Automated Termination and Complexity Analysis of Programs

Carsten Fuhs

Birkbeck, University of London

EuroProofNet Summer School on
Verification Technology, Systems & Applications 2022

Saarbrücken, Germany

5 & 7 September 2022

https://www.dcs.bbk.ac.uk/~carsten/vtsa2022/

Quality Assurance for Software by Program Analysis

Two approaches:

Quality Assurance for Software by Program Analysis

Two approaches:

- Dynamic analysis:

  Run the program on example inputs (testing).

  \+ goal: find errors

  – requires good choice of test cases

  – in general no guarantee for absence of errors

Quality Assurance for Software by Program Analysis

Two approaches:

- Dynamic analysis:
  Run the program on example inputs (testing).
  + goal: find errors
  — requires good choice of test cases
  — in general no guarantee for absence of errors
- Static analysis:
  Analyse the program text without actually running the program.
  + can prove (verify) correctness of the program
  $\longrightarrow$ important for safety-critical applications
  $\longrightarrow$ motivating example: first flight of Ariane 5 rocket in 1996
  https://www.youtube.com/watch?v=PK_yguLapgA
  https://en.wikipedia.org/wiki/Ariane_5_Flight_501
  — manual static analysis requires high effort and expertise
  $\Rightarrow$ for broad applicability:

Build automatic tools for static analysis!

Static Analysis: the User's Perspective (1/2)

For the user (programmer): Use static analysis tools as "black boxes".

Static Analysis: the User's Perspective (1/2)

For the user (programmer): Use static analysis tools as "black boxes".

What properties of programs do we want to analyse?

Static Analysis: the User's Perspective (1/2)

For the user (programmer): Use static analysis tools as "black boxes".

What properties of programs do we want to analyse?

- **Partial Correctness**
  $\longrightarrow$ will my program always produce the right result?

Static Analysis: the User's Perspective (1/2)

For the user (programmer): Use static analysis tools as "black boxes".

What properties of programs do we want to analyse?

- **Partial Correctness**
  $\longrightarrow$ will my program always produce the right result?
- **Assertions by the programmer**. `assert x > 0`
  $\longrightarrow$ will this always be true?

Static Analysis: the User's Perspective (1/2)

For the user (programmer): Use static analysis tools as "black boxes".

What properties of programs do we want to analyse?

- **Partial Correctness**
  $\longrightarrow$ will my program always produce the right result?
- **Assertions by the programmer**. `assert x > 0`
  $\longrightarrow$ will this always be true?
- **Equivalence**. Do two programs always produce the same result?
  $\longrightarrow$ correctness of refactoring

Static Analysis: the User's Perspective (1/2)

For the user (programmer): Use static analysis tools as "black boxes".

What properties of programs do we want to analyse?

- **Partial Correctness**
  $\longrightarrow$ will my program always produce the right result?
- **Assertions by the programmer**. `assert x > 0`
  $\longrightarrow$ will this always be true?
- **Equivalence**. Do two programs always produce the same result?
  $\longrightarrow$ correctness of refactoring
- **Confluence**. For languages with non-deterministic rules/commands: Does my program always produce the same result?

  > *Confluence is a property that establishes the global determinism of a computation despite possible local non-determinism.*
  > [Hristakiev, *PhD thesis '17*]

  $\longrightarrow$ does the order of applying compiler optimisation rules matter?

Static analysis: the user's perspective (2/2)

- **Memory Safety**
  - $\longrightarrow$ are my memory accesses always legal?

    ```
    int* x = NULL;  *x = 42;
    ```

  - $\longrightarrow$ undefined behaviour!
  - $\longrightarrow$ memory safety matters: Heartbleed (OpenSSL attack)

Static analysis: the user's perspective (2/2)

- **Memory Safety**

  $\longrightarrow$ are my memory accesses always legal?

  ```
  int* x = NULL;  *x = 42;
  ```

  $\longrightarrow$ undefined behaviour!

  $\longrightarrow$ memory safety matters: Heartbleed (OpenSSL attack)

- **Termination**

  $\longrightarrow$ will my program give an output for all inputs
  in finitely many steps?

Static analysis: the user's perspective (2/2)

- **Memory Safety**
  $\longrightarrow$ are my memory accesses always legal?

  ```
  int* x = NULL;  *x = 42;
  ```

  $\longrightarrow$ undefined behaviour!
  $\longrightarrow$ memory safety matters: Heartbleed (OpenSSL attack)
- **Termination**
  $\longrightarrow$ will my program give an output for all inputs in finitely many steps?
- **(Quantitative) Resource Use** aka **Complexity**
  $\longrightarrow$ how many steps will my program need in the worst case? (runtime complexity)
  $\longrightarrow$ how large can my data become? (size complexity)

Static analysis: the user's perspective (2/2)

- **Memory Safety**
  $\longrightarrow$ are my memory accesses always legal?
  `int* x = NULL;  *x = 42;`
  $\longrightarrow$ undefined behaviour!
  $\longrightarrow$ memory safety matters: Heartbleed (OpenSSL attack)
- **Termination**
  $\longrightarrow$ will my program give an output for all inputs
  in finitely many steps?
- **(Quantitative) Resource Use** aka **Complexity**
  $\longrightarrow$ how many steps will my program need in the worst case?
  (runtime complexity)
  $\longrightarrow$ how large can my data become? (size complexity)

Note: All these properties are **undecidable**!
$\Rightarrow$ use automatable sufficient criteria in practice

APROVE ... since 2001

- Program analysis tool developed in Aachen, London, Innsbruck, ...

APROVE . . . since 2001

- Program analysis tool developed in Aachen, London, Innsbruck, . . .
- Fully automated, hundreds of techniques for **termination**, **time complexity bounds**, . . .

Termination

Complexity

Non-Termination

AProVE ... since 2001

- Program analysis tool developed in Aachen, London, Innsbruck, ...
- Fully automated, hundreds of techniques for **termination**, **time complexity bounds**, ...
- Highly configurable via **strategy language**

Termination

Complexity

Non-Termination

APROVE . . . since 2001

- Program analysis tool developed in Aachen, London, Innsbruck, . . .
- Fully automated, hundreds of techniques for **termination**, **time complexity bounds**, . . .
- Highly configurable via **strategy language**
- Proofs usually have many steps $\longrightarrow$ construct **proof tree**

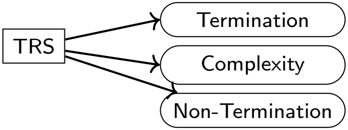
Termination

Complexity

Non-Termination

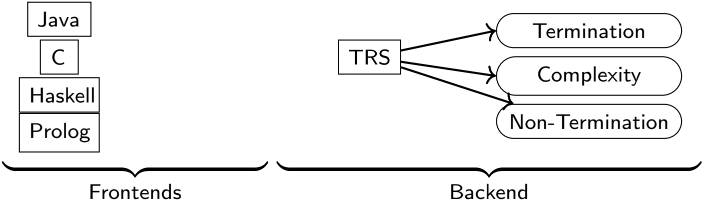
... since 2001

- Program analysis tool developed in Aachen, London, Innsbruck, ...
- Fully automated, hundreds of techniques for **termination**, **time complexity bounds**, ...
- Highly configurable via **strategy language**
- Proofs usually have many steps $\longrightarrow$ construct **proof tree**
- Founding tool of Termination Competition, since 2004
- Initially: analyse **termination** of **term rewrite systems (TRSs)**, later also complexity bounds



