Memory abstraction 1

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

Xavier Rival

INRIA, ENS, CNRS

Jan, 10th. 2021
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
- non relational **pointer structures abstraction**
- predicates based shape abstraction

**Next lecture:** separation logic and shape abstraction, shape/numerical abstraction
Outline

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

2. Pointer Abstractions

3. Shape analysis in Three-Valued Logic (TVL)

4. Conclusion
Assumptions for the two lectures on memory abstraction

Imperative programs viewed as ***transition systems***:

- set of **control states**: $L$ (program points)
- set of **variables**: $X$ (all assumed globals)
- set of **values**: $V$ (so far: $V$ consists of integers (or floats) only)
- set of **memory states**: $M$ (so far: $M = X \rightarrow V$)
- error state: $\Omega$
- states: $S$

\[ S = L \times M \]
\[ S_{\Omega} = S \uplus \{ \Omega \} \]

- transition relation:

\[ (\rightarrow) \subseteq S \times S_{\Omega} \]

**Abstraction** of sets of states

- abstract domain $D^#$
- concretization $\gamma : (D^#, \sqsubseteq^#) \rightarrow (P(S), \subseteq)$
Assumptions: syntax of programs

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

\[
\begin{align*}
\text{l} & ::= \text{l-values} \\
& \quad | \ x \quad (x \in X) \\
& \quad | \ \ldots \quad \text{we will add other kinds of l-values} \\
& \quad | \ \text{pointers, array dereference...} \\
\text{e} & ::= \text{expressions} \\
& \quad | \ c \quad (c \in V) \\
& \quad | \ l \quad (\text{lvalue}) \\
& \quad | \ e \oplus e \quad (\text{arith operation, comparison}) \\
\text{s} & ::= \text{statements} \\
& \quad | \ l = e \quad (\text{assignment}) \\
& \quad | \ s; \ldots s; \quad (\text{sequence}) \\
& \quad | \ \text{if}(e)\{s\} \quad (\text{condition}) \\
& \quad | \ \text{while}(e)\{s\} \quad (\text{loop})
\end{align*}
\]
Assumptions: semantics of programs

We assume **classical definitions for:**

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

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

**Reachable states semantics**

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

\[
F : \mathcal{P}(S) \rightarrow \mathcal{P}(S)
\]

\[
X \quad \mapsto \quad S_I \cup \{ s \in S \mid \exists s' \in X, \ s' \rightarrow s \}
\]

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 \( D_{\text{mem}} \)
- concretization function \( \gamma_{\text{mem}} : D_{\text{mem}} \rightarrow \mathcal{P}(M) \)

**Reachable states abstraction**

We construct \( D_{\#} = L \rightarrow D_{\text{mem}} \) and:

\[
\begin{align*}
\gamma : D_{\#} & \rightarrow \mathcal{P}(S) \\
X_{\#} & \mapsto \{(l, m) \in S | m \in \gamma_{\text{mem}}(X_{\#}(l))\}
\end{align*}
\]

The whole question is how do we choose \( D_{\text{mem}}, \gamma_{\text{mem}} \ldots \)

- previous lectures:
  - \( X \) is fixed and finite and, \( V \) is scalars (integers or floats), thus, \( M = V^n \)
- today:
  - we will extend the language thus, also need to extend \( D_{\text{mem}}, \gamma_{\text{mem}} \)
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**... records...

**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**

- \( \mathbb{M} \equiv \mathbb{M}_0 \times \mathbb{M}_1 \times \ldots \) where \( \mathbb{M}_i = \mathbb{X}_i \rightarrow \mathbb{V}_i \)
- **Concretization function** (case with two types)

\[
\gamma_{nr} : \mathcal{P}(\mathbb{M}_0) \times \mathcal{P}(\mathbb{M}_1) \quad \mapsto \quad \mathcal{P}(\mathbb{M}) \\
(m_0^#, m_1^#) \quad \mapsto \quad \{(m_0, m_1) \mid \forall i, m_i \in \gamma_i(m_i^#)\}
\]
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!**
Memory models
Towards memory properties

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: \( V_{\text{addr}} \subseteq V \)
- **Environments** \( e \in E \) map variables into their addresses
- **Heaps** \( (h \in H) \) map addresses into values

\[
\begin{align*}
E &= \mathbb{X} \to V_{\text{addr}} \\
H &= V_{\text{addr}} \to V
\end{align*}
\]

\( h \) 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)

<table>
<thead>
<tr>
<th>address</th>
<th>&amp;x = 300</th>
<th>304</th>
<th>&amp;y = 308</th>
<th>312</th>
<th>&amp;z = 312</th>
<th>316</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>64</td>
<td></td>
<td>88</td>
<td></td>
<td>0x0</td>
<td></td>
</tr>
</tbody>
</table>

$e: x \mapsto 300$
$y \mapsto 308$
$z \mapsto 312$

$fi: 300 \mapsto 64$
$304 \mapsto 312$
$308 \mapsto 312$
$312 \mapsto 88$
$316 \mapsto 0$
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**

