Separation Logic in the Presence of Garbage Collection

Chung-Kil Hur    Derek Dreyer    Viktor Vafeiadis

Max Planck Institute for Software Systems (MPI-SWS)
Kaiserslautern and Saarbrücken, Germany

LICS 2011
Toronto, Canada
Separation Logic =
Hoare Logic

\{ P \} \ C \ \{ Q \}

\iff \forall s, h \text{ such that } s, h \models P,
1. $C, s, h \leadsto^* \text{skip, } s', h'$
   then $s', h' \models Q$

\begin{itemize}
    \item Separating Conjunction \textbf{“*”}
\end{itemize}

$s, h \models P * Q$

\iff \exists h_1, h_2. h = h_1 \uplus h_2 \land s, h_1 \models P \land s, h_2 \models Q$
Frame rule

\[
\frac{\{P\} \ C \ \{Q\}}{\{P \ast R\} \ C \ \{Q \ast R\}} \quad FV(R) \cap \text{Mod}(C) = \emptyset
\]
Two main settings of separation logic

Low-level languages with manual memory management:
- *e.g.*, C with `malloc()`, `free()`

High-level languages with automatic memory management:
- *e.g.*, Java, ML
- Garbage collection not observable in operational semantics
Our focus: Low-level languages with garbage collection

Want to support local reasoning about low-level programs that interface to a garbage collector (GC)

- *e.g.*, the output of a compiler for a garbage-collected language, linked with some hand-coded assembly

Want to allow programs to violate the GC’s invariants in between calls to the memory allocator

- *e.g.*, creating dangling pointers, performing address arithmetic

Informal local reasoning principles clearly exist, so we should be able to codify them in separation logic!

- Only work on the topic: [Calcagno, O’Hearn, & Bornat 2003] and [McCreight, Shao, Lin & Li 2007]
Motivating example: Array initialization

\[
\begin{align*}
x & := \text{ALLOC}(n); \\
t & := x + 4 \cdot n; \\
\text{while } x < t \text{ do} \\
& \quad [x] := 0; \\
& \quad x := x + 4 \\
\text{od}; \\
x & := x - 4 \cdot n; \\
t & := 0
\end{align*}
\]
Motivating example: Array initialization

```
GC safe →
  x := ALLOC(n);
  t := x + 4n;
  while x < t do
    [x] := 0;
    x := x + 4
  od;
  x := x - 4n;
  t := 0
```

