(ar) = b \land v(aw) = c \).

Case \( a > 0 \). Let \( b \in \mathbb{N}, c \in \{0,1\}, i \in \mathbb{N}_n \). By assumption hypothesis there is \( v_1 \in Q \) such that \( v_1(pc_{\text{reader}}) = \text{read}, v_1(ww) = a - 1 \land v(ww) = b \land v(ww) = c \). Taking three steps of \( \text{writer}_1 \) from \( v_1 \) results in a state \( v_2 \in Q \) such that \( v_2(pc_{\text{writer}}) = \text{startwriteA}, v_2(ww) = a \land v(ww) = b \land v(ww) = c \). In particular, \( v_2(pc_{\text{writer}}) = \text{askwriteA} \). Taking three steps of \( \text{writer}_2 \) from \( v_1 \) results in a state \( v_3 \in Q \) such that \( v_3(pc_{\text{reader}}) = \text{read} \land v(ww) = a \land v(ww) = b \land v(ww) = c \).
\( \land v(3(ar)) = b \land v(3(aw)) = c. \) In particular, \( v(3(pc_{\text{writer}})) = \text{askwriteA}. \)

Combining \( v(2) \in Q \) and \( v(3) \in Q \) we get that the state \( v \) with \( v(pc_{\text{reader}}) = \text{read} \) all other threads are at their initial locations, \( v(ww) = a \land v(ar) = b \land v(aw) = c \) is in \( Q \).

(III) We claim that for every \( i \in N_n, a, b \in N_0, c \in \{0, 1\} \), the state \( v \) such that \( v(pc_{\text{reader}}) = \text{finishreadA} \land (\forall k \in N_m \setminus \{i\}: v(pc_{\text{reader}}) = \text{startreadA}) \land (\forall j \in N_m: v(pc_{\text{reader}}) = \text{askwriteA}) \land v(ww) = a \land v(ar) = b \land v(aw) = c \) is in \( Q \).

To see that, make one step from a state described in (II).

(IV) We claim that for all \( a, b \in N_0, c \in \{0, 1\}, j \in N_m \), the state \( v \) such that \( (\forall i \in N_n: v(pc_{\text{reader}}) = \text{startreadA}) \land v(pc_{\text{writer}}) = \text{startwriteA} \land (\forall k \in N_m \setminus \{j\}: v(pc_{\text{writer}}) = \text{askwriteA}) \land v(ww) = a \land v(ar) = b \land v(aw) = c \) in \( Q \). Let \( a \in N_0 \). We case split on \( a \).

Case \( a = 0 \). We’ll induct on \( b \).

Case \( b = 0 \). Let \( j \in N_m, c \in \{0, 1\} \). Making from the initial state (which is in \( Q \)) three steps of \( \text{writer}_j \) results in \( v1 \in Q \) such that \( v1(pc_{\text{writer}}) = \text{startwriteA} \). All other threads are at their initial locations, \( v1(ww) = 1 \land v1(ar) = v1(aw) = 0 \). Since \( m \geq 2 \), there is some \( k \in N_m \setminus \{j\} \). Taking three steps of \( \text{writer}_k \) from the initial state results in \( v2 \in Q \) such that \( v2(pc_{\text{writer}}) = \text{startwriteA} \), all other threads are at their initial locations, \( v2(ww) = 1 \land v2(ar) = v2(aw) = 0 \). Combining \( v1 \in Q \) and \( v2 \in Q \), we obtain a state \( v3 \in Q \) such that \( v3(pc_{\text{writer}}) = v3(pc_{\text{writer}}) = \text{startwriteA} \), all other threads are at their initial locations, \( v3(ww) = 1 \land v3(ar) = v3(aw) = 0 \). Making seven steps of \( \text{writer}_j \) from \( v3 \) results in a state \( v4 \in Q \) such that \( v4(pc_{\text{writer}}) = \text{startwriteA} \), all other threads are at their initial locations, \( v4(ww) = v4(ar) = v4(aw) = 0 \).

Case \( c = 0 \). Notice that \( v4 \) satisfies all the requirements for \( v \).

