Memory abstraction 1

MPRI — Cours 2.6 “Interprétation abstraite : application à la vérification et à l’analyse statique”

Xavier Rival

INRIA, ENS, CNRS

Oct, 30th. 2019
Overview of the lecture

So far, we have shown **numerical abstract domains**

- non relational: intervals, congruences...
- relational: polyhedra, octagons, ellipsoids...

How to deal with non purely numerical states ?
How to reason about complex data-structures ?

⇒ a very broad topic, and two lectures:

**This lecture**

- overview memory models and memory properties
- abstraction of pointer structures and separation logic based shape analysis

**Next lecture:** arrays, shape/numerical abstraction, composition of shape abstractions
Outline

1 Memory models
   - Towards memory properties
   - Formalizing concrete memory states
   - Treatment of errors
   - Language semantics

2 Pointer Abstractions

3 Separation Logic

4 A shape abstract domain relying on separation

5 Standard static analysis algorithms

6 Conclusion

7 Internships
Assumptions for the two lectures on memory abstraction

Imperative programs viewed as \textit{transition systems}:

- set of \textbf{control states}: $L$ (program points)
- set of \textbf{variables}: $X$ (all assumed globals)
- set of \textbf{values}: $V$ (so far: $V$ consists of integers (or floats) only)
- set of \textbf{memory states}: $M$ (so far: $M = X \rightarrow V$)
- error state: $\Omega$
- states: $S$
  \[
  S = L \times M \\
  S_{\Omega} = S \cup \{ \Omega \}
  \]
- transition relation:
  \[
  (\rightarrow) \subseteq S \times S_{\Omega}
  \]

\textbf{Abstraction} of sets of states

- \textbf{abstract domain} $D^#$
- \textbf{concretization} $\gamma : (D^#, \subseteq^#) \longrightarrow (P(S), \subseteq)$
Assumptions: syntax of programs

We start from the same language syntax and will extend l-values:

\[
\begin{align*}
l & ::= \text{l-values} \\
   & | \ x \quad (x \in X) \\
   & | \ldots \quad \text{we will add other kinds of l-values} \\
   & | \text{pointers, array dereference...} \\
\end{align*}
\]

\[
\begin{align*}
e & ::= \text{expressions} \\
   & | \ c \quad (c \in V) \\
   & | \ l \quad (lvalue) \\
   & | \ e \oplus e \quad (\text{arith operation, comparison}) \\
\end{align*}
\]

\[
\begin{align*}
s & ::= \text{statements} \\
   & | \ l = e \quad (\text{assignment}) \\
   & | \ s; \ldots \ s; \quad (\text{sequence}) \\
   & | \ \text{if}(e)\{s\} \quad (\text{condition}) \\
   & | \ \text{while}(e)\{s\} \quad (\text{loop})
\end{align*}
\]
Assumptions: semantics of programs

We assume classical definitions for:

- **l-values**: \([1] : M \to X\)
- **expressions**: \([e] : M \to V\)
- **programs and statements**:
  - we assume a label **before each statement**
  - each statement defines a **set of transitions** (\(\to\))

In this course, we rely on the usual **reachable states semantics**

### Reachable states semantics

The reachable states are computed as \([S]_R = \text{Ifp} F\) where

\[
F : \mathcal{P}(S) \longrightarrow \mathcal{P}(S) \\
X \longmapsto S_I \cup \{s \in S | \exists s' \in X, s' \rightarrow s\}
\]

and \(S_I\) denotes the set of initial states.
Assumptions: general form of the abstraction

We assume an abstraction for sets of memory states:

- memory abstract domain $\mathbb{D}_{\text{mem}}$
- concretization function $\gamma_{\text{mem}} : \mathbb{D}_{\text{mem}} \rightarrow \mathcal{P}(M)$

Reachable states abstraction

We construct $\mathbb{D} = \mathbb{L} \rightarrow \mathbb{D}_{\text{mem}}$ and:

$$
\begin{align*}
\gamma : & \mathbb{D} \rightarrow \mathcal{P}(S) \\
X & \mapsto \{(l, m) \in S | m \in \gamma_{\text{mem}}(X(l))\}
\end{align*}
$$

The whole question is how do we choose $\mathbb{D}_{\text{mem}}, \gamma_{\text{mem}}$...

- previous lectures:
  - $X$ is fixed and finite and, $V$ is scalars (integers or floats), thus, $M \equiv V^n$
- today:
  - we will extend the language thus, also need to extend $\mathbb{D}_{\text{mem}}, \gamma_{\text{mem}}$
**Abstraction of purely numeric memory states**

**Purely numeric case**

- $\mathbb{V}$ is a set of values of the same kind
- e.g., integers ($\mathbb{Z}$), machine integers ($\mathbb{Z} \cap [-2^{63}, 2^{63} - 1]$)...
- If the set of variables is fixed, we can use any abstraction for $\mathbb{V}^N$

**Example:** $N = 2$, $\mathbb{X} = \{x, y\}$

- Concrete set
- Interval domain
- Octagon domain
- Polyedra domain
Heterogeneous memory states

In real life languages, there are many kinds of values:
- **scalars** (integers of various sizes, boolean, floating-point values)...
- **pointers, arrays**...

Heterogeneous memory states and non relational abstraction

- **types** \( t_0, t_1, \ldots \) and **values** \( \mathbb{V} = \mathbb{V}_{t_0} \cup \mathbb{V}_{t_1} \cup \ldots \)
- finitely many **variables**; each has a **fixed type**: \( \mathbb{X} = \mathbb{X}_{t_0} \cup \mathbb{X}_{t_1} \cup \ldots \)
- **memory states**: \( \mathbb{M} = \mathbb{X}_{t_0} \rightarrow \mathbb{V}_{t_0} \times \mathbb{X}_{t_1} \rightarrow \mathbb{V}_{t_1} \ldots \)

**Principle**: compose abstractions for sets of memory states of each type

Non relational abstraction of heterogeneous memory states

- \( \mathbb{M} = \mathbb{M}_{0} \times \mathbb{M}_{1} \times \ldots \) where \( \mathbb{M}_i = \mathbb{X}_i \rightarrow \mathbb{V}_i \)
- **Concretization function** (case with two types)
  \[
  \gamma_{\text{nr}} : \mathcal{P}(\mathbb{M}_0) \times \mathcal{P}(\mathbb{M}_1) \rightarrow \mathcal{P}(\mathbb{M})
  \]
  \[
  (m_0^\#, m_1^\#) \mapsto \{ (m_0, m_1) \mid \forall i, m_i \in \gamma_i(m_i^\#) \} 
  \]
Common structures (non exhaustive list)

- **Structures, records, tuples**: sequences of cells accessed with fields
- **Arrays**: similar to structures; indexes are integers in $[0, n-1]$
- **Pointers**: numerical values corresponding to the address of a memory cell
- **Strings and buffers**: blocks with a sequence of elements and a terminating element (e.g., 0x0)
- **Closures** (functional languages): pointer to function code and (partial) list of arguments

To describe memories, the definition $M = X \rightarrow V$ is too restrictive

Generally, non relational, heterogeneous abstraction cannot handle many such structures all at once: relations are needed!
Specific properties to verify

**Memory safety**

Absence of memory errors (crashes, or undefined behaviors)

**Pointer errors:**
- Dereference of a null pointer / of an invalid pointer

**Access errors:**
- Out of bounds array access, buffer overruns (often used for attacks)

**Invariance properties**

Data should not become corrupted (values or structures...)

**Examples:**
- Preservation of structures, e.g., lists should remain connected
- Preservation of invariants, e.g., of balanced trees
Properties to verify: examples

A program closing a list of file descriptors

```c
// l points to a list
c = l;
while (c ≠ NULL){
    close(c → FD);
    c = c → next;
}
```

Correctness properties

1. memory safety
2. l is supposed to store all file descriptors at all times
   will its structure be preserved? yes, no breakage of a next link
3. closure of all the descriptors

Examples of structure preservation properties

- Algorithms manipulating trees, lists...
- Libraries of algorithms on balanced trees
- Not guaranteed by the language!
  e.g., the balancing of Maps in the OCaml standard library was incorrect for years (performance bug)
A more realistic model

No one-to-one relation between memory cells and program variables
- A variable may indirectly reference several cells (structures...)
- Dynamically allocated cells correspond to no variable at all...

Environment + Heap
- **Addresses** are values: $V_{addr} \subseteq V$
- **Environments** $e \in E$ map variables into their addresses
- **Heaps** ($h \in H$) map addresses into values

$$E = X \rightarrow V_{addr}$$
$$H = V_{addr} \rightarrow V$$

$h$ is actually only a partial function

- **Memory states** (or memories): $M = E \times H$

Note: Avoid confusion between heap (function from addresses to values) and dynamic allocation space (often referred to as “heap”)

Example of a concrete memory state (variables)

Example setup:
- \(x\) and \(z\) are two list elements containing values 64 and 88, and where the former points to the latter
- \(y\) stores a pointer to \(z\)

Memory layout
(pointer values underlined)

\[
\begin{array}{c|c}
\text{address} & \text{value} \\
\hline
\&x = 300 & 64 \\
300 & 304 \\
&y = 308 & 312 \\
308 & 312 \\
\&z = 312 & 88 \\
312 & 312 \\
& = 316 & 0x0 \\
316 & 316 \\
\end{array}
\]

- \(e\): \(x \mapsto 300\)
  \(y \mapsto 308\)
  \(z \mapsto 312\)

- \(h\):
  \(300 \mapsto 64\)
  \(304 \mapsto 312\)
  \(308 \mapsto 312\)
  \(312 \mapsto 88\)
  \(316 \mapsto 0\)
Example of a concrete memory state (variables + dyn. cell)

Example setup:
- same configuration
- + second field of \( z \) points to a dynamically allocated list element (in purple)

