universität innsbruck

supported by FWF project I 5943-N

# Automated Analysis of Logically Constrained Programs

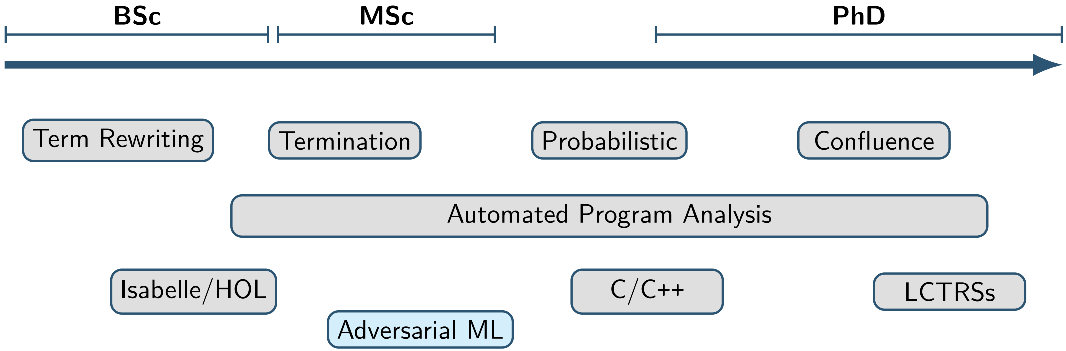
Jonas Schöpf

Data Lab Hell

4 March 2025

# Jonas Schöpf

- computer science @ UIBK
- Computational Logic
- mathematics ∩ computer science
- PhD in computer science (∼ summer 2025)



BSc

MSc

PhD

Term Rewriting

Termination

Probabilistic

Confluence

Automated Program Analysis

Isabelle/HOL

Adversarial ML

C/C++

LCTRSs

# Table of Contents

- Overview
- LCTRSs
- Confluence Analysis
- Automation

# Table of Contents

- Overview

- LCTRSs

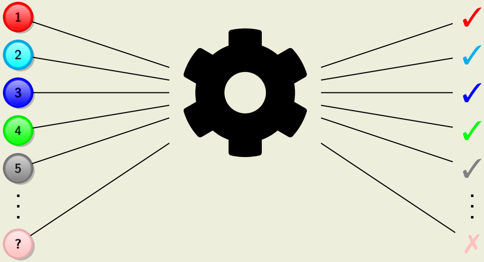
- Confluence Analysis

- Automation

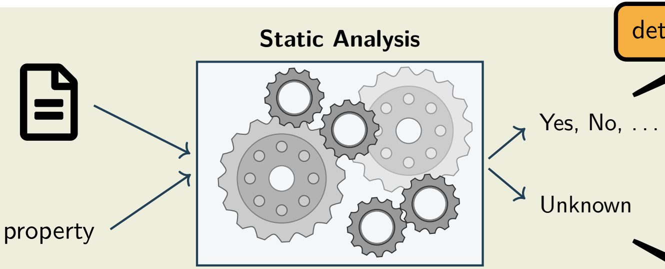
## How to Avoid Bugs?

- program carefully? skilled programmers?
- bugs are not obvious
- complex (million lines of code)
- bugs may not be detected by testing

## Testing?



# Static Program Analysis



detailed argumentation

no complete way exists

## Properties

- **termination** does the program finish in a finite amount of time?
- **confluence** does the program compute unique solutions?
- **complexity** how long does the program run?
- . . .

