universität innsbruck

supported by FWF project I 5943-N

Logically Constrained Analysis in CREST

Jonas Schöpf

ARI Final Meeting – Kira Onsen
21 February 2024

Overview

- Important Notions
- General Overview
- Pre-Processing
- Automation of Confluence Analysis
- Automation of Termination Analysis

Overview

- Important Notions
- General Overview
- Pre-Processing
- Automation of Confluence Analysis
- Automation of Termination Analysis

Important Definitions

- $\mathcal{LV}\text{ar}(\ell \to r\ [\varphi]) = \mathcal{V}\text{ar}(\varphi) \cup (\mathcal{V}\text{ar}(r) \setminus \mathcal{V}\text{ar}(\ell))$
- substitution $\gamma \vDash \ell \to r\ [\varphi]$ if
  - $\mathcal{D}\text{om}(\gamma) = \mathcal{V}\text{ar}(\ell) \cup \mathcal{V}\text{ar}(r) \cup \mathcal{V}\text{ar}(\varphi)$
  - $\gamma(x) \in \mathcal{V}\text{al}$ for all $x \in \mathcal{LV}\text{ar}(\ell \to r\ [\varphi])$
  - $\varphi\gamma$ is valid

Important Definitions

$\sigma \vDash \varphi$ if $\sigma(x) \in \mathcal{V}\text{al}$ for all $x \in \mathcal{V}\text{ar}(\varphi)$ and $\varphi\sigma$ is valid

Triviality

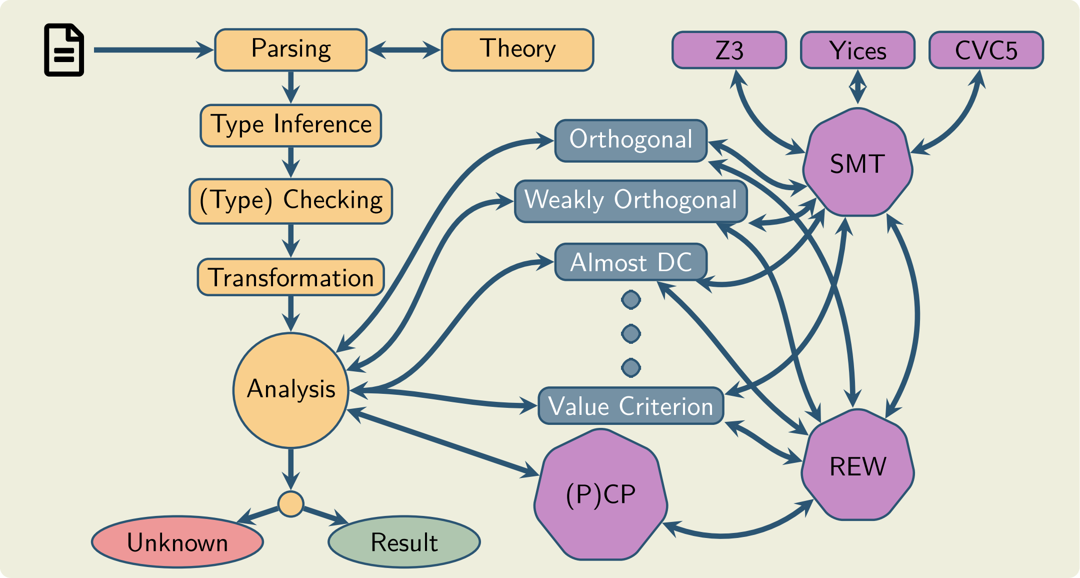
$s \approx t\ [\varphi]$ is trivial if $s\sigma = t\sigma$ for every σ with $\sigma \vDash \varphi$

Rewrite Relation

$\mathcal{R}_{\text{rc}}$ is the union of $\mathcal{R}$ and calculation rules $\mathcal{R}_{\text{ca}}$

$C[\ell\gamma]\ [\varphi] \to_{\text{rc}} C[r\gamma]\ [\varphi]$ if $\ell \to r\ [\varphi] \in \mathcal{R}_{\text{rc}}$ and $\gamma \vDash \ell \to r\ [\varphi]\rho\colon \ell \to r\ [\psi] \in \to_{\text{rc}}$, $\sigma(x) \in \mathcal{V}\text{al} \cup \mathcal{V}\text{ar}(\varphi)$ for all $x \in \mathcal{LV}\text{ar}(\rho), \varphi$ is satisfiable and $\varphi \Rightarrow \psi\sigma$ is valid

Overview


Parsing
Theory
Z3
Yices
CVC5
Type Inference
Orthogonal
SMT
(Type) Checking
Weakly Orthogonal
Transformation
Almost DC
Analysis
Value Criterion
REW
(P)CP
Unknown
Result

Use Cases for crest?