Case \( c = 1 \). Making seven steps of \( \text{writer}_j \) from \( v3 \) results in a state \( v5 \in Q \) such that \( v5(pc_{\text{writer}}) = \text{startwriteA} \), all other threads are at their initial locations, \( v5(ww) = v5(ar) = v5(aw) = 0 \). Combining \( v4 \in Q \), \( v5 \in Q \) and the definition of \( \rho_{\text{OG},mc} \), results in a state \( v6 \in Q \) such that \( v6(pc_{\text{writer}}) = v6(pc_{\text{writer}}) = \text{startwriteA} \), all other threads are at their initial locations, \( v6(ww) = v6(ar) = v6(aw) = 0 \). Making three steps of \( \text{writer}_j \) from \( v6 \) results in a state \( v7 \in Q \) such that \( v7(pc_{\text{writer}}) = \text{startwriteA} \land v7(pc_{\text{writer}}) = \text{write} \), all other threads are at their initial locations, \( v7(ww) = v7(ar) = 0 \land v7(aw) = 1 \). By (I) there is some state \( v8 \in Q \) in which all threads are at their initial locations and \( v8(ww) = v8(ar) = 0 \land v8(aw) = 1 \). Combining \( v7 \in Q \) and \( v8 \in Q \), we obtain the state \( v \in Q \) such that \( v(pc_{\text{writer}}) = \text{startwriteA} \), all other threads are at their initial locations, and \( v(ww) = v(ar) = 0 \land v(aw) = 1 \).

Case \( b = 1 \). Let \( j \in N_m, c \in \{0, 1\} \). By induction assumption there is some \( v1 \in Q \) such that \( v1(pc_{\text{writer}}) = \text{startwriteA} \), all other
threads are at their initial locations, \( v_1(ww) = 0 \land v_1(ar) = b - 1 \land v_1(aw) = c. \) Making three steps of \( \text{reader}_1 \) from \( v_1 \) results in a state \( v_2 \in Q \) such that \( v_2(pc_{\text{reader}_1}) = \text{read} \land v_2(pc_{\text{writer}}) = \text{startwriteA} \), all other threads are at their initial locations, \( v_2(ww) = 0 \land v_2(ar) = b \land v_2(aw) = c. \) Making three steps of \( \text{reader}_2 \) from \( v_1 \) results in a state \( v_3 \in Q \) such that \( v_3(pc_{\text{reader}_2}) = \text{read} \land v_3(pc_{\text{writer}}) = \text{startreadA} \), all other threads are at their initial locations, \( v_3(ww) = 0 \land v_3(ar) = b \land v_3(aw) = c. \) Notice that \( v_2(pc_{\text{reader}_1}) = v_3(pc_{\text{reader}_2}) \) = \( \text{startreadA} \). From \( v_2 \in Q, v_3 \in Q \) we get the state \( v \in Q \) such that \( v(pc_{\text{writer}}) = \text{startwriteA} \), all other threads are at their initial locations, \( v(ww) = 0 \land v(ar) = b \land v(aw) = c. \)

Case \( a \geq 1 \). Let \( j \in \mathbb{N}_m, b \in \mathbb{N}_0, c \in \{0, 1\} \). From (I) we obtain a state \( v_1 \in Q \) in which all threads are at their initial locations, \( v_1(ww) = a - 1 \land v_1(ar) = b \land v_1(aw) = c. \) Making three steps by \( \text{writer}_j \) results in a state \( v \in Q \) such that \( v(pc_{\text{writer}_j}) = \text{startwriteA} \), all other threads are at their initial locations, \( v(ww) = a \land v(ar) = b \land v(aw) = c. \)

(V) We claim that for all \( a, b \in \mathbb{N}_0, c \in \{0, 1\}, j \in \mathbb{N}_m \) the state \( v \) such that \( \forall i \in \mathbb{N}_m: v(pc_{\text{reader}_i}) = \text{startreadA} \land v(pc_{\text{writer}}) = \text{write} \land \forall k \in \mathbb{N}_m \setminus \{j\}: v(pc_{\text{writer}_k}) = \text{askwriteA} \land v(ww) = a \land v(ar) = b \land v(aw) = c \) is in \( Q \). We’ll use induction on \( a \).

Case \( a = 0 \). We’ll use induction on \( b \).

Case \( b = 0 \). Let \( c \in \{0, 1\}, j \in \mathbb{N}_m \).