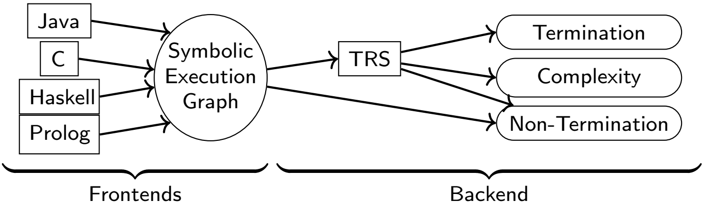
AProVE . . . since 2001

- Program analysis tool developed in Aachen, London, Innsbruck, . . .
- Fully automated, hundreds of techniques for **termination**, **time complexity bounds**, . . .
- Highly configurable via **strategy language**
- Proofs usually have many steps $\longrightarrow$ construct **proof tree**
- Founding tool of Termination Competition, since 2004
- Initially: analyse **termination** of **term rewrite systems (TRSs)**, later also complexity bounds
- Since 2006 more input languages: Prolog, Haskell, Java, C (via LLVM)



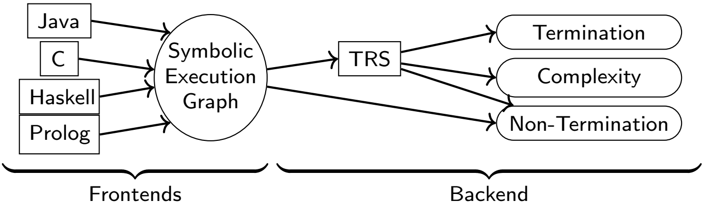
AProVE . . . since 2001

- Program analysis tool developed in Aachen, London, Innsbruck, . . .
- Fully automated, hundreds of techniques for **termination**, **time complexity bounds**, . . .
- Highly configurable via **strategy language**
- Proofs usually have many steps → construct **proof tree**
- Founding tool of Termination Competition, since 2004
- Initially: analyse **termination** of **term rewrite systems (TRSs)**, later also complexity bounds
- Since 2006 more input languages: Prolog, Haskell, Java, C (via LLVM)
  1. dedicated program analysis by symbolic execution and abstraction



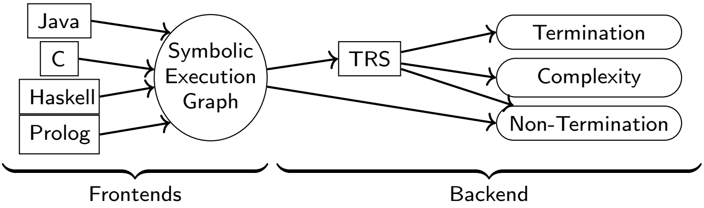
AProVE . . . since 2001

- Program analysis tool developed in Aachen, London, Innsbruck, . . .
- Fully automated, hundreds of techniques for **termination**, **time complexity bounds**, . . .
- Highly configurable via **strategy language**
- Proofs usually have many steps $\longrightarrow$ construct **proof tree**
- Founding tool of Termination Competition, since 2004
- Initially: analyse **termination** of **term rewrite systems (TRSs)**, later also complexity bounds
- Since 2006 more input languages: Prolog, Haskell, Java, C (via LLVM)
  1. dedicated program analysis by symbolic execution and abstraction
  2. extract rewrite system



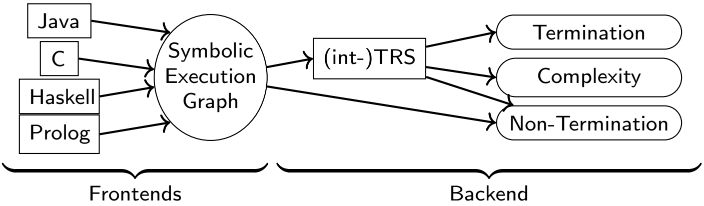
AProVE . . . since 2001

- Program analysis tool developed in Aachen, London, Innsbruck, . . .
- Fully automated, hundreds of techniques for **termination**, **time complexity bounds**, . . .
- Highly configurable via **strategy language**
- Proofs usually have many steps $\longrightarrow$ construct **proof tree**
- Founding tool of Termination Competition, since 2004
- Initially: analyse **termination** of **term rewrite systems (TRSs)**, later also complexity bounds
- Since 2006 more input languages: Prolog, Haskell, Java, C (via LLVM)
  1. dedicated program analysis by symbolic execution and abstraction
  2. extract rewrite system
  3. termination of rewrite system $\Rightarrow$ termination of program



AProVE . . . since 2001

- Program analysis tool developed in Aachen, London, Innsbruck, . . .
- Fully automated, hundreds of techniques for **termination**, **time complexity bounds**, . . .
- Highly configurable via **strategy language**
- Proofs usually have many steps $\longrightarrow$ construct **proof tree**
- Founding tool of Termination Competition, since 2004
- Initially: analyse **termination** of **term rewrite systems (TRSs)**, later also complexity bounds
- Since 2006 more input languages: Prolog, Haskell, Java, C (via LLVM)
  1. dedicated program analysis by symbolic execution and abstraction
  2. extract constrained rewrite system (constraints in integer arithmetic)
  3. termination of constrained rewrite system $\Rightarrow$ termination of program



What is Static Program Analysis About?

Goal: (Automatically) prove whether a given program P has (un)desirable property
Approach: Often in two phases

What is Static Program Analysis About?

Goal: (Automatically) prove whether a given program P has (un)desirable property
Approach: Often in two phases

Front-End

- Input: Program in Java, C, Prolog, Haskell, ...
- Output: Mathematical representation amenable to automated analysis (usually some kind of transition system)
- Often over-approximation, preserves the property of interest

What is Static Program Analysis About?

Goal: (Automatically) prove whether a given program P has (un)desirable property
Approach: Often in two phases

Front-End

- Input: Program in Java, C, Prolog, Haskell, ...
- Output: Mathematical representation amenable to automated analysis (usually some kind of transition system)
- Often over-approximation, preserves the property of interest

Back-End

- Performs the analysis of the desired property

⇒ Result carries over to original program

I. Termination Analysis

Why Analyse Termination?

Why Analyse Termination?

1. **Program**: produces result

Why Analyse Termination?

1. **Program**: produces result
2. **Input handler**: system reacts

Why Analyse Termination?

1. **Program**: produces result
2. **Input handler**: system reacts
3. **Mathematical proof**: the induction is valid

Why Analyse Termination?

1. **Program**: produces result
2. **Input handler**: system reacts
3. **Mathematical proof**: the induction is valid
4. **Biological process**: reaches a stable state

Why Analyse Termination?

1. **Program**: produces result
2. **Input handler**: system reacts
3. **Mathematical proof**: the induction is valid
4. **Biological process**: reaches a stable state

Variations of the same problem:

- 2 special case of 1
- 3 can be interpreted as 1
- 4 probabilistic version of 1

Why Analyse Termination?