GC unsafe →

```
Key Challenges

\{P\} GC() \{P\}

- Want to give a clean specification for the GC, essentially viewing it as equivalent to skip

The frame rule

- Soundness somewhat subtle due to lack of “heap locality”
High-level ideas
Problem 1: Unreachable blocks may be reclaimed

Conundrum due to [Reynolds 2000]:

\[
\{ \text{true} \} \\
x := \text{new}(); \ [x] := 5; \ x := \text{null}; \\
\{ x = \text{null} \land \exists \ell. \ell \mapsto 5 \}
\]
Problem 1: Unreachable blocks may be reclaimed

Conundrum due to [Reynolds 2000]:

\[
\begin{aligned}
\{ & \text{true} \} \\
x & := \text{new()}; \quad [x] := 5; \quad x := \text{null}; \\
\{ & x = \text{null} \land \exists \ell. \ell \hookrightarrow 5 \} \\
\text{GC()} \\
\{ & x = \text{null} \land \exists \ell. \ell \hookrightarrow 5 \}
\end{aligned}
\]
Problem 1: Unreachable blocks may be reclaimed

Conundrum due to [Reynolds 2000]:

\[
\{ \text{true} \} \\
x := \text{new}(); \ [x] := 5; \ x := \text{null}; \\
\{ x = \text{null} \land \exists \ell. \ \ell \rightarrow 5 \} \\
\text{GC}() \\
\{ x = \text{null} \land \exists \ell. \ \ell \rightarrow 5 \}
\]

Approach by [Calcagno et al. 2003]: Impose “monster-barring” syntactic restriction on assertions \( P \).
This triple is easy to validate, even if the GC relocates $x$:

$$\{ x \mapsto 7 \} \quad \text{GC()} \quad \{ x \mapsto 7 \}$$
This triple is hard to validate, because the GC could move $l$:

$\{x \leftarrow l \land l \leftarrow 7\}$  \hspace{1cm} GC()  \hspace{1cm} $\{x \leftarrow l \land l \leftarrow 7\}$
Problem 2: Pointers can be relocated

This triple is hard to validate, because the GC could move $\ell$:

\[
\{ x \leftrightarrow \ell \ast \ell \leftrightarrow 7 \} \quad \text{GC()} \quad \{ x \leftrightarrow \ell' \ast \ell' \leftrightarrow 7 \}
\]
Problem 2: Pointers can be relocated

This triple is hard to validate, because the GC could move $\ell$:

$$\{x \leftarrow \ell \ast \ell \leftarrow 7\} \quad \text{GC()} \quad \{x \leftarrow \ell' \ast \ell' \leftarrow 7\}$$

One approach: Avoid logical variables like $\ell$, and use auxiliary program variables instead.
Problem 2: Pointers can be relocated

This triple is hard to validate, because the GC could move $\ell$:

$$\{x \mapsto \ell * \ell \mapsto 7\} \quad \text{GC}() \quad \{x \mapsto \ell' * \ell' \mapsto 7\}$$

One approach: Avoid logical variables like $\ell$, and use auxiliary program variables instead

- But we would prefer to use logical variables
- Worse, auxiliary variables may affect the reachability of data
**Logical memory (adapted from [McCreight et al. 2007])**

\[ LM \overset{iso}{\sim} M: \text{ isomorphism between reachable blocks of } LM \text{ and } M \]

\[
\begin{array}{c}
   \text{LM} \\
   \overset{iso}{\sim} \\
   \text{M} \rightarrow \text{GC} \rightarrow \text{M}'
\end{array}
\]
Logical memory (adapted from [McCreight et al. 2007])

\[ LM \overset{\text{iso}}{\sim} M: \text{ isomorphism between reachable blocks of } LM \text{ and } M \]

\[ \ell \leftrightarrow 5 \]

\[ 0x80 \leftrightarrow 5 \]

\[ \{ \text{true} \} \]

