Software Verification (Fall 2013)  
Lecture 5: Separation Logic  
Parts I - II

Chris Poskitt
A recent separation logic success story

Facebook buys code-checking Silicon Roundabout startup Monoidics

Acquisition of company which carries out tests to find crashing bugs will see its technology applied to mobile apps and site

Facebook buys UK startup Monoidics

Facebook has acquired assets behind Monoidics, a London-based startup whose technology is used to detect coding errors.
Main sources for these lectures

Peter W. O’Hearn:

A primer on separation logic
(and automatic program verification and analysis)

Main sources for these lectures

Peter W. O'Hearn, John C. Reynolds, Hongseok Yang

Local Reasoning about Programs that Alter Data Structures

What is separation logic for?

- for reasoning about shared mutable data structures in imperative programs
  - structures where an updatable field can be referenced from more than one point
  - correctness of such programs depends upon complex restrictions on sharing
  - classical methods like Hoare logic suffer from extreme complexity; reasoning does not match programmers’ intuitions
Some shared mutable data structures
Problem illustration
(from O’Hearn)

• the following program disposes the elements of a tree

```
procedure DispTree(p)
local i, j;
if ¬isatom?(p) then
  i := p→l;
  j := p→r;
  DispTree(i)
  DispTree(j)
  dispose(p)
```

• can we prove its correctness using classical Hoare logic?
Problem illustration: Hoare logic

- here is a possible specification:

\[
\{ \text{tree}(p) \land \text{reach}(p,n) \} \\
\text{DispTree}(p) \\
\{ \neg \text{allocated}(n) \}
\]

i.e. if before execution there is a node \( n \) in the tree that \( p \) points to, then after execution, \( n \) is not allocated

\( \text{have we specified enough?} \)
Problem illustration: Hoare logic

- what does DispTree(p) do to nodes outside of the tree p?

```
procedure DispTree(p)
local i, j;
if ¬isatom?(p) then
  i := p→l;
  j := p→r;
  DispTree(i);
  DispTree(j);
  dispose(p)
```

specification too weak! does not rule out that DispTree(i) did not alter subtree j...
...might no longer be a tree! (precondition violation)

\{ tree(i) ∧ reach(i,n) \}
DispTree(i)
\{ ¬allocated(n) \}
Problem illustration: Hoare logic

• can strengthen the specification with frame axioms
  i.e. clauses specifying what does not change

\[
\begin{align*}
\{ & \text{tree}(p) \land \text{reach}(p,n) \land \neg \text{reach}(p,m) \land \text{allocated}(m) \land m.f = m' \land \neg \text{allocated}(q) \} \\
\text{DispTree}(p) & \\
\{ & \neg \text{allocated}(n) \land \neg \text{reach}(p,m) \land \text{allocated}(m) \land m.f = m' \land \neg \text{allocated}(q) \} 
\end{align*}
\]

• complicated; certainly does not scale!

• does not match the intuition that programmers use
How does separation logic help?

• separation logic extends Hoare logic to facilitate local reasoning

• assertion language offers spatial connectives, allowing one to reason about smaller parts of the program state

• this locality allows us to:
  - avoid mentioning the frame in specifications
  - but to bring the frame condition in when needed

\[ p \ast q \]
Next on the agenda

(1) model of program states for separation logic

(2) assertions and spatial connectives

(3) axioms and inference rules

(4) program proofs
Recap: program states

• in Hoare logic a program state comprises a variable store

i.e. a partial function mapping variables to integers
Recap: program states

- in Hoare logic a program state comprises a variable store

i.e. a partial function mapping variables to integers

\[ s(x) = 0 \]
\[ s(y) = 0 \]
\[ s(z) = 3 \]

\[ s : \begin{array}{c}
  x & \rightarrow & 0 \\
  y & \rightarrow & -1 \\
  z & \rightarrow & 3 \\
\end{array} \]
Recap: satisfaction of assertions