1. **Program**: produces result
2. **Input handler**: system reacts
3. **Mathematical proof**: the induction is valid
4. **Biological process**: reaches a stable state

Variations of the same problem:

- 2 special case of 1
- 3 can be interpreted as 1
- 4 probabilistic version of 1

2011: PHP and Java issues with floating-point number parser

- http://www.exploringbinary.com/php-hangs-on-numeric-value-2-2250738585072011e-308/
- http://www.exploringbinary.com/java-hangs-when-converting-2-2250738585072012e-308/

The Bad News

Theorem (Turing 1936)

The question if a given program terminates on a fixed input is undecidable.

The Bad News

Theorem (Turing 1936)

The question if a given program terminates on a fixed input is undecidable.

- We want to solve the (harder) question if a given program terminates on **all** inputs.

The Bad News

Theorem (Turing 1936)

The question if a given program terminates on a fixed input is undecidable.

- We want to solve the (harder) question if a given program terminates on **all** inputs.
- That's not even semi-decidable!

The Bad News

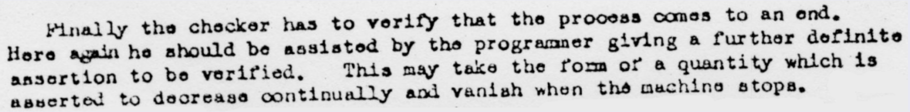
Theorem (Turing 1936)

The question if a given program terminates on a fixed input is undecidable.

- We want to solve the (harder) question if a given program terminates on **all** inputs.
- That's not even semi-decidable!
- But, fear not ...

Termination Analysis, Classically

Turing 1949



Finally the checker has to verify that the process comes to an end. Here again he should be assisted by the programmer giving a further definite assertion to be verified. This may take the form of a quantity which is asserted to decrease continually and vanish when the machine stops.

"Finally the checker has to verify that the process comes to an end. [...] This may take the form of a quantity which is asserted to decrease continually and vanish when the machine stops."

Termination Analysis, Classically

Turing 1949

Finally the checker has to verify that the process comes to an end. Here again he should be assisted by the programmer giving a further definite assertion to be verified. This may take the form of a quantity which is asserted to decrease continually and vanish when the machine stops.

"Finally the checker has to verify that the process comes to an end. [...] This may take the form of a quantity which is asserted to decrease continually and vanish when the machine stops."

1. Find **ranking function** f ("quantity")

Termination Analysis, Classically

Turing 1949

Finally the checker has to verify that the process comes to an end. Here again he should be assisted by the programmer giving a further definite assertion to be verified. This may take the form of a quantity which is asserted to decrease continually and vanish when the machine stops.

"Finally the checker has to verify that the process comes to an end. [...] This may take the form of a quantity which is asserted to decrease continually and vanish when the machine stops."

1. Find **ranking function** f ("quantity")
2. Prove f to have a **lower bound** ("vanish when the machine stops")

Termination Analysis, Classically

Turing 1949

Finally the checker has to verify that the process comes to an end. Here again he should be assisted by the programmer giving a further definite assertion to be verified. This may take the form of a quantity which is asserted to decrease continually and vanish when the machine stops.

"Finally the checker has to verify that the process comes to an end. [...] This may take the form of a quantity which is asserted to decrease continually and vanish when the machine stops."

1. Find **ranking function** f ("quantity")
2. Prove f to have a **lower bound** ("vanish when the machine stops")
3. Prove that f **decreases** over time

Termination Analysis, Classically

Turing 1949

Finally the checker has to verify that the process comes to an end. Here again he should be assisted by the programmer giving a further definite assertion to be verified. This may take the form of a quantity which is asserted to decrease continually and vanish when the machine stops.

"Finally the checker has to verify that the process comes to an end. [...] This may take the form of a quantity which is asserted to decrease continually and vanish when the machine stops."

1. Find **ranking function** f ("quantity")
2. Prove f to have a **lower bound** ("vanish when the machine stops")
3. Prove that f **decreases** over time

Example (Termination can be simple)

while $x > 0$:
  $x = x - 1$

Question: Does program P terminate?

Termination Analysis, in the Era of Automated Reasoning

Question: Does program P terminate?

Approach: Encode termination proof **template** to logical constraint φ, ask SMT solver

Termination Analysis, in the Era of Automated Reasoning

Question: Does program P terminate?

Approach: Encode termination proof **template** to logical constraint φ, ask SMT solver

$\rightarrow$ **SMT** = **SAT**isfiability **M**odulo **T**heories, solve constraints like

$$b > 0 \quad \wedge \quad (4\,a\,b - 7\,b^2 > 1 \quad \vee \quad 3\,a + c \geq b^3)$$

Question: Does program P terminate?

Approach: Encode termination proof **template** to logical constraint φ, ask SMT solver

$\rightarrow$ **SMT** = **SAT**isfiability **M**odulo **T**heories, solve constraints like

$$b > 0 \quad \wedge \quad (4\,a\,b - 7\,b^2 > 1 \quad \vee \quad 3\,a + c \geq b^3)$$

Answer:

Termination Analysis, in the Era of Automated Reasoning

Question: Does program P terminate?

Approach: Encode termination proof **template** to logical constraint φ, ask SMT solver

$\longrightarrow$ **SMT** = **SAT**isfiability **M**odulo **T**heories, solve constraints like

$$b > 0 \quad \wedge \quad (4\,a\,b - 7\,b^2 > 1 \quad \vee \quad 3\,a + c \geq b^3)$$

Answer:

1. φ satisfiable, model M (e.g., $a = 3, b = 1, c = 1$):
   $\Rightarrow P$ terminating, M fills in the gaps in the termination proof

Termination Analysis, in the Era of Automated Reasoning

Question: Does program P terminate?

Approach: Encode termination proof **template** to logical constraint φ, ask SMT solver

$\longrightarrow$ **SMT** = **SAT**isfiability **M**odulo **T**heories, solve constraints like

$$b > 0 \quad \wedge \quad (4\,a\,b - 7\,b^2 > 1 \quad \vee \quad 3\,a + c \geq b^3)$$

Answer:

1. φ satisfiable, model M (e.g., $a = 3, b = 1, c = 1$):
   $\Rightarrow$ P terminating, M fills in the gaps in the termination proof
2. φ unsatisfiable:
   $\Rightarrow$ termination status of P unknown
   $\Rightarrow$ try a different template (proof technique)

Termination Analysis, in the Era of Automated Reasoning

Question: Does program P terminate?

Approach: Encode termination proof **template** to logical constraint φ, ask SMT solver

$\longrightarrow$ **SMT** = **SAT**isfiability **M**odulo **T**heories, solve constraints like

$$b > 0 \quad \wedge \quad (4\,a\,b - 7\,b^2 > 1 \quad \vee \quad 3\,a + c \geq b^3)$$

Answer:

1. φ satisfiable, model M (e.g., $a = 3, b = 1, c = 1$):
   $\Rightarrow$ P terminating, M fills in the gaps in the termination proof
2. φ unsatisfiable:
   $\Rightarrow$ termination status of P unknown
   $\Rightarrow$ try a different template (proof technique)

In practice:

- Encode only one proof **step** at a time
  $\longrightarrow$ try to prove only **part** of the program terminating
- **Repeat** until the whole program is proved terminating

The Rest of Today's Session

Termination proving in the back-end

1. Term Rewrite Systems (TRSs)
2. Imperative Programs (as Integer Transition Systems, ITSs)
3. Both together! Logically Constrained Term Rewrite Systems

The Rest of Today's Session

Termination proving in the back-end

1. Term Rewrite Systems (TRSs)
2. Imperative Programs (as Integer Transition Systems, ITSs)
3. Both together! Logically Constrained Term Rewrite Systems

Processing practical programming languages in the front-end

4. Java
5. C (via LLVM)

I.1 Termination Analysis of Term Rewrite Systems

What's Term Rewriting?