## Term Rewrite Systems (TRSs)

| | |
|---|---|
| set of function symbols | $\{\mathsf{max}, \mathsf{0}\}$ |
| set of variables | $\{x, y, z, \ldots\}$ |
| terms | $\mathsf{max}(x, y), \mathsf{max}(\mathsf{max}(x, \mathsf{0}), z), \ldots$ |
| rules | $\mathsf{max}(\mathsf{s}(\mathsf{0}), \mathsf{0}) \to \mathsf{s}(\mathsf{0})$ |
| set of rules | $\{\mathsf{max}(\mathsf{s}(\mathsf{0}), \mathsf{0}) \to \mathsf{s}(\mathsf{0}), \ldots\}$ |

- terms represent program states
- rewriting represents computation
- term rewriting is Turing-complete

# Term Rewrite System

signature $\{\mathsf{max}, \mathsf{ite}, \mathsf{s}, \mathsf{p}, \mathsf{geq}, \mathsf{geq2}, \mathsf{0}, \mathsf{true}, \mathsf{false}\}$ and rules

$$\begin{aligned}
\mathsf{max}(x,y) &\to \mathsf{ite}(\mathsf{geq}(x,y),x,y) & \mathsf{ite}(\mathsf{true},x,y) &\to x \\
\mathsf{max}(x,y) &\to \mathsf{max}(y,x) & \mathsf{ite}(\mathsf{false},x,y) &\to y \\
\mathsf{s}(\mathsf{p}(x)) &\to x & \mathsf{p}(\mathsf{s}(x)) &\to x \\
\mathsf{geq}(x,y) &\to \mathsf{geq2}(x,y,\mathsf{0},\mathsf{0}) & \mathsf{geq2}(\mathsf{s}(x),y,z,u) &\to \mathsf{geq2}(x,y,\mathsf{s}(z),u) \\
\mathsf{geq2}(\mathsf{p}(x),y,z,u) &\to \mathsf{geq2}(x,y,z,\mathsf{s}(u)) & \mathsf{geq2}(\mathsf{0},\mathsf{s}(x),y,z) &\to \mathsf{geq2}(\mathsf{0},x,y,\mathsf{s}(z)) \\
\mathsf{geq2}(\mathsf{0},\mathsf{p}(x),y,z) &\to \mathsf{geq2}(\mathsf{0},x,\mathsf{s}(y),z) & \mathsf{geq2}(\mathsf{0},\mathsf{0},\mathsf{s}(x),\mathsf{s}(y)) &\to \mathsf{geq2}(\mathsf{0},\mathsf{0},x,y) \\
\mathsf{geq2}(\mathsf{0},\mathsf{0},x,\mathsf{0}) &\to \mathsf{true} & \mathsf{geq2}(\mathsf{0},\mathsf{0},\mathsf{0},\mathsf{s}(x)) &\to \mathsf{false}
\end{aligned}$$

compute $\max(4,5)$: $\mathsf{max}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{0})))),\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{0}))))))$

$$\begin{aligned}
\mathsf{max}(\mathsf{s}^4(\mathsf{0}),\mathsf{s}^5(\mathsf{0})) &\to \mathsf{ite}(\mathsf{geq}(\mathsf{s}^4(\mathsf{0}),\mathsf{s}^5(\mathsf{0})),\mathsf{s}^4(\mathsf{0}),\mathsf{s}^5(\mathsf{0})) \\
&\to \mathsf{ite}(\mathsf{geq2}(\mathsf{s}^4(\mathsf{0}),\mathsf{s}^5(\mathsf{0})),\mathsf{s}^4(\mathsf{0}),\mathsf{s}^5(\mathsf{0}),\mathsf{0},\mathsf{0}) \\
&\to^{12} \mathsf{s}^5(\mathsf{0}) = \mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{0})))))
\end{aligned}$$

## Rewriting Formalisms

MSTRS

HRS

SRS

AFS

CTRS

**LCTRS**

CRS

CSTRS

TRS

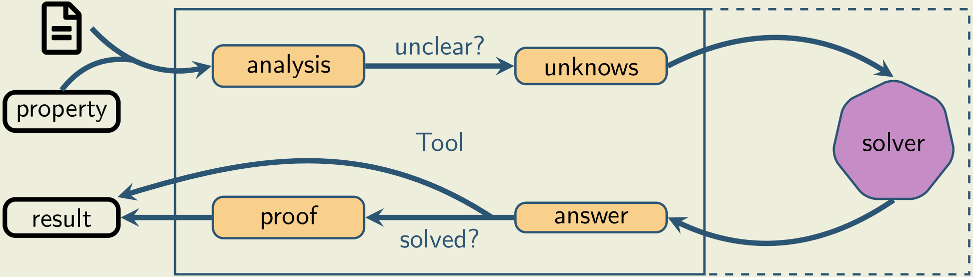
LCSTRS

LCTRS (Ciobâcă et al.)