<table>
<thead>
<tr>
<th>address</th>
<th>&amp;x = 300</th>
<th>&amp;y = 308</th>
<th>&amp;z = 312</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>64</td>
<td>312</td>
<td>88</td>
</tr>
<tr>
<td>300</td>
<td>312</td>
<td>312</td>
<td>508</td>
</tr>
<tr>
<td>304</td>
<td>312</td>
<td>312</td>
<td>312</td>
</tr>
<tr>
<td>312</td>
<td>508</td>
<td>312</td>
<td>512</td>
</tr>
<tr>
<td>508</td>
<td>25</td>
<td>312</td>
<td>512</td>
</tr>
<tr>
<td>512</td>
<td>0x0</td>
<td>312</td>
<td>0</td>
</tr>
</tbody>
</table>

\[ e : \begin{array}{l} x \mapsto 300 \\ y \mapsto 308 \\ z \mapsto 312 \end{array} \]

\[ h : \begin{array}{l} 300 \mapsto 64 \\ 304 \mapsto 312 \\ 308 \mapsto 312 \\ 312 \mapsto 88 \\ 316 \mapsto 508 \\ 508 \mapsto 25 \\ 512 \mapsto 0 \end{array} \]
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:** \([1] : \mathcal{M} \to \mathbb{V}_{\text{addr}}\)

  \[ \llbracket x \rrbracket(e, h) = e(x) \]

- **Semantics of expressions** \([e] : \mathcal{M} \to \mathbb{V}\), mostly unchanged

  \[ \llbracket 1 \rrbracket(e, h) = h(\llbracket 1 \rrbracket(e, h)) \]

- **Semantics of assignment** \(l_0 : l := e; l_1 : \ldots:\)

  \[ (l_0, e, h_0) \to (l_1, e, h_1) \]

  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 \(\forall m_1 \in \mathbb{M}, (l_0, m_0) \rightarrow (l_1, m_1)\)

**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
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...

```c
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**: 
  \( *p \) 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

Language dependent items

- **Clear error cases** or **undefined behaviors**
  for analysis, a semantics with clear error cases is preferable

- **Composite objects**: structure fully exposed or not

- **Pointers to object fields**: allowed or not

- **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 these two lectures

**Abstraction for pointers and dynamic data-structures:**

- **pointer abstractions** \( \rightarrow \) short, simple techniques
- **three-valued logic**-based abstraction for **dynamic structures**
- **separation logic**-based abstraction for **dynamic structures**
- **combination** of **value** and **structure** abstractions

**Abstract operations:**

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

1. Memory models
2. Pointer Abstractions
3. Shape analysis in Three-Valued Logic (TVL)
4. Conclusion
Syntax extension: we add pointer operations

\[
\begin{align*}
l & ::= \text{l-values} \\
& \quad \text{x} \quad (x \in \mathbb{X}) \\
& \quad \ldots \\
& \quad \ast e \quad \text{pointer dereference} \\
& \quad l \cdot f \quad \text{field read}
\end{align*}
\]

\[
\begin{align*}
e & ::= \text{expressions} \\
& \quad l \\
& \quad \ldots \\
& \quad \& l \quad \text{"address of" operator}
\end{align*}
\]

\[
\begin{align*}
s & ::= \text{statements} \\
& \quad \ldots \\
& \quad x = \text{malloc}(c) \quad \text{allocation of } c \text{ bytes} \\
& \quad \text{free}(x) \quad \text{deallocation of the block pointed to by } x
\end{align*}
\]

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

Case of l-values:

\[
\begin{align*}
[x](e, h) & = e(x) \\
*[e](e, h) & = \begin{cases} 
    h([e](e, h)) & \text{if } [e](e, h) \neq 0 \land [e](e, h) \in \text{Dom}(h) \\
    \Omega & \text{otherwise}
\end{cases} \\
1 \cdot f(e, h) & = [1](e, h) + \text{offset}(f) \text{ (numeric offset)}
\end{align*}
\]

Case of expressions:

\[
\begin{align*}
[1](e, h) & = h([1](e, h)) \text{ (evaluates into the contents)} \\
& \& 1(e, h) & = [1](e, h) \text{ (evaluates into the address)}
\end{align*}
\]

Case of statements:

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

- memory deallocation free(\(x\)): \((e, h) \rightarrow (e, h')\) where \(k = e(x)\) and
  \[
  h = h' \uplus \{ k \mapsto v_k, k + 1 \mapsto v_{k+1}, \ldots, k + c - 1 \mapsto v_{k+c-1} \}
  \]
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, and show how such abstraction lift into abstraction for sets of heaps.
Pointer non relational abstraction: null pointers

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:

- $\gamma_{\text{ptr}}(\perp) = \emptyset$
- $\gamma_{\text{ptr}}(\top) = \mathbb{V}_{\text{addr}}$
- $\gamma_{\text{ptr}}(\neq \text{NULL}) = \mathbb{V}_{\text{addr}} \setminus \{0\}$

- 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
Pointer Abstractions

Pointer non-relational abstraction: dangling pointers

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:

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

- very lightweight, can typically resolve rather trivial cases
- useful for C, useless for Java (initialization requirement + GC)
Pointer non relational abstraction: points-to sets

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:
  
  \[ A^\# = \{ &x, &y, \ldots, &t, a_0^\#, a_1^\#, \ldots, a_N^\# \} \]

  where $a_0^\#, \ldots, a_N^\#$ is a collection of $N + 1$ fixed abstract addresses

- Concrete addresses are abstracted into $A^\#$ by $\phi_A : \mathbb{V}_{\text{addr}} \rightarrow A^\# \cup \{ \top \}$
  Assumption: $\phi_A$ surjective (no useless abstract address).

- A pointer value is abstracted by the abstraction of the addresses it may point to, i.e.,
  \[ D_{\text{ptr}}^\# = \mathcal{P}(A^\#) \]
  and
  \[ \gamma_{\text{ptr}}(a^\#) = \{ a \in \mathbb{V}_{\text{addr}} \mid \phi_A(a) = a^\# \} \]
Abstraction of pointer states

We consider all values are of pointer type, i.e., heaps are of the form 
\( h : \mathbb{V}_{\text{addr}} \rightarrow \mathbb{V}_{\text{addr}} \).

**Intuition:**
- collect information separately for each element of \( \mathbb{A}^\# \)
- use a pointer value abstract element for each abstract address

**Lifting a pointer abstraction to heap abstraction**

We let 
\( D^\#_{\text{mem}} = \mathbb{A}^\# \rightarrow D^\#_{\text{ptr}} \) and define

\[
\gamma_{\text{mem}}(h^\#) = \{ h \in \mathbb{H} | \forall a \in \mathbb{V}_{\text{addr}}, \forall a^\# \in \mathbb{A}^\#, \phi_{\mathbb{A}}(a) = a^\# \rightarrow \phi_{\mathbb{A}}(h(a)) \in \gamma_{\text{ptr}}(h^\#(a^\#)) \}
\]

**Examples** of properties described by this abstraction:
- \( p \) may point to \( \{ &x \} \)
- \( p \) points to some address described by \( a^\# \) and, at all addresses described by \( a^\# \), we can read another address described by \( a^\# \)
Points-to sets computation example

Example code:

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

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>
Pointers Abstractions

Points-to sets computation and imprecision