What's Term Rewriting?

Syntactic approach for reasoning in equational first-order logic

What's Term Rewriting?

Syntactic approach for reasoning in equational first-order logic

Core functional programming language without many restrictions (and features) of "real" FP:

What's Term Rewriting?

Syntactic approach for reasoning in equational first-order logic

Core functional programming language without many restrictions (and features) of "real" FP:

- first-order (usually)
- no fixed evaluation strategy $\longrightarrow$ non-determinism!
- no fixed order of rules to apply (Haskell: top to bottom) $\longrightarrow$ non-determinism!
- untyped (unless you really want types)
- no pre-defined data structures (integers, arrays, ...)

Show Me an Example!

Represent natural numbers by terms (inductively defined data structure):

$$\mathsf{0},\ \mathsf{s}(\mathsf{0}),\ \mathsf{s}(\mathsf{s}(\mathsf{0})),\ \ldots$$

Show Me an Example!

Represent natural numbers by terms (inductively defined data structure):

$$0,\ \mathsf{s}(0),\ \mathsf{s}(\mathsf{s}(0)),\ \ldots$$

Example (A Term Rewrite System (TRS) for Division)

$$\mathcal{R} = \left\{ \begin{array}{rcl} \mathsf{minus}(x, 0) & \to & x \\ \mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{minus}(x, y) \\ \mathsf{quot}(0, \mathsf{s}(y)) & \to & 0 \\ \mathsf{quot}(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{s}(\mathsf{quot}(\mathsf{minus}(x, y), \mathsf{s}(y))) \end{array} \right.$$

Show Me an Example!

Represent natural numbers by terms (inductively defined data structure):

$$0,\ \mathsf{s}(0),\ \mathsf{s}(\mathsf{s}(0)),\ \ldots$$

Example (A Term Rewrite System (TRS) for Division)

$$\mathcal{R} = \left\{ \begin{array}{rcl} \mathsf{minus}(x, 0) & \to & x \\ \mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{minus}(x, y) \\ \mathsf{quot}(0, \mathsf{s}(y)) & \to & 0 \\ \mathsf{quot}(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{s}(\mathsf{quot}(\mathsf{minus}(x, y), \mathsf{s}(y))) \end{array} \right.$$

Calculation:

$$\mathsf{minus}(\mathsf{s}(\mathsf{s}(0)), \mathsf{s}(0)) \quad \to_{\mathcal{R}} \quad \mathsf{minus}(\mathsf{s}(0), 0) \quad \to_{\mathcal{R}} \quad \mathsf{s}(0)$$

Why Care about Termination of Term Rewriting?

- Termination needed by theorem provers

Why Care about Termination of Term Rewriting?

- Termination needed by theorem provers
- Translate program P with inductive data structures (trees) to TRS, represent data structures as terms

  $\Rightarrow$ Termination of TRS implies termination of P

Why Care about Termination of Term Rewriting?

- Termination needed by theorem provers

- Translate program P with inductive data structures (trees) to TRS, represent data structures as terms

  $\Rightarrow$ Termination of TRS implies termination of P

  - Logic programming: Prolog
    [van Raamsdonk, *ICLP '97*; Schneider-Kamp et al, *TOCL '09*; Giesl et al, *PPDP '12*]

Why Care about Termination of Term Rewriting?

- Termination needed by theorem provers
- Translate program P with inductive data structures (trees) to TRS, represent data structures as terms

  $\Rightarrow$ Termination of TRS implies termination of P

  - Logic programming: Prolog
    [van Raamsdonk, *ICLP '97*; Schneider-Kamp et al, *TOCL '09*; Giesl et al, *PPDP '12*]
  - (Lazy) functional programming: Haskell [Giesl et al, *TOPLAS '11*]

Why Care about Termination of Term Rewriting?

- Termination needed by theorem provers

- Translate program P with inductive data structures (trees) to TRS, represent data structures as terms

  $\Rightarrow$ Termination of TRS implies termination of P

  - Logic programming: Prolog
    [van Raamsdonk, *ICLP '97*; Schneider-Kamp et al, *TOCL '09*; Giesl et al, *PPDP '12*]
  - (Lazy) functional programming: Haskell [Giesl et al, *TOPLAS '11*]
  - Object-oriented programming: Java [Otto et al, *RTA '10*]

Example (Division)

$$\mathcal{R} = \left\{ \begin{array}{rcl} \mathsf{minus}(x, \mathsf{0}) & \to & x \\ \mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{minus}(x, y) \\ \mathsf{quot}(\mathsf{0}, \mathsf{s}(y)) & \to & \mathsf{0} \\ \mathsf{quot}(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{s}(\mathsf{quot}(\mathsf{minus}(x, y), \mathsf{s}(y))) \end{array} \right.$$

Term rewriting: Evaluate terms by applying rules from $\mathcal{R}$

$$\mathsf{minus}(\mathsf{s}(\mathsf{s}(\mathsf{0})), \mathsf{s}(\mathsf{0})) \to_{\mathcal{R}} \mathsf{minus}(\mathsf{s}(\mathsf{0}), \mathsf{0}) \to_{\mathcal{R}} \mathsf{s}(\mathsf{0})$$

Example (Division)

$$\mathcal{R} = \begin{cases} \mathsf{minus}(x, \mathsf{0}) & \to & x \\ \mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{minus}(x, y) \\ \mathsf{quot}(\mathsf{0}, \mathsf{s}(y)) & \to & \mathsf{0} \\ \mathsf{quot}(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{s}(\mathsf{quot}(\mathsf{minus}(x, y), \mathsf{s}(y))) \end{cases}$$

Term rewriting: Evaluate terms by applying rules from $\mathcal{R}$

$$\mathsf{minus}(\mathsf{s}(\mathsf{s}(\mathsf{0})), \mathsf{s}(\mathsf{0})) \to_{\mathcal{R}} \mathsf{minus}(\mathsf{s}(\mathsf{0}), \mathsf{0}) \to_{\mathcal{R}} \mathsf{s}(\mathsf{0})$$

Termination: No infinite evaluation sequences $t_1 \to_{\mathcal{R}} t_2 \to_{\mathcal{R}} t_3 \to_{\mathcal{R}} \ldots$

Example (Division)

$$\mathcal{R} = \begin{cases} \mathsf{minus}(x, \mathsf{0}) & \rightarrow & x \\ \mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) & \rightarrow & \mathsf{minus}(x, y) \\ \mathsf{quot}(\mathsf{0}, \mathsf{s}(y)) & \rightarrow & \mathsf{0} \\ \mathsf{quot}(\mathsf{s}(x), \mathsf{s}(y)) & \rightarrow & \mathsf{s}(\mathsf{quot}(\mathsf{minus}(x, y), \mathsf{s}(y))) \end{cases}$$