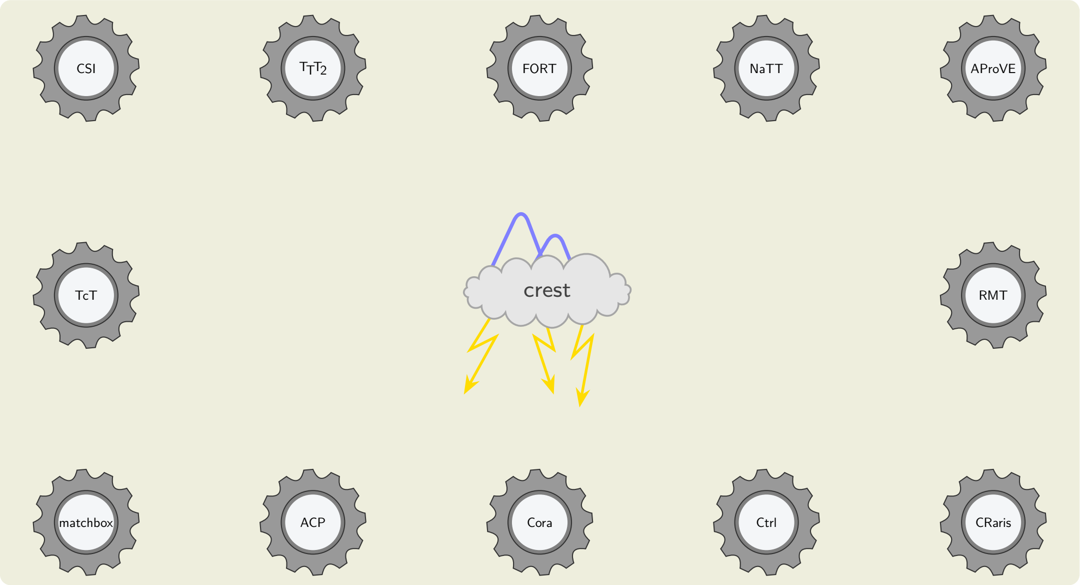
CSCTRS

# Automation

- tedious & error-prone by hand
- large & complex systems
- properties involve non-trivial checks



# Tools



CSI

$\mathsf{T_TT_2}$

FORT

NaTT

AProVE

TcT

crest

RMT

matchbox

ACP

Cora

Ctrl

CRaris

## Table of Contents

- Overview
- LCTRSs
- Confluence Analysis
- Automation

# Example

LCTRS $\mathcal{M}$

$$\mathcal{I}_{\mathsf{Bool}} = \mathbb{B} \qquad \mathcal{I}_{\mathsf{Int}} = \mathbb{Z}$$

$$\begin{aligned}
\mathcal{F}_{\mathsf{te}} &= \quad \ldots, -1, 0, 1, \ldots : \mathsf{Int} & \mathsf{max} &: [\mathsf{Int}] \Rightarrow \mathsf{Int} \\
\mathcal{F}_{\mathsf{th}} &= \quad \ldots, -1, 0, 1, \ldots : \mathsf{Int} & \wedge &: [\mathsf{Bool} \times \mathsf{Bool}] \Rightarrow \mathsf{Bool} \\
& \qquad \mathsf{true}, \mathsf{false} : \mathsf{Bool} & +, - &: [\mathsf{Int} \times \mathsf{Int}] \Rightarrow \mathsf{Int} \\
& \qquad \neg : [\mathsf{Bool}] \Rightarrow \mathsf{Bool} & \leqslant, \geqslant, = &: [\mathsf{Int} \times \mathsf{Int}] \Rightarrow \mathsf{Bool}
\end{aligned}$$