Memory layout

\[
\begin{align*}
\text{address} & \quad \text{value} \\
&x = 300 & 64 \\
304 & 312 \\
&y = 308 & 312 \\
308 & 312 \\
&z = 312 & 88 \\
312 & 508 \\
508 & 25 \\
512 & 0\times0
\end{align*}
\]

\[
\begin{align*}
e: & \\
x & \mapsto 300 \\
y & \mapsto 308 \\
z & \mapsto 312
\end{align*}
\]

\[
\begin{align*}
h: & \\
300 & \mapsto 64 \\
304 & \mapsto 312 \\
308 & \mapsto 312 \\
312 & \mapsto 88 \\
316 & \mapsto 508 \\
508 & \mapsto 25 \\
512 & \mapsto 0
\end{align*}
\]
Extending the semantic domains

Some slight modifications to the semantics of the initial language:

- **Addresses are values:** $\mathbb{V}_{\text{addr}} \subseteq \mathbb{V}$

- **L-values evaluate into addresses:** $\llbracket 1 \rrbracket : \mathcal{M} \rightarrow \mathbb{V}_{\text{addr}}$
  \[
  \llbracket x \rrbracket (e, h) = e(x)
  \]

- **Semantics of expressions** $\llbracket e \rrbracket : \mathcal{M} \rightarrow \mathbb{V}$, mostly unchanged
  \[
  \llbracket 1 \rrbracket (e, h) = h(\llbracket 1 \rrbracket (e, h))
  \]

- **Semantics of assignment** $l_0 : l := e; l_1 : \ldots :$
  \[
  (l_0, e, h_0) \rightarrow (l_1, e, h_1)
  \]
  where
  \[
  h_1 = h_0[\llbracket 1 \rrbracket (e, h_0) \leftarrow \llbracket e \rrbracket (e, h_0)]
  \]
Realistic definitions of memory states

Our model is still not very accurate for most languages

- Memory cells do not all have the same size
- **Memory management algorithms** usually do not treat cells one by one, e.g., `malloc` returns a pointer to a block applying `free` to that pointer will dispose the whole block

Other refined models

- **Partition of the memory** in blocks with a base address and a size
- **Partition of blocks** into cells with a size
- Description of fields with an offset
- Description of pointer values with a base address and an offset...

For a very formal description of such concrete memory states:
see **CompCert** project source files (Coq formalization)
Language semantics: program crash

In an abnormal situation, we assume that the program will crash

- advantage: very clear semantics
- disadvantage (for the compiler designer): dynamic checks are required

Error state

- $\Omega$ denotes an error configuration
- $\Omega$ is a blocking: $(\rightarrow) \subseteq S \times (\{\Omega\} \cup S)$

OCaml:

- out-of-bound array access:
  
  Exception: Invalid_argument "index out of bounds".

- no notion of a null pointer

Java:

- exception in case of out-of-bound array access, null dereference:
  
  java.lang.ArrayIndexOutOfBoundsException
Language semantics: undefined behaviors

**Alternate choice:** leave the behavior of the program **unspecified** when an abnormal situation is encountered

- **advantage:** easy implementation (often architecture driven)
- **disadvantage:** unintuitive semantics, errors hard to reproduce
different compilers may make different choices...
or in fact, make no choice at all (= let the program evaluate even when performing invalid actions)

**Modeling of undefined behavior**

- Very hard to capture what a program operation may modify
- Abnormal situation at \((l_0, m_0)\) such that \(\forall m_1 \in M, (l_0, m_0) \rightarrow (l_1, m_1)\)

- **In C:**
  array out-of-bound accesses and dangling pointer dereferences lead to undefined behavior (and potentially, memory corruption) whereas a null-pointer dereference always result into a crash
Composite objects

How are contiguous blocks of information organized?

Java objects, OCaml struct types
- sets of fields
- each field has a type
- **no assumption** on physical storage, **no pointer arithmetics**

C composite structures and unions
- **physical mapping** defined by the norm
- each field has a specified **size** and a specified **alignment**
- **union types / casts:** implementations may allow several views
Pointers and records / structures / objects

Many languages provide pointers or references and allow to manipulate addresses, but with different levels of expressiveness.

What kind of objects can be referred to by a pointer?

Pointers only to records / structures / objects

- **Java**: only pointers to objects
- **OCaml**: only pointers to records, structures...

Pointers to fields

- **C**: pointers to any valid cell...

```
struct {int a; int b} x;
int * y = &(x·b);
```
What kind of operations can be performed on a pointer?

Classical pointer operations

- **Pointer dereference**: 
  \[ p \rightarrow \]
  \( \ast p \) returns the contents of the cell of address \( p \)

- **“Address of” operator**: \( \& x \)
  returns the address of variable \( x \)

- Can be analyzed with a rather coarse pointer model
  e.g., symbolic base + symbolic field

Arithmetics on pointers, requiring a more precise model

- **Addition of a numeric constant**: 
  \( p + n \)
  address contained in \( p + n \) times the size of the type of \( p \)

  Interaction with pointer casts...

- **Pointer subtraction**: returns a numeric offset
Manual memory management

Allocation of unbounded memory space
- How are new memory blocks **created** by the program?
- How do old memory blocks get **freed**?

OCaml memory management
- implicit allocation
  when declaring a new object
- garbage collection: purely automatic process, that frees unreachable blocks

C memory management
- manual allocation: **malloc** operation returns a pointer to a new block
- manual de-allocation: **free** operation (block base address)

Manual memory management is not safe:
- memory leaks: growing unreachable memory region; memory exhaustion
- dangling pointers if freeing a block that is still referred to
Summary on the memory model

<table>
<thead>
<tr>
<th>Language dependent items</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Clear error cases</strong> or <strong>undefined behaviors</strong></td>
</tr>
<tr>
<td><strong>Composite objects</strong>: structure fully exposed or not</td>
</tr>
<tr>
<td><strong>Pointers to object fields</strong>: allowed or not</td>
</tr>
</tbody>
</table>
| **Pointer arithmetic**: allowed or not  
  *i.e.*, are pointer values symbolic values or numeric values |
| **Memory management**: automatic or manual |

In this course, we start with a simple model, and study specific features one by one and in isolation from the others.
Rest of the course

Structures for which we introduce abstractions:

- **pointers** and **dynamically allocated pointer structures** (today)
- **arrays** (in a few weeks)
- **combinations of structures** (in a few weeks)

Abstract operations:

- post-condition for the **reading** of a cell defined by an l-value
  e.g., \( x = a[i] \) or \( x = *p \)
- post-condition for the **writing of a heap cell**
  e.g., \( a[i] = p \) or \( p -> f = x \)
- **abstract join**, that approximates unions of concrete states
Outline

1. Memory models
2. Pointer Abstractions
3. Separation Logic
4. A shape abstract domain relying on separation
5. Standard static analysis algorithms
6. Conclusion
7. Internships
Programs with pointers: syntax

Syntax extension: we add pointer operations

\[
\begin{align*}
\text{l} & ::= \text{l-values} \\
& | \quad x \quad (x \in X) \\
& | \quad \ldots \\
& | \quad *e \quad \text{pointer dereference} \\
& | \quad l \cdot f \quad \text{field read} \\
\text{e} & ::= \text{expressions} \\
& | \quad l \\
& | \quad \ldots \\
& | \quad &l \quad \text{"address of" operator} \\
\text{s} & ::= \text{statements} \\
& | \quad \ldots \\
& | \quad x = \text{malloc}(c) \quad \text{allocation of } c \text{ bytes} \\
& | \quad \text{free}(x) \quad \text{deallocation of the block pointed to by } x
\end{align*}
\]

We do not consider pointer arithmetics here
Programs with pointers: semantics

Case of l-values:

\[
\begin{align*}
\llbracket x \rrbracket (e, \tilde{h}) &= e(x) \\
\llbracket *e \rrbracket (e, \tilde{h}) &= \begin{cases} h(\llbracket e \rrbracket (e, \tilde{h})) & \text{if } \llbracket e \rrbracket (e, \tilde{h}) \neq 0 \land \llbracket e \rrbracket (e, \tilde{h}) \in \text{Dom}(h) \\
\Omega & \text{otherwise} \end{cases} \\
\llbracket l \cdot f \rrbracket (e, \tilde{h}) &= \llbracket l \rrbracket (e, \tilde{h}) + \text{offset}(f) \text{ (numeric offset)}
\end{align*}
\]

Case of expressions:

\[
\begin{align*}
\llbracket l \rrbracket (e, \tilde{h}) &= h(\llbracket l \rrbracket (e, \tilde{h})) \quad \text{(evaluates into the contents)} \\
\llbracket &l \rrbracket (e, \tilde{h}) &= \llbracket l \rrbracket (e, \tilde{h}) \quad \text{(evaluates into the address)}
\end{align*}
\]

Case of statements:

- **memory allocation** \( x = \text{malloc}(c) \): \((e, \tilde{h}) \rightarrow (e, \tilde{h}')\) where 
  \[
  \tilde{h}' = \tilde{h}[e(x) \leftarrow k] \sqcup \{ k \mapsto v_k, k+1 \mapsto v_{k+1}, \ldots, k+c-1 \mapsto v_{k+c-1} \} \text{ and } k, \ldots, k+c-1 \text{ are fresh and unused in } \tilde{h} \]

- **memory deallocation** \( \text{free}(x) \): \((e, \tilde{h}) \rightarrow (e, \tilde{h}')\) where \( k = e(x) \) and 
  \[
  \tilde{h} = \tilde{h}' \sqcup \{ k \mapsto v_k, k+1 \mapsto v_{k+1}, \ldots, k+c-1 \mapsto v_{k+c-1} \} \]
We rely on the **non relational abstraction of heterogeneous states** that was introduced earlier, with a few changes:

- We let $V = V_{\text{addr}} \cup V_{\text{int}}$ and $X = X_{\text{addr}} \cup X_{\text{int}}$
- **Concrete memory cells** now include **structure fields**, and fields of **dynamically allocated regions**
- **Abstract cells** $C^\#$ finitely summarize concrete cells
- We apply a **non relational abstraction**:

**Non relational pointer abstraction**

- Set of **pointer abstract values** $D^\#_{\text{ptr}}$
- **Concretization** $\gamma_{\text{ptr}} : D^\#_{\text{ptr}} \to \mathcal{P}(V_{\text{addr}})$ into pointer sets

We will see **several instances** of this kind of abstraction
The dereference of a null pointer will cause a crash

To establish safety: compute which pointers may be null

Null pointer analysis

Abstract domain for addresses:
- $\gamma_{\text{ptr}}(\bot) = \emptyset$
- $\gamma_{\text{ptr}}(\top) = \forall_{\text{addr}}$
- $\gamma_{\text{ptr}}(\neq \text{NULL}) = \forall_{\text{addr}} \setminus \{0\}$

- we may also use a lattice with a fourth element $= \text{NULL}$
  
  exercise: what do we gain using this lattice?

