AN INTRODUCTION TO
SEPARATION LOGIC

1. An Overview

John C. Reynolds
Carnegie Mellon University

January 7, 2011

©2011 John C. Reynolds
A Program for In-place List Reversal

\[
LREV \overset{\text{def}}{=} j := \text{nil}; \quad \text{while } i \neq \text{nil} \text{ do (} k := [i + 1]; [i + 1] := j; j := i; i := k \text{).}
\]

To prove \{
\text{list } \alpha \ i\}\ LREV \ \{\text{list } \alpha^\dagger \ j\}, \text{ the invariant}

\[
\exists \alpha, \beta. \ \text{list } \alpha \ i \land \text{list } \beta \ j \land \alpha^\dagger_0 = \alpha^\dagger \cdot \beta,
\]

(where \text{list } \epsilon \ i \overset{\text{def}}{=} i = \text{nil} \text{ and } \text{list}(a \cdot \alpha) \ i \overset{\text{def}}{=} \exists j. \ i \leftrightarrow a, j \land \text{list } \alpha \ j) \text{ is inadequate.
An adequate invariant (in Hoare logic):

$$(\exists \alpha, \beta. \text{list } \alpha \ i \land \text{list } \beta \ j \land \alpha_0^\dagger = \alpha^\dagger \cdot \beta)$$
$$\land (\forall k. \text{reachable}(i, k) \land \text{reachable}(j, k) \Rightarrow k = \text{nil}).$$

An adequate invariant (in separation logic):

$$(\exists \alpha, \beta. \text{list } \alpha \ i \ast \text{list } \beta \ j) \land \alpha_0^\dagger = \alpha^\dagger \cdot \beta.$$ 

where $\ast$ is the separating conjunction.
To prove \( \{ \text{list } \alpha \ i \ * \ \text{list } \gamma \ x \} \ LREV \ {\text{list } \alpha^{\dagger} \ j \ * \ \text{list } \gamma \ x \} \) in Hoare
logic, we need the stronger invariant:

\[
\begin{align*}
(\exists \alpha, \beta . \text{list } \alpha \ i \wedge \text{list } \beta \ j \wedge \alpha_0^\dagger &= \alpha^\dagger \cdot \beta) \\
\wedge (\forall k. \text{reachable}(i, k) \wedge \text{reachable}(j, k) \Rightarrow k = \text{nil}) \\
\wedge \text{list } \gamma \ x \\
\wedge (\forall k. \text{reachable}(x, k) \\
\wedge (\text{reachable}(i, k) \vee \text{reachable}(j, k)) \Rightarrow k = \text{nil}).
\end{align*}
\]

But in separation logic, we can use:

\[
(\exists \alpha, \beta . \text{list } \alpha \ i \ * \ \text{list } \beta \ j \ * \ \text{list } \gamma \ x) \wedge \alpha_0^\dagger = \alpha^\dagger \cdot \beta).
\]
Framing

Actually, in separation logic, from

\[
\{\text{list } \alpha \ i\} \ LREV \ \{\text{list } \alpha^\dagger \ j\},
\]

we can use the frame rule to infer directly that

\[
\{\text{list } \alpha \ i \ast \ \text{list } \gamma \ x\} \ LREV \ \{\text{list } \alpha^\dagger \ j \ast \ \text{list } \gamma \ x\}.
\]
Overview of Separation Logic

- Low-level programming language
  - Extension of simple imperative language
  - Commands for allocating, accessing, mutating, and deallocating data structures
  - Dangling pointer faults (if pointer is dereferenced)

- Program specification and proof
  - Extension of Hoare logic
  - Separating (independent, spatial) conjunction ($\ast$) and implication ($\neg \ast$)

- Inductive definitions over abstract structures
Early History

- Distinct Nonrepeating Tree Systems (Burstall 1972)
- Adding Separating Conjunction to Hoare Logic (Reynolds 1999, with flaws)
- Bunched Implication (BI) Logics (O’Hearn and Pym 1999)
- Classical Separation Logic (Ishtiaq and O’Hearn 2001)
- Adding Address Arithmetic (Reynolds 2001)
- Concurrent Separation Logic (O’Hearn and Brookes 2004)
States

Without address arithmetic (old version):

Values = Integers \cup Atoms \cup Addresses
where Integers, Atoms, and Addresses are disjoint

