CS615: Formal Specification and Verification of Programs 2019

Lecture 16: Abstract interpretation - combination

Instructor: Ashutosh Gupta

IITB, India

Compile date: 2019-10-17

Topic 16.1

Domain combination

Multiple domains in a tool

A typical abstract interpretation tool implements many abstract domains.

The domains can potentially help each other for better precision.

We will discuss a few schemes for combining the domains.

Commentary: The content on combination is based on `https://arxiv.org/pdf/1309.5146.pdf`

Two abstract domains

Let us consider two abstract domains

$$(D_1, \sqsubseteq_1, \sqcup_1, \sqcap_1) \qquad \text{and} \qquad (D_2, \sqsubseteq_2, \sqcup_2, \sqcap_2)$$

Let us suppose both the domains form the Galois connection with the concrete world C

$$(C, \subseteq) \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} (D_1, \sqsubseteq_1) \qquad \text{and} \qquad (C, \subseteq) \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} (D_2, \sqsubseteq_2).$$

Example 16.1

In the lecture, we will use the following domains

- $D_1 = \{\top, Even, Odd, \bot\}$ *aka parity domain*
- $D_2 =$ *interval domain (we have seen in the earlier lecture)*

Two abstract domains II

We also assume that the following implementable operators available for the domains

- $\alpha_1 : C \to D_1$
- $\sqcup_1 : D_1 \times D_1 \to D_1$
- $\nabla : D_1 \times D_1 \to D_1$, and
- $sp^{\#_1}$: abstract post

- $\alpha_2 : C \to D_2$
- $\sqcup_2 : D_2 \times D_2 \to D_2$
- $\nabla : D_2 \times D_2 \to D_2$, and
- $sp^{\#_2}$: abstract post

How do we combine the domains?

Product domain

Let us define a product domain

$$(D_1 \times D_2, \sqsubseteq)$$

where $(a, b) \sqsubseteq (a', b') \triangleq a \sqsubseteq_1 a'$ and $b \sqsubseteq_2 b'$.

The other operators for the combined domain are not fixed automatically.

The combination schemes make choices for α, $sp^{\#}$, and $\triangledown$.

We will drop narrowing from our discussion.(why?)

Combination schemes

We will consider the following domain combination schemes

1. Cartesian product
2. Reduced product
3. Granger product
4. Reduced cardinal power

Cartesian product : simplest combination

We define the domain operators as follows

1. $\alpha(c) = (\alpha_1(c), \alpha_2(c))$
2. $sp^{\#}((a, b), \rho) = (sp^{\#_1}(a, \rho), sp^{\#_2}(b, \rho))$
3. $(a, b)\nabla(a', b') = (a\nabla_1 a', b\nabla_2 b')$

There is no interaction between the two domains.

The result would be as if the two abstract domains are applied independently and the results are combined.

Exercise 16.1

What is γ? *Recall: α fixes gamma.*

Exercise: cartesian product

Exercise 16.2

Apply the following operators

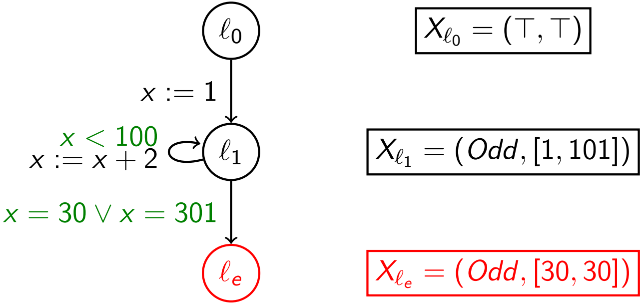
- $\alpha(\{1, 3, 5\})$
- $\alpha(\{1, 4\})$
- $\mathit{sp}^{\#}((\mathit{Even}, [2, 4]), \texttt{x} := \texttt{x} + 1)$
- $\alpha(\emptyset)$

Example: cartesian product

Example 16.2

Let us suppose D_1 = *parity domain and* D_2 = *interval domain.*

Consider the following program



Exercise 16.3

X_{ℓ_e} *is not* $(\bot, \bot)$, *how do we conclude that* ℓ_e *is unreachable?*

Example: interaction helps

Example 16.3

Consider abstract state $(Odd, [30, 30])$.