• we write $s \models p$ if store $s$ (i.e. a program state) satisfies assertion $p$

• typically $\models$ is defined inductively

\[
\begin{align*}
  s \models p \land q & \text{ if } s \models p \text{ and } s \models q \\
  s \models \exists x. \ p & \text{ if there exists some integer } v \text{ such that } s[x \mapsto v] \models p \\
  & \vdots \\
  s \models B & \text{ if } [\|B\|]_s = \text{true}
\end{align*}
\]

(where $[\|B\|]_s$ denotes the evaluation of $B$ w.r.t. $s$)
Recap: satisfaction of assertions

• For example:

\[(x \mapsto 5, y \mapsto 10) \models x < y \land x > 0\]

\[(x \mapsto 25) \models \exists y. y > x\]

\[(x \mapsto 0) \not\models \exists y. y < x \land y \geq 0\]
The Heaplet model

• in separation logic, program states comprise both a variable store and a heap

i.e. a function mapping locations (pointers) to integers

we define locations as a subset of the integers
The Heaplet model

- in separation logic, program states comprise both a variable store and a heap

i.e. a function mapping locations (pointers) to integers

\[ h : \begin{array}{c} 1 \\ 3 \\ 5 \end{array} \rightarrow \begin{array}{c} 25 \\ 0 \\ -56 \end{array} \]

we define locations as a subset of the integers
The Heaplet model

- the **store**: state of the local variables

  Variables $\rightarrow$ Integers

- the **heap**: state of dynamically-allocated objects

  Locations $\rightarrow$ Integers

where: Locations $\subseteq$ Integers
Example store and heap
Next on the agenda

(1) model of program states for separation logic

(2) assertions and spatial connectives

(3) axioms and inference rules

(4) program proofs
Syntax of assertions

false  logical false
$p \land q$  classical conjunction
$p \lor q$  classical disjunction
$p \Rightarrow q$  classical implication
$p \star q$  separating conjunction
$p \leftarrow q$  separating implication
$e = f$  equality of expressions
$e \mapsto f$  points to (in the heap)
emp  empty heap
$\exists x. \ p$  existential quantifier

(e,f range over integer expressions; x over variables; p,q over assertions)
Semantics of assertions

• we write $s,h \models p$ if store $s$ and heap $h$ (together the program state) satisfies assertion $p$

\[
\begin{align*}
  &s, h \models \text{false} \quad \text{never} \\
  &s, h \models p \land q \quad \text{if} \quad s, h \models p \quad \text{and} \quad s, h \models q \\
  &s, h \models p \lor q \quad \text{if} \quad s, h \models p \quad \text{or} \quad s, h \models q \\
  &s, h \models p \Rightarrow q \quad \text{if} \quad s, h \models p \implies s, h \models q \\
  &s, h \models e = f \quad \text{if} \quad \llbracket e \rrbracket_s = \llbracket f \rrbracket_s
\end{align*}
\]

(where $\llbracket e \rrbracket_s$ denotes the evaluation of $e$ with respect to $s$)
Semantics of empty heap

- the semantics of the remaining assertions all rely on the heap $h$

$$s, h \models \text{emp} \quad \text{if} \quad h = \{\}$$
Semantics of points to

\[ s, h \models e \mapsto f \quad \text{if} \quad h = \{ [[ e ] ] s \to [[ f ] ] s \} \]

The heap \( h \) has exactly one location: the value of \( e \)...
...and the contents at that location is the value of \( f \)

What about larger heaps?
Example of points to

Store

Heap

\(x\)

7
Example of points to

\[ x \rightarrow 7 \]
Semantics of separating conjunction

\[ s, h \models p \land q \]

- informally: the heap \( h \) can be divided in two so that \( p \) is true of one partition and \( q \) of the other
Semantics of separating conjunction

\[ s, h \models p \ast q \]