\[ x := \text{new()}; \ [x] := 5; \ x := \text{null}; \]

\[ \{ x = \text{null} \land \exists \ell. \ell \leftrightarrow 5 \} \]
**Logical memory (adapted from [McCreight et al. 2007])**

$LM \xrightarrow{iso} M$: isomorphism between reachable blocks of $LM$ and $M$

\[
\begin{align*}
\ell & \mapsto 5 \\
0x80 & \mapsto 5 \\
\{true\} & \\
\end{align*}
\]

\[
\begin{align*}
x := \text{new}(); & \quad [x] := 5; & \quad x := \text{null}; \\
\{x = \text{null} \land \exists \ell. \ell \mapsto 5\} & \\
\text{GC()} & \\
\{x = \text{null} \land \exists \ell. \ell \mapsto 5\} & \\
\end{align*}
\]
Logical memory (adapted from [McCreight et al. 2007])

$$LM \overset{iso}{\sim} M: \text{isomorphism between reachable blocks of } LM \text{ and } M$$

$x \leftrightarrow \ell \ast \ell \leftrightarrow 7$

$\{x \leftrightarrow \ell \ast \ell \leftrightarrow 7\}$
Logical memory (adapted from [McCreight et al. 2007])

$LM \cong M$: isomorphism between reachable blocks of $LM$ and $M$

$x \leftarrow \ell \cdot \ell \rightarrow 7$

$LM$

$x \leftarrow \ell \cdot \ell \rightarrow 7$

$x \leftarrow 0x40 \cdot 0x40 \rightarrow 7$

$M \xrightarrow{GC} M'$

$x \leftarrow 0x60 \cdot 0x60 \rightarrow 7$

$\{x \leftarrow \ell \cdot \ell \rightarrow 7\} \quad GC() \quad \{x \leftarrow \ell \cdot \ell \rightarrow 7\}$
Semantics of Hoare triples with logical memories

\[
\{\{ P \}\} \ C \ \{\{ Q \}\}
\]

\[ \iff \forall M, LM \text{ such that } LM \models P \land LM \overset{\text{iso}}{\sim} M \]

1. C, M does not get stuck
2. if C, M \overset{*}{\Rightarrow} \text{skip}, M'
   then \exists LM'. LM' \models Q \land LM' \overset{\text{iiso}}{\sim} M'

But in order to guarantee \{\{ P \}\} \text{GC()} \{\{ P \}\}, we need to ensure that we only invoke the GC under GC-safe memories.

C.-K. Hur, D. Dreyer, V. Vafeiadis

Separation Logic in the Presence of Garbage Collection
Semantics of Hoare triples with logical memories

\[\{\{ P \}\} \ C \ \{\{ Q \}\}\]

\[\iff \forall M, LM \text{ such that } LM \models P \land LM \overset{\text{iso}}{\sim} M\]

1. \(C, M\) does not get stuck
2. if \(C, M \overset{*}{\Rightarrow} \text{skip}, M'\)
   then \(\exists LM'. LM' \models Q \land LM' \overset{\text{iso}}{\sim} M'\)

But in order to guarantee \(\{\{ P \}\} \ GC() \ \{\{ P \}\}\), we need to ensure that we only invoke the GC under GC-safe memories.
Semantics of Hoare triples with logical memories

\[ \{\{ P \} \} \ C \ \{\{ Q \} \} \]
\[ \iff \forall M, LM \text{ such that } LM \models P \land LM \iso M \land LM \text{ safe} \]
1. \( C, M \) does not get stuck
2. if \( C, M \leadsto^* \text{ skip, } M' \)
   \[ \exists LM'. LM' \models Q \land LM' \iso M' \land LM' \text{ safe} \]

But in order to guarantee \( \{\{ P \} \} \ GC() \ \{\{ P \} \} \), we need to ensure that we only invoke the GC under GC-safe memories.
\( LM = (s, h) \)

\( v \text{ safe} : v \) is either a non-pointer word 
or a pointer to the head of an allocated block.

\( s \text{ safe} : \) all program variables in \( s \) contain safe values.

\( h \text{ safe} : \) all reachable blocks in \( h \) contain safe values.