- very lightweight, can typically resolve rather trivial cases

- useful for C, but also for Java
The dereference of a null pointer will cause a crash

To establish safety: compute which pointers may be dangling

Null pointer analysis

Abstract domain for addresses:

- $\gamma_{\text{ptr}}(\bot) = \emptyset$
- $\gamma_{\text{ptr}}(\top) = \mathbb{V}_{\text{addr}} \times \mathbb{H}$
- $\gamma_{\text{ptr}}(\text{Not dangling}) = \{ (v, h) \mid h \in \mathbb{H} \land v \in \text{Dom}(h) \}$

- very lightweight, can typically resolve rather trivial cases
- useful for C, useless for Java (initialization requirement + GC)
Determine where a pointer may store a reference to

1: int x, y;
2: int * p;
3: y = 9;
4: p = &x;
5: *p = 0;

- what is the final value for x? 0, since it is modified at line 5...
- what is the final value for y? 9, since it is not modified at line 5...

Basic pointer abstraction

- We assume a set of abstract memory locations $A^\#$ is fixed:
  $$A^\# = \{&x, &y, \ldots, &t, a_0, a_1, \ldots, a_N\}$$
- Concrete addresses are abstracted into $A^\#$ by $\phi_A : A \rightarrow A^\# \uplus \{\top\}$
- A pointer value is abstracted by the abstraction of the addresses it may point to, i.e.,
  $$D_{ptr}^\# = \mathcal{P}(A^\#)$$
  and
  $$\gamma_{ptr}(a^\#) = \{a \in A \mid \phi_A(a) = a^\#\}$$

- example: p may point to {&x}
Example code:

1:   int x, y;
2:   int * p;
3:   y = 9;
4:   p = &x;
5:   *p = 0;
6:   ...

Abstract locations: \{&x, &y, &p\}

Analysis results:

<table>
<thead>
<tr>
<th></th>
<th>&amp;x</th>
<th>&amp;y</th>
<th>&amp;p</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>2</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>3</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>4</td>
<td>T</td>
<td>[9, 9]</td>
<td>T</td>
</tr>
<tr>
<td>5</td>
<td>T</td>
<td>[9, 9]</td>
<td>{&amp;x}</td>
</tr>
<tr>
<td>6</td>
<td>[0, 0]</td>
<td>[9, 9]</td>
<td>{&amp;x}</td>
</tr>
</tbody>
</table>
Points-to sets computation and imprecision

\[ x \in [-10, -5]; \ y \in [5, 10] \]

1: \textbf{int} * p;
2: \textbf{if}(?){
3: \quad p = &x;
4: } \textbf{else} {
5: \quad p = &y;
6: }
7: \star p = 0;
8: ...

- What is the final range for \( x \)?
- What is the final range for \( y \)?

\textbf{Abstract locations:} \{&x, &y, &p\}

<table>
<thead>
<tr>
<th></th>
<th>&amp;x</th>
<th>&amp;y</th>
<th>&amp;p</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>[-10, -5]</td>
<td>[5, 10]</td>
<td>\top</td>
</tr>
<tr>
<td>2</td>
<td>[-10, -5]</td>
<td>[5, 10]</td>
<td>\top</td>
</tr>
<tr>
<td>3</td>
<td>[-10, -5]</td>
<td>[5, 10]</td>
<td>\top</td>
</tr>
<tr>
<td>4</td>
<td>[-10, -5]</td>
<td>[5, 10]</td>
<td>{&amp;x}</td>
</tr>
<tr>
<td>5</td>
<td>[-10, -5]</td>
<td>[5, 10]</td>
<td>\top</td>
</tr>
<tr>
<td>6</td>
<td>[-10, -5]</td>
<td>[5, 10]</td>
<td>{&amp;y}</td>
</tr>
<tr>
<td>7</td>
<td>[-10, -5]</td>
<td>[5, 10]</td>
<td>{&amp;x, &amp;y}</td>
</tr>
<tr>
<td>8</td>
<td>[-10, 0]</td>
<td>[0, 10]</td>
<td>{&amp;x, &amp;y}</td>
</tr>
</tbody>
</table>

\textbf{Imprecise results}

- The abstract information about both \( x \) and \( y \) are weakened
- The fact that \( x \neq y \) is lost
Weak-updates

We can formalize this imprecision a bit more:

**Weak updates**

- The modified concrete cell cannot be uniquely mapped into a well identified abstract cell that describes only it.
- The resulting abstract information is obtained by joining the new value and the old information.

**Effect in pointer analysis**, in the case of an assignment:

- If the points-to set contains **exactly one element**, the analysis can perform a strong update.
  As in the first example: \( p \Rightarrow \{&x\} \)

- If the points-to set may contain **more than one element**, the analysis needs to perform a weak-update.
  As in the second example: \( p \Rightarrow \{&x, &y\} \)
Pointer aliasing based on equivalence on access paths

Aliasing relation

Given \( m = (e, h) \), pointers \( p \) and \( q \) are aliases iff \( h(e(p)) = h(e(q)) \)

Abstraction to infer pointer aliasing properties

- An access path describes a sequence of dereferences to resolve an l-value (i.e., an address); e.g.:

  \[
  a ::= x \mid a \cdot f \mid \ast a
  \]

- An abstraction for aliasing is an over-approximation for equivalence relations over access paths

Examples of aliasing abstractions:

- set abstractions: map from access paths to their equivalence class
  (ex: \( \{\{p_0, p_1, &x\}, \{p_2, p_3\}, \ldots\} \) )

- numerical relations, to describe aliasing among paths of the form \( x(-\rightarrow n)^k \)
  (ex: \( \{x(-\rightarrow n)^k, (x(-\rightarrow n)^{k+1}) \mid k \in \mathbb{N}\} \) )
Limitation of basic pointer analyses seen so far

Weak updates:
- imprecision in updates that spread out as soon as points-to set contain several elements
- impact client analyses severely (e.g., low precision on numerical)

Unsatisfactory abstraction of unbounded memory:
- common assumption that $C^\#$ be finite
- programs using dynamic allocations often perform unbounded numbers of malloc calls (e.g., allocation of a list)

Unable to express well structural invariants:
- for instance, that a structure should be a list, a tree...
- very indirect abstraction in numeric / path equivalence abstraction

A common solution: shape abstraction
Outline

1 Memory models

2 Pointer Abstractions

3 Separation Logic

4 A shape abstract domain relying on separation

5 Standard static analysis algorithms

6 Conclusion

7 Internships
Separation logic principle: avoid weak updates

How to deal with weak updates?

Avoid them!

- Always materialize exactly the cell that needs to be modified.
- Can be very costly to achieve, and not always feasible.

- Notion of property that holds over a memory region: special separating conjunction operator $\ast$

- Local reasoning:
  powerful principle, which allows to consider only part of the memory

- Separation logic has been used in many contexts, including manual verification, static analysis, etc...
Two kinds of formulas:
- **pure formulas** behave like formulas in first-order logic, i.e., are not attached to a memory region
- **spatial formulas** describe properties attached to a memory region

**Pure formulas** denote value properties

\[
\begin{align*}
e & ::= n \quad (n \in \mathbb{N}) & \text{constants} \\
& | 1 & \text{l-value} \\
& | e_0 + e_1 & \text{binary operations} \\
& | \ldots \\

P & ::= e_0 = e_1 \mid P' \lor P'' \mid P' \land P'' \ldots & \text{pure predicates}
\end{align*}
\]

**Pure formulas semantics:** \( \gamma(P) \subseteq \mathbb{E} \times \mathbb{M} \)
Separation logic: points-to predicates

The next slides introduce the main separation logic formulas \( F ::= \ldots \)

We start with the most basic predicate, that describes a single cell:

**Points-to predicate**

- **Predicate:**
  \[
  F ::= \ldots | \ a \mapsto v \quad \text{where } a \text{ is an address and } v \text{ is a value}
  \]

- **Concretization:**
  \[
  (e, h) \in \gamma(l \mapsto v) \quad \text{if and only if} \quad h = [[1]](e, h) \mapsto v
  \]

- **Example:**
  \[
  F = &x \mapsto 18 \quad \quad \text{&x = 308} \quad \begin{array}{c}
  \hline
  & 18 \\
  \hline
  \end{array}
  \]

  We also note \( l \mapsto e \), as an l-value \( l \) denotes an address.
Separation logic: separating conjunction

**Merge of concrete heaps:** let \( h_0, h_1 \in (\forall \text{addr} \to \forall) \), such that \( \text{dom}(h_0) \cap \text{dom}(h_1) = \emptyset \); then, we let \( h_0 \otimes h_1 \) be defined by:

\[
\begin{align*}
h_0 \otimes h_1 : & \quad \text{dom}(h_0) \cup \text{dom}(h_1) \to \forall \\
& \quad x \in \text{dom}(h_0) \quad \mapsto h_0(x) \\
& \quad x \in \text{dom}(h_1) \quad \mapsto h_1(x)
\end{align*}
\]