```
x ∈ [−10, −5]; y ∈ [5, 10]
1: int * p;
2: if(?){
3:    p = &x;
4: } else {
5:    p = &y;
6: }
7: *p = 0;
8: ...
```

Case 1: p := &x
\( y ∈ [5, 10] \quad x = 0 \)

Case 2: p := &y
\( y = 0 \quad x ∈ (−10, −5) \)

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

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

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:

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: \( p \mapsto \{ \&x \} \)

- if the points-to set may contain more than one element, the analysis needs to perform a weak-update
  as in the second example: \( p \mapsto \{ \&x, \&y \} \)
Weak updates

We recall:

- \( \mathcal{A}^\# = \{ \&x, \&y, \ldots, \&t, a_0^\#, a_1^\#, \ldots, a_N^\# \} \)

- \( \phi_{\mathcal{A}} : \mathcal{V}_{\text{addr}} \to \mathcal{A}^\# \cup \{ \top \} \), surjective

Moreover, we assume an abstract state \( h^\# \) and an assignment \( 1 := c \) where 1 is an l-value. We note the abstract evaluation of the l-value:

\[
\mathcal{L} := \phi_{\mathcal{A}}^{-1}(\llbracket 1 \rrbracket^\#(h^\#)) = \{ a \in \mathcal{A}^\# \mid \phi_{\mathcal{A}}(a) \in \llbracket 1 \rrbracket^\#(h^\#) \}
\]

We have two cases, based on the cardinality of \( \mathcal{L} \):

1. \( |\mathcal{L}| \leq 1 \): strong update
   - then, exactly one abstract value needs to be updated (\( \phi_{\mathcal{A}}(a) \) if \( \mathcal{L} = \{a\} \))

2. \( |\mathcal{L}| > 1 \):
   - then, there exists two distinct addresses \( a_0, a_1 \in \mathcal{L} \); since the assignment overwrites one cell exactly:
     - if the content of \( a_0 \) is modified, then that of \( a_1 \) stays the same...
     - the other way around too, of course
   - thus the post-condition need to map \( \phi_{\mathcal{A}}(a_0) \) to something weaker than \( h^\#(a_0) \), and the same for \( a_1 \), which means we have a weak update
Weak updates

We consider:

- abstract heap $h^\#$
- assignment $l := c$
- the abstract evaluation of the l-value:

$$\mathcal{L} := \phi^{-1}_A ([1]^\#(h^\#)) = \{ a \in A^\# \mid \phi_A(a) \in [1]^\#(h^\#) \}$$

So, when does the weak update happen?

There are two (non exclusive) situations:

1. **when** $|[1]^\#(h^\#)| > 1$:
   - this includes that the evaluation of $l$ is not precise in the abstract

2. **when there exists** $a \in [1]^\#(h^\#)$ **such that** $|\phi^{-1}_A(\{a\})| > 1$:
   - this means that one of the addresses $l$ may evaluate to corresponds to several distinct concrete cells

Both cases can be expected to happen frequently in pointer analysis...
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 \((i.e., \text{an address})\); e.g.:
  \[
  a ::= x \mid a \cdot f \mid *a
  \]
- 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 $\mathbb{C}$ 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. Shape analysis in Three-Valued Logic (TVL)
   - Principles of Three-Valued Logic based abstraction
   - Comparing and concretizing Three-Valued Logic abstractions
   - Weakening Three-Valued Logic abstractions
   - Transfer functions
   - Focusing

4. Conclusion
Representation of memory states: memory graphs

Observation: representation of memory states by graphs

- **Nodes** (aka, atoms) denote variables, memory locations
- **Edges** denote properties of addresses / pointers, such as:
  - “field f of location u points to v”
  - “variable x is stored at location u”
- This representation is also relevant in the case of separation logic based shape abstraction

A couple of examples:

**Two alias pointers:**