\( LM \text{ safe} : LM.s \text{ safe} \land LM.h \text{ safe}. \)
Semantics of Hoare triples with logical memories

$$\{\{ P \} \} \ C \ \{\{ Q \} \}$$

$$\iff \forall M, LM\text{ such that } LM \models P \land LM \overset{\text{iso}}{\sim} M \land LM \text{ safe}$$

1. \( C, M \) does not get stuck
2. if \( C, M \overset{*}{\Rightarrow} \text{skip}, M' \)
   then \( \exists LM'. LM' \models Q \land LM' \overset{\text{iso}}{\sim} M' \land LM' \text{ safe} \)

But in order to guarantee \( \{\{ P \} \} \ \text{GC()} \ \{\{ P \} \} \), we need to ensure that we only invoke the GC under GC-safe memories
Motivating example: Array initialization

\[
\begin{align*}
\text{GC safe } \rightarrow \\
x &:= \text{ALLOC}(n); \\
t &:= x + 4n; \\
\text{while } x < t \text{ do} \\
\hspace{1cm} [x] &:= 0; \\
\hspace{1cm} x &:= x + 4 \\
\text{GC unsafe } \rightarrow \\
\text{od}; \\
x &:= x - 4n; \\
t &:= 0 \\
\text{GC safe } \rightarrow
\end{align*}
\]
Two-level logic

- **Outer-level logic**
  \[
  \begin{align*}
  \{\{P\}\} & \ C \ \{\{Q\}\} \\
  \iff & \quad \forall M, LM \text{ such that } LM \models P \land LM \overset{\text{iso}}{\sim} M \land LM \text{ safe} \\
  & \quad \begin{align*}
    & 1. C, M \text{ does not get stuck} \\
    & 2. \text{if } C, M \overset{*}{\rightsquigarrow} \text{ skip, } M' \\
    & \quad \text{then } \exists LM'. \ LM' \models Q \land LM' \overset{\text{iso}}{\sim} M' \land LM' \text{ safe}
  \end{align*}
  \end{align*}
  \]

- **Inner-level logic**
  \[
  \begin{align*}
  \{P\} & \ C \ \{Q\} \\
  \iff & \quad \forall M, LM \text{ such that } LM \models P \land LM \overset{\text{iso}}{\sim} M \\
  & \quad \begin{align*}
    & 1. C, M \text{ does not get stuck} \\
    & 2. \text{if } C, M \overset{*}{\rightsquigarrow} \text{ skip, } M' \\
    & \quad \text{then } \exists LM'. \ LM' \models Q \land LM' \overset{\text{iso}}{\sim} M'
  \end{align*}
  \end{align*}
  \]
Towards an “inclusion” rule

Obviously unsound:

$$\{ P \} \ C \ \{ Q \} \ \frac{}{\{ \{ P \} \} \ C \ \{ \{ Q \} \} }$$
Towards an “inclusion” rule

We want something like this . . .

\[
\begin{align*}
\{ P \land \text{mem is GC-safe} \} & \quad C \quad \{ Q \land \text{mem is GC-safe} \} \\
\{\{ P \}\} & \quad C \quad \{\{ Q\}\}
\end{align*}
\]

Solution: We make a simplifying assumption.
In the inner-level logic, the store may contain unsafe values, but the heap may not. This is OK, given how interior pointers are typically used.
Towards an “inclusion” rule

We want something like this . . .

\[
\{P \land \text{mem is GC-safe}\} \ C \ \{Q \land \text{mem is GC-safe}\}
\]

\[
\{\{P\}\} \ C \ \{\{Q\}\}
\]

. . . but how do we characterize \text{mem is GC-safe}?
Towards an “inclusion” rule

We want something like this . . .

\[
\{ P \land \text{mem is GC-safe} \} \quad C \quad \{ Q \land \text{mem is GC-safe} \} \\
\{\{ P \}\} \quad C \quad \{\{ Q \}\}
\]

. . . but how do we characterize \text{mem is GC-safe}?

**Solution:** We make a simplifying assumption.

- In the inner-level logic, the store may contain unsafe values, but the heap may not.
