Numeric Domains meet Algebraic Data Types
NSAD @ SPLASH 2020

Santiago Bautista    Thomas Jensen    Benoit Montagu

November 17, 2020
Motivation

Interactive Theorem Proving

Example

ProvenCore & Correlations: 2 proof obligations discharged
Motivation

Interactive Theorem Proving

Requires manual effort
Motivation

Interactive Theorem Proving

Static Analysis

Requires manual effort

Can alleviate manual effort
Motivation

Interactive Theorem Proving

Requires manual effort

Static Analysis

Can alleviate manual effort

Example

ProvenCore & Correlations: $\frac{2}{3}$ proof obligations discharged
Overview

Numeric Domains:
- Octagons
- Polyhedra
- Zones
- Zonotopes

Algebraic Types:
- Correlations
- Trees
- Lists
- Thread status
- Network sockets
Overview

Numeric Domains
- Octagons
- Polyhedra
- Zonotopes
- Zones

Algebraic Types
- Trees
- Lists
- Thread status
- Network sockets

Correlations (equalities)

Correlations (inequalities)
Overview

Numeric Domains
- Octagons
- Polyhedra
- Zonotopes
- Zones

Algebraic Types
- Correlations (equalities)
- Correlations (inequalities)
- Trees
- Lists
- Thread status
- Network sockets

S. Bautista, T. Jensen and B. Montagu
Overview

Numeric Domains
- Octagons
- Polyhedra
- Zonotopes
- Zones

Algebraic Types
- Trees
- Lists
- Network sockets
- Thread status

Correlations (equalities)
- NPRs

Correlations (inequalities)
**Product types**

**A product type**

```plaintext
type point = 
{absciss: number,
 ordinate: number}
```

**A record**

```plaintext
value origin = 
{ abciss = 0,
 ordinate = 0}
```

**Product types**

\[
\left\{ f_i \rightarrow \tau_i \mid i \in I \right\}
\]
A sum type

```haskell
type card =
    | Spades(Number)
    | Hearts(Number)
    | Clubs(Number)
    | Diamonds(Number)
```

A variant

```haskell
value hearts_queen =
    Hearts(12)
```

Sum types

\[
\left[ \sum_{i\in I} A_i \rightarrow \tau_i \right]
\]
Algebraic Types

Example

type thread_status =
    | Running {thread_id: Number, priority: Number}
    | Asleep {seconds : Number, thread_id: Number, priority: Number}

Definition

Arbitrary nesting of sum types and product types

\[
\tau ::= \text{Number} \mid \left\{ f_i \rightarrow \tau_i \right\}_{i \in I} \mid \left[ A_i \rightarrow \tau_i \right]_{i \in I}
\]
Algebraic Types

Example

```
type thread_status =
    | Running {thread_id: Number, priority: Number}
    | Asleep {seconds: Number, thread_id: Number, priority: Number}
```

Definition

Arbitrary nesting of sum types and product types

```
τ ::= Number | \{ f_i \rightarrow τ_i \}_{i \in I} | \left[ A_i \rightarrow τ_i \right]_{i \in I}
```

Limitation

We do not handle recursive types.
Numeric domains

Abstract domains

Polyhedra

Octagons

Zonotopes
Numeric domains

Abstract domains
- Polyhedra
- Octagons
- Zonotopes

Abstract values
- Constraints (Variables)
Numeric domains

Abstract domains
- Polyhedra
- Octagons
- Zonotopes

Abstract values
- Constraints (Variables)

Program
```java
    r := 1;
    while (n > 1) {
        r := n * r;
        n := n - 1;
    }
```
Numeric domains

Abstract domains

Polyhedra

Octagons

Zonotopes

Abstract values

Constraints (Variables)

Program

r := 1 ;
while (n > 1) {
    r := n * r ;
    n := n − 1 ;
}

Variables

n   r
Abstract domains

Polyhedra
Octagons
Zonotopes

Program
r := 1;
while (n > 1) {
    r := n * r;
    n := n - 1;
}

Variables
n  r

Program point
Abstract domains

Polyhedra

Octagons

Zonotopes

Abstract values

Constraints (Variables)

Program

r := 1 ;
while (n > 1) {
    r := n * r ;
    n := n - 1 ;
}

Program point

Variables

n    r

Constraint

r \geq n + 1
Numeric domains

Abstract domains
- Polyhedra
- Octagons
- Zonotopes

Abstract values
- Constraints (Variables)