Case \( c = 0 \). Making six steps of \( \text{writer}_j \) from the initial state results in a state \( v_1 \in Q \) such that \( v_1(pc_{\text{writer}_j}) = \text{write} \), other threads are at their initial locations, \( v_1(ww) = v_1(aw) = 1 \) and \( v_1(ar) = 0 \). Let \( k \in \mathbb{N}_m \setminus \{j\} \). Making six steps of \( \text{writer}_k \) from the initial state results in a state \( v_2 \in Q \) such that \( v_2(pc_{\text{writer}_j}) = \text{write} \), other threads are at their initial locations, \( v_2(ww) = v_2(aw) = 1 \) and \( v_2(ar) = 0 \). Combining \( v_2 \in Q, v_3 \in Q \) and \( k \neq j \), we obtain a state \( v_3 \in Q \) such that \( v_3(pc_{\text{writer}_j}) = v_3(pc_{\text{writer}_k}) = \text{write} \), other threads are at their initial locations, \( v_3(ww) = v_3(aw) = 1 \) and \( v_3(ar) = 0 \). Making four steps of \( \text{writer}_j \) from \( v_3 \) results in the state \( v \in Q \) such that \( v(pc_{\text{writer}_j}) = \text{write} \), all other threads are at their initial locations, \( v(ww) = v(aw) = v(ar) = 0 \).

Case \( c = 1 \). By (IV) the state \( v_1 \) such that \( v_1(pc_{\text{writer}_j}) = \text{startwriteA}, \) all other threads are at their initial locations, \( v_1(ww) = v_1(ar) = v_1(aw) = 0 \) is in \( Q \). Make three steps by thread \( \text{writer}_j \).

Case \( b \geq 1 \). Let \( c \in \{0, 1\}, j \in \mathbb{N}_m \).

By induction assumption, there is a state \( v_1 \in Q \) such that \( v_1(pc_{\text{writer}_j}) = \text{write} \), other threads are at their initial locations, \( v_1(ww) = 0 \land v_1(ar) = b - 1 \land v_1(aw) = c. \) Making three steps of \( \text{reader}_1 \) from \( v_1 \) results in a state \( v_2 \in Q \) such that \( v_2(pc_{\text{reader}_1}) = \text{read}, v_2(pc_{\text{reader}_2}) = \text{read}, \) all other threads (including \( \text{reader}_2 \)) are at
their initial locations, \( v_2(ww) = 0 \land v_2(ar) = b \land v_2(aw) = c \). Making three steps of \( reader_2 \) from \( v_1 \) results in a state \( v_3 \in Q \) such that \( v_3(p_{\text{writer}}) = \text{write}, v_3(p_{\text{reader}_1}) = \text{read} \), all other threads (including \( reader_1 \)) are at their initial locations, \( v_3(ww) = 0 \land v_3(ar) = b \land v_3(aw) = c \). Combining \( v_2 \in Q \) and \( v_3 \in Q \) we get the state \( v \in Q \) such that \( v(p_{\text{writer}}) = \text{write}, v(p_{\text{reader}_1}) = \text{read} \), all other threads are at their initial locations and \( v(ww) = 0 \land v(ar) = b \land v(aw) = c \).

Case \( a \geq 1 \). Let \( b \in N_0, c \in \{0,1\}, j \in N_m \). By induction hypothesis, there is some \( v_1 \in Q \) such that \( v_1(p_{\text{writer}}) = \text{write} \), all other threads are at their initial locations, \( v_1(ww) = a - 1, v_1(ar) = b, v_1(aw) = c \). Since \( m \geq 2 \), there is \( k \in N_m \) such that \( k \neq j \). Making three steps of \( writer_k \) from \( v_1 \) results in a state \( v_2 \in Q \) such that \( v_2(p_{\text{writer}}) = \text{write} \), \( v_2(p_{\text{writer}_j}) = \text{startwriteA} \), \( v_2(ww) = a, v_2(ar) = b, v_2(aw) = c \). By (I), there is a state \( v_3 \in Q \) in which all threads are at their initial locations, \( v_3(ww) = a, v_3(ar) = b, v_3(aw) = c \). In particular, \( v_3(p_{\text{writer}_j}) = \text{askwriteA} \). From \( v_2 \in Q \) and \( v_3 \in Q \) we obtain that the state \( v \) such that \( v(p_{\text{writer}}) = \text{write}, v(p_{\text{reader}_j}) = \text{write} \), all other threads are at their initial locations, \( v(ww) = a \land v(ar) = b \land v(aw) = c \) is in \( Q \).