**Separating conjunction**

- **Predicate:**

\[
F ::= \ldots | F_0 \ast F_1
\]

- **Concretization:**

\[
\gamma(F_0 \ast F_1) = \{(e, h_0 \otimes h_1) \mid (e, h_0) \in \gamma(F_0) \land (e, h_1) \in \gamma(F_1)\}
\]
An example

Concrete memory layout
(pointer values underlined)

<table>
<thead>
<tr>
<th>address</th>
<th>&amp;x = 300</th>
<th>304</th>
<th>&amp;y = 308</th>
<th>308</th>
<th>&amp;z = 312</th>
<th>312</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>64</td>
<td>312</td>
<td>312</td>
<td>312</td>
<td>88</td>
<td>312</td>
</tr>
<tr>
<td></td>
<td>0x0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A formula that abstracts away the addresses:

\[ &x \mapsto \langle 64, &z \rangle \ast &y \mapsto &z \ast &z \mapsto \langle 88, 0 \rangle \]
Separation logic: non separating conjunction

We can also add the **conventional conjunction operator**, with its **usual concretization**:

### Non separating conjunction

- **Predicate:**
  \[
  F ::= \ldots \mid F_0 \land F_1
  \]

- **Concretization:**
  \[
  \gamma(F_0 \land F_1) = \gamma(F_0) \cap \gamma(F_1)
  \]

**Exercise:** describe and compare the concretizations of

- \&a \mapsto \&b \land \&b \mapsto \&a
- \&a \mapsto \&b \ast \&b \mapsto \&a
Separating conjunction vs non separating conjunction

- **Classical conjunction**: properties for the same memory region
- **Separating conjunction**: properties for disjoint memory regions

\[
\&a \mapsto \&b \land \&b \mapsto \&a
\]
- the same heap verifies \(\&a \mapsto \&b\) and \(\&b \mapsto \&a\)
- there can be only one cell
- thus \(a = b\)

\[
\&a \mapsto \&b \ast \&b \mapsto \&a
\]
- two separate sub-heaps respectively satisfy \(\&a \mapsto \&b\) and \(\&b \mapsto \&a\)
- thus \(a \neq b\)

Separating conjunction and non-separating conjunction have very different properties
- Both express very different properties
  e.g., no ambiguity on weak / strong updates
Separating and non separating conjunction

Logic rules of the two conjunction operators of SL:

- **Separating conjunction:**

  \[
  (e, h_0) \in \gamma(F_0) \quad (e, h_1) \in \gamma(F_1) \\
  \quad \quad \Rightarrow \quad (e, h_0 \otimes h_1) \in \gamma(F_0 \ast F_1)
  \]

- **Non separating conjunction:**

  \[
  (e, h) \in \gamma(F_0) \quad (e, h) \in \gamma(F_1) \\
  \quad \quad \Rightarrow \quad (e, h) \in \gamma(F_0 \land F_1)
  \]

Reminiscent of Linear Logic [Girard87]:
resource aware / non resource aware conjunction operators
Separation logic: empty store

Empty store

- **Predicate:**
  \[ F ::= \ldots | \text{emp} \]

- **Concretization:**
  \[ \gamma(\text{emp}) = \{(e, []) | e \in \mathbb{E}\} = \mathbb{E} \times \{[]\} \]

  where [] denotes the empty store

- **emp** is the **neutral element for** \( \ast \)
  (monoid structure induced by \( \ast \))

- by contrast the **neutral element for** \( \land \) is \text{TRUE}, with concretization:
  \[ \gamma(\text{TRUE}) = \mathbb{E} \times \mathbb{H} \]
Separation logic: other connectors

**Disjunction:**

- $F ::= \ldots | F_0 \lor F_1$
- concretization:
  $$\gamma(F_0 \lor F_1) = \gamma(F_0) \cup \gamma(F_1)$$

**Spatial implication (aka, magic wand):**

- $F ::= \ldots | F_0 \rightarrow^* F_1$
- concretization:
  $$\gamma(F_0 \rightarrow^* F_1) = \{(e, h) | \forall h_0 \in \mathbb{H}, (e, h_0) \in \gamma(F_0) \implies (e, h \otimes h_0) \in \gamma(F_1)\}$$

- very powerful connector to describe **structure segments**, used in complex SL proofs
Summary of the main separation logic constructions seen so far:

### Separation logic main connectors

- \( \gamma(\text{emp}) = E \times \{[]\} \)
- \( \gamma(\text{TRUE}) = E \times H \)
- \( \gamma(1 \mapsto v) = \{(e, [[[1]](e, h) \mapsto v]) | e \in E\} \)
- \( \gamma(F_0 \ast F_1) = \{(e, h_0 \oplus h_1) | (e, h_0) \in \gamma(F_0) \land (e, h_1) \in \gamma(F_1)\} \)
- \( \gamma(F_0 \land F_1) = \gamma(F_0) \cap \gamma(F_1) \)
- \( \gamma(F_0 \rightarrow F_1) = \{(e, h) | \forall h_0 \in H, (e, h_0) \in \gamma(F_0) \Rightarrow (e, h \otimes h_0) \in \gamma(F_1)\} \)

Concretization of pure formulas is standard

**How does this help for program reasoning?**
Separation logic triple

Program proofs based on Hoare triples

- **Notation:** \( \{F\}p\{F'\} \) if and only if:
  \[
  \forall s, s' \in S, \ s \in \gamma(F) \land s' \in [p](s) \implies s' \in \gamma(F')
  \]

- **Application:** formalize proofs of programs

A few rules (straightforward proofs):

\[
\begin{align*}
  F_0 \implies F'_0 & \quad \{F'_0\}b\{F'_1\} & \quad F'_1 \implies F_1 & \quad \text{consequence} \\
  \{F_0\}b\{F_1\} & \quad \{\&x \mapsto ?\}x := e\{\&x \mapsto e\} & \quad \text{mutation} \\
  x \text{ does not appear in } F & \quad \{\&x \mapsto ? \ast F\}x := e\{\&x \mapsto e \ast F\} & \quad \text{mutation-2}
\end{align*}
\]

(we assume that \( e \) does not allocate memory)
The frame rule

What about the resemblance between rules “mutation” and “mutation-2”?

**Theorem: the frame rule**

\[
\text{freevar}(F) \cap \text{write}(b) = \emptyset \\
\{F_0 \ast F\}b\{F_1 \ast F\} \\
\frac{\{F_0\}b\{F_1\}}{} \quad \text{frame}
\]

- Proof by induction on the logical rules on program statements, *i.e.*, essentially a large case analysis
  (see biblio for a more complete set of rules)
- Rules are proved by case analysis on the program syntax

The frame rule allows to reason locally about programs
Application of the frame rule

A program with intermittent invariants, derived using the frame rule, since each step impacts a disjoint region:

```plaintext
int i;
int * x;
int * y;
{&i ↦? * &x ↦? * &y ↦?}
x = &i;
{&i ↦? * &x ↦ &i * &y ↦?}
y = &i;
{&i ↦? * &x ↦ &i * &y ↦ &i}
*x = 42;
{&i ↦ 42 * &x ↦ &i * &y ↦ &i}
```

Many other program proofs done using separation logic e.g., verification of the Deutsch-Shorr-Waite algorithm (biblio)
Summarization and inductive definitions

What do we still miss?

So far, formulas denote **fixed sets of cells**
Thus, no summarization of unbounded regions...

**Example** all lists pointed to by \( x \), such as:

How to precisely abstract these stores with a single formula
* i.e., no infinite disjunction ?
Inductive definitions in separation logic

List definition

\[ \alpha \cdot \text{list} := \begin{cases} \alpha = 0 \land \text{emp} \lor \alpha \neq 0 \land \alpha \cdot \text{next} \mapsto \delta \ast \alpha \cdot \text{data} \mapsto \beta \ast \delta \cdot \text{list} \end{cases} \]

- Formula abstracting our set of structures:
  \[ \&x \mapsto \alpha \ast \alpha \cdot \text{list} \]
- **Summarization:**
  this formula is finite and describe infinitely many heaps
- **Concretization:** next slide...

Practical implementation in verification/analysis tools

- **Verification:** hand-written definitions
- **Analysis:** either built-in or user-supplied, or partly inferred
Concretization by unfolding

**Intuitive semantics of inductive predicates**

- Inductive predicates can be **unfolded**, by **unrolling their definitions**
  - Syntactic unfolding is noted $\mathcal{U}$
- A formula $F$ with inductive predicates describes all stores described by all formulas $F'$ such that $F \xrightarrow{\mathcal{U}} F'$

**Example:**

- Let us start with $x \mapsto \alpha_0 \ast \alpha_0 \cdot \text{list}$; we can unfold it as follows:
  
  $\&x \mapsto \alpha_0 \ast \alpha_0 \cdot \text{list}$
  
  $\xrightarrow{\mathcal{U}} \quad \&x \mapsto \alpha_0 \ast \alpha_0 \cdot \text{next} \mapsto \alpha_1 \ast \alpha_0 \cdot \text{data} \mapsto \beta_1 \ast \alpha_1 \cdot \text{list}$
  
  $\xrightarrow{\mathcal{U}} \quad \&x \mapsto \alpha_0 \ast \alpha_0 \cdot \text{next} \mapsto \alpha_1 \ast \alpha_0 \cdot \text{data} \mapsto \beta_1 \ast \text{emp} \land \alpha_1 = 0x0$

- We get the concrete state below:
Example: tree

Example:

\[
\begin{align*}
\alpha \cdot \text{tree} & := \\
\alpha & = 0 \land \text{emp} \\
\lor \alpha & \neq 0 \land \alpha \cdot \text{left} \mapsto \beta \ast \alpha \cdot \text{right} \mapsto \delta \\
\ast \beta \cdot \text{tree} \ast \delta \cdot \text{tree}
\end{align*}
\]
Example: doubly linked list

![Diagram of a doubly linked list]