Program
```
r := 1;
while (n > 1) {
    r := n * r;
    n := n - 1;
}
```

Variables
```
n
r
```

Constraint
```
r \geq n + 1
```
The Apron interface

**Numeric domain D**

Abstract values Constraints(Variables)
The Apron interface

Numeric domain $D$

Abstract values

Concretization function $\gamma^D$

Abstract intersection $\cap^D$

Abstract union $\cup^D$
The Apron interface

**Numeric domain D**

Abstract values $\text{Constraints(Variables)}$

Concretization function $\gamma^D$

Abstract intersection $\cap^D$

Abstract union $\cup^D$

Adding variables Add

Removing variables Remove

Renaming variables Rename
The Apron interface

Numeric domain $D$

- Abstract values
- Concretization function $\gamma^D$
- Abstract intersection $\cap^D$
- Abstract union $\cup^D$
- Adding variables Add
- Removing variables Remove
- Renaming variables Rename
numeric domains
- octagons
- zones
- polyhedra
- zonotopes

algebraic types
- correlations (equalities)
- trees
- lists
- thread status
- network sockets

correlations (inequalities)
Numeric Domains

Octagons
Zones
Polyhedra
Zonotopes

Correlations (equalities)

NPRs

Algebraic Types

Trees
Lists
Thread status
Network sockets
Numeric path relations

Apron interface

Numeric domain $D$

Abstract values $\text{Constraints(Variables)}$

Concretization function $\gamma^D$

Abstract intersection $\cap^D$

Abstract union $\cup^D$

Adding variables $\text{Add}$

Removing variables $\text{Remove}$

Renaming variables $\text{Rename}$
Numeric path relations

Apron interface

Numeric domain $D$

- Abstract values
- Concretization function $\gamma^D$
- Abstract intersection $\cap^D$
- Abstract union $\cup^D$
- Adding variables Add
- Removing variables Remove
- Renaming variables Rename

Numeric Path Relations
Numeric path relations

Apron interface

Numeric domain $D$  Numeric Path Relations

Abstract values  Constraints($\text{Variables}$)  Constraints($\text{Variables} \times \text{Paths}$)

Concretization function  $\gamma^D$

Abstract intersection  $\cap^D$

Abstract union  $\cup^D$

Adding variables  Add

Removing variables  Remove

Renaming variables  Rename
Numeric path relations

Apron interface

Numeric domain D

Abstract values
Concretization function
Abstract intersection
Abstract union
Adding variables
Removing variables
Renaming variables

Constraints(Variables)

Constraints(Variables × Paths)

$\gamma^D$

$\gamma^{NPR}$

$\cap^D$

$\cap^{NPR}$

$\cup^D$

$\cup^{NPR}$

Add
Remove
Rename
Projection over a path

\[
\text{Running} \times \text{thread\_id} \times \text{priority} \quad 42 \times 7
\]
Projection over a path

\[
\text{Running} \downarrow \text{val} \ @ \text{Running.thread_id} = 7
\]

\[
\begin{array}{c}
\times \\
\text{thread_id} & \text{priority} \\
42 & 7
\end{array}
\]
Projection over extended variables

Extended variables
Pair of a variable name and a path

Examples

\((x, \@\text{Running}.\text{thread}._\text{id})\) and \((x, \@\text{Running}.\text{priority})\)

\[
[x \mapsto \text{th}] \downarrow^{\text{env}} \{(x, \@\text{Running}.\text{id}), (x, \@\text{Running}.\text{priority})\} = \\
\begin{bmatrix}
(x, \@\text{Running}.\text{thread}._\text{id}) & \mapsto 42 \\
(x, \@\text{Running}.\text{priority}) & \mapsto 7
\end{bmatrix}
\]
function tick (x) =
  match x with
  | Asleep {seconds = s, thread_id = id, priority = p} →
    if (seconds == 1)
    then r := Running {thread_id = id, priority = p}
    else r := Asleep {seconds = s - 1, thread_id = id, priority = p}
  | _ → r := x ;
  return r

\[
\begin{align*}
  (r, \@\text{Asleep}.\text{seconds}) &= (x, \@\text{Asleep}.\text{seconds}) - 1, \\
  (r, \@\text{Asleep}.\text{thread\_id}) &= (x, \@\text{Asleep}.\text{thread\_id}), \\
  (r, \@\text{Asleep}.\text{priority}) &= (x, \@\text{Asleep}.\text{priority}) \\
  (r, \@\text{Running}.\text{thread\_id}) &= (x, \@\text{Asleep}.\text{thread\_id}), \\
  (r, \@\text{Running}.\text{priority}) &= (x, \@\text{Asleep}.\text{priority})
\end{align*}
\]
Transferred properties

Apron interface

Numeric domain D \( \cap^D \) is exact

\[ \text{Soundness properties} \]

Numeric Path Relations \( \cap^{NPR} \) is exact

\[ \text{Soundness properties} \]
Take away and future work

Numeric Path Relations:
- Extend any numeric domain (given the Apron Interface)
- Preserve soundness properties
- Preserve exactness of abstract intersection

Future work:
- Recursive types
- Implementation
Images from https://www.flaticon.com

TO BE COMPLETED

Go to https://www.flaticon.com/authors/<author_name> for more of their icons