$$\mathcal{M} = \qquad \mathsf{max}(x, y) \to x\ [x \geqslant y] \qquad \mathsf{max}(x, y) \to y\ [y \geqslant x] \qquad \mathsf{max}(x, y) \to \mathsf{max}(y, x)$$

compute $\max(4, 5)$: $\qquad \mathsf{max}(4, 5) \to 5$

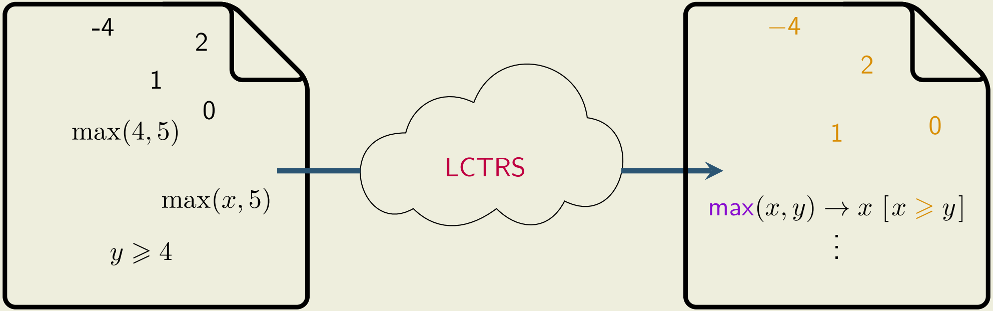
$\mathsf{max}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(0)))), \mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(0)))))) \to^{14} \mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(0)))))$

## Utilize SMT Solver

- solving formula with special interpretations
- built-in structures (e.g. integers)
- term (syntax) & theory (semantics)
- automation via SMT-solvers
  - recently more powerful
  - real numbers, integers, bit-vectors, arrays, . . .
  - Z3, CVC5, . . .

# Computational Model

- difficult on real programs
- use computational model
- formal methods



-4 2 1 0 $\max(4,5)$

$\max(x,5)$

$y \geqslant 4$

LCTRS

$-4$ 2 1 0

$\mathsf{max}(x,y) \to x\ [x \geqslant y]$

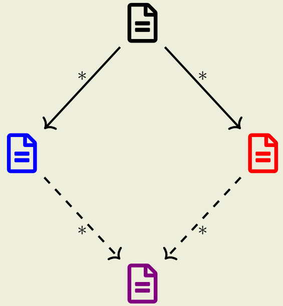
$\vdots$

# Table of Contents

- Overview
- LCTRSs
- Confluence Analysis
- Automation

## Confluence

- no general way
- test this for all computations?
- extract critical parts



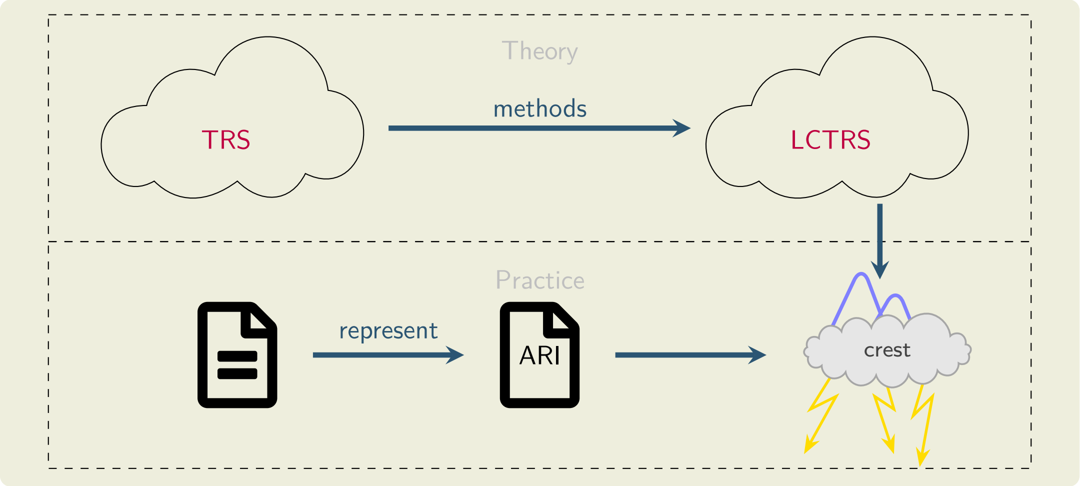
## Term Rewrite System (TRS)