**Example:**

$$\alpha \cdot dll(\delta) := \begin{cases} \alpha = 0 \land emp \\ \vee \alpha \neq 0 \land \alpha \cdot next \mapsto \beta \ast \alpha \cdot prev \mapsto \delta \\ \ast \beta \cdot dll(\alpha) \end{cases}$$
Example: sortedness

- **Example:** sorted list

  ![Sorted list diagram]

Inductive definition

- Each element should be greater than the previous one
- The first element simply needs be greater than $-\infty$...
- We need to propagate the lower bound, using a scalar parameter

\[
\alpha \cdot \text{lsort}_{\text{aux}}(n) \\
= \begin{cases} \\
\alpha = 0 \land \text{emp} \\
\lor \alpha \neq 0 \land n \leq \beta \land \alpha \cdot \text{next} \mapsto \delta \\
\ast \alpha \cdot \text{data} \mapsto \beta \ast \delta \ast \text{lsort}_{\text{aux}}(\beta) \\
\end{cases}
\]

\[
\alpha \cdot \text{lsort}() \\
= \alpha \cdot \text{lsort}_{\text{aux}}(-\infty)
\]
Outline

1. Memory models
2. Pointer Abstractions
3. Separation Logic
4. A shape abstract domain relying on separation
5. Standard static analysis algorithms
6. Conclusion
7. Internships
A lot of things are missing to turn SL into an abstract domain

Set of logical predicates:

- separation logic formulas are very expressive
  e.g., arbitrary alternations of $\land$ and $\ast$
- such expressiveness is not necessarily required in static analysis

Representation:

- unstructured formulas can be represented as ASTs,
  but this representation is not easy to manipulate efficiently
- intuition over memory states typically involves graphs

Analysis algorithms:

- inference of “optimal” invariants in SL, with numerical predicates obviously not computable
Basic abstraction: structures and their contents (1/2)

- **Concrete memory states**
  - very low level description
    - numeric offsets / field names
  - pointers, numeric values:
    - raw sequences of bits

\[
\begin{align*}
&(x \cdot n) = 0x\ldots a_0 & 17 \\
&(x \cdot d) = 0x\ldots a_4 & 0x\ldots b_0 \\
&(y \cdot n) = 0x\ldots b_0 & 17 \\
&(y \cdot d) = 0x\ldots b_4 & 0x0
\end{align*}
\]
Basic abstraction: structures and their contents (1/2)

- **Concrete memory states**

- **Abstraction of values into symbolic variables** (nodes)

  - characterized by **valuation** $\nu$
  - $\nu$ maps **symbolic variables** into **concrete addresses**

  
  $\nu(\alpha_0) = 0x...a0$
  $\nu(\alpha_1) = 17$
  $\nu(\alpha_2) = 0x...b0$
  $\nu(\alpha_3) = 17$
  $\nu(\alpha_4) = 0x0$
Basic abstraction: structures and their contents (1/2)

- Concrete memory states

- Abstraction of values into symbolic variables / nodes

- Abstraction of regions into points-to edges

\[ \nu(\alpha_0) = 0x\ldots a0 \]
\[ \nu(\alpha_1) = 17 \]
\[ \nu(\alpha_2) = 0x\ldots b0 \]
\[ \nu(\alpha_3) = 17 \]
\[ \nu(\alpha_4) = 0x0 \]
Basic abstraction: structures and their contents (1/2)

- **Concrete memory states**

- **Abstraction of values into symbolic variables / nodes**

- **Abstraction of regions into points-to edges**

- **Shape graph concretization**

\[ \gamma_{sh}(G) = \{(h, \nu) \mid \ldots\} \]

valuation \( \nu \) plays an important role to combine abstraction...
Structure of shape graphs

Valuations bridge the gap between nodes and values

Symbolic variables / nodes and intuitively abstract concrete values:

Symbolic variables

We let \( \mathbb{V}^\# \) denote a countable set of symbolic variables; we usually let them be denoted by Greek letters in the following: \( \mathbb{V}^\# = \{ \alpha, \beta, \delta, \ldots \} \)

When concretizing a shape graph, we need to characterize how the concrete instance evaluates each symbolic variable, which is the purpose of the valuation functions:

Valuations

A valuation is a function from symbolic variables into concrete values (and is often denoted by \( \nu \)): \( \text{Val} = \mathbb{V}^\# \to \mathbb{V} \)

Note that valuations treat in the same way addresses and raw values
Structure of shape graphs

Distinct edges describe separate regions

In particular, if we **split** a graph into **two parts**:

**Separating conjunction**

\[
\gamma_{\text{sh}}(S_0 \times S_1) = \{(f_0 \otimes f_1, \nu) \mid (f_0, \nu) \in \gamma_{\text{sh}}(S_0) \land (f_1, \nu) \in \gamma_{\text{sh}}(S_1)\}
\]

Similarly, when considering the **empty set of edges**, we get the empty heap (where \(\mathbb{V}^\#\) is the set of nodes):

\[
\gamma_{\text{sh}}(\text{emp}) = \{(\emptyset, \nu) \mid \nu : \mathbb{V}^\# \rightarrow \mathbb{V}\}
\]
A single points-to edge represents one heap cell

A points-to edge encodes basic points to predicate in separation logic:

Points-to edges

- Syntax

  Graph edge: \( \alpha \xrightarrow{f} \beta \)
  Separation logic formula: \( \alpha \cdot f \rightarrow \beta \)
  Concrete view:
  \[
  \nu(\alpha) \quad \text{offset}(f) \quad \nu(\beta)
  \]

- Concretization:

  \[
  \gamma_{sh}(\alpha \cdot f \rightarrow \beta) = \{ ([\nu(\alpha) + \text{offset}(f) \rightarrow \nu(\beta)], \nu) \mid \nu : \{\alpha, \beta, \ldots\} \rightarrow \mathbb{N} \} \]
Abstraction of contiguous regions

Contiguous regions are described by adjacent points-to edges

To describe **blocks** containing series of **cells** (e.g., in a **C structure**), shape graphs utilize several outgoing edges from the node representing the base address of the block.

Field splitting model

- Separation impacts edges / fields, *not pointers*

  - Shape graph accounts for both abstract states below:

  \[
  \nu(\alpha)_{\text{offset}(f)} = \nu(\beta_0) = \nu(\beta_1)
  \]

  \[
  \nu(\alpha)_{\text{offset}(g)} = \nu(\beta_0) = \nu(\beta_1)
  \]

In other words, in a field splitting model, separation:

- asserts addresses are distinct
- says nothing about contents
A shape abstract domain relying on separation

Abstraction of the environment

Environments bind variables to their (concrete / abstract) address

\[ \begin{align*}
&x &= & (x \cdot n) = 0x...a0 \\
& & & (x \cdot d) = 0x...a4 \\
&y &= & (y \cdot n) = 0x...b0 \\
& & & (y \cdot d) = 0x...b4
\end{align*} \]

\[ \begin{array}{c|c}
17 & 17 \\
0x...b0 & 0x0
\end{array} \]

\[ \begin{array}{ccc}
\alpha_0 & \alpha_1 \\
\alpha_2 & \alpha_3 \\
\alpha_4 & \\
\end{array} \]

\[ e^\# : 
\begin{align*}
x & \mapsto \alpha_0 \quad (\nu \mapsto 0x...a0) \\
y & \mapsto \alpha_2 \quad (\nu \mapsto 0x...b0)
\end{align*} \]

\[ \nu : \alpha_0 \mapsto 0x...a0 \\
\alpha_2 \mapsto 0x...b0 \\
\ldots \mapsto \ldots \]

Abstract environments

- An **abstract environment** is a function \( e^\# \) from variables to symbolic nodes
- The **concretization** extends as follows:

\[ \gamma_{mem}(e^\#, S^\#) = \{ (e, h, \nu) | (h, \nu) \in \gamma_{sh}(S^\#) \land e = \nu \circ e^\# \} \]
A shape abstract domain relying on separation

Basic abstraction: summarization

Set of all lists of any length:

\[ \& x \ 0x0 \quad \& x \ 0x... \quad \& x \ 0x...
\]

Well-founded list inductive def.

\[ \alpha \cdot \text{list} := \\
(\text{emp} \land \alpha = 0x0) \lor \\
(\alpha \cdot d \mapsto \beta_0 \ast \alpha \cdot n \mapsto \beta_1 \ast \beta_1 \cdot \text{list} \land \alpha \neq 0x0) \]

well-founded predicate

Inductive summary predicates

Concretization based on unfolding and least-fixpoint:

- \[ \overset{U}{\longrightarrow} \] replaces an \( \alpha \cdot \text{list} \) predicate with one of its premises

\[ \gamma(S^\#, F) = \bigcup \{ \gamma(S^\#_u, F_u) \mid (S^\#, F) \overset{U}{\longrightarrow} (S^\#_u, F_u) \} \]
Inductive structures: a few instances

As before, many interesting inductive predicates encode nicely into graph inductive definitions:

- **More complex shapes: trees**

- **Relations among pointers: doubly-linked lists**

- **Relations between pointers and numerical: sorted lists**
Inductive segments

A frequent pattern:

\[ \&x \mapsto \alpha \star \alpha \cdot \text{list} \]

\[ \&y \mapsto \beta \star \beta \cdot \text{list} \]

A first attempt:

- \( x \) points to a list, so \( \&x \mapsto \alpha \star \alpha \cdot \text{list} \) holds
- \( y \) points to a list, so \( \&y \mapsto \beta \star \beta \cdot \text{list} \) holds

However, the following does not hold

\[ \&x \mapsto \alpha \star \alpha \cdot \text{list} \star \&y \mapsto \beta \star \beta \cdot \text{list} \]

Why? violation of separation!