\text{nil} \in Atoms

Stores_{V} = V \rightarrow Values

Heaps = \bigcup_{A \subseteq \text{Addresses}}^{\text{fin}} (A \rightarrow \text{Values}^{+})

States_{V} = \text{Stores}_{V} \times \text{Heaps}

where \(V\) is a finite set of variables.
With address arithmetic (new version):

Values = Integers
Atoms $\cup$ Addresses $\subseteq$ Integers

where Atoms and Addresses are disjoint

$\text{nil} \in$ Atoms

Stores$_V = V \rightarrow$ Values

Heaps $= \bigcup_{A \subseteq \text{Addresses}}^{\text{fin}} (A \rightarrow \text{Values})$

States$_V = \text{Stores}_V \times$ Heaps

where $V$ is a finite set of variables.

(We assume that all but a finite number of nonnegative integers are addresses.)
The Programming Language: An Informal View

The simple imperative language:

\[
\begin{align*}
\text{:=} & \quad \text{skip} ; \quad \text{if} - \text{then} - \text{else} - \quad \text{while} - \text{do} - \\
\end{align*}
\]

plus:

\begin{itemize}
\item \textbf{Allocation} \quad x := \text{cons}(1, 2) ; \\
\quad \text{Store:} \quad x: 3, \ y: 4 \\
\quad \text{Heap:} \quad \text{empty}
\]

\begin{itemize}
\item \textbf{Lookup} \quad y := [x] ; \\
\quad \text{Store:} \quad x: 37, \ y: 4 \\
\quad \text{Heap:} \quad 37: 1, \ 38: 2
\]

\begin{itemize}
\item \textbf{Mutation} \quad [x + 1] := 3 ; \\
\quad \text{Store:} \quad x: 37, \ y: 1 \\
\quad \text{Heap:} \quad 37: 1, \ 38: 2
\]

\begin{itemize}
\item \textbf{Deallocation} \quad \text{dispose}(x + 1) \\
\quad \text{Store:} \quad x: 37, \ y: 1 \\
\quad \text{Heap:} \quad 37: 1
\end{itemize}
\end{itemize}
Note that:

- Expressions depend only upon the store.
  - no side effects or nontermination.
  - \texttt{cons} and \texttt{[–]} are parts of commands.
- Allocation is nondeterminate.
Memory Faults

Allocation \( x := \text{cons}(1, 2) \);

\[
\begin{align*}
\text{Store} & : x: 3, y: 4 \\
\text{Heap} & : \text{empty}
\end{align*}
\]

\[
\downarrow
\]

\[
\begin{align*}
\text{Store} & : x: 37, y: 4 \\
\text{Heap} & : 37: 1, 38: 2
\end{align*}
\]

Lookup \( y := [x] \);

\[
\downarrow
\]

\[
\begin{align*}
\text{Store} & : x: 37, y: 1 \\
\text{Heap} & : 37: 1, 38: 2
\end{align*}
\]

Mutation \([x + 2] := 3 \);

\[
\text{abort}
\]

Faults can also be caused by out-of-range lookup or deallocation.
Assertions

Standard predicate calculus:

\[ \land \quad \lor \quad \neg \quad \Rightarrow \quad \forall \quad \exists \]

plus:

- **emp**  
  The heap is empty.

- **e \leftrightarrow e'**  
  The heap contains one cell, at address \( e \) with contents \( e' \).

- **p_1 * p_2**  
  The heap can be split into two disjoint parts such that \( p_1 \) holds for one part and \( p_2 \) holds for the other.

- **p_1 \rightarrow* p_2**  
  If the heap is extended with a disjoint part in which \( p_1 \) holds, then \( p_2 \) holds for the extended heap.
Some Abbreviations

\[ e \mapsto - \overset{\text{def}}{=} \exists x'. e \mapsto x' \quad \text{where } x' \text{ not free in } e \]

\[ e \mapsto e' \overset{\text{def}}{=} e \mapsto e' \ast \text{true} \]

\[ e \mapsto e_1, \ldots, e_n \overset{\text{def}}{=} e \mapsto e_1 \ast \cdots \ast e + n - 1 \mapsto e_n \]

\[ e \mapsto e_1, \ldots, e_n \overset{\text{def}}{=} e \mapsto e_1 \ast \cdots \ast e + n - 1 \mapsto e_n \quad \text{iff} \quad e \mapsto e_1, \ldots, e_n \ast \text{true} \]
Examples of Separating Conjunction

1. $x \mapsto 3, y$ asserts that $x$ points to an adjacent pair of cells containing 3 and $y$. 