(VI) We claim that for all \( a, b \in N_0, c \in \{0,1\}, j \in N_m \) the state \( v \in Q \) such that (\( \forall i \in N_n : v(p_{\text{reader}}) = \text{startreadA} \) \( \land v(p_{\text{writer}}) = \text{finishwriteA} \) \( \land (\forall k \in N_m \setminus \{j\} : v(p_{\text{writer}_k}) = \text{askwriteA}) \) \( \land v(ww) = a \land v(ar) = b \land v(aw) = c \) in \( Q \). To see that, let \( a, b \in N_0, c \in \{0,1\}, j \in N_m \), and make one step of \( writer_j \) from the corresponding state from (V).

(VII) We claim that for all \( a, b \in N_0, c \in \{0,1\}, j \in N_m \), any state \( v \) such that (\( \forall i \in N_n : v(p_{\text{reader}}) \in \text{NonCritR} \) \( \land (\forall j \in N_n : v(p_{\text{writer}}) \in \text{NonCritW} \) \( \land v(ww) = a \land v(ar) = b \land v(aw) = c \) in \( Q \). This follows from (I), (II), (III), (IV), (V), (VI) and the definition of \( \rho_{\text{OG,mc}} \).

(VIII) We claim that for all \( b \in N_0, c \in \{0,1\}, i \in N_n \), any state \( v \) such that \( v(p_{\text{reader}}) = \text{startreadB} \) \( \land (\forall k \in N_n \setminus \{i\} : v(p_{\text{reader}_k}) \in \text{NonCritR} \) \( \land (\forall j \in N_n : v(p_{\text{writer}}) \in \text{NonCritW} \) \( \land v(ww) = 0 \land v(ar) = b \land v(aw) = c \) in \( Q \). To see that, let \( b \in N_0, c \in \{0,1\}, i \in N_n \), and \( v \) as above. By (VII), the state \( v_1 = v(p_{\text{reader},\rightarrow} \text{startreadA}) \) is in \( Q \). Make one step of \( reader_1 \).

(IX) We claim that for all \( b \in N^+, c \in \{0,1\}, i \in N_n \), any state \( v \) such that \( v(p_{\text{reader}}) = \text{startreadC} \) \( \land (\forall k \in N_n \setminus \{i\} : v(p_{\text{reader}_k}) \in \text{NonCritR} \) \( \land (\forall j \in N_n : v(p_{\text{writer}}) \in \text{NonCritW} \) \( \land v(ww) = 0 \land v(ar) = b \land v(aw) = c \) in \( Q \). To see that, let \( b \in N^+, c \in \{0,1\}, i \in N_n \) and \( v \) as stated. By (VIII) the state \( v_1 = v(p_{\text{reader},\rightarrow} \text{startreadB},ar\rightarrow b-1) \) is in \( Q \). Make one step of thread \( reader_1 \).

(X) We claim that for all \( a, b \in N_0, c \in \{0,1\}, i \in N_n \), any state \( v \) such that \( v(p_{\text{reader}}) = \text{finishreadB} \) \( \land (\forall k \in N_n \setminus \{i\} : v(p_{\text{reader}_k}) \in \text{NonCritR} \) \( \land (\forall j \in N_n : v(p_{\text{writer}}) \in \text{NonCritW} \) \( \land v(ww) = a \land v(ar) = b \land v(aw) = c \) in \( Q \).
To see that, let $a, b \in \mathbb{N}_0, c \in \{0,1\}, i \in \mathbb{N}_m$, $v$ as required. By (VII), the state $v_1 = v[p_{\text{reader}} \rightarrow \text{finishreadA}]$ is in $Q$. Take one step by reader, from $v_1$.

(XI) We claim that for all $a, b \in \mathbb{N}_0, c \in \{0,1\}, i \in \mathbb{N}_m$, any state $v$ such that $v(p_{\text{reader}}) = \text{finishreadC} \land (\forall k \in \mathbb{N}_m \setminus \{i\}) : v(p_{\text{reader}}) \in \text{NonCritR}) \land (\forall j \in \mathbb{N}_m : v(p_{\text{writer}}) \in \text{NonCritW}) \land v(ww) = a \land v(ar) = b \land v(aw) = c$ is in $Q$.

To see that, let $a, b \in \mathbb{N}_0, c \in \{0,1\}, i \in \mathbb{N}_m$ and $v$ as above. By (X), the state $v_1 = v[p_{\text{reader}} \rightarrow \text{finishreadB}, ar \rightarrow b + 1]$ is in $Q$. Take one step by thread reader.