A second attempt:

\[(\&x \mapsto \alpha \star \alpha \cdot \text{list} \star \text{TRUE}) \land (\&y \mapsto \beta \star \beta \cdot \text{list} \star \text{TRUE})\]

Why is it still not all that good? relation lost!
A frequent pattern:

Could be **expressed directly** as an inductive with a parameter:

\[
\alpha \cdot \text{list}_\text{endp}(\pi) \ := \ \begin{cases} 
\text{emp}, \alpha = \pi \\
\alpha \cdot \text{next} \leftrightarrow \beta_0 \ast \alpha \cdot \text{data} \leftrightarrow \beta_1 \\
\ast \beta_0 \cdot \text{list}_\text{endp}(\pi), \alpha \neq 0
\end{cases}
\]

This definition **straightforwardly derives** from list
Thus, we make **segments** part of the **fundamental predicates of the domain**

**Multi-segments**: possible, but harder for analysis
Shape graphs and separation logic

Semantic preserving translation $\Pi$ of graphs into separation logic formulas:

<table>
<thead>
<tr>
<th>Graph $S^# \in D^#_{\text{sh}}$</th>
<th>Translated formula $\Pi(S^#)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha \xrightarrow{f} \beta$</td>
<td>$\alpha \cdot f \mapsto \beta$</td>
</tr>
<tr>
<td>$S_0^#$ and $S_1^#$</td>
<td>$\Pi(S_0^#) \ast \Pi(S_1^#)$</td>
</tr>
<tr>
<td>$\alpha \xrightarrow{\text{list}}$</td>
<td>$\alpha \cdot \text{list}$</td>
</tr>
<tr>
<td>$\alpha \xrightarrow{\text{list}}\delta$</td>
<td>$\alpha \cdot \text{list}_\text{endp}(\delta)$</td>
</tr>
<tr>
<td>other inductives and segments</td>
<td>similar</td>
</tr>
</tbody>
</table>

Note that:
- shape graphs can be encoded into separation logic formula
- the opposite is usually not true

Value information:
- discussed in the next course
- intuitively, assume we maintain numerical information next to shape graphs
Outline

1. Memory models
2. Pointer Abstractions
3. Separation Logic
4. A shape abstract domain relying on separation
5. Standard static analysis algorithms
   - Overview of the analysis
   - Post-conditions and unfolding
   - Folding: widening and inclusion checking
   - Abstract interpretation framework: assumptions and results
6. Conclusion
7. Internships
Static analysis overview

**A list insertion function:**

\[
\text{list } \ast l \text{ assumed to point to a list} \\
\text{list } \ast t \text{ assumed to point to a list element} \\
\text{list } \ast c = l; \\
\text{while}(c \neq \text{NULL} \&\& c \rightarrow \text{next} \neq \text{NULL} \&\& (\ldots))\{
\text{c} = c \rightarrow \text{next}; \\
\} \\
t \rightarrow \text{next} = c \rightarrow \text{next}; \\
c \rightarrow \text{next} = t;
\]

- **list** inductive structure def.
- Abstract precondition:

\[
\begin{align*}
&\begin{array}{c}
&\text{l} \\
&\text{list} \\
&\text{next} \\
&\text{data} \\
&\text{t}
\end{array}
\end{align*}
\]

Result of the (interprocedural) analysis

- **Over-approximations** of reachable concrete states
  e.g., after the insertion:
Transfer functions

Abstract interpreter design

- **Follows the semantics** of the language under consideration
- The abstract domain should provide **sound transfer functions**

Transfer functions:

- **Assignment**: $x \rightarrow f = y \rightarrow g$ or $x \rightarrow f = e_{\text{arith}}$
- **Test**: analysis of conditions (if, while)
- Variable **creation** and **removal**
- **Memory management**: malloc, free

Abstract operators:

- **Join** and **widening**: over-approximation
- **Inclusion checking**: check stabilization of abstract iterates

Should be **sound**, i.e., not forget any concrete behavior
Abstract operations

Denotational style abstract interpreter

- Concrete **denotational semantics** $\llbracket b \rrbracket : S \rightarrow P(S)$
- **Abstract post-condition** $\llbracket b \rrbracket^\#(S)$, computed by the analysis:

$$s \in \gamma(S) \implies \llbracket b \rrbracket(s) \subseteq \gamma(\llbracket b \rrbracket^\#(S))$$

Analysis by induction on the syntax using **domain operators**

$$\begin{align*}
\llbracket b_0; b_1 \rrbracket^\#(S) &= \llbracket b_1 \rrbracket^\# \circ \llbracket b_0 \rrbracket^\#(S) \\
\llbracket l = e \rrbracket^\#(S) &= \text{assign}(l, e, S) \\
\llbracket l = \text{malloc}(n) \rrbracket^\#(S) &= \text{alloc}(l, n, S) \\
\llbracket \text{free}(l) \rrbracket^\#(S) &= \text{free}(l, n, S) \\
\llbracket \text{if}(e) \ b_t \ \text{else} \ b_f \rrbracket^\#(S) &= \begin{cases} 
\text{join}(\llbracket b_t \rrbracket^\#(\text{test}(e, S))), \\
\llbracket b_f \rrbracket^\#(\text{test}(e = \text{false}, S))) 
\end{cases} \\
\llbracket \text{while}(e) \ b \rrbracket^\#(S) &= \text{test}(e = \text{false}, \text{ifp}^\#_S F^\#) \\
\text{where, } F^\#: S_0 &\mapsto \llbracket b \rrbracket^\#(\text{test}(e, S_0))
\end{align*}$$
The algorithms underlying the transfer functions

- **Unfolding**: cases analysis on summaries

  \[
  \begin{align*}
  x &\xrightarrow{\text{list}} y \\ x &\xrightarrow{\text{list}} y
  \end{align*}
  \Rightarrow
  \begin{align*}
  x &\xrightarrow{\text{list}} y \\ x &\xrightarrow{\text{next}} y \\ y &\xrightarrow{\text{list}} y
  \end{align*}
  \]

- **Abstract postconditions**, on “exact” regions, e.g. insertion

  \[
  \begin{align*}
  x &\xrightarrow{\text{list}} y \\ x &\xrightarrow{\text{next}} y \\
  y &\xrightarrow{\text{data}} list
  \end{align*}
  \Rightarrow
  \begin{align*}
  x &\xrightarrow{\text{list}} y \\ x &\xrightarrow{\text{next}} y \\ y &\xrightarrow{\text{data}} list
  \end{align*}
  \]

- **Widening**: builds summaries and ensures termination

  \[
  \begin{align*}
  x &\xrightarrow{\text{list}} y \\ x &\xrightarrow{\text{list}} y
  \end{align*}
  \n  \Rightarrow
  \begin{align*}
  x &\xrightarrow{\text{list}} y \\ x &\xrightarrow{\text{next}} y \\ y &\xrightarrow{\text{data}} list
  \end{align*}
  \]

\[
\begin{align*}
\end{align*}
\]
Outline

1. Memory models
2. Pointer Abstractions
3. Separation Logic
4. A shape abstract domain relying on separation
5. Standard static analysis algorithms
   - Overview of the analysis
   - Post-conditions and unfolding
   - Folding: widening and inclusion checking
   - Abstract interpretation framework: assumptions and results
6. Conclusion
7. Internships
Analysis of an assignment in the graph domain

Steps for analyzing $x = y \rightarrow \text{next}$ (local reasoning)

1. Evaluate l-value $x$ into points-to edge $\alpha \mapsto \beta$
2. Evaluate r-value $y \rightarrow \text{next}$ into node $\beta'$
3. Replace points-to edge $\alpha \mapsto \beta$ with points-to edge $\alpha \mapsto \beta'$

With pre-condition:

- Step 1 produces $\alpha_0 \mapsto \beta_0$
- Step 2 produces $\beta_2$
- End result:

With pre-condition:

- Step 1 produces $\alpha_0 \mapsto \beta_0$
- Step 2 fails
- Abstract state too abstract
- We need to refine it
Unfolding as a local case analysis

Unfolding principle

- **Case analysis**, based on the inductive definition
- Generates *symbolic disjunctions* (analysis performed in a *disjunction domain*, e.g., trace partitioning)

Example, for lists:

\[ \alpha \xrightarrow{\text{list}} \]  \[ \U \]  \[ \alpha \xrightarrow{\text{alpha} = 0} \]

\[ \alpha \xrightarrow{\text{list}} \]  \[ \U \]  \[ \alpha \xrightarrow{\text{alpha} \neq 0} \]

- **Numeric predicates**: next course on shape + value abstraction

Soundness: by definition of the concretization of inductive structures

\[ \gamma_{\text{sh}}(S^\#) \subseteq \bigcup \{ \gamma_{\text{sh}}(S_0^\#) | S^\# \xrightarrow{\U} S_0^\# \} \]
Analysis of an assignment, with unfolding

**Principle**

- We have $\gamma_{sh}(\alpha \cdot \iota) = \bigcup \{ \gamma_{sh}(S^\#) \mid \alpha \cdot \iota \mathrel{\mathcal{U}} S^\# \}$
- Replace $\alpha \cdot \iota$ with a finite number of disjuncts and continue

**Disjunct 1:**

- Step 1 produces $\alpha_0 \mapsto \beta_0$
- Step 2 fails: Null pointer!
- In a **correct** program, would be ruled out by a condition $y \neq 0$
  
  i.e., $\beta_1 \neq 0$ in $D_{num}^\#$

**Disjunct 2:**

- Step 1 produces $\alpha_0 \mapsto \beta_0$
- Step 2 produces $\beta_2$
- **End result:**

Standard static analysis algorithms

Unfolding and degenerated cases

assume(l points to a dll)
c = l;
① while(c ≠ NULL && condition)
   c = c -> next;
② if(c ≠ 0 && c -> prev ≠ 0)
   c = c -> prev → prev;

⇒ non trivial unfolding

Materialization of c -> prev:

Segment splitting lemma: basis for segment unfolding

Materialization of c -> prev -> prev:

Implementation issue: discover which inductive edge to unfold very hard!
Outline

1. Memory models
2. Pointer Abstractions
3. Separation Logic
4. A shape abstract domain relying on separation
5. **Standard static analysis algorithms**
   - Overview of the analysis
   - Post-conditions and unfolding
   - Folding: widening and inclusion checking
   - Abstract interpretation framework: assumptions and results
6. Conclusion
7. Internships
Need for a folding operation

Back to the list traversal example:

**First iterates** in the loop:
- at iteration 0 (before entering the loop):
  
  \[ l, c \]

- at iteration 1:
  
  \[ \text{assume}(l \text{ points to a list}) \]
  
  
  \[ c = l; \]
  
  \[ \text{while}(c \neq \text{NULL}){ \}
  
  \[ c = c \rightarrow \text{next}; \]

- at iteration 2:
  
  The analysis **unfolds**, but **never folds**:

  \[ S_0 \rightarrow S_1 \rightarrow S_2 \ldots \]

  How to guarantee **termination** of the analysis?  
  How to **introduce segment edges / perform abstraction**?
Widening

- The lattice of shape abstract values has **infinite height**
- Thus iteration sequences **may not terminate**

**Definition of a widening operator $\nabla$**

- **Over-approximates join:**

  \[
  \begin{align*}
  \gamma(X^\#) & \subseteq \gamma(X^\# \nabla Y^\#) \\
  \gamma(Y^\#) & \subseteq \gamma(X^\# \nabla Y^\#)
  \end{align*}
  \]

- **Enforces termination:** for all sequence $(X^\#_n)_{n \in \mathbb{N}}$, the sequence $(Y^\#_n)_{n \in \mathbb{N}}$ defined below is ultimately stationary

  \[
  \begin{align*}
  Y^\#_0 & = X^\#_0 \\
  \forall n \in \mathbb{N}, \quad Y^\#_{n+1} & = Y^\#_n \nabla X^\#_{n+1}
  \end{align*}
  \]
Canonicalization

Upper closure operator

\[ \rho : \mathbb{D}^\# \rightarrow \mathbb{D}^\#_{\text{can}} \subseteq \mathbb{D}^\# \] is an upper closure operator (uco) iff it is monotone, extensive and idempotent.

Canonicalization

- **Disjunctive completion:** \( \mathbb{D}^\#_{\vee} \) = finite disjunctions over \( \mathbb{D}^\# \)
- **Canonicalization operator** \( \rho_{\vee} \) defined by \( \rho_{\vee} : \mathbb{D}^\#_{\vee} \rightarrow \mathbb{D}^\#_{\text{can} \vee} \) and \( \rho_{\vee}(X^\#) = \{ \rho(x^\#) \mid x^\# \in X^\# \} \) where \( \rho \) is an uco and \( \mathbb{D}^\#_{\text{can}} \) is finite

- Canonicalization is used in many shape analysis tools
- **Easier to compute** but **less powerful** than widening: does not exploit history of computation
Weakening: definition

To design inclusion test, join and widening algorithms, we first study a more general notion of weakening:

**Weakening**

We say that $S_0^\#$ can be weakened into $S_1^\#$ if and only if

$$\forall (h, \nu) \in \gamma_{sh}(S_0^\#), \exists \nu' \in \text{Val}, (h, \nu') \in \gamma_{sh}(S_1^\#)$$

We then note $S_0^\# \preceq S_1^\#$

**Applications:**

- **inclusion test** (comparison) inputs $S_0^\#, S_1^\#$; if returns true $S_0^\# \preceq S_1^\#$
- **canonicalization** (unary weakening) inputs $S_0^\#$ and returns $\rho(S_0^\#)$ such that $S_0^\# \preceq \rho(S_0^\#)$
- **widening / join** (binary weakening ensuring termination or not) inputs $S_0^\#, S_1^\#$ and returns $S_{up}^\#$ such that $S_i^\# \preceq S_{up}^\#$
Weakening: example

We consider $S_0^\#$ defined by:

$\alpha_0$ & $\alpha_1$ & $\alpha_2$

$\alpha_1$ \text{ next} \to \alpha_2$

$\text{list}$

and $S_1^\#$ defined by:

$\beta_0$ & $\beta_1$

$\beta_1$ \text{ data} \to \alpha_2$

$\alpha_2$

$\text{list}$

Then, we have the weakening $S_0^\# \preceq S_1^\#$ up-to a renaming in $S_1^\#$:

$\Psi : \begin{align*}
\beta_0 & \mapsto \alpha_0 \\
\beta_1 & \mapsto \alpha_1
\end{align*}$

- weakening up-to renaming is generally required as graphs do not have the same name space
- formalized a bit later...
Local weakening: separating conjunction rule

We can apply the local reasoning principle to weakening

If $S_0 \equiv S_{0,\text{weak}}$ and $S_1 \equiv S_{1,\text{weak}}$ then:

\[
S_0 \circ S_1 \equiv S_{0,\text{weak}} \circ S_{1,\text{weak}}
\]

Separating conjunction rule ($\equiv^\ast$)

Let us assume that

- $S_0$ and $S_1$ have distinct set of source nodes
- we can weaken $S_0$ into $S_{0,\text{weak}}$
- we can weaken $S_1$ into $S_{1,\text{weak}}$

then:

we can weaken $S_0 \ast S_1$ into $S_{0,\text{weak}} \ast S_{1,\text{weak}}$
Local weakening: unfolding rule, identity rule

Weakening unfolded region ($\preceq_U$)

Let us assume that $S_0^\# \xrightarrow{U} S_1^\#$. Then, by definition of the concretization of unfolding

$$\text{we can weaken } S_1^\#\text{ into } S_0^\#$$

- the proof follows from the definition of unfolding
- it can be applied locally, on graph regions that differ due to unfolding of inductive definitions

Identity weakening ($\preceq_{\text{Id}}$)

$$\text{we can weaken } S^\#\text{ into } S^\#$$

- the proof is trivial:
  $$\gamma_{\text{sh}}(S^\#) \subseteq \gamma_{\text{sh}}(S^\#)$$
- on itself, this principle is not very useful, but it can be applied locally, and combined with ($\preceq_U$) on graph regions that are not equal
Local weakening: example

By rule ($\preceq_{\text{Id}}$):

Thus, by rule ($\preceq_{\text{U}}$):

Additionally, by rule ($\preceq_{\text{Id}}$):

Thus, by rule ($\preceq_{*}$):
Inclusion checking rules in the shape domain

Graphs to compare have distinct sets of nodes, thus inclusion check should carry out a **valuation transformer** \( \Psi : \forall^\#(S_1^\#) \rightarrow \forall^\#(S_0^\#) \) (important when dealing also with content values).

Using (and extending) the weakening principles, we obtain the following rules (considering only inductive definition **list**, though these rules would extend to other definitions straightforwardly):

- **Identity rules:**
  \[
  \forall i, \quad \Psi(\beta_i) = \alpha_i \quad \implies \quad \alpha_0 \cdot f \mapsto \alpha_1 \quad \not\subseteq^\#_\Psi \quad \beta_0 \cdot f \mapsto \beta_1 \\
  \Psi(\beta) = \alpha \quad \implies \quad \alpha \cdot \text{list} \quad \not\subseteq^\#_\Psi \quad \beta \cdot \text{list} \\
  \forall i, \quad \Psi(\beta_i) = \alpha_i \quad \implies \quad \alpha_0 \cdot \text{list}_\mathit{endp}(\alpha_1) \not\subseteq^\#_\Psi \quad \beta_0 \cdot \text{list}_\mathit{endp}(\beta_1)
  \]

- **Rules on inductives:**
  \[
  \forall i, \quad \Psi(\beta_i) = \alpha \quad \implies \quad \text{emp} \quad \not\subseteq^\#_\Psi \quad \beta_0 \cdot \text{list}_\mathit{endp}(\beta_1) \\
  S_0^\# \not\subseteq^\#_\Psi \quad S_1^\# \quad \beta \cdot \iota \quad \xrightarrow{u} \quad S_1^\# \quad \implies \quad S_0^\# \not\subseteq^\#_\Psi \quad \beta \cdot \iota \\
  \text{if } \beta_1 \text{ fresh, } \Psi' = \Psi[\beta_1 \mapsto \alpha_1] \text{ and } \Psi(\beta_0) = \alpha_0 \text{ then,} \\
  S_0^\# \not\subseteq^\#_\Psi \quad \beta_1 \cdot \text{list} \quad \implies \quad \alpha_0 \cdot \text{list}_\mathit{endp}(\alpha_1) \ast S_0^\# \not\subseteq^\#_\Psi \quad \beta_0 \cdot \iota
  \]
Inclusion checking algorithm

Comparison of \((e_0^\#, S_0^\#)\) and \((e_1^\#, S_1^\#)\)

1. start with \(\Psi\) defined by \(\Psi(\beta) = \alpha\) if and only if there exists a variable \(x\) such that \(e_0^\#(x) = \alpha \land e_1^\#(x) = \beta\)
2. iteratively apply local rules, and extend \(\Psi\) when needed
3. return \textbf{true} when both shape graphs become empty

- the first step ensures both environments are consistent

This algorithm is sound:

Soundness

\[(e_0^\#, S_0^\#) \equiv^\# (e_1^\#, S_1^\#) \implies \gamma(e_0^\#, S_0^\#) \subseteq \gamma(e_1^\#, S_1^\#)\]
Over-approximation of union

The principle of join and widening algorithm is similar to that of $\sqsubseteq^\#$:

- It can be computed region by region, as for weakening in general:
  
  If $\forall i \in \{0, 1\}$, $\forall s \in \{\text{lft}, \text{rgh}\}$, $S^\#_{i,s} \preceq S^\#_s$,

  $\Psi : \forall^\#(S^\#_{\text{lft}}) \times \forall^\#(S^\#_{\text{rgh}}) \rightarrow \forall^\#(S^\#)$

- The computation of the shape join progresses by the application of local join rules, that produce a new (output) shape graph, that weakens both inputs
Over-approximation of union: syntactic identity rules

In the next few slides, we focus on $\triangledown$
though the abstract union would be defined similarly in the shape domain.