• informally: the heap \( h \) can be \textit{divided} in two so that
\( p \) is true of one partition and \( q \) of the other

\[
s, h \models p \ast q \quad \text{if} \quad \exists h_1, h_2. \ (h_1 \perp h_2), \ (h_1 \circ h_2 = h), \quad s, h_1 \models p \quad \text{and} \quad s, h_2 \models q
\]
Example of separating conjunction
Example of separating conjunction

\[ x \leftarrow 5 \times 5 \leftarrow z \times z \leftarrow 10 \]
Example of separating conjunction
(from Calcagno)
Example of separating conjunction
(from Calcagno)

\[
\text{emp} \times x \rightarrow y \times y \rightarrow z \times z \rightarrow x
\]
Notation

let $e \mapsto f_0, \ldots, f_n$

abbreviate $e \mapsto f_0 \ast e + 1 \mapsto f_1 \ast \cdots \ast e + n \mapsto f_n$
Notation

let \( e \mapsto f_0, \ldots, f_n \)

abbreviate \( e \mapsto f_0 \cdot e + 1 \mapsto f_1 \cdot \cdots \cdot e + n \mapsto f_n \)
Notation

let $e \mapsto f_0, \ldots, f_n$

abbreviate $e \mapsto f_0 \cdot e + 1 \mapsto f_1 \cdot \cdots \cdot e + n \mapsto f_n$

\[\begin{array}{c}
\text{Store} \\
x \\
y
\end{array}\] \quad \begin{array}{c}
\text{Heap} \\
\{4, 5\} \\
\{2, 3, 4\}
\end{array}\]

\[
x \mapsto 4, 5 \cdot y \mapsto 2, 3, 4
\]

\[
x \mapsto 4, 5 \cdot \text{true}
\]
Exercises
(from Parkinson)

A:

Store

\( x \)

\( y \)

Heap

\( 4 \mid 4 \)

\( 4 \mid 4 \)

B:

Store

\( x \)

\( y \)

Heap

\( 4 \mid 4 \)

\( 4 \mid 4 \)

---

\( x \mapsto 4, 4 \)

\( x \mapsto 4, 4 \ast \text{true} \)

\( x \mapsto 4, 4 \ast y \mapsto 4, 4 \)

\( x \mapsto 4, 4 \land y \mapsto 4, 4 \)

\( (x \mapsto 4, 4 \ast \text{true}) \land (y \mapsto 4, 4 \ast \text{true}) \)
Exercises
(from Parkinson)

A:

Store

\( x \)

\( y \)

Heap

\( 4 \quad 4 \)

\( 4 \quad 4 \)

B:

Store

\( x \)

\( y \)

Heap

\( 4 \quad 4 \)

\( 4 \quad 4 \)

\( x \mapsto 4, 4 \)

\( x \mapsto 4, 4 \land y \mapsto 4, 4 \)

\( y \mapsto 4, 4 \land \text{true} \)

\( x \mapsto 4, 4 \land y \mapsto 4, 4 \land (x \mapsto 4, 4 \land y \mapsto 4, 4 \land (y \mapsto 4, 4 \land \text{true})) \)

A | B
---|---
X | ✓
Exercises
(from Parkinson)

A:

<table>
<thead>
<tr>
<th>Store</th>
<th>Heap</th>
</tr>
</thead>
<tbody>
<tr>
<td>x</td>
<td>4 4</td>
</tr>
<tr>
<td>y</td>
<td>4 4</td>
</tr>
</tbody>
</table>

B:

<table>
<thead>
<tr>
<th>Store</th>
<th>Heap</th>
</tr>
</thead>
<tbody>
<tr>
<td>x</td>
<td>4 4</td>
</tr>
<tr>
<td>y</td>
<td>4 4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>x → 4, 4</td>
<td>✓</td>
</tr>
<tr>
<td>x → 4, 4 * true</td>
<td>✓</td>
</tr>
<tr>
<td>x → 4, 4 * y → 4, 4</td>
<td>✓</td>
</tr>
<tr>
<td>x → 4, 4 ∧ y → 4, 4</td>
<td>✓</td>
</tr>
<tr>
<td>(x → 4, 4 * true) ∧ (y → 4, 4 * true)</td>
<td>✓</td>
</tr>
</tbody>
</table>
Exercises
(from Parkinson)