Term rewriting: Evaluate terms by applying rules from $\mathcal{R}$

$$\mathsf{minus}(\mathsf{s}(\mathsf{s}(\mathsf{0})), \mathsf{s}(\mathsf{0})) \rightarrow_{\mathcal{R}} \mathsf{minus}(\mathsf{s}(\mathsf{0}), \mathsf{0}) \rightarrow_{\mathcal{R}} \mathsf{s}(\mathsf{0})$$

Termination: No infinite evaluation sequences $t_1 \rightarrow_{\mathcal{R}} t_2 \rightarrow_{\mathcal{R}} t_3 \rightarrow_{\mathcal{R}} \dots$
Show termination using Dependency Pairs

Example (Division)

$$\mathcal{R} = \begin{cases} \mathsf{minus}(x, \mathsf{0}) & \to & x \\ \mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{minus}(x, y) \\ \mathsf{quot}(\mathsf{0}, \mathsf{s}(y)) & \to & \mathsf{0} \\ \mathsf{quot}(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{s}(\mathsf{quot}(\mathsf{minus}(x, y), \mathsf{s}(y))) \end{cases}$$

Dependency Pairs [Arts, Giesl, *TCS '00*]

Example (Division)

$$\mathcal{R} = \begin{cases} \mathsf{minus}(x, \mathsf{0}) & \to & x \\ \mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{minus}(x, y) \\ \mathsf{quot}(\mathsf{0}, \mathsf{s}(y)) & \to & \mathsf{0} \\ \mathsf{quot}(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{s}(\mathsf{quot}(\mathsf{minus}(x, y), \mathsf{s}(y))) \end{cases}$$

$$\mathcal{DP} = \begin{cases} \mathsf{minus}^\sharp(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{minus}^\sharp(x, y) \\ \mathsf{quot}^\sharp(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{minus}^\sharp(x, y) \\ \mathsf{quot}^\sharp(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{quot}^\sharp(\mathsf{minus}(x, y), \mathsf{s}(y)) \end{cases}$$

Dependency Pairs [Arts, Giesl, *TCS '00*]

- For TRS $\mathcal{R}$ build dependency pairs $\mathcal{DP}$ (∼ function calls)
- Show: No ∞ call sequence with $\mathcal{DP}$ (eval of $\mathcal{DP}$'s args via $\mathcal{R}$)

Example (Division)

$$\mathcal{R} = \left\{ \begin{array}{rcl} \mathsf{minus}(x, \mathsf{0}) & \to & x \\ \mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{minus}(x, y) \\ \mathsf{quot}(\mathsf{0}, \mathsf{s}(y)) & \to & \mathsf{0} \\ \mathsf{quot}(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{s}(\mathsf{quot}(\mathsf{minus}(x, y), \mathsf{s}(y))) \end{array} \right.$$

$$\mathcal{DP} = \left\{ \begin{array}{rcl} \mathsf{minus}^\sharp(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{minus}^\sharp(x, y) \\ \mathsf{quot}^\sharp(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{minus}^\sharp(x, y) \\ \mathsf{quot}^\sharp(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{quot}^\sharp(\mathsf{minus}(x, y), \mathsf{s}(y)) \end{array} \right.$$

Dependency Pairs [Arts, Giesl, *TCS '00*]

- For TRS $\mathcal{R}$ build dependency pairs $\mathcal{DP}$ (∼ function calls)
- Show: No ∞ call sequence with $\mathcal{DP}$ (eval of $\mathcal{DP}$'s args via $\mathcal{R}$)
- Dependency Pair Framework [Giesl et al, *JAR '06*] (simplified):

Example (Division)

$$\mathcal{R} = \begin{cases} \mathsf{minus}(x, \mathsf{0}) & \to & x \\ \mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{minus}(x, y) \\ \mathsf{quot}(\mathsf{0}, \mathsf{s}(y)) & \to & \mathsf{0} \\ \mathsf{quot}(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{s}(\mathsf{quot}(\mathsf{minus}(x, y), \mathsf{s}(y))) \end{cases}$$

$$\mathcal{DP} = \begin{cases} \mathsf{minus}^\sharp(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{minus}^\sharp(x, y) \\ \mathsf{quot}^\sharp(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{minus}^\sharp(x, y) \\ \mathsf{quot}^\sharp(\mathsf{s}(x), \mathsf{s}(y)) & \to & \mathsf{quot}^\sharp(\mathsf{minus}(x, y), \mathsf{s}(y)) \end{cases}$$

Dependency Pairs [Arts, Giesl, *TCS '00*]

- For TRS $\mathcal{R}$ build dependency pairs $\mathcal{DP}$ ($\sim$ function calls)
- Show: No ∞ call sequence with $\mathcal{DP}$ (eval of $\mathcal{DP}$'s args via $\mathcal{R}$)
- Dependency Pair Framework [Giesl et al, *JAR '06*] (simplified):
  while $\mathcal{DP} \neq \emptyset$:

Example (Division)

$$\mathcal{R} = \begin{cases} \mathsf{minus}(x, \mathsf{0}) & \succsim & x \\ \mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) & \succsim & \mathsf{minus}(x, y) \\ \mathsf{quot}(\mathsf{0}, \mathsf{s}(y)) & \succsim & \mathsf{0} \\ \mathsf{quot}(\mathsf{s}(x), \mathsf{s}(y)) & \succsim & \mathsf{s}(\mathsf{quot}(\mathsf{minus}(x, y), \mathsf{s}(y))) \end{cases}$$

$$\mathcal{DP} = \begin{cases} \mathsf{minus}^\sharp(\mathsf{s}(x), \mathsf{s}(y)) & \succsim & \mathsf{minus}^\sharp(x, y) \\ \mathsf{quot}^\sharp(\mathsf{s}(x), \mathsf{s}(y)) & \succsim & \mathsf{minus}^\sharp(x, y) \\ \mathsf{quot}^\sharp(\mathsf{s}(x), \mathsf{s}(y)) & \succsim & \mathsf{quot}^\sharp(\mathsf{minus}(x, y), \mathsf{s}(y)) \end{cases}$$

Dependency Pairs [Arts, Giesl, *TCS '00*]

- For TRS $\mathcal{R}$ build dependency pairs $\mathcal{DP}$ ($\sim$ function calls)
- Show: No ∞ call sequence with $\mathcal{DP}$ (eval of $\mathcal{DP}$'s args via $\mathcal{R}$)
- Dependency Pair Framework [Giesl et al, *JAR '06*] (simplified):
  while $\mathcal{DP} \neq \emptyset$:
  - find well-founded order $\succ$ with $\mathcal{DP} \cup \mathcal{R} \subseteq \succsim$