Since there is no even number in the range $[30, 30]$, *we may reduce the state to*

$$(\bot, \bot).$$

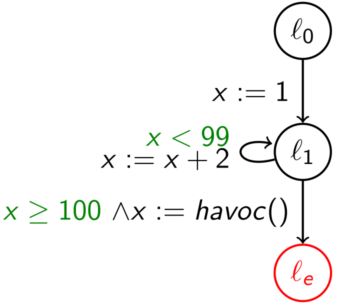
Abstract states may help each other for precision.

Example: interaction during fixedpoint computation

Example 16.4

Let us suppose D_1 = parity domain and D_2 = interval domain.

Consider the following program



$$\boxed{X_{\ell_0} = (\top, \top)}$$

$$\boxed{X_{\ell_1} = (Odd, [1, 100])}$$

$$\boxed{X_{\ell_e} = (\top, [100, 100])}$$

Exercise 16.4

Did we prove that ℓ_e is unreachable?

Reduced product : reduced function

We may define a reduction function

$$\rho : D_1 \times D_2 \rightarrow D_1 \times D_2.$$

ρ takes the product abstract state and returns a reduced states such that

$$\rho((a,b)) = \sqcap\{(a',b') | \gamma(a,b) \subseteq \gamma(a',b')\}$$

where $\gamma(a,b) = \gamma_1(a) \cap \gamma_2(b)$.

We can not implement the above definition in general. However, ρ satisfying the following is acceptable.

1. $\rho(a,b) \sqsubseteq (a,b)$
2. $\gamma(\rho(a,b)) = \gamma((a,b))$

Reduced product

We define the operators for reduced product as follows

1. $\alpha(c) = \rho(\alpha_1(c), \alpha_2(c))$
2. $sp^{\#}((a,b),\rho) = \rho(sp^{\#_1}(a,\rho), sp^{\#_2}(b,\rho))$
3. $(a,b)\nabla(a',b') = \rho(a\nabla_1 a', b\nabla_2 b')$✗

The ∇ operator may not satisfy the definition of widening operator.
Therefore, no guarantee of convergence.

Exercise 16.5

Show that if the following condition holds, then the above widening operator ensures convergence.

$$\forall a, a' \in D_1, b, b' \in D_2 \quad \exists a'' \in D_1, b'' \in D_2, \qquad (a\nabla_1 a', b\nabla_2 b') \in \rho(a'', b'')$$

Reduced product worked around for widening

If the condition in the last exercise holds, then well and good.

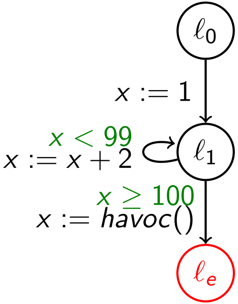
Then, we may simply choose not to apply reduction operator after widening, i.e.,

$$(a, b)\nabla(a', b') = (a\nabla_1 a', b\nabla_2 b').$$

We loose precision due to the above choice.

Example: reduced product

Example 16.5



Cartesian	Reduced
$\boxed{X_{\ell_0} = (\top, \top)}$	$\boxed{X_{\ell_0} = (\top, \top)}$
$\boxed{X_{\ell_1} = (Odd, [1, 100])}$	$\boxed{X_{\ell_1} = (Odd, [1, 99])}$
$\boxed{X_{\ell_e} = (\top, [100, 100])}$	$\boxed{X_{\ell_e} = (\top, \bot)}$

Now we have proven that ℓ_e is unreachable.

Granger product

Implementing, the reduction operator ρ is not entirely clear.

In granger product, the reduction operator is modular, i.e, each domains declare how it takes in the information form other.

$$\rho_i : D_1 \times D_2 \rightarrow D_i$$

where $i \in \{1, 2\}$.

ρ_1 and ρ_2 must satisfy the following conditions.