2. $y \mapsto 3, x$ asserts that $y$ points to an adjacent pair of cells containing 3 and $x$. 

3. $x \mapsto 3, y \ast y \mapsto 3, x$ asserts that situations (1) and (2) hold for separate parts of the heap. 

4. $x \mapsto 3, y \land y \mapsto 3, x$ asserts that situations (1) and (2) hold for the same heap, which can only happen if the values of $x$ and $y$ are the same. 

5. $x \mapsto 3, y \land y \mapsto 3, x$ asserts that either (3) or (4) may hold, and that the heap may contain additional cells.
An Example of Separating Implication

Suppose \( p \) holds for

\[
\text{Store: } x: \alpha, \ldots \\
\text{Heap: } \alpha: 3, \alpha + 1: 4, \ldots
\]

Then \( (x \mapsto 3, 4) \rightarrow p \) holds for

\[
\text{Store: } x: \alpha, \ldots \\
\text{Heap: } \ldots
\]

and \( x \mapsto 1, 2 \ast ((x \mapsto 3, 4) \rightarrow p) \) holds for

\[
\text{Store: } x: \alpha, \ldots \\
\text{Heap: } \alpha: 1, \alpha + 1: 2, \ldots
\]

In particular,

\[
\{ x \mapsto 1, 2 \ast ((x \mapsto 3, 4) \rightarrow p) \} [x] := 3; [x + 1] := 4 \{p\},
\]

and more generally,

\[
\{ x \mapsto -, -, \ast ((x \mapsto 3, 4) \rightarrow p) \} [x] := 3; [x + 1] := 4 \{p\}.
\]
Rules and Axiom Schemata for $\ast$ and $\neg\ast$

\[
\begin{align*}
p_1 \ast p_2 &\iff p_2 \ast p_1 \\
(p_1 \ast p_2) \ast p_3 &\iff p_1 \ast (p_2 \ast p_3) \\
p \ast \text{emp} &\iff p \\
(p_1 \lor p_2) \ast q &\iff (p_1 \ast q) \lor (p_2 \ast q) \\
(p_1 \land p_2) \ast q &\Rightarrow (p_1 \ast q) \land (p_2 \ast q) \\
(\exists x. p_1) \ast p_2 &\iff \exists x. (p_1 \ast p_2) \quad \text{when } x \text{ not free in } p_2 \\
(\forall x. p_1) \ast p_2 &\Rightarrow \forall x. (p_1 \ast p_2) \quad \text{when } x \text{ not free in } p_2 \\
\frac{p_1 \Rightarrow p_2 \quad q_1 \Rightarrow q_2}{p_1 \ast q_1 \Rightarrow p_2 \ast q_2} \quad \text{(monotonicity)}
\end{align*}
\]

\[
\begin{align*}
p_1 \ast p_2 &\Rightarrow p_3 \\
p_1 \Rightarrow (p_2 \ast p_3) &\iff p_1 \Rightarrow (p_2 \ast p_3) \quad \text{(currying)} \\
p_1 \ast p_2 &\Rightarrow p_3
\end{align*}
\]

\[
\begin{align*}
p_1 \Rightarrow (p_2 \Rightarrow p_3) &\iff p_1 \Rightarrow (p_2 \ast p_3) \quad \text{(decurrying)} \\
p_1 \ast p_2 &\Rightarrow p_3.
\end{align*}
\]
Two Unsound Axiom Schemata

\[ p \Rightarrow p \ast p \]  
(Contraction — unsound)

\[ \text{e.g. } p : x \mapsto 1 \]

\[ p \ast q \Rightarrow p \]  
(Weakening — unsound)

\[ \text{e.g. } p : x \mapsto 1 \]
\[ q : y \mapsto 2 \]
Some Axiom Schemata for $\mapsto$ 

$$e_1 \mapsto e'_1 \land e_2 \mapsto e'_2 \iff e_1 \mapsto e'_1 \land e_1 = e_2 \land e'_1 = e'_2$$

$$e_1 \mapsto e'_1 \ast e_2 \mapsto e'_2 \Rightarrow e_1 \neq e_2$$

$$\text{emp} \iff \forall x. \neg(x \mapsto -)$$

$$(e \mapsto e') \land p \Rightarrow (e \mapsto e') \ast ((e \mapsto e') \ast p).$$

(Regrettably, these are far from complete.)
Specifications

- \{p\} c \{q\} (partial correctness)