Example (Division)

$$\mathcal{R} = \begin{cases} \mathsf{minus}(x, \mathsf{0}) & \succsim & x \\ \mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) & \succsim & \mathsf{minus}(x, y) \\ \mathsf{quot}(\mathsf{0}, \mathsf{s}(y)) & \succsim & \mathsf{0} \\ \mathsf{quot}(\mathsf{s}(x), \mathsf{s}(y)) & \succsim & \mathsf{s}(\mathsf{quot}(\mathsf{minus}(x, y), \mathsf{s}(y))) \end{cases}$$

$$\mathcal{DP} = \begin{cases} \mathsf{minus}^\sharp(\mathsf{s}(x), \mathsf{s}(y)) & \overset{\succ}{(\sim)} & \mathsf{minus}^\sharp(x, y) \\ \mathsf{quot}^\sharp(\mathsf{s}(x), \mathsf{s}(y)) & \overset{\succ}{(\sim)} & \mathsf{minus}^\sharp(x, y) \\ \mathsf{quot}^\sharp(\mathsf{s}(x), \mathsf{s}(y)) & \overset{\succ}{(\sim)} & \mathsf{quot}^\sharp(\mathsf{minus}(x, y), \mathsf{s}(y)) \end{cases}$$

Dependency Pairs [Arts, Giesl, *TCS '00*]

- For TRS $\mathcal{R}$ build dependency pairs $\mathcal{DP}$ ($\sim$ function calls)
- Show: No ∞ call sequence with $\mathcal{DP}$ (eval of $\mathcal{DP}$'s args via $\mathcal{R}$)
- Dependency Pair Framework [Giesl et al, *JAR '06*] (simplified):
  while $\mathcal{DP} \neq \emptyset$ **:**
  - find well-founded order $\succ$ with $\mathcal{DP} \cup \mathcal{R} \subseteq \succsim$
  - delete $s \longrightarrow t$ with $s \succ t$ from $\mathcal{DP}$

Example (Division)

$$\mathcal{R} = \begin{cases} \mathsf{minus}(x, \mathsf{0}) & \succsim & x \\ \mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) & \succsim & \mathsf{minus}(x, y) \\ \mathsf{quot}(\mathsf{0}, \mathsf{s}(y)) & \succsim & \mathsf{0} \\ \mathsf{quot}(\mathsf{s}(x), \mathsf{s}(y)) & \succsim & \mathsf{s}(\mathsf{quot}(\mathsf{minus}(x, y), \mathsf{s}(y))) \end{cases}$$

$$\mathcal{DP} = \begin{cases} \mathsf{minus}^\sharp(\mathsf{s}(x), \mathsf{s}(y)) & \underset{(\sim)}{\succ} & \mathsf{minus}^\sharp(x, y) \\ \mathsf{quot}^\sharp(\mathsf{s}(x), \mathsf{s}(y)) & \underset{(\sim)}{\succ} & \mathsf{minus}^\sharp(x, y) \\ \mathsf{quot}^\sharp(\mathsf{s}(x), \mathsf{s}(y)) & \underset{(\sim)}{\succ} & \mathsf{quot}^\sharp(\mathsf{minus}(x, y), \mathsf{s}(y)) \end{cases}$$

Dependency Pairs [Arts, Giesl, *TCS '00*]

- For TRS $\mathcal{R}$ build dependency pairs $\mathcal{DP}$ ($\sim$ function calls)
- Show: No ∞ call sequence with $\mathcal{DP}$ (eval of $\mathcal{DP}$'s args via $\mathcal{R}$)
- Dependency Pair Framework [Giesl et al, *JAR '06*] (simplified):
  while $\mathcal{DP} \neq \emptyset$ **:**
  - find well-founded order $\succ$ with $\mathcal{DP} \cup \mathcal{R} \subseteq \succsim$
  - delete $s \longrightarrow t$ with $s \succ t$ from $\mathcal{DP}$
- Find $\succ$ automatically and efficiently

Polynomial Interpretations

Get $\succ$ via polynomial interpretations $[\,\cdot\,]$ over $\mathbb{N}$ [Lankford '75]

Example

$$\mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) \ \succsim \ \mathsf{minus}(x, y)$$

Polynomial Interpretations

Get $\succ$ via polynomial interpretations $[\cdot]$ over $\mathbb{N}$ [Lankford '75]

Example

$$\mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) \quad \succsim \quad \mathsf{minus}(x, y)$$

Use $[\cdot]$ with

- $[\mathsf{minus}](x_1, x_2) = x_1$
- $[\mathsf{s}](x_1) = x_1 + 1$

Polynomial Interpretations

Get $\succ$ via polynomial interpretations $[\,\cdot\,]$ over $\mathbb{N}$ [Lankford '75]

Example

$$\forall x, y. \quad x + 1 \;=\; [\mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y))] \;\geq\; [\mathsf{minus}(x, y)] \;=\; x$$

Use $[\,\cdot\,]$ with

- $[\mathsf{minus}](x_1, x_2) = x_1$
- $[\mathsf{s}](x_1) = x_1 + 1$

Extend to terms:

- $[x] = x$
- $[\,f(t_1, \ldots, t_n)] = [\,f]([t_1], \ldots, [t_n])$

$\succ$ boils down to $>$ over $\mathbb{N}$

Example (Constraints for Division)

$$
\mathcal{R} = \left\{
\begin{array}{rcl}
\mathsf{minus}(x, \mathsf{0}) & \succsim & x \\
\mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) & \succsim & \mathsf{minus}(x, y) \\
\mathsf{quot}(\mathsf{0}, \mathsf{s}(y)) & \succsim & \mathsf{0} \\
\mathsf{quot}(\mathsf{s}(x), \mathsf{s}(y)) & \succsim & \mathsf{s}(\mathsf{quot}(\mathsf{minus}(x, y), \mathsf{s}(y)))
\end{array}
\right.
$$

$$
\mathcal{DP} = \left\{
\begin{array}{rcl}
\mathsf{minus}^\sharp(\mathsf{s}(x), \mathsf{s}(y)) & \underset{(\sim)}{\succ} & \mathsf{minus}^\sharp(x, y) \\
\mathsf{quot}^\sharp(\mathsf{s}(x), \mathsf{s}(y)) & \underset{(\sim)}{\succ} & \mathsf{minus}^\sharp(x, y) \\
\mathsf{quot}^\sharp(\mathsf{s}(x), \mathsf{s}(y)) & \underset{(\sim)}{\succ} & \mathsf{quot}^\sharp(\mathsf{minus}(x, y), \mathsf{s}(y))
\end{array}
\right.
$$

Example (Constraints for Division)

$$\mathcal{R} = \begin{cases} \mathsf{minus}(x, \mathsf{0}) & \succsim & x \\ \mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) & \succsim & \mathsf{minus}(x, y) \\ \mathsf{quot}(\mathsf{0}, \mathsf{s}(y)) & \succsim & \mathsf{0} \\ \mathsf{quot}(\mathsf{s}(x), \mathsf{s}(y)) & \succsim & \mathsf{s}(\mathsf{quot}(\mathsf{minus}(x, y), \mathsf{s}(y))) \end{cases}$$

$$\mathcal{DP} = \begin{cases} \mathsf{minus}^\sharp(\mathsf{s}(x), \mathsf{s}(y)) & \succ & \mathsf{minus}^\sharp(x, y) \\ \mathsf{quot}^\sharp(\mathsf{s}(x), \mathsf{s}(y)) & \succ & \mathsf{minus}^\sharp(x, y) \\ \mathsf{quot}^\sharp(\mathsf{s}(x), \mathsf{s}(y)) & \succ & \mathsf{quot}^\sharp(\mathsf{minus}(x, y), \mathsf{s}(y)) \end{cases}$$