1. $\rho_1(a, b) \sqsubseteq a$
2. $\gamma_1(\rho(a, b)) \cap \gamma_2(b) = \gamma_1(a) \cap \gamma_2(b)$
3. $\rho_2(a, b) \sqsubseteq b$
4. $\gamma_1(a) \cap \gamma_2(\rho(a, b)) = \gamma_1(a) \cap \gamma_2(b)$

Granger product: ρ from ρ_is

The rest of scheme remains the same as reduced product. We implement ρ using ρ_is.

We compute $\rho(a, b)$ using the following iterates.

$$(a^0, b^0) := (a, b)$$
$$(a^n, b^n) := (\rho_1(a^{n-1}, b^{n-1}), \rho_2(a^{n-1}, b^{n-1}))$$

We interate until the sequence $(a^n, b^n)_{n \in \mathbb{N}}$ stabilizes.

The stabilized value is our $\rho(a, b)$.

Example: Granger product

Example 16.6

Consider state $(Even, [1,1])$

Let us first apply ρ_2

$$\rho_2(Even, [1,1]) = \bot$$

So we obtain state $(Even, \bot)$*.*

Let us apply ρ_1

$$\rho_1(Even, \bot) = \bot$$

So we obtain state $(\bot, \bot)$*.*

Why Granger product?

In principle, Granger product is same as reduced product.

The practical advantage of the Granger product is that we can separately define and implement $\rho_1$and ρ_2.

Therefore, an abstract interpretation tool can have modular implementation of domains.

Reduced cardinal power : exotic combination

We may compose two domains in completely different way.

Let us define the product domain

$$(D_1^{D_2}, \sqsubseteq)$$

where $\sqsubseteq$ is defined as follows

$$f \sqsubseteq g \qquad \triangleq \qquad \forall a \in D_1.\ f(a) \sqsubseteq_2 g(a).$$

Example 16.7

Let us suppose D_1 = parity domain and D_2 = interval domain.
$\{Even \mapsto [2,3], Odd \mapsto [19,3000]\} \in D_1^{D_2}$.

Exercise 16.6

Let x and y be variables in a program. Does the following hold?

- $\{Even_x \mapsto [2,3]_y, Odd_x \mapsto [1,3]_y\} \sqsubseteq \{Even_x \mapsto [2,6], Odd_x \mapsto [6,9]_y\}$
- $\{Even_x \mapsto [2,3]_y, Odd_x \mapsto \bot_y\} \sqsubseteq \{Even_x \mapsto [2,40], Odd_x \mapsto [1,33]_y\}$

Operators for reduced cardinal power

1. $\alpha(c) = \{a \to \alpha_2(c \cap \gamma_1(a)) | a \in D_1\}$
2. $f \triangledown f' = \{a \to f(a) \triangledown_2 f'(a) | a \in D_1\}$
3. $sp^{\#}((a, b), \rho) =$ (Need custom implementations!)

Since we have α, one may say that we can implement $sp^{\#}$.
However, α enumerates elements of D_1, which may be expensive.

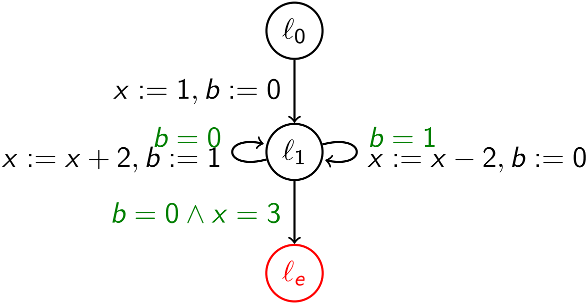
Widening also needs enumeration over D_1, therefore D_1 must be finite.

Example: reduced cardinal product

Example 16.8

Again, let us suppose $D_1 = \{b = 0, b = 1\}$ *and* $D_2 =$ *interval domain.*

Consider the following program



We need $X_{\ell_1} = \{b = 0 \mapsto x = 1, b = 1 \mapsto \top\}$ to prove the property.
Therefore, the need of reduced cardinal product.

End of Lecture 16