(XII) We claim that for all $a, b \in \mathbb{N}_0, c \in \{0,1\}, i \in \mathbb{N}_m$ any state $v$ such that $(\forall i \in \mathbb{N}_m : v(p_{\text{reader}}) \in \text{NonCritR}) \land v(p_{\text{writer}}) = \text{askwriteB} \land (\forall k \in \mathbb{N}_m \setminus \{j\}) : v(p_{\text{writer}}) \in \text{NonCritW}) \land v(ww) = a \land v(ar) = b \land v(aw) = c$ is in $Q$.

To see that, let $a, b \in \mathbb{N}_0, c \in \{0,1\}, j \in \mathbb{N}_m$ and $v$ as stated. By (VII), the state $v_1 = v[p_{\text{writer}} \rightarrow \text{askwriteA}]$ is in $Q$. Apply one step of writer, to $v_1$.

(XIII) We claim that for all $a \in \mathbb{N}_0$, $b \in \mathbb{N}_0, c \in \{0,1\}, j \in \mathbb{N}_m$ any state $v$ such that $(\forall i \in \mathbb{N}_m : v(p_{\text{reader}}) \in \text{NonCritR}) \land v(p_{\text{writer}}) = \text{startwriteB} \land (\forall k \in \mathbb{N}_m \setminus \{j\}) : v(p_{\text{writer}}) \in \text{NonCritW}) \land v(ww) = a \land v(ar) = v(aw) = 0$ is in $Q$.

To see that, let $a, b \in \mathbb{N}_0, j \in \mathbb{N}_m$ and $v$ as stated. By (VII) the state $v_1 = v[p_{\text{writer}} \rightarrow \text{startwriteA}]$ is in $Q$. Apply one step of writer, to $v_1$.

(XIV) We claim that for all $a \in \mathbb{N}_0$, $b \in \mathbb{N}_0$ any state $v$ such that $(\forall i \in \mathbb{N}_m : v(p_{\text{reader}}) \in \text{NonCritR}) \land v(p_{\text{writer}}) = \text{startwriteC} \land (\forall k \in \mathbb{N}_m \setminus \{j\}) : v(p_{\text{writer}}) \in \text{NonCritW}) \land v(ww) = a \land v(ar) = 0 \land v(aw) = 1$ is in $Q$.

To see that, let $a, b \in \mathbb{N}_0, j \in \mathbb{N}_m$ and $v$ as stated. By (XIV) the state $v_1 = v[p_{\text{reader}} \rightarrow \text{startwriteB}, aw \rightarrow 0]$ is in $Q$. Make one step from $v_1$ by thread writer, to $v_1$.

(XV) We claim that for all $a \in \mathbb{N}_0, b \in \mathbb{N}_0, c \in \{0,1\}, j \in \mathbb{N}_m$ any state $v$ such that $(\forall i \in \mathbb{N}_m : v(p_{\text{reader}}) \in \text{NonCritR}) \land v(p_{\text{writer}}) = \text{finishwriteB} \land (\forall k \in \mathbb{N}_m \setminus \{j\}) : v(p_{\text{writer}}) \in \text{NonCritW}) \land v(ww) = a \land v(ar) = b \land v(aw) = c$ is in $Q$.

To see that, let $a, b \in \mathbb{N}_0, c \in \{0,1\}, j \in \mathbb{N}_m, v$ as stated. By (VII) the state $w = v[p_{\text{writer}} \rightarrow \text{finishwriteA}]$ is in $Q$. Apply one step of writer, from $w$.

(XVI) We claim that for all $a, b \in \mathbb{N}_0, j \in \mathbb{N}_m$ any state $v$ such that $(\forall i \in \mathbb{N}_m : v(p_{\text{reader}}) \in \text{NonCritR}) \land v(p_{\text{writer}}) = \text{finishwriteC} \land (\forall k \in \mathbb{N}_m \setminus \{j\}) : v(p_{\text{writer}}) \in \text{NonCritW}) \land v(ww) = a \land v(ar) = b \land v(aw) = 0$ is in $Q$. 

To see that, let $a, b \in \mathbb{N}_0, j \in \mathbb{N}_m, v$ as stated. By (VII) the state $w = v[p_{\text{writer}} \rightarrow \text{finishwriteB}]$ is in $Q$. Apply one step of writer, from $w$. 

62
To see that, let $a, b \in \mathbb{N}_0$, $j \in \mathbb{N}_m$, $v$ as stated. By (XVI) the state $w = v[p_{\text{writer}, r} \rightarrow \text{finishwrite} B, aw \rightarrow l]$ is in $Q$. Apply one step of $\text{writer}$ from $w$.