Several rules derive from $(\preceq_{Id})$:

- If $S_{lft}^{\#} = \alpha_0 \cdot f \mapsto \alpha_1$
  and $S_{lft}^{\#} = \beta_0 \cdot f \mapsto \beta_1$
  and $\Psi(\alpha_0, \beta_0) = \delta_0$, $\Psi(\alpha_1, \beta_1) = \delta_1$, then:

\[
S_{lft}^{\#} \triangledown S_{rgh}^{\#} = \delta_0 \cdot f \mapsto \delta_1
\]

- If $S_{lft}^{\#} = \alpha_0 \cdot \text{list}$
  and $S_{lft}^{\#} = \beta_0 \cdot \text{list}_1$
  and $\Psi(\alpha_0, \beta_0) = \delta_0$, then:

\[
S_{lft}^{\#} \triangledown S_{rgh}^{\#} = \delta_0 \cdot \text{list}
\]
Over-approximation of union: segment introduction rule

Rule

if

\[ S_{\text{left}}^{\#} \bowtie S_{\text{right}}^{\#} = \delta_0 \text{ list} \to \delta_1 \]

then

\[ \begin{aligned}
(\alpha, \beta_0) &\leftrightarrow \psi \delta_0 \\
(\alpha, \beta_1) &\leftrightarrow \psi \delta_1 
\end{aligned} \]

Application to list traversal, at the end of iteration 1:

- **before iteration 0:**

- **end of iteration 0:**

- **join, before iteration 1:**

\[ \begin{aligned}
\Psi(\alpha_0, \beta_0) &= \delta_0 \\
\Psi(\alpha_0, \beta_1) &= \delta_1 
\end{aligned} \]
Over-approximation of union: segment extension rule

**Rule**

\[
S_{\text{lft}}\triangleright S_{\text{rgh}} \quad \text{then} \quad \begin{cases} 
S_{\text{lft}} \triangleright S_{\text{rgh}} = \delta_0 \\
(\alpha_0, \beta_0) \leftrightarrow \delta_0 \\
(\alpha_1, \beta_1) \leftrightarrow \delta_1
\end{cases}
\]

**Application to list traversal**, at the end of iteration 1:
- **previous invariant before iteration 1:**
  \[
  \begin{array}{c}
  \alpha_0 \quad \text{list} \\
  \beta_0 \quad \text{list}
  \end{array}
  \]
- **end of iteration 1:**
  \[
  \begin{array}{c}
  \alpha_0 \quad \text{list} \\
  \beta_0 \quad \text{list}
  \end{array}
  \]
- **join, before iteration 1:**
  \[
  \begin{array}{c}
  \delta_0 \quad \text{list} \\
  \delta_1 \quad \text{list}
  \end{array}
  \]

\[
\begin{align*}
\Psi(\alpha_0, \beta_0) &= \delta_0 \\
\Psi(\alpha_1, \beta_2) &= \delta_1
\end{align*}
\]
Over-approximation of union: rewrite system properties

- Comparison, canonicalization and widening algorithms can be considered **rewriting systems over tuples of graphs**

- **Success configuration**: weakening applies on all components, *i.e.*, the inputs are fully "consumed" in the weakening process

- **Failure configuration**: some components cannot be weakened *i.e.*, the algorithm should return the conservative answer (*i.e.*, $\top$)

**Termination**

- The systems are **terminating**

- This ensures comparison, canonicalization, widening are **computable**

**Non confluence!**

- The results depends on the order of application of the rules

- Implementation requires the choice of an **adequate strategy**
Over-approximation of union in the combined domain

**Widening of \((e_0^#, S_0^#)\) and \((e_1^#, S_1^#)\)**

1. define \(\Psi, e\) by \(\Psi(\alpha, \beta) = e(x) = \delta\) (where \(\delta\) is a fresh node) if and only if \(e_0^#(x) = \alpha \land e_1^#(x) = \beta\)

2. iteratively apply join local rules, and extend \(\Psi\) when new relations are inferred (for instance for points-to edges)

3. return the result obtained when all regions of both inputs are approximated in the output graph

This algorithm is sound:

**Soundness**

\[
\gamma(e_0^#, S_0^#) \cup \gamma(e_1^#, S_1^#) \subseteq \gamma(e^#, S^#)
\]

Widening also enforces **termination** (it only introduces segments, and the growth induced by the introduction of segments is bounded)
Outline

1 Memory models
2 Pointer Abstractions
3 Separation Logic
4 A shape abstract domain relying on separation
5 Standard static analysis algorithms
   • Overview of the analysis
   • Post-conditions and unfolding
   • Folding: widening and inclusion checking
   • Abstract interpretation framework: assumptions and results
6 Conclusion
7 Internships
Assumptions

What assumptions do we make?
How do we prove soundness of the analysis of a loop?

- **Assumptions in the concrete level**, and for block $b$:

  $$(\mathcal{P}(M), \subseteq)$$ is a complete lattice, hence a CPO
  
  $F : \mathcal{P}(M) \rightarrow \mathcal{P}(M)$$ is the concrete semantic (“post”) function of $b$

  thus, the concrete semantics writes down as $[b] = \text{lfp}_0 F$

- **Assumptions in the abstract level**:

  $M^\#$ set of abstract elements, no order a priori
  
  $m^\# ::= (e^\#, S^\#)$

  $\gamma_{\text{mem}} : M^\# \rightarrow \mathcal{P}(M)$ concretization

  $F^\# : M^\# \rightarrow M^\#$ sound abstract semantic function

  i.e., such that $F \circ \gamma_{\text{mem}} \subseteq \gamma_{\text{mem}} \circ F^#$

  $\bigtriangledown : M^\# \times M^\# \rightarrow M^\#$ widening operator, terminates, and such that

  $\gamma_{\text{mem}}(m^\#_0) \cup \gamma_{\text{mem}}(m^\#_1) \subseteq \gamma_{\text{mem}}(m^\#_0 \bigtriangledown m^\#_1)$
Computing a loop abstract post-condition

Loop abstract semantics

The abstract semantics of loop \texttt{while(rand())}\{b\} is calculated as the limit of the sequence of abstract iterates below:

\[
\begin{aligned}
\left\{ 
  m_0^\# &= \bot \\
  m_{n+1}^\# &= m_n^\# \triangledown F^\#(m_n^\#)
\right. \\
\end{aligned}
\]

Soundness proof:

- by induction over \( n \), \( \bigcup_{k \leq n} F^k(\emptyset) \subseteq \gamma_{\text{mem}}(m_n^\#) \)
- by the property of widening, the abstract sequence converges at a rank \( N \):
  \( \forall k \geq N, \, m_k^\# = m_N^\# \), thus

\[
\text{lfp}_\emptyset F = \bigcup_{k} F^k(\emptyset) \subseteq \gamma_{\text{mem}}(m_N^\#)
\]
Discussion on the abstract ordering

How about the abstract ordering? We assumed *NONE* so far...

- **Logical ordering**, induced by concretization, used for **proofs**
  \[ m_0 \preceq m_1 \iff \gamma_{\text{mem}}(m_0) \subseteq \gamma_{\text{mem}}(m_1) \]

- **Approximation of the logical ordering**, implemented as a function
  \[ \text{is\_le} : M^\# \times M^\# \rightarrow \{\text{true}, \top\} \], used to test the convergence of abstract iterates
  \[ \text{is\_le}(m_0, m_1) = \text{true} \quad \Rightarrow \quad \gamma_{\text{mem}}(m_0) \subseteq \gamma_{\text{mem}}(m_1) \]

Abstract semantics is not assumed (and is actually most likely NOT) monotone with respect to either of these orders...

- Also, **computational ordering** would be used for **proving widening termination**
Outline

1. Memory models
2. Pointer Abstractions
3. Separation Logic
4. A shape abstract domain relying on separation
5. Standard static analysis algorithms
6. Conclusion
7. Internships
Updates and summarization

Weak updates cause significant precision loss...
Separation logic makes updates strong

Separation logic

Separating conjunction combines properties on disjoint stores

- Fundamental idea: *forces to identify what is modified*
- Before an **update** (or a **read**) takes place, memory cells need to be **materialized**
- **Local reasoning**: properties on unmodified cells pertain

Summaries

**Inductive predicates** describe unbounded memory regions

- Last lecture: **array segments** and **transitive closure** (TVLA)
Bibliography

- **[JR]**: *Separation Logic: A Logic for Shared Mutable Data Structures.*
  John C. Reynolds.
  In LICS’02, pages 55–74, 2002.

- **[DHY]**: *A Local Shape Analysis Based on Separation Logic.*
  Dino Distefano, Peter W. O’Hearn and Hongseok Yang.
  In TACAS’06, pages 287–302.

- **[CR]**: *Relational inductive shape analysis.*
  Bor-Yuh Evan Chang and Xavier Rival.
Assignment and paper reading

The Frame rule:

- formalize the Hoare logic rules for a language with pointer assignments and condition tests
- prove the Frame rule by induction over the syntax of programs

Reading:

**Separation Logic: A Logic for Shared Mutable Data Structures.**

*John C. Reynolds.*

In LICS’02, pages 55–74, 2002.

Formalizes the Frame rule, among others
Outline

1. Memory models
2. Pointer Abstractions
3. Separation Logic
4. A shape abstract domain relying on separation
5. Standard static analysis algorithms
6. Conclusion
7. Internships
Internships on memory abstraction

**Summarization based on universal quantification:**

- memory abstractions use **summaries**
  today, we consider inductive linked structures; we will also see arrays...
- **another form of summarization** based on an **unbounded set** $E$

\[
\forall \{ P(x) \mid x \in E \}
\]

requires the definition of fold / unfold, analysis operations...

- towards a parametric abstract domain:
  - generic dictionary abstraction
  - arrays (generalization of existing)
  - union finds and DAGs

**Other topics:**

application to the verification of Operating System components