Starting in any state in which \( p \) holds:
- No execution of \( c \) aborts.
- When some execution of \( c \) terminates in a final state, then \( q \) holds in the final state.
\[ [p] \ c \ [q] \quad \text{(total correctness)} \]

Starting in any state in which \( p \) holds:

- No execution of \( c \) aborts.
- Every execution of \( c \) terminates.
- When some execution of \( c \) terminates in a final state, then \( q \) holds in the final state.
The Differences with Hoare Logic

- Specifications are universally quantified implicitly over both stores and heaps,
- Specifications are universally quantified implicitly over all possible executions.
- Any execution (starting in a state satisfying $p$) that gives a memory fault falsifies both partial and total specifications. Thus:

  - Well-specified programs don’t go wrong.
  — and memory-fault checking is unnecessary.
Enforcing Record Boundaries

The fact that specifications preclude memory faults acts in concert with the indeterminacy of allocation to prohibit violations of record boundaries. For example, in

\[ c_0 \cdot x := \text{cons}(1, 2) ; c_1 ; [x + 2] := 7, \]

no allocation performed by the subcommand \(c_0\) or \(c_1\) can be guaranteed to allocate the location \(x + 2\).

As long as \(c_0\) and \(c_1\) terminate and \(c_1\) does not modify \(x\), the above command may abort.

It follows that there is no postcondition that makes the specification

\[ \{\text{true}\} c_0 ; x := \text{cons}(1, 2) ; c_1 ; [x + 2] := 7 \{?\} \]

valid.

—
On the Other Hand (Gluing Records)

\[
\begin{align*}
\{ x & \mapsto - \ast y \mapsto - \} \\
\text{if } y &= x + 1 \text{ then skip else} \\
&\quad \text{if } x = y + 1 \text{ then } x := y \text{ else} \\
&\quad \quad (\text{dispose } x; \text{dispose } y; x := \text{cons}(1, 2)) \\
\{ x & \mapsto -, - \}. 
\end{align*}
\]
Hoare’s Inference Rules

The command-specific inference rules of Hoare logic remain sound, as do structural rules such as

- Strengthening Precedent

\[
\begin{array}{c}
p \Rightarrow q \\
\{q\} \hspace{1em} c \hspace{1em} \{r\}
\end{array}
\]

\[
\frac{}{\{p\} \hspace{1em} c \hspace{1em} \{r\}}.
\]

- Weakening Consequent

\[
\begin{array}{c}
\{p\} \hspace{1em} c \hspace{1em} \{q\}
\end{array}
\]

\[
q \Rightarrow r
\]

\[
\frac{}{\{p\} \hspace{1em} c \hspace{1em} \{r\}}.
\]
• Existential Quantification (Ghost Variable Elimination)

\[
\frac{\{p\} c \{q\}}{\exists v. \{p\} c \{\exists v. q\}},
\]
where \(v\) is not free in \(c\).

• Conjunction

\[
\frac{\{p\} c \{q_1\} \quad \{p\} c \{q_2\}}{\{p\} c \{q_1 \land q_2\}},
\]

• Substitution

\[
\frac{\{p\} c \{q\}}{\{p/\delta\} (c/\delta) \{q/\delta\}},
\]
where \(\delta\) is the substitution \(v_1 \rightarrow e_1, \ldots, v_n \rightarrow e_n, v_1, \ldots, v_n\) are the variables occurring free in \(p, c,\) or \(q\), and, if \(v_i\) is modified by \(c\), then \(e_i\) is a variable that does not occur free in any other \(e_j\).
The Failure of the Rule of Constancy

On the other hand,

- Rule of Constancy

\[
\frac{\{p\} \ c \ \{q\}}{\{p \land r\} \ c \ \{q \land r\}},
\]

where no variable occurring free in \( r \) is modified by \( c \).

is unsound, since, for example

\[
\{x \mapsto \neg\} \ [x] := 4 \ \{x \mapsto 4\}
\]

\[
\{x \mapsto \neg \land y \mapsto 3\} \ [x] := 4 \ \{x \mapsto 4 \land y \mapsto 3\}
\]

fails when \( x = y \).

—
The Frame Rule

Instead, we have the

- Frame Rule (O’Hearn)

\[
\frac{\{p\} \ c \ \{q\} \ \{p \ast r\} \ c \ \{q \ast r\},}

where no variable occurring free in \(r\) is modified by \(c\).

