Advanced Static Analysis Techniques

20190065 김기환 (kimkihwan@kaist.ac.kr)

* Abstract domains =

1. Non-relational

2. Relational

3. Product domain

Use two or more different abstract domains together

3-1. Reduced Product

Each abstraction refines other abstraction to be more precise

4. Disjunctive Completion

Use multiple abstraction with ‘exact abstract join’

In practice, it cost much and sometimes it’s not possible to construct ‘e.a.j.’

5. Cardinal Power

Abstraction is consisted with conjunction of implications

Because of left-hand-side of implication, it looks like partition under

5-1. State Partitioning

Cardinal power abstract domain for memory

flow-sensitive = Compute on each program point

set as a label of program

context-sensitive = Compute on each context of procedure calls

set as an info. context of procedure call

5-2. dynamic partitioning

Choose an abstract domain that fit the target program

5-3. Trace Partitioning

Cardinal power abstract domain for program point

* Abstract domain = set of logical properties + abstract operators
* Abstract operators =

1. abstract lattice operation =

2. transfer function =

3. abstraction relation =

* Abstract iteration =

1. Loop unrolling

* a