Let $v \in \text{RHS}$. If $\text{control}$ is available in $v$, apply (VII). Otherwise there is some thread at a critical location ... B or ... C. If the critical location is in a reader, apply one of (VIII), (IX), (XI), if the critical location is in a writer, apply one of (XII), (XIII), (XIV), (XV), (XVI), (XVII).

Thus the precision of the Owicki-Gries core and abstract interpretation with $\rho_{\text{OG,mc}}$ coincide on Readers-Writers.

Example 60 (Upper). Consider the RPL transition system Upper. We’ll show that $\rho_{\text{OG,mc}}(\text{init})$ is a subset of $\text{init}$.

Let $v \in \rho_{\text{OG,mc}}(\text{init})$. For the left thread we have some $v_1 \in \text{init}$ such that $v \sim_{(p_{c_1}, u, z, x, y, l)} v_1$. Thus $v(p_{c_1}) = A$ and $v(u) \neq v(z) = v(x) = v(y) = v(l)$. For the right thread we have some $v_2 \in \text{init}$ such that $v \sim_{(p_{c_2}, u, z, x, y, l)} v_2$. Thus $v(p_{c_2}) = 0$. Then $v \in \text{init}$.

Then $\rho_{\text{OG,mc}}(\text{init} \cup \text{post}(\text{init})) \subseteq \rho_{\text{OG,mc}}(\text{init}) \subseteq \text{init}$. Thus $\text{lfp}(\lambda x. \rho_{\text{OG,mc}}(\text{init} \cup \text{post}(x))) = \text{init}$.

Thus the result of abstract interpretation with $\rho_{\text{OG,mc}}$ is strictly stronger than the strongest Owicki-Gries-core-provable property.

Example 61 (SepThreads). Consider an RPL transition system from SepThreads. For the syntactic structure $\text{StrSepThreads}$ and $Q \in D$ we have $\rho_{\text{OG,mc}}(Q) = \{v \in \text{ConsState} \mid \forall t \in \text{Tid} \exists \bar{v} \in Q; \: v \sim_{\text{DatOrder}} \bar{v} \} \subseteq \{v \in \text{ConsState} \mid \forall t \in \text{Tid} \exists \bar{v} \in Q; \: v \sim_{\text{Local}} \bar{v} \} = \rho(Q)$. Thus $\text{lfp}(\lambda x. \text{init} \cup \text{post}(x)) \subseteq \text{lfp}(\lambda x. \rho_{\text{OG,mc}}(\text{init} \cup \text{post}(x))) \subseteq \text{lfp}(\lambda x. \rho(\text{init} \cup \text{post}(x))) \subseteq$ [Example 22] $\text{lfp}(\lambda x. \rho_{\text{OG,mc}}(\text{init} \cup \text{post}(x)))$. The precision of Owicki-Gries-core and abstract interpretation with $\rho_{\text{OG,mc}}$ is the same on RPL transition systems from SepThreads.

Example 62. In Fig. 6 we see two threads executing the same code, together with its smallest Owicki-Gries-core proof.

\[
\text{resource } r(x) \text{ initially } x = 0; \\
A: \{\text{true}\} \quad A: \{\text{true}\} \\
\text{with } r \text{ do} \quad \text{with } r \text{ do} \\
B: \{x = 0\} \quad B: \{x = 0\} \quad x := 1; \\
\text{C: } \{x = 1\} \quad \text{C: } \{x = 1\} \\
\text{assume false} \quad \text{assume false} \\
D: \{\text{false}\} \quad D: \{\text{false}\} \quad \text{endwith} \quad \text{endwith} \\
E: \{\text{false}\} \quad E: \{\text{false}\} \\
I_r = \{x = 0\}
\]

Fig. 6: RPL transition system progAssign1 with its smallest Owicki-Gries-core proof.
Notice that the RPL program given by Fig. 7 has multithreaded Cartesian abstraction, adapted to RPL in the most straightforward way. Consider the upper fixpoint iteration sequence \( (X^{(i)})_{i \in \omega} \) for \( \lambda x. \rho_{OG,mc}(init \cup post(x)) \):

\[
X^{(0)} = \emptyset,
\]

\[
X^{(1)} = \{ [x\mapsto 0, pc_1 \mapsto A, pc_2 \mapsto A] \},
\]