The frame rule is the key to “local reasoning” about the heap:

To understand how a program works, it should be possible for reasoning and specification to be confined to the cells that the program actually accesses. The value of any other cell will automatically remain unchanged. (O’Hearn)
Local Reasoning

- The set of variables and heap cells that may actually be used by a command (starting from a given state) is called its footprint.
- If \{p\} c \{q\} is valid, then \(p\) will assert that the heap contains all the cells in the footprint of \(c\) (excluding the cells that are freshly allocated by \(c\)).
- If \(p\) asserts that the heap contains only cells in the footprint of \(c\), then \{p\} c \{q\} is a local specification.
- If \(c'\) contains \(c\), it may have a larger footprint described, say, by \(p \ast r\). Then the frame rule is needed to move from \{p\} c \{q\} to \{p \ast r\} c \{q \ast r\}.
Inference Rules for Mutation

• Local

\[
\{ e \mapsto - \} [e] := e' \{ e \mapsto e' \}.
\]

• Global

\[
\{ (e \mapsto -) \ast r \} [e] := e' \{ (e \mapsto e') \ast r \}.
\]

• Backward Reasoning

\[
\{ (e \mapsto -) \ast ((e \mapsto e') \ast p) \} [e] := e' \{ p \}.
\]
Inference Rules for Deallocation

- Local

\[ \{ e \mapsto - \} \text{dispose } e \{ \text{emp} \} . \]

- Global, Backwards Reasoning

\[ \{(e \mapsto -) \star r\} \text{dispose } e \{r\} . \]
Inference Rules for Nonoverwriting Allocation

- **Local**

  \[
  \{\text{emp}\} \quad v := \text{cons}(\overline{e}) \quad \{v \mapsto \overline{e}\},
  \]

  where \( v \) is not free in \( \overline{e} \stackrel{\text{def}}{=} e_1, \ldots, e_n \).

- **Global**

  \[
  \{r\} \quad v := \text{cons}(\overline{e}) \quad \{(v \mapsto \overline{e}) \ast r\},
  \]

  where \( v \) is not free in \( \overline{e} \) or \( r \).

(We postpone more complex rules with quantifiers.)
An Example of an Annotated Specification: Gluing Records

\[
\begin{align*}
\{ x \mapsto - & \quad y \mapsto - \} \\
\text{if } y &= x + 1 \text{ then} & \{ x \mapsto - , - \} \\
& \quad \text{skip} \\
\text{else if } x &= y + 1 \text{ then} & \{ y \mapsto - , - \} \\
& \quad x \mathrel{:=} y \\
\text{else} & \left( \{ x \mapsto - \quad y \mapsto - \} \right) \\
& \quad \text{dispose } x ; \\
& \quad \{ y \mapsto - \} \\
& \quad \text{dispose } y ; \\
& \quad \{ \text{emp} \} \\
& \quad x \mathrel{:=} \text{cons}(1, 2) \right) \\
& \{ x \mapsto - , - \}. 
\end{align*}
\]
Another Example: Relative Pointers

\[
\begin{align*}
\{\text{emp}\} \\
x &:= \text{cons}(a, a) ; \\
\{x \mapsto a, a\} \\
y &:= \text{cons}(b, b) ; \\
\{(x \mapsto a, a) \ast (y \mapsto b, b)\} \\
\{(x \mapsto a, -) \ast (y \mapsto b, -)\} \\
[x + 1] &:= y - x ; \\
\{(x \mapsto a, y - x) \ast (y \mapsto b, -)\} \\
[y + 1] &:= x - y ; \\
\{(x \mapsto a, y - x) \ast (y \mapsto b, x - y)\} \\
\{\exists o. (x \mapsto a, o) \ast (x + o \mapsto b, -o)\}.
\end{align*}
\]
Singly-linked Lists

list $\alpha_i$:

$$i \quad \quad \quad \alpha_1 \quad \quad \quad \alpha_2 \quad \quad \quad \cdots \quad \quad \quad \alpha_n \quad \quad \quad \quad \quad \text{nil}$$

is defined by

$$\text{list } \epsilon_i \overset{\text{def}}{=} \text{emp} \land i = \text{nil}$$

$$\text{list } (a \cdot \alpha) i \overset{\text{def}}{=} \exists j. i \mapsto a, j * \text{list } \alpha_j,$$

where

- $\epsilon$ is the empty sequence.
- $\alpha \cdot \beta$ is the concatenation of $\alpha$ followed by $\beta$.