- This is OK, given how interior pointers are typically used.
Towards an “inclusion” rule

We want something like this . . .

\[
\begin{align*}
\{ P \land \text{store is GC-safe} \} & \implies \{ Q \land \text{store is GC-safe} \} \\
\{ \{ P \} \} & \implies \{ \{ Q \} \}
\end{align*}
\]

. . . but how do we characterize \text{store is GC-safe}?

\textbf{Solution:} We make a simplifying assumption.

- In the inner-level logic, the store may contain unsafe values, but the heap may not.
- This is OK, given how interior pointers are typically used.
Inclusion rule

\[ \{ P \land \text{safe}(V) \} \ C \ \{ Q \land \text{safe}(\text{Mod}(C)) \} \]
\[ \{\{ P \}\} \ C \ \{\{ Q \}\} \]
\[ V \subseteq \text{ProgVars} \]

- safe is a new primitive predicate in our inner-level logic.
Two-level logic (revisited)

- **Outer-level logic**

\[
\{\{ P \}\} \ C \ \{\{ Q \}\}
\]

\[\iff \forall M, LM \text{ such that } LM \models P \land LM \mathbin{\overset{\text{iso}}{\sim}} M \land LM \text{ safe}
\]

1. \(C, M\) does not get stuck
2. if \(C, M \leadsto^* \text{ skip, } M'\)
   then \(\exists LM'. LM' \models Q \land LM' \mathbin{\overset{\text{iso}}{\sim}} M' \land LM' \text{ safe}\)

- **Inner-level logic**

\[
\{P\} \ C \ \{Q\}
\]

\[\iff \forall M, LM \text{ such that } LM \models P \land LM \mathbin{\overset{\text{iso}}{\sim}} M \]

1. \(C, M\) does not get stuck
2. if \(C, M \leadsto^* \text{ skip, } M'\)
   then \(\exists LM'. LM' \models Q \land LM' \mathbin{\overset{\text{iso}}{\sim}} M'\)
Two-level logic (revisited)

- **Outer-level logic**
  \[
  \{\{P\}\} \; C \; \{\{Q\}\}
  \]
  \[\iff \forall M, LM \text{ such that } LM \models P \land LM^{\text{iso}} \sim M \land LM \text{ safe} \]
  
  1. $C, M$ does not get stuck
  2. if $C, M \rightsquigarrow^* \text{skip, } M'$
     then $\exists LM'. \; LM' \models Q \land LM^{\text{iso}} \sim M' \land LM' \text{ safe}$

- **Inner-level logic**
  \[
  \{P\} \; C \; \{Q\}
  \]
  \[\iff \forall M, LM \text{ such that } LM \models P \land LM^{\text{iso}} \sim M \land LM \cdot h \text{ safe} \]
  
  1. $C, M$ does not get stuck
  2. if $C, M \rightsquigarrow^* \text{skip, } M'$
     then $\exists LM'. \; LM' \models Q \land LM^{\text{iso}} \sim M' \land LM' \cdot h \text{ safe}$
Frame rule

\[
\frac{\{P\} \enspace C \enspace \{Q\}}{\{P \ast R\} \enspace C \enspace \{Q \ast R\}} \quad FV(R) \cap \text{Mod}(C) = \emptyset
\]

Our semantics so far doesn’t support frame, because the presence of a GC violates “heap locality”

- Solution: Following [Birkedal et al. 2006], we bake the frame rule into the semantics of triples
Baking the frame rule in

**Outer-level logic**

\[
\{\{P\}\} \ C \ {\{Q\}\}
\]

\[\iff \forall M, LM \text{ such that } LM \models P \land LM \iso M \land LM \text{ safe}
\]

1. \(C, M\) does not get stuck
2. if \(C, M \rightsquigarrow* \text{skip}, M'\)
   then \(\exists LM'. LM' \models Q \land LM' \iso M' \land LM' \text{ safe}\)

**Inner-level logic**

\[
\{P\} \ C \ \{Q\}
\]

\[\iff \forall M, LM \text{ such that } LM \models P \land LM \iso M \land LM.h \text{ safe}
\]

1. \(C, M\) does not get stuck