- (parallel) constrained critical pairs
- DP graph and SCCs
- confluence/termination analysis
- LCTRS tagging tool

General

- Haskell
- static compilation using musl (Linux)
- HTML benchmarks
- currently Ints, Reals and IntReals theories
- near future also FixedSizedBitvectors

Overview

- Important Notions
- General Overview
- Pre-Processing
- Automation of Confluence Analysis
- Automation of Termination Analysis

Parsing

- ARI syntax
- theory specified in SMTLIB
- infer some sort information

Type Inference & Checking

- type inference algorithm
- union-find
- check inferred sorts and LCTRS specifics

Transformations

- values from lhs to constraint
- unify rules
- split CCPs

Moving Values

$$\mathsf{f}(3) \to \mathsf{a}\ [\mathsf{true}]$$
$$\Downarrow$$
$$\mathsf{f}(x) \to \mathsf{a}\ [x = 3]$$

Unifying Rules

$$\mathsf{f}(3, \mathsf{g}(x)) \to y\ [x > 1]$$
$$\mathsf{f}(3, \mathsf{g}(y)) \to x\ [y < 1]$$
$$\Downarrow$$
$$\mathsf{f}(3, \mathsf{g}(x)) \to y\ [x < 1 \vee x > 1]$$

Splitting Critical Pairs

$$\begin{array}{rl} \mathsf{f}(1) \to \mathsf{b} & \mathsf{f}(x) \approx \mathsf{a}\ [1 \leqslant x \leqslant 2] \\ \mathsf{f}(2) \to \mathsf{b} & \Downarrow \\ \mathsf{a} \to \mathsf{b} & \mathsf{f}(x) \approx \mathsf{a}\ [1 \leqslant x \leqslant 2 \wedge x = 1] \\ & \mathsf{f}(x) \approx \mathsf{a}\ [1 \leqslant x \leqslant 2 \wedge x \neq 1] \end{array}$$

Overview

- Important Notions
- General Overview
- Pre-Processing
- Automation of Confluence Analysis
- Automation of Termination Analysis

Weak Orthogonality

left-linear LCTRS with only trivial critical pairs

Automation

- computation of CCPs
- no CCPs and left-linear then orthogonal
- some CCPs and left-linear then check triviality

Example

$$\begin{aligned} \mathsf{ack}(0, n) &\to n + 1 \ [n \geqslant 0] \\ \mathsf{ack}(m, 0) &\to \mathsf{ack}(m - 1, 1) \ [m > 0] \\ \mathsf{ack}(m, n) &\to \mathsf{ack}(m - 1, \mathsf{ack}(m, n - 1)) \ [m > 0 \land n > 0] \\ \mathsf{ack}(m, n) &\to 0 \ [m < 0 \lor n < 0] \end{aligned}$$

Strongly Closedness CCP

1. $s \approx t\ [\varphi]\ \tilde{\rightarrow}^{*}_{\geqslant 1} \cdot \tilde{\rightarrow}^{=}_{\geqslant 2}\ u \approx v\ [\psi]$ for some trivial $u \approx v\ [\psi]$
2. $s \approx t\ [\varphi]\ \tilde{\rightarrow}^{*}_{\geqslant 2} \cdot \tilde{\rightarrow}^{=}_{\geqslant 1}\ u \approx v\ [\psi]$ for some trivial $u \approx v\ [\psi]$

Automation

- no equivalence steps
- approximate transitive step by heuristic
- compute all possible reducts
- find trivial constrained equation

Example

$$\mathsf{f}(\mathsf{g}(x), y) \to \mathsf{f}(\mathsf{b}, y) \qquad \mathsf{g}(x) \to \mathsf{a} \qquad \mathsf{f}(\mathsf{a}, x) \to x \qquad \mathsf{f}(\mathsf{b}, x) \to x$$

$$\mathsf{f}(\mathsf{a}, y) \approx \mathsf{f}(\mathsf{b}, y)\ [\mathsf{true}] \to_{\geqslant 2} \mathsf{f}(\mathsf{a}, y) \approx y\ [\mathsf{true}] \to_{\geqslant 1} y \approx y\ [\mathsf{true}]$$

Almost Parallel Closedness CCP

inner critical pair is parallel closed and overlays

$$s \approx t\ [\varphi]\ \tilde{\twoheadrightarrow\!\!\!\!\!\!+}_{\geqslant 1} \cdot \tilde{\rightarrow}^*_{\geqslant 2}\ u \approx v\ [\psi]$$

for trivial $u \approx v\ [\psi]$

Automation

- similar to strongly closedness
- perform parallel step

Example

$$\mathsf{f}(x,y) \to \mathsf{g}(\mathsf{a}, y+y)\ [y \geqslant x \land y = 1] \qquad \mathsf{a} \to \mathsf{b}$$
$$\mathsf{f}(x,y) \to \mathsf{g}(\mathsf{b}, 2)\ [x \geqslant y] \qquad \mathsf{g}(x,y) \to \mathsf{g}(y,x)$$

$$\mathsf{g}(\mathsf{b},2) \approx \mathsf{g}(\mathsf{a}, y+y)\ [x = y \land y = 1]\ \tilde{\twoheadrightarrow\!\!\!\!\!\!+}_{\geqslant 2}\ \mathsf{g}(\mathsf{b},2) \approx \mathsf{g}(\mathsf{b},2)\ [\mathsf{true}]$$