One can also derive an emptiness test:

$$\text{list } \alpha i \Rightarrow (i = \text{nil} \iff \alpha = \epsilon).$$
Reversing a List

\{\text{list } \alpha_0 \ i\}\{\text{list } \alpha_0 \ i \ast (\text{emp} \land \text{nil} = \text{nil})\}\n
j := \text{nil};\{\text{list } \alpha_0 \ i \ast (\text{emp} \land j = \text{nil})\}\{\text{list } \alpha_0 \ i \ast \text{list } \epsilon \ j\}\n
\{\exists \alpha, \beta. (\text{list } \alpha \ i \ast \text{list } \beta \ j) \land \alpha_0^\dagger = \alpha^\dagger \cdot \beta\}\n
\text{while } i \neq \text{nil} \text{ do}\n
\left(\{\exists a, \alpha, \beta. (\text{list } (a \cdot \alpha) \ i \ast \text{list } \beta \ j) \land \alpha_0^\dagger = (a \cdot \alpha)^\dagger \cdot \beta\}\{\exists a, \alpha, \beta, k. (i \mapsto a, k \ast \text{list } \alpha \ k \ast \text{list } \beta \ j) \land \alpha_0^\dagger = (a \cdot \alpha)^\dagger \cdot \beta\}\right)\n
k := [i + 1]\; ;\{\exists a, \alpha, \beta. (i \mapsto a, k \ast \text{list } \alpha \ k \ast \text{list } \beta \ j) \land \alpha_0^\dagger = (a \cdot \alpha)^\dagger \cdot \beta\}\n
[i + 1] := j;\{\exists a, \alpha, \beta. (i \mapsto a, j \ast \text{list } \alpha \ k \ast \text{list } \beta \ j) \land \alpha_0^\dagger = (a \cdot \alpha)^\dagger \cdot \beta\}\\{\exists a, \alpha, \beta. (\text{list } \alpha \ k \ast \text{list } (a \cdot \beta) \ i) \land \alpha_0^\dagger = \alpha^\dagger \cdot a \cdot \beta\}\\{\exists \alpha, \beta. (\text{list } \alpha \ k \ast \text{list } \beta \ i) \land \alpha_0^\dagger = \alpha^\dagger \cdot \beta\}\n
j := i; \ i := k\{\exists a, \alpha, \beta. (\text{list } \alpha \ i \ast \text{list } \beta \ j) \land \alpha_0^\dagger = \alpha^\dagger \cdot \beta\}\right)\{\exists a, \alpha. \text{list } \beta \ j \land \alpha_0^\dagger = \alpha^\dagger \cdot \beta \land \alpha = \epsilon\}\{\text{list } \alpha_0^\dagger \ j\}
S-expressions (à la LISP)

\[ \tau \in \text{S-exps} \text{ iff } \]

\[ \tau \in \text{Atoms} \]

or \( \tau = (\tau_1 \cdot \tau_2) \) where \( \tau_1, \tau_2 \in \text{S-exps} \).
For $\tau \in \text{S-exps}$, we define the assertion

$$\text{tree } \tau \ (i)$$

by structural induction:

$$\text{tree } a \ (i) \ \text{iff } \text{emp} \land i = a$$

$$\text{tree } (\tau_1 \cdot \tau_2) \ (i) \ \text{iff}$$

$$\exists i_1, i_2. \ i \mapsto i_1, i_2 \ast \text{tree } \tau_1 \ (i_1) \ast \text{tree } \tau_2 \ (i_2).$$
Representing S-expressions by Dags (with sharing)

For $\tau \in \text{S-exps}$, we define $\text{dag } \tau (i)$ by:

\[
\text{dag } a (i) \text{ iff } i = a
\]

\[
\text{dag } (\tau_1 \cdot \tau_2) (i) \text{ iff }
\exists i_1, i_2. \ i \mapsto i_1, i_2 \ast (\text{dag } \tau_1 (i_1) \land \text{dag } \tau_2 (i_2)).
\]
Array Allocation

\[
\langle \text{comm} \rangle ::= \cdots \mid \langle \text{var} \rangle ::= \text{allocate} \langle \text{exp} \rangle
\]

Store: x: 3, y: 4
Heap: empty

\[
x := \text{allocate } y
\]

\[
\downarrow
\]