2. if \(C, M \rightsquigarrow* \text{skip}, M'\)
   then \(\exists LM'. LM' \models Q \land LM' \iso M' \land LM'.h \text{ safe}\)
Baking the frame rule in

● Outer-level logic

{{P}} C {{Q}}

\[\iff \forall M, LM, LM_f \text{ such that } LM \models P \land LM \cup LM_f \isomorphism M \land LM \cup LM_f \text{ safe}\]

1. C, M does not get stuck
2. if C, M \rightarrowstar skip, M'
   then \(\exists LM'. LM' \models Q \land LM' \cup LM_f \isomorphism M' \land LM' \cup LM_f \text{ safe}\)

● Inner-level logic

{P} C {Q}

\[\iff \forall M, LM, LM_f \text{ such that } LM \models P \land LM \cup LM_f \isomorphism M \land (LM \cup LM_f).h \text{ safe}\]

1. C, M does not get stuck
2. if C, M \rightarrowstar skip, M'
   then \(\exists LM'. LM' \models Q \land LM' \cup LM_f \isomorphism M' \land (LM' \cup LM_f).h \text{ safe}\)
Proof rules & Examples
Words $\overset{\text{def}}{=} \{ w \in \mathbb{Z} \}$
Locs $\overset{\text{def}}{=} \{ \ell_1, \ell_2, \ldots \}$
LogPtrs $\overset{\text{def}}{=} \{ \ell^i | \ell \in \text{Locs} \land i \in \mathbb{Z} \}$
LogVals $\overset{\text{def}}{=} \{ v \in \text{Words} \cup \text{LogPtrs} \}$
LStores $\overset{\text{def}}{=} \{ s \in \text{ProgVars} \rightarrow \text{LogVals} \}$
LHeaps $\overset{\text{def}}{=} \{ h \in \text{Locs} \rightarrow_{\text{fin}} \mathbb{N} \rightarrow_{\text{fin}} \text{LogVals} \}$


**Outer-level assertions**

\[ P := E \mid \text{logptr}(E) \mid \text{word}(E) \]

\[ \quad \mid E \leftrightarrow E \mid P \ast P \mid P \rightarrow P \]

\[ \quad \mid P \Rightarrow P \mid P \land P \mid P \lor P \mid \forall v. P \mid \exists v. P \]

**Inner-level assertions**

\[ P := \text{safe}(E) \]

\[ \quad \mid E \mid \text{logptr}(E) \mid \text{word}(E) \]

\[ \quad \mid E \leftrightarrow E \mid P \ast P \mid P \rightarrow P \]

\[ \quad \mid P \Rightarrow P \mid P \land P \mid P \lor P \mid \forall v. P \mid \exists v. P \]
Selected proof rules

\[
\begin{align*}
\{ x = v \land E = E \} & \quad x := E \quad \{ x = E[v/x] \} \\
\{ x = u \land E \leftrightarrow v \} & \quad x := [E] \quad \{ x = v \land E[u/x] \leftrightarrow v \} \\
\{ E \leftrightarrow \neg \land \text{safe}(E') \} & \quad [E] := E' \quad \{ E \leftrightarrow E' \} \\
\{ \text{true} \} & \quad x := \text{ALLOC}(n) \quad \{ x \leftrightarrow_{n-} \ldots , - \} 
\end{align*}
\]

(Assign)  
(Read)  
(Write)  
(Alloc)
Example 1: Array initialization

\[
x := \text{ALLOC}(n);
\]
\[
t := x + 4n;
\]
while \(x < t\) do

\[
[x] := 0;
\]
\[
x := x + 4
\]
\[
od;
\]
\[
x := x - 4n;
\]
\[
t := 0
\]
Example 1: Array initialization

\[
x := \text{ALLOC}(n);
\]

\[
\begin{array}{c}
([x] := 0; \ x := x + 4); \quad \ldots \quad ([x] := 0; \ x := x + 4) \\
\end{array}
\]

\[
x := x - 4n
\]
Example 1: Array initialization

\([\{\text{true}\}\}]\)

\(x := \text{ALLOC}(n);\)

\(\{\{x \leftrightarrow n - , \ldots , - \}\}\)

\(n \text{ times}\)

\(([x] := 0; \ x := x + 4); \ \ldots ; \ ([x] := 0; \ x := x + 4)\)

\(x := x - 4n\)

\(\{\{x \leftrightarrow n \ 0, \ldots , 0\}\}\)
Example 1: Array initialization

\[
\begin{align*}