A:

\[
\begin{array}{c}
\text{Store} \\
x \\
y
\end{array}
\begin{array}{c}
\text{Heap} \\
4 \quad 4
\end{array}
\]

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x \mapsto 4, 4 )</td>
<td>X ✔</td>
</tr>
<tr>
<td>( x \mapsto 4, 4 \land y \mapsto 4, 4 )</td>
<td>✔ X</td>
</tr>
</tbody>
</table>

B:

\[
\begin{array}{c}
\text{Store} \\
x \\
y
\end{array}
\begin{array}{c}
\text{Heap} \\
4 \quad 4
\end{array}
\]

\( (x \mapsto 4, 4 \land y \mapsto 4, 4) \land (y \mapsto 4, 4 \land true) \)
Exercises
(from Parkinson)

A:

\[
\begin{array}{c}
\text{Store} \\
x \quad y
\end{array} \quad \begin{array}{c}
\text{Heap} \\
4 \quad 4 \quad 4 \quad 4
\end{array}
\]

\[
\begin{array}{c}
\text{A} \\
x \mapsto 4, 4
\end{array}
\]
\[
\begin{array}{c}
\text{B} \\
x \mapsto 4, 4 \ast \text{true}
\end{array}
\]

\[
\begin{array}{c}
\text{A} \\
x \mapsto 4, 4 \ast y \mapsto 4, 4
\end{array}
\]
\[
\begin{array}{c}
\text{B} \\
x \mapsto 4, 4 \land y \mapsto 4, 4
\end{array}
\]

\[
\begin{array}{c}
\text{A} \\
(x \mapsto 4, 4 \ast \text{true}) \\
\land (y \mapsto 4, 4 \ast \text{true})
\end{array}
\]
Exercises
(from Parkinson)

A:

\[
\begin{array}{c|c}
\text{Store} & \text{Heap} \\
\hline
x & 4 \ 4 \\
\hline
y & 4 \ 4 \\
\end{array}
\]

B:

\[
\begin{array}{c|c}
\text{Store} & \text{Heap} \\
\hline
x & 4 \ 4 \\
\hline
y & 4 \ 4 \\
\end{array}
\]

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>(x \mapsto 4, 4)</td>
<td>(x \mapsto 4, 4 \land y \mapsto 4, 4)</td>
</tr>
<tr>
<td>(x \mapsto 4, 4 \land y \mapsto 4, 4)</td>
<td>(x \mapsto 4, 4 \land y \mapsto 4, 4)</td>
</tr>
</tbody>
</table>
Semantics of separating implication

\[ s, h \models p \rightarrow^* q \]

- \textit{aka the magic wand}
- \textit{informally: asserts that extending} \( h \) \textit{with a disjoint part} \( h' \) \textit{that satisfies} \( p \) \textit{results in a new heap satisfying} \( q \)
- \textit{metatheoretic uses}, e.g. proving completeness results
∧ versus ∗
(from Parkinson)

Similarities

\[ p \land q \text{ iff } q \land p \]
\[ p \land \text{true} \text{ iff } p \]
\[ p \land (p \Rightarrow q) \text{ implies } q \]
\[ p \ast q \text{ iff } q \ast p \]
\[ p \ast \text{emp} \text{ iff } p \]
\[ p \ast (p \ast \ast q) \text{ implies } q \]

Differences

\[ p \text{ implies } p \land p \]
\[ p \land p \text{ implies } p \]
\[ \text{one does not imply } \text{one} \ast \text{one} \]
\[ \text{one} \ast \text{one} \text{ does not imply } \text{one} \]

where one is defined by: \[ \exists x, y. x \mapsto y \]
Unsatisfiable...?