- many methods for confluence
- decades of research
- difficult for real programs

## Logically Constrained TRS (LCTRS)

- extension of TRS
- built-in computations (including solvers)
- not many methods
- re-use existing knowledge

# My Research



## Example

computation rules

$$\mathsf{max}(x, y) \to x\ [x \geqslant y] \qquad \mathsf{max}(x, y) \to y\ [y \geqslant x] \qquad \mathsf{max}(x, y) \to \mathsf{max}(y, x)$$

critical parts

$$x \approx y\ [y \geqslant x \wedge x \geqslant y] \qquad \underbrace{x \approx \mathsf{max}(y, x)\ [x \geqslant y]} \qquad y \approx \mathsf{max}(y, x)\ [y \geqslant x]$$

confluence criterion

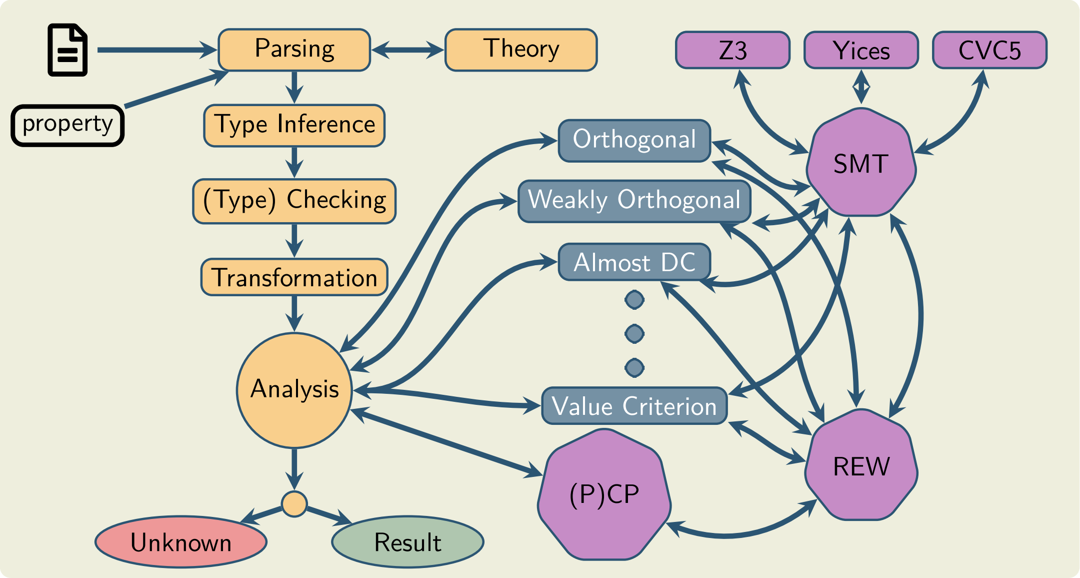
$$\ldots \qquad x \approx \mathsf{max}(y, x)\ [x \geqslant y] \to x \approx x\ [x \geqslant y] \qquad \ldots$$

$\Longrightarrow$ confluence

# Table of Contents

- Overview
- LCTRSs
- Confluence Analysis
- Automation

# Simplified Overview of crest



## Confluence Competititon

- annual competition since 2012
- LCTRS category 2024
- 1st place for crest

## Confluence Experiments on 107 Problems

| tool | ✓ | ✗ | solved | time (total) |
|---|---|---|---|---|
| CRaris | 58 | 0 | 54 % | 14 s |
| crest | 72 | 26 | 92 % | 197 s |
| Ctrl | 54 | 0 | 50 % | 18 s |

## Summary

- programs have bugs & testing may not suffice
- program analysis with computational model (LCTRSs)
- methods for confluence of LCTRSs
- push-button automation