\{\{\text{true}\}\} & \quad \frac{\{P \land \text{safe}(V)\} \quad C \quad \{Q \land \text{safe}(\text{Mod}(C))\}}{\{\{P\}\} \quad C \quad \{\{Q\}\}} \\
\text{x := ALLOC}(n); & \\
\{\{x \mapsto n -, \ldots, -\}\} & \\
\{x \mapsto n -, \ldots, - \land \text{safe}(x)\} & \\
\text{n times} & \\
([x] := 0; \ x := x + 4); \ldots; ([x] := 0; \ x := x + 4) & \\
\text{x := x} - 4n & \\
\{x \mapsto n 0, \ldots, 0 \land \text{safe}(x)\} & \\
\{\{x \mapsto n 0, \ldots, 0\}\} & \\
\text{C.-K. Hur, D. Dreyer, V. Vafeiadis} & \\
\text{Separation Logic in the Presence of Garbage Collection}
\end{align*}
\]
Example 1: Array initialization

\[
\begin{array}{c}
\{\{\text{true}\}\} \\
\hline
\{P \land \text{safe}(V)\} \ C \ \{Q \land \text{safe}(\text{Mod}(C))\} \\
\{\{P\}\} \ C \ \{\{Q\}\}
\end{array}
\]

\[
x := \text{ALLOC}(n);
\]
\[
\{\{x \leftarrow n -, \ldots, -\}\} \ \\
\{x \leftarrow n -, \ldots, - \land \text{safe}(x)\}
\]

\[
\begin{array}{c}
\underbrace{([x] := 0; \ x := x + 4); \ \ldots; ([x] := 0; \ x := x + 4)}_{n \ \text{times}} \\
\{x - 4n \leftarrow n 0, \ldots, 0 \land \text{safe}(x - 4n)\}
\end{array}
\]

\[
x := x - 4n
\]
\[
\{x \leftarrow n 0, \ldots, 0 \land \text{safe}(x)\}
\]
\[
\{\{x \leftarrow n 0, \ldots, 0\}\}
\]
Example 1: Array initialization

For the original example, note that the setting of $t$ to a safe value is important, since $t$ is modified by the program.

\[
x := \text{ALLOC}(n); \\
t := x + 4n; \\
\text{while } x < t \text{ do} \\
\quad [x] := 0; \\
\quad x := x + 4 \\
\text{od}; \\
x := x - 4n; \\
t := 0
\]
Example 2: Add & Square

\[
i := (i + j - 2) \div 2;
\]

\[
i := i \times i; \ i := 2 \times i + 1
\]
Example 2: Add & Square

\[
\{i = 2n + 1 \land j = 2m + 1\}
\]

\[
i := (i + j - 2) \div 2;
\]

\[
i := i \times i; \; i := 2 \times i + 1
\]

\[
\{i = 2(n + m)^2 + 1 \land j = 2m + 1\}
\]
Example 2: Add & Square

\[ \{ i = 2n + 1 \land j = 2m + 1 \} \]
\[ \{ i = 2n + 1 \land j = 2m + 1 \land \text{word}(n, m) \} \]
\[ i := (i + j - 2) \div 2; \]
\[ \{ i = n + m \land j = 2m + 1 \land \text{word}(n, m) \} \]
\[ i := i \times i; \; i := 2 \times i + 1 \]
\[ \{ i = 2(n + m)^2 + 1 \land j = 2m + 1 \} \]
\[ \{ i = 2(n + m)^2 + 1 \land j = 2m + 1 \land \text{safe}(i) \} \]
\[ \{ i = 2(n + m)^2 + 1 \land j = 2m + 1 \} \]
Summary

Separation logic to reason about low-level programs that might violate GC safety in between calls to the GC

Key ideas:
- Logical memory
- Two-level logic with “inclusion” rule & safe predicate

Detailed soundness proof (in the technical appendix)
Conclusion

Summary

- Separation logic to reason about low-level programs that might violate GC safety in between calls to the GC
- Key ideas:
  - Logical memory
  - Two-level logic with “inclusion” rule & safe predicate
- Detailed soundness proof (in the technical appendix)

Limitations

- Only accounts for stop-the-world collectors
- Conjunction rule is unsound
- Example we should but can’t prove in general:

\[
\begin{align*}
\{ & x = v \land y = w \} \\
& x := x \text{ xor } y; \quad y := x \text{ xor } y; \quad x := x \text{ xor } y \\
& \{x = w \land y = v \}
\end{align*}
\]