\[
X^{(2)} = \left\{ [x\mapsto 0, pc_1 \mapsto A, pc_2 \mapsto A], [x\mapsto 0, pc_1 \mapsto A, pc_2 \mapsto B], [x\mapsto 0, pc_1 \mapsto B, pc_2 \mapsto A] \right\},
\]

\[
init \cup post(X^{(2)}) = \left\{ [x\mapsto 0, pc_1 \mapsto A, pc_2 \mapsto A], [x\mapsto 0, pc_1 \mapsto A, pc_2 \mapsto B], [x\mapsto 0, pc_1 \mapsto B, pc_2 \mapsto A], [x\mapsto 1, pc_1 \mapsto A, pc_2 \mapsto A] \right\},
\]

\[
X^{(3)} = \left\{ [x\mapsto 0, pc_1 \mapsto A, pc_2 \mapsto A], [x\mapsto 0, pc_1 \mapsto A, pc_2 \mapsto B], [x\mapsto 0, pc_1 \mapsto B, pc_2 \mapsto A], [x\mapsto 1, pc_1 \mapsto A, pc_2 \mapsto A] \right\},
\]

\[
init \cup post(X^{(3)}) = \left\{ [x\mapsto 0, pc_1 \mapsto A, pc_2 \mapsto A], [x\mapsto 0, pc_1 \mapsto A, pc_2 \mapsto B], [x\mapsto 0, pc_1 \mapsto B, pc_2 \mapsto A], [x\mapsto 1, pc_1 \mapsto A, pc_2 \mapsto A], [x\mapsto 1, pc_1 \mapsto A, pc_2 \mapsto C], [x\mapsto 1, pc_1 \mapsto B, pc_2 \mapsto A], [x\mapsto 1, pc_1 \mapsto B, pc_2 \mapsto C], [x\mapsto 1, pc_1 \mapsto C, pc_2 \mapsto A] \right\},
\]

\[
X^{(4)} = \left\{ [x\mapsto 0, pc_1 \mapsto A, pc_2 \mapsto A], [x\mapsto 0, pc_1 \mapsto A, pc_2 \mapsto B], [x\mapsto 0, pc_1 \mapsto B, pc_2 \mapsto A], [x\mapsto 1, pc_1 \mapsto A, pc_2 \mapsto A], [x\mapsto 1, pc_1 \mapsto A, pc_2 \mapsto B], [x\mapsto 1, pc_1 \mapsto B, pc_2 \mapsto A], [x\mapsto 1, pc_1 \mapsto B, pc_2 \mapsto C], [x\mapsto 1, pc_1 \mapsto C, pc_2 \mapsto A] \right\},
\]

\[
init \cup post(X^{(4)}) = \left\{ [x\mapsto 0, pc_1 \mapsto A, pc_2 \mapsto A], [x\mapsto 0, pc_1 \mapsto A, pc_2 \mapsto B], [x\mapsto 0, pc_1 \mapsto B, pc_2 \mapsto A], [x\mapsto 1, pc_1 \mapsto A, pc_2 \mapsto A], [x\mapsto 1, pc_1 \mapsto A, pc_2 \mapsto B], [x\mapsto 1, pc_1 \mapsto B, pc_2 \mapsto A], [x\mapsto 1, pc_1 \mapsto B, pc_2 \mapsto C], [x\mapsto 1, pc_1 \mapsto C, pc_2 \mapsto A] \right\},
\]

\[
X^{(5)} = X^{(4)}. \]

Notice that \( \gamma_{OG} \inf \mathcal{D} \subseteq \text{lfp}(\lambda x. \rho_{OG,mc}(init \cup post(x))) \).
So abstract interpretation with \( \rho_{OG,mc} \) produces a strictly weaker property than the strongest Owicki-Gries-core proof on this example. \( \square \)

From Examples 60 and 62 we obtain that Owicki-Gries core is incomparable with multithreaded Cartesian abstraction, adapted to RPL in the most straightforward way.

**Example 63.** The RPL program given by Fig. 7 has \( Tid = \{1, 2\}, PL = \{A, B\}, \forall t \in PL \cup \{0, 1\}, \text{Res} = \emptyset, \text{Local}_1 = \{pc_1, l_1\}, \text{Local}_2 = \{pc_2, l_2\}, \text{ProofVar} = \emptyset, rsc(A) = rsc(B) = \emptyset. \)

64
integer $l_1 = l_2 \in \{0, 1\}$

\[
\begin{align*}
A: \{\text{true}\} & \quad \text{assume } \text{false;} \quad A: \{\text{true}\} \quad \text{assume } \text{false;} \\
B: \{\text{false}\} & \quad B: \{\text{false}\} \\
l_1 := 0 & \quad l_2 := 0 \\
C: \{\text{false}\} & \quad C: \{\text{false}\}
\end{align*}
\]

Fig. 7: RPL transition system progAssign2 with its smallest Owicki-Gries-core proof.