Store: x: 37, y: 4
Heap: 37: −, 38: −, 39: −, 40: −
Iterated Separating Conjunction

\[ \langle \text{assert} \rangle ::= \cdots \mid \bigcirc_{\langle \text{var} \rangle = \langle \text{exp} \rangle} \langle \text{assert} \rangle \]

Let \( I \) be the contiguous set

\[ I = \{ v \mid e \leq v \leq e' \} \]

of integers between the values of \( e \) and \( e' \). Then \( \bigcirc_{v=e}^{e'} p(v) \) is true iff the heap can be partitioned into a family of disjoint sub-heaps, indexed by \( I \), such that \( p(v) \) is true for the \( v \)th subheap.
An Inference Rule

\[
\{r\} \; v := \text{allocate } e \; \{ (\bigodot_{i \equiv v}^{v+e-1} i \mapsto -) \ast r \},
\]

where \( v \) does not occur free in \( r \) or \( e \).
A Cyclic Buffer

We assume that an $n$-element array has been allocated at address $l$, e.g., by $l := \text{allocate } n$, and we use the variables

- $m$ number of active elements
- $i$ address of first active element
- $j$ address of first inactive element.

Then when the buffer contains a sequence $\alpha$, it should satisfy

$$0 \leq m \leq n \land l \leq i < l + n \land l \leq j < l + n \land$$
$$j = i \oplus m \land m = \#\alpha \land$$
$$(\bigcirc_{k=0}^{m-1} i \oplus k \mapsto \alpha_{k+1}) \ast (\bigcirc_{k=0}^{n-m-1} j \oplus k \mapsto -))$$

where $x \oplus y = x + y \mod n$, and $l \leq x \oplus y < l + n$. 

___
• We abandon address arithmetic, and require all records to contain two address fields and two boolean fields.
• Only reachable cells are in heap.
Let

\[ \text{allocated}(x) \overset{\text{def}}{=} x \leftrightarrow -, -, -, - \]
\[ \text{markedR} \overset{\text{def}}{=} \forall x. \text{allocated}(x) \Rightarrow x \leftrightarrow -, -, -, \text{true} \]
\[ \text{noDangling}(x) \overset{\text{def}}{=} (x = \text{nil}) \lor \text{allocated}(x) \]
\[ \text{noDanglingR} \overset{\text{def}}{=} \forall x, l, r. (x \leftrightarrow l, r, -, -) \Rightarrow \text{noDangling}(l) \land \text{noDangling}(r). \]

Then the invariant of the program is

\[ \text{noDanglingR} \land \text{noDangling}(t) \land \text{noDangling}(p) \land \]
\[ \left( \text{listMarkedNodesR}(\text{stack}, p) \ast \left( \text{restoredlistR}(\text{stack}, t) \rightarrow \text{spansR}(\text{STree}, \text{root}) \right) \right) \land \]
\[ \left( \text{markedR} \ast \left( \text{unmarkedR} \land \left( \forall x. \text{allocated}(x) \Rightarrow \right) \right) \right) \]
\[ \left( \text{reach}(t, x) \lor \text{reachRightChildInList}(\text{stack}, x) \right) \)}). \]
Proving Schorr-Waite (continued)

\[\text{noDanglingR} \land \text{noDangling}(t) \land \text{noDangling}(p) \land \]
\[
(\text{listMarkedNodesR}(\text{stack, p}) \ast \\
(\text{restoredListR}(\text{stack, t}) \rightarrow \text{spansR}(\text{STree, root}))) \land \\
(\text{markedR} \ast (\text{unmarkedR} \land (\forall x. \text{allocated}(x) \Rightarrow \\
(\text{reach}(t, x) \lor \text{reachRightChildInList}(\text{stack, x}))))))
\]

\text{restoredListR}(\text{stack, t}): \quad \text{listMarkedNodesR}(\text{stack, p}):
Shared-Variable Concurrency
(O’Hearn and Brookes)

Without Critical Regions

Hoare (1972):

\[
\begin{align*}
\{p_1\} & \ c_1 \ \{q_1\} \quad \{p_2\} \ c_2 \ \{q_2\} \\
\{p_1 \land p_2\} & \ c_1 \parallel c_2 \ \{q_1 \land q_2\},
\end{align*}
\]

when the free variables of \(p_1\), \(c_1\), and \(q_1\) are not modified by \(c_2\), and vice-versa.