```
  y -> u1
   
  x -> u0

  u1 -> u2
```

**A list of length 2 or 3:**

```
x -> u0^n -> u1^n -> u2^n
```

We need to over-approximate sets of shape graphs
Memory graphs and predicates: variables

Before we apply some abstraction, we formalize memory graphs using some predicates, such as:

**“Variable content” predicate**

We note \( x(u) = 1 \) if node \( u \) represents the contents of \( x \).

Examples:

- **Two alias pointers:**

  ![Diagram of two alias pointers]

  Then, we have \( x(u_0) = 1 \) and \( y(u_1) = 1 \), and \( x(u) = 0 \) (resp., \( y(u) = 0 \)) in all the other cases.

- **A list of length 2:**

  ![Diagram of a list of length 2]

  Then, we have \( x(u_0) = 1 \) and \( x(u) = 0 \) in all the other cases.
Memory graphs and predicates: (field) pointers

"Field content pointer" predicate

- We note $n(u, v)$ if the field $n$ of $u$ stores a pointer to $v$
- We note $0(u, v)$ if $u$ stores a pointer to $v$ (base address field is at offset 0)

Examples:

- **Two alias pointers:**

  ![Diagram of two alias pointers]

  Then, we have $0(u_0, u_2) = 1$ and $0(u_1, u_2) = 1$, and $0(u, v) = 0$ in all the other cases

- **A list of length 2:**

  ![Diagram of a list of length 2]

  Then, we have $n(u_0, u_1) = 1$ and $n(u_1, u_2) = 1$, and $n(u, v) = 0$ in all the other cases
2-structures and concretization

We can represent the memory graphs using **tables of predicate values**:

**Two-structures and concretization**

We assume a set \( \mathcal{P} = \{p_0, p_1, \ldots, p_n\} \) of **predicates** (we write \( k_i \) for the arity of predicate \( p_i \)). A formal representation of a memory graph is a **2-structure** \((\mathcal{U}, \phi) \in \mathbb{D}^2_2\) defined by:

- a set \( \mathcal{U} = \{u_0, u_1, \ldots, u_m\} \) of **atoms**
- a **truth table** \( \phi \) such that \( \phi(p_i, u_1, \ldots, u_{k_i}) \) denotes the truth value of \( p_i \) for \( u_1, \ldots, u_{k_i} \) (where arities of predicates are respected)

Then, \( \gamma_2(\mathcal{U}, \phi) \) is the set of \((e, h, \nu)\) where \( \nu : \mathcal{U} \to \mathbb{V}_{\text{addr}} \) and that satisfy exactly the truth tables defined by \( \phi \):

- \((e, h, \nu)\) satisfies \( x(u) \) iff \( e(x) = \nu(u) \)
- \((e, h, \nu)\) satisfies \( f(u, \nu) \) iff \( h(\nu(u), f) = \nu(v) \)

- the name "two-structure" will become clear (very) soon
- the set of two-structures is parameterized by the data of a set of predicates \( x(.), y(.), 0(.,.), n(., .) \) (additional predicates will be added soon...)
Examples of two-structures

Two alias pointers:

\[
\begin{array}{ccc}
y & \rightarrow & u_1 \\
x & \rightarrow & u_0 \\
\end{array}
\]

<table>
<thead>
<tr>
<th></th>
<th>x</th>
<th>y</th>
</tr>
</thead>
<tbody>
<tr>
<td>u_0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>u_1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>u_2</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

A list of length 2:

\[
\begin{array}{ccc}
x & \rightarrow & u_0 \\
\cdot n & \rightarrow & u_1 \\
\cdot n & \rightarrow & u_2 \\
\end{array}
\]

<table>
<thead>
<tr>
<th></th>
<th>x</th>
<th>\cdot n</th>
</tr>
</thead>
<tbody>
<tr>
<td>u_0</td>
<td>1</td>
<td>u_0</td>
</tr>
<tr>
<td>u_1</td>
<td>0</td>
<td>u_1</td>
</tr>
<tr>
<td>u_2</td>
<td>0</td>
<td>u_2</td>
</tr>
</tbody>
</table>

A list of length 2:

\[
\begin{array}{ccc}
x & \rightarrow & u_0 \\
\cdot n & \rightarrow & u_1 \\
\cdot n & \rightarrow & u_2 \\
\end{array}
\]

<table>
<thead>
<tr>
<th></th>
<th>x</th>
<th>y</th>
<th>\cdot n</th>
</tr>
</thead>
<tbody>
<tr>
<td>u_0</td>
<td>1</td>
<td>0</td>