Use interpretation $[\,\cdot\,]$ over $\mathbb{N}$ with

$$[\mathsf{quot}^\sharp](x_1, x_2) = x_1 \qquad [\mathsf{quot}](x_1, x_2) = x_1 + x_2$$

$$[\mathsf{minus}^\sharp](x_1, x_2) = x_1 \qquad [\mathsf{minus}](x_1, x_2) = x_1$$

$$[\mathsf{0}] = 0 \qquad [\mathsf{s}](x_1) = x_1 + 1$$

$\curvearrowright$ order solves all constraints

Example (Constraints for Division)

$$\mathcal{R} = \left\{ \begin{array}{rcl} \mathsf{minus}(x, \mathsf{0}) & \succsim & x \\ \mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) & \succsim & \mathsf{minus}(x, y) \\ \mathsf{quot}(\mathsf{0}, \mathsf{s}(y)) & \succsim & \mathsf{0} \\ \mathsf{quot}(\mathsf{s}(x), \mathsf{s}(y)) & \succsim & \mathsf{s}(\mathsf{quot}(\mathsf{minus}(x, y), \mathsf{s}(y))) \end{array} \right.$$

$$\mathcal{DP} = \left\{ \right.$$

Use interpretation $[\,\cdot\,]$ over $\mathbb{N}$ with

$$\begin{array}{rcl} [\mathsf{quot}^\sharp](x_1, x_2) & = & x_1 \\ [\mathsf{minus}^\sharp](x_1, x_2) & = & x_1 \\ [\mathsf{0}] & = & 0 \end{array} \qquad \begin{array}{rcl} [\mathsf{quot}](x_1, x_2) & = & x_1 + x_2 \\ [\mathsf{minus}](x_1, x_2) & = & x_1 \\ [\mathsf{s}](x_1) & = & x_1 + 1 \end{array}$$

$\curvearrowright$ order solves all constraints

$\curvearrowright$ $\mathcal{DP} = \emptyset$

$\curvearrowright$ termination of division algorithm proved $\square$

Remark

Polynomial interpretations play several roles for program analysis:

Use interpretation $[\,\cdot\,]$ over $\mathbb{N}$ with

$$
\begin{aligned}
[\mathsf{quot}^\sharp](x_1, x_2) &= x_1 & \qquad [\mathsf{quot}](x_1, x_2) &= x_1 + x_2 \\
[\mathsf{minus}^\sharp](x_1, x_2) &= x_1 & \qquad [\mathsf{minus}](x_1, x_2) &= x_1 \\
[\mathsf{0}] &= 0 & \qquad [\mathsf{s}](x_1) &= x_1 + 1
\end{aligned}
$$

$\curvearrowright$ order solves all constraints

$\curvearrowright$ $\mathcal{DP} = \emptyset$

$\curvearrowright$ termination of division algorithm proved □

Remark

Polynomial interpretations play several roles for program analysis:

- Ranking function: $[\mathsf{quot}^\sharp]$ and $[\mathsf{minus}^\sharp]$

Use interpretation $[\,\cdot\,]$ over $\mathbb{N}$ with

$$\begin{aligned}[\mathsf{quot}^\sharp](x_1,x_2) &= x_1 & \qquad [\mathsf{quot}](x_1,x_2) &= x_1+x_2\\ [\mathsf{minus}^\sharp](x_1,x_2) &= x_1 & [\mathsf{minus}](x_1,x_2) &= x_1\\ [\mathsf{0}] &= 0 & [\mathsf{s}](x_1) &= x_1+1\end{aligned}$$

$\curvearrowright$ order solves all constraints

$\curvearrowright$ $\mathcal{DP} = \emptyset$

$\curvearrowright$ termination of division algorithm proved $\square$

Remark

Polynomial interpretations play several roles for program analysis:

- Ranking function: $[\mathsf{quot}^\sharp]$ and $[\mathsf{minus}^\sharp]$
- Summary: $[\mathsf{quot}]$ and $[\mathsf{minus}]$

Use interpretation $[\,\cdot\,]$ over $\mathbb{N}$ with

$$
\begin{aligned}
[\mathsf{quot}^\sharp](x_1, x_2) &= x_1 & \qquad [\mathsf{quot}](x_1, x_2) &= x_1 + x_2 \\
[\mathsf{minus}^\sharp](x_1, x_2) &= x_1 & \qquad [\mathsf{minus}](x_1, x_2) &= x_1 \\
[\mathsf{0}] &= 0 & \qquad [\mathsf{s}](x_1) &= x_1 + 1
\end{aligned}
$$

$\curvearrowright$ order solves all constraints

$\curvearrowright$ $\mathcal{DP} = \emptyset$

$\curvearrowright$ termination of division algorithm proved □

Remark

Polynomial interpretations play several roles for program analysis:

- Ranking function: $[\mathsf{quot}^\sharp]$ and $[\mathsf{minus}^\sharp]$
- Summary: $[\mathsf{quot}]$ and $[\mathsf{minus}]$
- Abstraction (aka norm) for data structures: $[\mathsf{0}]$ and $[\mathsf{s}]$

Use interpretation $[\,\cdot\,]$ over $\mathbb{N}$ with

$$\begin{aligned} [\mathsf{quot}^\sharp](x_1,x_2) &= x_1 \\ [\mathsf{minus}^\sharp](x_1,x_2) &= x_1 \\ [\mathsf{0}] &= 0 \end{aligned} \qquad \begin{aligned} [\mathsf{quot}](x_1,x_2) &= x_1 + x_2 \\ [\mathsf{minus}](x_1,x_2) &= x_1 \\ [\mathsf{s}](x_1) &= x_1 + 1 \end{aligned}$$

$\curvearrowright$ order solves all constraints

$\curvearrowright$ $\mathcal{DP} = \emptyset$

$\curvearrowright$ termination of division algorithm proved $\square$

Automation

Task: Solve $\mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) \gtrsim \mathsf{minus}(x, y)$

Automation

Task: Solve $\mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) \gtrsim \mathsf{minus}(x, y)$

1. Fix template polynomials with parametric coefficients, get interpretation template:

$$[\mathsf{minus}](x, y) = a_{\mathsf{m}} + b_{\mathsf{m}}\, x + c_{\mathsf{m}}\, y, \quad [\mathsf{s}](x) = a_{\mathsf{s}} + b_{\mathsf{s}}\, x$$

Automation

Task: Solve $\mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) \gtrsim \mathsf{minus}(x, y)$

1. Fix template polynomials with parametric coefficients, get interpretation template:

$$[\mathsf{minus}](x, y) = a_{\mathsf{m}} + b_{\mathsf{m}}\, x + c_{\mathsf{m}}\, y, \quad [\mathsf{s}](x) = a_{\mathsf{s}} + b_{\mathsf{s}}\, x$$