\[ p \land \neg p \quad \text{and} \quad p \ast \neg p \]
Unsatisfiable...?

\[ p \land \neg p \]

\[ p \ast \neg p \]

“to understand separation logic assertions you should always think locally”
Next on the agenda

(1) model of program states for separation logic

(2) assertions and spatial connectives

(3) axioms and inference rules

(4) program proofs
Some program constructs for pointers

\[ v := e \] variable assignment
\[ v := [e] \] fetch assignment
\[ [e] := f \] heap assignment
\[ v := \text{cons}(e_1, \ldots, e_n) \] allocation assignment
\[ \text{dispose}(e) \] pointer disposal
Some program constructs for pointers

\[ v := e \quad \text{variable assignment} \]

\[ v := [e] \quad \text{fetch assignment} \]

- evaluate \( e \) (with respect to store) to get a location \( l \)
- fault if \( l \) is not in the heap
- otherwise assign contents of \( l \) in heap to variable \( v \)
Some program constructs for pointers

\[ v := e \quad \text{variable assignment} \]

\[ [e] := f \quad \text{heap assignment} \]

- evaluate e (with respect to store) to get a location l
- fault if l is not in the heap
- otherwise assign value of f as contents of l in the heap
Some program constructs for pointers

\[ v := e \] variable assignment

- choose \( n \) consecutive locations not in the heap
- say \( l, l+1, \ldots \)
- extend the heap by adding \( l, l+1, \ldots \) to it
- assign \( l \) to variable \( v \) in the store
- assign values of \( e_1, \ldots, e_n \) to contents of \( l, l+1, \ldots \)

\[ v := \text{cons}(e_1, \ldots, e_n) \] allocation assignment
Some program constructs for pointers

\[ v := e \quad \text{variable assignment} \]

- evaluate \( e \) (with respect to store) to get a location \( l \)
- fault if \( l \) is not in the heap
- otherwise \text{remove } l \text{ from the heap}

\text{dispose}(e) \quad \text{pointer disposal}
Some program constructs for pointers

\[ v := e \] variable assignment

\[ v := [e] \] fetch assignment

\[ [e] := f \] heap assignment

\[ v := \text{cons}(e_1, \ldots, e_n) \] allocation assignment

\text{dispose}(e) \] pointer disposal
Example program
(from Parkinson)

\[
x := \text{cons}(3,3);
y := \text{cons}(4,4);
[x+1] := y;
[y+1] := x;
y := x + 1;
dispose x;
y := [y];
\]
\begin{align*}
x &:= \text{cons}(3,3); \\
y &:= \text{cons}(4,4); \\
[x+1] &:= y; \\
[y+1] &:= x; \\
y &:= x+1; \\
\text{dispose } x; \\
y &:= [y];
\end{align*}
Example program
(from Parkinson)

\[
x := \text{cons}(3,3);
\]
\[
y := \text{cons}(4,4);
\]
\[
[x+1] := y;
\]
\[
[y+1] := x;
\]
\[
y := x+1;
\]
\[
dispose x;
\]
\[
y := [y];
\]
Example program
(from Parkinson)

\[
x := \text{cons}(3,3);
y := \text{cons}(4,4);
[x+1] := y;
[y+1] := x;
y := x+1;
dispose x;
y := [y];
\]
Example program
(from Parkinson)

\[
x := \text{cons}(3,3);
y := \text{cons}(4,4);
[x+1] := y;
[y+1] := x;
y := x+1;
dispose x;
y := [y];
\]
x := cons(3,3);
y := cons(4,4);
[x+1] := y;
[y+1] := x;
y := x+1;
dispose x;
y := [y];
Example program
(from Parkinson)