<td>u_0</td>
</tr>
<tr>
<td>u_1</td>
<td>0</td>
<td>1</td>
<td>u_1</td>
</tr>
<tr>
<td>u_2</td>
<td>0</td>
<td>0</td>
<td>u_2</td>
</tr>
</tbody>
</table>

Lists of arbitrary length? More on this later
Unknown value: three valued logic

How to abstract away some information?

i.e., how to abstract several graphs into one?

**Example**: pointer variable p alias with x or y

A boolean lattice

- Use **predicate tables**
- Add a $\top$ boolean value;
  (denoted to by $\frac{1}{2}$ in TVLA papers)

Graph representation:
- **dotted edges**

Abstract graph:
Summary nodes

At this point, we cannot talk about **unbounded memory states** with **finitely many** nodes, since one node represents at most one memory cell.

**An idea**

- Choose a node to represent *several* concrete nodes
- Similar to *smashing* of arrays using segments

**Definition: summary node**

A **summary node** is an atom that may denote several concrete atoms

- Intuition: we are using a **non injective function** $\phi_A : V_{addr} \rightarrow \mathbb{A}^#$
- Representation: double circled nodes

**Lists of lengths 1, 2, 3:**

- $x \rightarrow u_0 \xrightarrow{n} u_1$
- $x \rightarrow u_0 \xrightarrow{n} u_1 \xrightarrow{n} u_2$
- $x \rightarrow u_0 \xrightarrow{n} u_1 \xrightarrow{n} u_2 \xrightarrow{n} u_3$

**Attempt at a summary graph:**

- Edges to $u_1$ are dotted
Additional graph predicate: sharing

We now define a few higher level predicates based on the previously seen atomic predicates describing the graphs.

Example: a cell is shared if and only if there exists several distinct pointers to it

"Is shared" predicate

The predicate $\text{sh}(u)$ holds if and only if

\[
\exists v_0, v_1, \begin{cases} 
  v_0 \neq v_1 \\
  n(v_0, u) \\
  n(v_1, u)
\end{cases}
\]

(for concision, we assume only $n$ pointers)

- $\text{sh}(u_0) = \text{sh}(u_1) = \text{sh}(u_3) = 0$
- $\text{sh}(u_2) = 1$
Additional graph predicate: reachability

We can also define higher level predicates using induction:

For instance, a cell is reachable from $u$ if and only if it is $u$ or it is reachable from a cell pointed to by $u$.

"Reachability" predicate

The predicate $r(u, v)$ holds if and only if:

$$u = v \lor \exists u_0, n(u, u_0) \land r(u_0, v)$$

(for concision, we assume only $n$ pointers)

"Acyclicity" predicate

The predicate $acy(u)$ holds iff $\exists v, v \neq u \land r(u, v) \land r(v, u)$ does not hold.
Three structures

As for 2-structures, we assume a set \( \mathcal{P} = \{ p_0, p_1, \ldots, p_n \} \) of predicates fixed and write \( k_i \) for the arity of predicate \( p_i \).

**Definition: 3-structures**

A **3-structure** is a tuple \((\mathcal{U}, \phi)\) defined by:

- a set \( \mathcal{U} = \{ u_0, u_1, \ldots, u_m \} \) of **atoms**
- a **truth table** \( \phi \) such that \( \phi(p_i, u_{l_1}, \ldots, u_{l_{k_i}}) \) denotes the truth value of \( p_i \) for \( u_{l_1}, \ldots, u_{l_{k_i}} \).

Note: truth values are elements of the lattice \( \{0, \frac{1}{2}, 1\} \)

We write \( \mathbb{D}_3 \) for the set of three-structures.

In the following we build up an abstract domain of 3-structures (but a bit more work is needed for the definition of the concretization)
Main predicates and concretization

We have already seen:

<table>
<thead>
<tr>
<th>predicate</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x(u) )</td>
<td>variable ( x ) contains the address of ( u )</td>
</tr>
<tr>
<td>( n(u,v) )</td>
<td>field of ( u ) points to ( v )</td>
</tr>
<tr>
<td>( \text{sum}(u) )</td>
<td>whether ( u ) is a summary node (convention: either 0 or ( \frac{1}{2} ))</td>