O’Hearn (2002):

\[
\begin{align*}
\{p_1\} & \ c_1 \ \{q_1\} \quad \{p_2\} \ c_2 \ \{q_2\} \\
\{p_1 \ast p_2\} & \ c_1 \parallel c_2 \ \{q_1 \ast q_2\}
\end{align*}
\]

(with the same side condition as above).

—
With Critical Regions: A Simple Buffer

\{\text{emp}\}
\{\text{emp} \times \text{emp}\}

\{\text{emp}\}
\{\text{emp} \times \text{emp}\}

\{\text{emp}\}
\{\text{emp} \times \text{emp}\}

\{\text{emp}\}
\{\text{emp}\}

x := \text{cons}(\ldots, \ldots) ;
{x \mapsto -,-} \quad \| \quad \{y \mapsto -,-\}
\text{put}(x) ;
\{\text{emp}\}

\{\text{emp}\}
\{\text{emp}\}

\text{get}(y) ;
\{y \mapsto -,-\}
\text{"Use y" ;}
\{y \mapsto -,-\}
\text{dispose } y ;
\{\text{emp}\}

\{\text{emp}\}
\{\text{emp}\}

\text{Behind the scenes:}
\text{put}(x) = \text{with buf when } \neg \text{full do } (c := x ; \text{full} := \text{true})
\text{get}(y) = \text{with buf when full do } (y := c ; \text{full} := \text{false})
The Resource Invariant

\[ \mathbf{R} \overset{\text{def}}{=} (\mathsf{full} \land c \mapsto -, -) \lor (\neg \mathsf{full} \land \mathsf{emp}). \]

\[
\begin{align*}
\text{put}(x) &= \{ x \mapsto -, - \} \\
\text{with buf when } \neg \mathsf{full} \text{ do (} & \\
\{ (R \ast x \mapsto -, -) \land \neg \mathsf{full} \} \\
\{ \mathsf{emp} \ast x \mapsto -, - \} \\
\{ x \mapsto -, - \} \\
c := x ; \mathsf{full} := \text{true} \\
\{ \mathsf{full} \land c \mapsto -, - \} \\
\{ R \} \\
\{ R \ast \mathsf{emp} \} \\
\{ \mathsf{emp} \} \\
\end{align*}
\]

\[
\begin{align*}
\text{get}(y) &= \{ \mathsf{emp} \} \\
\text{with buf when } \mathsf{full} \text{ do (} & \\
\{ (R \ast \mathsf{emp}) \land \mathsf{full} \} \\
\{ c \mapsto -, - \ast \mathsf{emp} \} \\
\{ c \mapsto -, - \} \\
y := c ; \mathsf{full} := \text{false} \\
\{ \neg \mathsf{full} \land y \mapsto -, - \} \\
\{ (\neg \mathsf{full} \land \mathsf{emp}) \ast y \mapsto -, - \} \\
\{ R \ast y \mapsto -, - \} \\
\{ y \mapsto -, - \} \\
\end{align*}
\]
The Overall Program

\[
\{ R \ast \text{emp} \}\n\]

resource \text{buf} in

\[
\{ \text{emp} \}\n\]

\[
\{ \text{emp} \ast \text{emp} \}\n\]

\[
: \quad \| \quad : \n\]

\[
\{ \text{emp} \ast \text{emp} \}\n\]

\[
\{ \text{emp} \}\n\]

\[
\{ R \ast \text{emp} \}\n\]
Fractional Permissions (Bornat, following Boyland)

We write \( e \mapsto e' \), where \( z \) is a real number such that \( 0 < z \leq 1 \), to assert \( e \) points to \( e' \) with permission \( z \).

- \( e \xrightarrow{1} e' \) is the same as \( e \mapsto e' \), so that a permission of one allows all operations.
- Only lookup is allowed when \( z < 1 \).

Then

\[
e \xrightarrow{z} e' \ \ast \ \ e \xrightarrow{z'} e' \ \text{iff} \ e \xrightarrow{z+z'} e'
\]

and

\[
\{ \text{emp} \} v := \text{cons}(e_1, \ldots, e_n)\{ e \xrightarrow{1} e_1, \ldots, e_n \}
\]

\[
\{ e \xrightarrow{1} - \} \text{dispose}(e)\{ \text{emp} \}
\]

\[
\{ e \xrightarrow{1} - \}[e] := e'\{ e \xrightarrow{1} e' \}
\]

\[
\{ e \xrightarrow{z} e' \} v := [e]\{ e \xrightarrow{z} e' \land v = e' \}
\]

(with appropriate restrictions on variable occurrences).

---