\[
\begin{align*}
x & := \text{cons}(3,3); \\
y & := \text{cons}(4,4); \\
[x+1] & := y; \\
[y+1] & := x; \\
y & := x+1; \\
dispose x; \\
y & := [y];
\end{align*}
\]
Example program
(from Parkinson)

x := cons(3,3);
y := cons(4,4);
[x+1] := y;
[y+1] := x;
y := x+1;
dispose x;
y := [y];
New axioms for separation logic

\[
\{ e \mapsto _* \} \ [e] := f \ \{ e \mapsto f \} \\
\{ e \mapsto _* \} \ \text{dispose}(e) \ \{ \text{emp} \}
\]

\[
\{ X = x \land e \mapsto Y \} \ x := [e] \ \{ e[X/x] \mapsto Y \land Y = x \}
\]

\[
\{ \text{emp} \} \ x := \text{cons}(e_0, \ldots, e_n) \ \{ x \mapsto e_0, \ldots, e_n \}
\]

(where \( e \mapsto _* \) means “the location given by the evaluation of \( e \) points to something”)
Recall the problem in verifying this program:

\[
\text{procedure } \text{DispTree}(p) \\
\text{local } i, j; \\
\text{if } \neg \text{isatom?}(p) \text{ then} \\
\quad i := p \rightarrow l; \\
\quad j := p \rightarrow r; \\
\quad \text{DispTree}(i) \\
\quad \text{DispTree}(j) \\
\quad \text{dispose}(p)
\]

\[
\{ \text{tree}(p) \land \text{reach}(p,n) \land \neg \text{reach}(p,m) \land \text{allocated}(m) \\
\land m.f = m' \land \neg \text{allocated}(q) \} 
\]

\[
\text{DispTree}(p) \\
\{ \neg \text{allocated}(n) \land \neg \text{reach}(p,m) \land \text{allocated}(m) \\
\land m.f = m' \land \neg \text{allocated}(q) \}
\]

Framing!
The frame rule
(the most important rule!)

\[
\begin{array}{c}
\{p\} \quad C \quad \{q\} \\
\{p \ast r\} \quad C \quad \{q \ast r\}
\end{array}
\]

• side condition: no variable modified by C appears free in r

• enables local reasoning: programs that execute correctly in a small state (\(\models p\)) also execute correctly in a bigger state (\(\models p \ast r\))
Warning: interpretation of triples!

- interpretation of triples slightly stronger in separation logic than partial correctness

\[ \models \{p\} \ C \ \{q\} \]

- “if \( C \) is executed on a state satisfying \( p \), then it will not fault, and if it terminates, that state will satisfy \( q \)”
Why no faulting?

- if we don’t insist that programs do not fault, then strange “proofs” like the following will be possible:

\[
\begin{align*}
\{\text{true}\} & \quad [x] := 7 & \{\text{true}\} \\
\{\text{true} \ast x \rightarrow 4\} & \quad [x] := 7 & \{\text{true} \ast x \rightarrow 4\}
\end{align*}
\]
Next on the agenda

(1) model of program states for separation logic
(2) assertions and spatial connectives
(3) axioms and inference rules
(4) program proofs
Exercise (for next time): prove this!

{x := cons(3,3);
y := cons(4,4);
[x+1] := y;
[y+1] := x;
y := x+1;
dispose x;
y := [y];
{y|->4 * true}
Exercise (for next time): prove this!

{x := cons(3,3);
y := cons(4,4);
[x+1] := y;
[y+1] := x;
y := x+1;
dispose x;
y := [y];
{y|->4 * true}

- the frame rule is crucial!
- reason forwards
  e.g. use the “forward” assignment axiom
- try a proof outline (proof trees too large)
Summary

• separation logic is an extension of Hoare logic for shared mutable data structures

• program states are now modelled by variable stores and heaps

• spatial connectives allow assertions to focus on resources used by programs

• frame rule enables local reasoning
Thank you! Questions?

Next lecture:

• writing proofs in separation logic
• inductive definitions in assertions