</tr>
<tr>
<td>( \text{sh}(u) )</td>
<td>whether there exists several distinct pointers to ( u )</td>
</tr>
<tr>
<td>( \text{r}(u,v) )</td>
<td>whether ( v ) is reachable starting from ( u )</td>
</tr>
<tr>
<td>( \text{acy}(v) )</td>
<td>( v ) may not be on a cycle</td>
</tr>
</tbody>
</table>

**Concretization for 2 structures:**

\[
(e, h, v) \in \gamma_2(U, \phi) \iff \bigwedge_{p \in P} (\text{env}, h, v) \text{ evaluates } p \text{ as specified in } \phi
\]

**Concretization for 3 structures:**

- predicates with value \( \frac{1}{2} \) may concretize either to true or to false
- but the concretization of summary nodes is still unclear...
Outline

1 Memory models

2 Pointer Abstractions

3 Shape analysis in Three-Valued Logic (TVL)
   - Principles of Three-Valued Logic based abstraction
   - Comparing and concretizing Three-Valued Logic abstractions
   - Weakening Three-Valued Logic abstractions
   - Transfer functions
   - Focusing

4 Conclusion
Embedding

Reasons why we need to set up a relation among structures:

- learn how to compare two 3-structures
- describe the concretization of 3-structures into 2-structures

The embedding principle

Let $S_0 = (U_0, \phi_0)$ and $S_1 = (U_1, \phi_1)$ be two three structures, with the same sets of predicates $\mathcal{P}$. Let $f : U_0 \rightarrow U_1$, surjective. We say that $f$ embeds $S_0$ into $S_1$ iff

\[
\phi_0(u_{l_1}, \ldots, u_{l_k_i}) \sqsubseteq \phi_1(f(u_{l_1}), \ldots, f(u_{l_k_i}))
\]

Then, we write $S_0 \sqsubseteq^f S_1$

- Note: we use the order $\sqsubseteq$ of the lattice \{0, $\frac{1}{2}$, 1\}
- Intuition: embedding defines an abstract pre-order i.e., when $S_0 \sqsubseteq^f S_1$, any property that is satisfied by $S_0$ is also satisfied by $S_1$
Embedding examples

A few examples of the embedding relation:

\[ x \xrightarrow{n} u_0 \xrightarrow{n} u_1 \xrightarrow{n} u_2 \]

where \( f : u_0 \mapsto u_0; u_1 \mapsto u_1; u_2 \mapsto u_1 \)

\[ x \xrightarrow{n} u_0 \xrightarrow{n} u_1 \xrightarrow{n} u_2 \xrightarrow{n} u_3 \]

where \( f : u_0 \mapsto u_0; u_1 \mapsto u_1; u_2 \mapsto u_1; u_3 \mapsto u_1 \)

\[ x \xrightarrow{n} u_0 \xrightarrow{n} u_1 \xrightarrow{n} u_2 \]

where \( f : u_0 \mapsto u_0; u_1 \mapsto u_1; u_2 \mapsto u_1 \)

The last example shows summary nodes are not enough to capture just lists:

- **reachability** would be necessary to constrain it be a list
- alternatively: list cells **should not be shared**
Concretization of three-structures

**Intuitions:**

- Concrete memory states correspond to 2-structures
- Embedding applies uniformly to 2-structures and 3-structures (in fact, 2-structures are a subset of 3-structures)
- 2-structures can be embedded into 3-structures, that abstract them

This suggests a *concretization of 3-structures in two steps*:

1. Turn it into a set of 2-structures that can be embedded into it
2. Concretize these 2-structures

---

**Concretization of 3-structures**

Let $S$ be a 3-structure. Then:

$$\gamma_3(S) = \bigcup \{ \gamma_2(S') \mid S' \text{ 2-structure s.t. } \exists f, S' \subseteq^f S \}$$
Concretization examples

Without reachability:

\[
\begin{align*}
\text{where } f &: u_0 \mapsto u_0; u_1 \mapsto u_1; u_2 \mapsto u_1; u_3 \mapsto u_1
\end{align*}
\]

With reachability:

\[
\begin{align*}
\text{where } f &: u_0 \mapsto u_0; u_1 \mapsto u_1; u_2 \mapsto u_1
\end{align*}
\]

Note the first item of the above case does not work here
Disjunctive completion

- Do 3-structures allow for a **sufficient level of precision**?
- How to **over-approximate a set of 2-structures**?