Almost Development Closedness CCP

not overlay then development closed, or overlay and $s \approx t\ [\varphi] \xrightarrow{\sim}\!\!\!\!\circ_{\geqslant 1} \cdot \xrightarrow{\sim}{}^{*}_{\geqslant 2} u \approx v\ [\psi]$ for trivial $u \approx v\ [\psi]$

Automation

- compute all possible multisteps
- again find trivial constrained equation

Example

$$\mathsf{f}(x,y) \to \mathsf{h}(\mathsf{g}(y, 2 \cdot 2))\ [x \leqslant y \wedge y = 2] \qquad \mathsf{g}(x,y) \to \mathsf{g}(y,x) \qquad \mathsf{h}(x) \to x$$

$$\mathsf{f}(x,y) \to \mathsf{c}(4,x)\ [y \leqslant x] \qquad \mathsf{c}(x,y) \to \mathsf{g}(4,2)\ [x \neq y]$$

$$\mathsf{h}(\mathsf{g}(y, 2 \cdot 2)) \approx \mathsf{c}(4,x)\ [\varphi] \qquad \mathsf{c}(4,x) \approx \mathsf{h}(\mathsf{g}(y, 2 \cdot 2))\ [\varphi]$$

1-Parallel Closedness CCP

$s \approx t\ [\varphi] \mathrel{\overset{\sim}{\mathrel{\|}\!\!\!\!\rightarrow}}_{\geqslant 1} \cdot \overset{\sim}{\rightarrow}{}^{*}_{\geqslant 2}\ u \approx v\ [\psi]$ for some trivial $u \approx v\ [\psi]$

2-Parallel Closedness CCP

for $\ell\sigma[r_p\sigma]_{p \in P} \approx r\sigma\ [\varphi]$ exists Q such that

$$\ell\sigma[r_p\sigma]_{p \in P} \approx r\sigma\ [\varphi] \mathrel{\overset{\sim}{\mathrel{\|}\!\!\!\!\rightarrow}}{}^{Q}_{\geqslant 2} \cdot \overset{\sim}{\rightarrow}{}^{*}_{\geqslant 1}\ u \approx v\ [\psi]$$

for trivial $u \approx v\ [\psi]$ and $\mathcal{TV}\mathsf{ar}(v, \psi, Q) \subseteq \mathcal{TV}\mathsf{ar}(\ell\sigma, \varphi, P)$.

Parallel Closed (P)CPs

LCTRS is parallel closed if it is 1-parallel closed and 2-parallel closed

Automation

- synthesize Q with the desired property
- check variable condition
- remaining similar

Example

$$\mathsf{f}(\mathsf{a}) \to \mathsf{g}(4,4) \qquad \mathsf{a} \to \mathsf{g}(1+1,3+1) \qquad \mathsf{g}(x,y) \to \mathsf{f}(\mathsf{g}(z,y))\ [z = x - 2]$$

$$\mathsf{f}(\mathsf{g}(1+1,3+1)) \approx \mathsf{g}(4,4)\ [\mathsf{true}] \qquad \mathsf{f}(\mathsf{g}(z,y)) \approx \mathsf{f}(\mathsf{g}(z',y))\ [z = x - 2 \land z' = x - 2]$$

Non-Confluence

- normal form
- non-trivial constrained equation which is in normal form

Example

CCP $\mathsf{f}(x) \approx \mathsf{g}(x)\ [1 \leqslant x \leqslant 2]$ and rules

$$\mathsf{f}(1) \to \mathsf{g}(1) \qquad \mathsf{f}(2) \to \mathsf{g}(2)$$

in normal form by standard notion

Overview

- Important Notions
- General Overview
- Pre-Processing
- Automation of Confluence Analysis
- Automation of Termination Analysis

Automation of Termination

- initially bachelor project
- rewritten
- dependency pairs, DP graph, value criterion, constrained reduction order
- some mistakes and inaccuracies in Kop WST paper

Example

$$\begin{aligned} \mathsf{ack}(0, n) &\to n + 1 \ [n \geqslant 0] \\ \mathsf{ack}(m, 0) &\to \mathsf{ack}(m - 1, 1) \ [m > 0] \\ \mathsf{ack}(m, n) &\to \mathsf{ack}(m - 1, \mathsf{ack}(m, n - 1)) \ [m > 0 \wedge n > 0] \\ \mathsf{ack}(m, n) &\to 0 \ [m < 0 \vee n < 0] \end{aligned}$$

Experiments

HTML Produced by crest

Outlook

- improve termination implementation
- bachelor project for completion
- open bachelor project about termination
- bitvectors (for Coco 2024)
- labeling techniques?
- ...