Then

\[
\gamma_{OG}(\inf \Omega) = \{ [l_1 \mapsto 0, l_2 \mapsto 0, pc_1 \mapsto A, pc_2 \mapsto A], [l_1 \mapsto 0, l_2 \mapsto 1, pc_1 \mapsto A, pc_2 \mapsto A], [l_1 \mapsto 1, l_2 \mapsto 0, pc_1 \mapsto A, pc_2 \mapsto A], [l_1 \mapsto 1, l_2 \mapsto 1, pc_1 \mapsto A, pc_2 \mapsto A] \},
\]

and

\[
\rho_{OG,mc}(\text{init}) = \text{init}, \quad \text{thus } \text{lfp}(\lambda x. \rho_{OG,mc}(\text{init} \cup \text{post}(x))) = \text{init}.
\]

So the strongest Owicki-Gries-core-provable property is strictly weaker than the strongest property provable by abstract interpretation with $\rho_{OG,mc}$. □

Both progAssign1 and progAssign2 belong to Simple. For progAssign2 the strongest Owicki-Gries-core-provable property is strictly weaker than the strongest property provable by abstract interpretation with $\rho_{OG,mc}$. For progAssign1 the strongest Owicki-Gries-core provable property is strictly stronger. Thus, for Simple, the Owicki-Gries core is in general incomparable with abstract interpretation with $\rho_{OG,mc}$.

Owicki-Gries for RPL and general programs target different verification tasks. Owicki-Gries for RPL allows verifying properties assuming mutual exclusion (external verification). Owicki-Gries for general programs (= multithreaded Cartesian abstraction) allows checking synchronization details without assuming mutual exclusion (internal verification). This section presents an initial step in comparing the two proof systems. The incomparability result shows that if both systems can be unified, it is not going to be trivial.

Although it is impossible to present a verification methodology that has exactly the same precision as both proof systems, there is a verification method that produces properties which are stronger than both proof systems, and which can be viewed as a generalization of both proof systems, namely the deny-guarantee framework [12], SL+ [27], SAGL [13], or RGSep [29, 30]. These logics, however, do not generalize the "pure" Owicki-Gries system, but separation-logic-based approaches.

We also conjecture that it is possible to prove all Owicki-Gries-core-provable properties by abstract interpretation with $\rho_{OG,mc}$ with the following fixed choice of auxiliary variables. Namely, for each resource, we add a resource variable that indicates which thread is in the critical section for that resource.

I Practical implications

Now we look at the importance of results for practical verification.
Many real-life specified properties of programs are simple: they involve only few variables, which are, for example, local, or all belong to the same resource. In this case the property is likely to be a fixpoint of one of the considered closures, which retain dependencies between certain variables. Checking this fact is easy: it does not depend on the program’s transition relation. If in addition the property is expected to be inductive, we obtain a clear choice of an analysis to confirm our expectation: it would be abstract interpretation with any closure for which the property is a fixpoint.

Abstract interpretation with a chosen closure might also derive a property which is coarser than expected. In this case, in the chain

\[ \rho_c \rightarrow \rho \rightarrow \text{Owicki-Gries core} \rightarrow \rho \rightarrow \text{identity} \]

it is useless to try out analyses with a lower precision. On the contrary, an analysis with a higher precision, which tracks more variable dependencies, might help.

An analysis from this chain might also run out of time or space, failing to produce any property. Without further assumptions, predicting time or space consumption of other analyses is hard. However, for certain finite-state scenarios predictions are still possible. For example, abstract interpretation with \( \rho_c \) and the Owicki-Gries core can be easily executed as fixpoint iterations on the domains of Cartesian products and program annotations, respectively. The worst-case space for storing the iterates is larger for the Owicki-Gries core than for \( \rho_c \), also the height of the domain of program annotations is larger than the height of the domain of products of blocks. If the worst case is expected (e.g., by an insight of an expert), machines which are slow or have low memory might be too restricted to execute the Owicki-Gries core, so abstract interpretation with \( \rho_c \) should be recommended to attempt first.