```
int * x; int * y; ...
int * p = NULL;
if(...){
    p = x;
} else{
    p = y;
}
printf("%d", *p);
*p = ...;
```

After the if statement:
abstracting would be imprecise

Abstraction based on disjunctive completion

- In the following, we use **partial disjunctive completion**
  *i.e.*, TVLA manipulates **finite disjunctions** of 3-structures
We write $\mathcal{D}^\#_P(3)$ for the abstract domain made of finite sets of 3-structures in $\mathcal{D}^\#_3$

- How to ensure disjunctions **will not grow infinite**?
the set of atoms is **unbounded**, so it is not necessarily true!
Outline

1. Memory models

2. Pointer Abstractions

3. Shape analysis in Three-Valued Logic (TVL)
   - Principles of Three-Valued Logic based abstraction
   - Comparing and concretizing Three-Valued Logic abstractions
   - Weakening Three-Valued Logic abstractions
   - Transfer functions
   - Focusing

4. Conclusion
Canonical abstraction

To prevent disjunctions from growing infinite, we propose to normalize (in a precision losing manner) abstract states:

- the analysis may use all 3-structures at most points
- at selected points (including loop heads), only 3-structures in a finite set $D^\#_{\text{can}(3)}$ are allowed
- there is a function to coarsen 3-structures into elements of $D^\#_{\text{can}(3)}$

Canonicalization function

Let $\mathcal{L}$ be a lattice, $\mathcal{L}' \subseteq \mathcal{L}$ be a finite sub-lattice and $\text{can} : \mathcal{L} \rightarrow \mathcal{L}'$:

- operator $\text{can}$ is called canonicalization if and only if it defines an upper closure operator
- then it extends into a canonicalization operator $\text{can} : \mathcal{P}(\mathcal{L}) \rightarrow \mathcal{P}(\mathcal{L}')$ for the disjunctive completion domain:
  \[
  \text{can}(\mathcal{E}) = \{ \text{can}(x) \mid x \in \mathcal{E} \}
  \]

- proof of the extension to disjunctive completion domains: left as an exercise
- to make the powerset domain work, we simply need a can over 3-structures
Shape analysis in Three-Valued Logic (TVL)

Weakening Three-Valued Logic abstractions

**Canonical abstraction**

**Definition of a finite lattice** $\mathbb{D}_{\text{can}}^\#(3)$

We partition the set of predicates $\mathcal{P}$ into two subsets $\mathcal{P}_a$ and $\mathcal{P}_o$:

- $\mathcal{P}_a$ and defines **abstraction predicates** and should contains only unary predicates and have a finite truth table whatever the number of atoms
- $\mathcal{P}_o$ denotes **non-abstraction predicates**, and may define truth tables of unbounded size

Then, we let $\mathbb{D}_{\text{can}}^\#(3)$ be the set of 3-structures such that no pair of atoms have the same value of the $\mathcal{P}_a$ predicates. It defines a finite set of 3-structures.

This sub-lattice defines a clear “canonicalization” algorithm:

**Canonical abstraction by truth blurring**

1. **Identify** nodes that have different abstraction predicates
2. When several nodes have the same abstraction predicate introduce a summary node
3. **Compute new predicate values** by doing a join over truth values
Canonical abstraction examples

Most common TVLA instantiation:

- **ae** assume there are \( n \) variables \( x_1, \ldots, x_n \)
  thus the number of unary predicates is finite, and provides a good choice for \( P_a \)

- **sub-lattice**: structures with atoms distinguished by the values of the unary predicates \( x_1, \ldots, x_n \)

Examples:

<table>
<thead>
<tr>
<th>Elements not merged:</th>
<th>Elements merged:</th>
<th>Abstract into:</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Diagram" /></td>
<td><img src="image2" alt="Diagram" /></td>
<td><img src="image3" alt="Diagram" /></td>
</tr>
</tbody>
</table>

- Lists of lengths 1, 2, 3:
  - Abstract into:
    - \( x(u_0^n u_1) \)
    - \( x(u_0^n u_1) \)
    - \( x(u_0^n u_1) \)
    - \( r(x) \)
    - \( x(u_0^n u_1) \)
Outline

1. Memory models

2. Pointer Abstractions

3. Shape analysis in Three-Valued Logic (TVL)
   - Principles of Three-Valued Logic based abstraction
   - Comparing and concretizing Three-Valued Logic abstractions
   - Weakening Three-Valued Logic abstractions
   - Transfer functions
   - Focusing

4. Conclusion
Principle for the design of sound transfer functions

- Intuitively, **concrete states** correspond to **2-structures**
- The **analysis** should track **3-structures**, thus the analysis and its soundness proof need to **rely on the embedding relation**

**Embedding theorem**

We assume that

- \( S_0 = (\mathcal{U}_0, \phi_0) \) and \( S_1 = (\mathcal{U}_1, \phi_1) \) define a pair of 3-structures
- \( f : \mathcal{U}_0 \to \mathcal{U}_1 \), is such that \( S_0 \sqsubseteq^f S_1 \) (embedding)
- \( \Psi \) is a logical formula, with variables in \( X \)
- \( g : X \to \mathcal{U}_0 \) is an assignment for the variables of \( \Psi \)

Then, the semantics (evaluation) of logical formulae is such that

\[
\llbracket \Psi|_g \rrbracket (S_0) \sqsubseteq \llbracket \Psi|_{f \circ g} \rrbracket (S_1)
\]

**Intuition**: this theorem ties the evaluation of conditions in the concrete and in the abstract in a general manner
Principle for the design of sound transfer functions

Transfer functions for static analysis

- **Semantics of concrete statements is encoded into boolean formulas**
- **Evaluation in the abstract is sound (embedding theorem)**

**Example:** analysis of an assignment $y := x$

1. Let $y'$ be a new predicate that denotes the *new* value of $y$
2. Then we can add the constraint $y'(u) = x(u)$ *(using the embedding theorem to prove soundness)*
3. Rename $y'$ into $y$

**Advantages:**

- **Abstract transfer functions** derive directly from the concrete transfer functions *(intuition: $\alpha \circ f \circ \gamma ...$)*
- The same solution works for *weakest pre-conditions*

**Disadvantage:** Precision will require some care, more on this later!
Assignment: a simple case

<table>
<thead>
<tr>
<th>Statement $l_0 : y = y \rightarrow n; l_1 : \ldots$</th>
<th>Pre-condition $S$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$l_0 : y = y \rightarrow n; l_1 : \ldots$</td>
<td>$x, y \xrightarrow{u_0,n} u_1 \xrightarrow{n} u_2$</td>
</tr>
</tbody>
</table>

Transfer function computation:

- It should produce an over-approximation of $\{ m_1 \in \mathcal{M} \mid (l_0, m_0) \rightarrow (l_1, m_1) \}$.
- **Encoding** using “primed predicates” to denote predicates after the evaluation of the assignment, to evaluate them in the same structure (non primed variables are removed afterwards and primed variables renamed):

\[
\begin{align*}
  x'(u) &= x(u) \\
  y'(u) &= \exists v, y(v) \land n(v, u) \\
  n'(u, v) &= n(u, v)
\end{align*}
\]

- Resulting structure:

\[
\begin{array}{ccc}
  x_0 & \xrightarrow{n} & u_1 \\
  \downarrow & & \downarrow \\
  x & & y \\
  \uparrow & & \uparrow \\
  u_0 & \xrightarrow{n} & u_2
\end{array}
\]

This is exactly the expected result.
Outline

1. Memory models

2. Pointer Abstractions

3. Shape analysis in Three-Valued Logic (TVL)
   - Principles of Three-Valued Logic based abstraction
   - Comparing and concretizing Three-Valued Logic abstractions
   - Weakening Three-Valued Logic abstractions
   - Transfer functions
   - Focusing

4. Conclusion
Assignment: a more involved case

**Statement** $l_0 : y = y \rightarrow n; l_1 : \ldots$

**Pre-condition** $S$

- Let us try to **resolve the update in the same way as before**:

  $x'(u) = x(u)$
  $y'(u) = \exists v, y(v) \land n(v, u)$
  $n'(u, v) = n(u, v)$

- We **cannot resolve** $y'$:

  $$\left\{ \begin{array}{l}
y'(u_0) = 0 \\
y'(u_1) = \frac{1}{2}
\end{array} \right.$$

**Imprecision**: after the statement, $y$ may point to anywhere in the list, save for the first element...

- The assignment transfer function **cannot be computed immediately**
- **We need to refine the 3-structure first**
Focusing on a formula

We assume a 3-structure $S$ and a boolean formula $f$ are given, we call a focusing $S$ on $f$ the generation of a set $\hat{S}$ of 3-structures such that:

- $f$ evaluates to 0 or 1 on all elements of $\hat{S}$
- precision was gained: $\forall S' \in \hat{S}, S' \subseteq S$ (embedding)
- soundness is preserved: $\gamma(S) = \bigcup\{\gamma(S') \mid S' \in \hat{S}\}$

Details of focusing algorithms are rather complex: not detailed here

They involve splitting of summary nodes, solving of boolean constraints

Example: focusing on $y'(u) = \exists v, y(v) \land n(v, u)$

We obtain (we show $y$ and $y'$):
Focus and coerce

Some of the 3-structures generated by focus are not precise

\( u_1 \) is reachable from \( x \), but there is no sequence of \( n \) fields: this structure has empty concretization

\( u_0 \) has an \( n \)-field to \( u_1 \) so \( u_1 \) denotes a unique atom and cannot be a summary node

Coerce operation

It enforces logical constraints among predicates and discards 3-structures with an empty concretization

Result: one case removed (bottom), two possibly summary nodes non summary
Focus, transfer, abstract...

**Computation of a transfer function**

We consider a transfer function encoded into boolean formula $f$

$S_p^{\pre} \xrightarrow{\text{summary}} S_p^#$

$\hat{S}_p^{\pre} \xrightarrow{\text{focus coerce}} \hat{S}_p^{\pre}$

$f \xrightarrow{S_p^#} \hat{S}_p^{\post}$

**Soundness proof** steps:

1. **sound encoding of the semantics of program statements into formulas** (typically, no loss of precision at this stage)

2. **focusing** produces a **refined** over-approximation (disjunction)

3. **canonicalization** over-approximates graphs (truth blurring)

A common picture in shape analysis
Shape analysis with three valued logic

Abstract states; two abstract domains are used:

- **infinite domain** $\mathbb{D}^\#_P(3)$: finite disjunctions of 3-structures in $\mathbb{D}^3$ for general abstract computations
- **finite domain** $\mathbb{D}^\#_P(\text{can}(3))$: disjunctions of finite domain $\mathbb{D}^\#_{\text{can}(3)}$ to simplify abstract states and for loop iteration
- **concretization** via $\mathbb{D}^\#_2$

Abstract post-conditions:

1. start from $\mathbb{D}^\#_P(3)$ or $\mathbb{D}^\#_{\text{can}(3)}$
2. focus and coerce when needed
3. apply the concrete transformation
4. apply can to weaken abstract states; result in $\mathbb{D}^\#_P(\text{can}(3))$

Analysis of loops:

- iterations in $\mathbb{D}^\#_P(\text{can}(3))$ terminate, as it is finite
Outline

1. Memory models
2. Pointer Abstractions
3. Shape analysis in Three-Valued Logic (TVL)
4. Conclusion
Updates and summarization

**Weak updates cause significant precision loss...**

- Basic pointer abstractions suffer weak update issues leading to high precision loss
- Various techniques exist to mitigate this effect
- Today, we saw shape analysis based on three-valued predicates as a way to circumvent it
  Next week, another technique will be presented...

A **novel family of abstract interpretation based static analyses:**
- Some analysis operations require **local concretization** of abstract predicates
- A reverse operation makes **abstract states more abstract**

**Internships**
Conclusion

Assignment: formalization and paper reading

**Formalization of the concretization of 2-structures:**

- describe the concretization formula, assuming that we consider the predicates discussed in the course
- run it on the list abstraction example (from the 3-structure to a few select 2-structures, and down to memory states)
- prove the correctness and termination of the widening of the cofibered abstract domain

**Reading:**

**Parametric Shape Analysis via 3-Valued Logic.**

Shmuel Sagiv, Thomas W. Reps et Reinhard Wilhelm.

Assignment: a simple analysis in TVLA

\[ l \rightarrow 1 \rightarrow 2 \quad k \rightarrow A \rightarrow B \]

1, k assumed to be disjoint lists

\[ \text{while}(l \neq 0) \{
    t = l \rightarrow n; \\
    l \rightarrow n = k; \\
    k = \emptyset; \\
    l = t;
\} \]

\[ l \rightarrow 1 \rightarrow 2 \quad k \rightarrow A \rightarrow B \]

Focus on \( u_0 \)

Can \( \{k\} \) from \( 2t \) to \( l \)