2. From term constraint to polynomial constraint:

$$s \gtrsim t \;\curvearrowright\; [s] \geq [t]$$

Here: $\forall x, y.\; (a_{\mathsf{s}}\, b_{\mathsf{m}} + a_{\mathsf{s}}\, c_{\mathsf{m}}) + (b_{\mathsf{s}}\, b_{\mathsf{m}} - b_{\mathsf{m}})\, x + (b_{\mathsf{s}}\, c_{\mathsf{m}} - c_{\mathsf{m}})\, y \geq 0$

Automation

Task: Solve $\mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) \succsim \mathsf{minus}(x, y)$

1. Fix template polynomials with parametric coefficients, get interpretation template:

$$[\mathsf{minus}](x, y) = a_{\mathsf{m}} + b_{\mathsf{m}}\, x + c_{\mathsf{m}}\, y, \quad [\mathsf{s}](x) = a_{\mathsf{s}} + b_{\mathsf{s}}\, x$$

2. From term constraint to polynomial constraint:

$$s \succsim t \;\curvearrowright\; [s] \geq [t]$$

Here: $\forall x, y.\; (a_{\mathsf{s}}\, b_{\mathsf{m}} + a_{\mathsf{s}}\, c_{\mathsf{m}}) + (b_{\mathsf{s}}\, b_{\mathsf{m}} - b_{\mathsf{m}})\, x + (b_{\mathsf{s}}\, c_{\mathsf{m}} - c_{\mathsf{m}})\, y \geq 0$

3. Eliminate $\forall x, y$ by absolute positiveness criterion [Hong, Jakuš, *JAR '98*]:

Here: $a_{\mathsf{s}}\, b_{\mathsf{m}} + a_{\mathsf{s}}\, c_{\mathsf{m}} \geq 0 \;\wedge\; b_{\mathsf{s}}\, b_{\mathsf{m}} - b_{\mathsf{m}} \geq 0 \;\wedge\; b_{\mathsf{s}}\, c_{\mathsf{m}} - c_{\mathsf{m}} \geq 0$

Automation

Task: Solve $\mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) \gtrsim \mathsf{minus}(x, y)$

1. Fix template polynomials with parametric coefficients, get interpretation template:

$$[\mathsf{minus}](x, y) = a_\mathsf{m} + b_\mathsf{m}\, x + c_\mathsf{m}\, y, \quad [\mathsf{s}](x) = a_\mathsf{s} + b_\mathsf{s}\, x$$

2. From term constraint to polynomial constraint:

$$s \gtrsim t \curvearrowright [s] \geq [t]$$

Here: $\forall x, y.\ (a_\mathsf{s}\, b_\mathsf{m} + a_\mathsf{s}\, c_\mathsf{m}) + (b_\mathsf{s}\, b_\mathsf{m} - b_\mathsf{m})\, x + (b_\mathsf{s}\, c_\mathsf{m} - c_\mathsf{m})\, y \geq 0$

3. Eliminate $\forall x, y$ by absolute positiveness criterion [Hong, Jakuš, *JAR '98*]:

Here: $a_\mathsf{s}\, b_\mathsf{m} + a_\mathsf{s}\, c_\mathsf{m} \geq 0 \ \wedge\ b_\mathsf{s}\, b_\mathsf{m} - b_\mathsf{m} \geq 0 \ \wedge\ b_\mathsf{s}\, c_\mathsf{m} - c_\mathsf{m} \geq 0$

Automation

Task: Solve $\mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) \succsim \mathsf{minus}(x, y)$

1. Fix template polynomials with parametric coefficients, get interpretation template:

$$[\mathsf{minus}](x, y) = a_{\mathsf{m}} + b_{\mathsf{m}}\, x + c_{\mathsf{m}}\, y, \quad [\mathsf{s}](x) = a_{\mathsf{s}} + b_{\mathsf{s}}\, x$$

2. From term constraint to polynomial constraint:

$$s \succsim t \;\curvearrowright\; [s] \geq [t]$$

Here: $\forall x, y.\ (a_{\mathsf{s}}\, b_{\mathsf{m}} + a_{\mathsf{s}}\, c_{\mathsf{m}}) + (b_{\mathsf{s}}\, b_{\mathsf{m}} - b_{\mathsf{m}})\, x + (b_{\mathsf{s}}\, c_{\mathsf{m}} - c_{\mathsf{m}})\, y \geq 0$

3. Eliminate $\forall x, y$ by absolute positiveness criterion [Hong, Jakuš, *JAR '98*]:

Here: $a_{\mathsf{s}}\, b_{\mathsf{m}} + a_{\mathsf{s}}\, c_{\mathsf{m}} \geq 0 \;\wedge\; b_{\mathsf{s}}\, b_{\mathsf{m}} - b_{\mathsf{m}} \geq 0 \;\wedge\; b_{\mathsf{s}}\, c_{\mathsf{m}} - c_{\mathsf{m}} \geq 0$

Automation

Task: Solve $\mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) \succsim \mathsf{minus}(x, y)$

1. Fix template polynomials with parametric coefficients, get interpretation template:

$$[\mathsf{minus}](x, y) = a_{\mathsf{m}} + b_{\mathsf{m}}\, x + c_{\mathsf{m}}\, y, \quad [\mathsf{s}](x) = a_{\mathsf{s}} + b_{\mathsf{s}}\, x$$

2. From term constraint to polynomial constraint:

$$s \succsim t \ \curvearrowright\ [s] \geq [t]$$

Here: $\forall x, y.\ (a_{\mathsf{s}}\, b_{\mathsf{m}} + a_{\mathsf{s}}\, c_{\mathsf{m}}) + (b_{\mathsf{s}}\, b_{\mathsf{m}} - b_{\mathsf{m}})\, x + (b_{\mathsf{s}}\, c_{\mathsf{m}} - c_{\mathsf{m}})\, y \geq 0$

3. Eliminate $\forall x, y$ by absolute positiveness criterion [Hong, Jakuš, *JAR '98*]:

Here: $a_{\mathsf{s}}\, b_{\mathsf{m}} + a_{\mathsf{s}}\, c_{\mathsf{m}} \geq 0 \ \wedge\ b_{\mathsf{s}}\, b_{\mathsf{m}} - b_{\mathsf{m}} \geq 0 \ \wedge\ b_{\mathsf{s}}\, c_{\mathsf{m}} - c_{\mathsf{m}} \geq 0$

Non-linear constraints, even for linear interpretations

Automation

Task: Solve $\mathsf{minus}(\mathsf{s}(x), \mathsf{s}(y)) \succsim \mathsf{minus}(x, y)$

1. Fix template polynomials with parametric coefficients, get interpretation template:

$$[\mathsf{minus}](x, y) = a_\mathsf{m} + b_\mathsf{m}\, x + c_\mathsf{m}\, y, \quad [\mathsf{s}](x) = a_\mathsf{s} + b_\mathsf{s}\, x$$

2. From term constraint to polynomial constraint:

$$s \succsim t \;\curvearrowright\; [s] \geq [t]$$

Here: $\forall x, y.\; (a_\mathsf{s}\, b_\mathsf{m} + a_\mathsf{s}\, c_\mathsf{m}) + (b_\mathsf{s}\, b_\mathsf{m} - b_\mathsf{m})\, x + (b_\mathsf{s}\, c_\mathsf{m} - c_\mathsf{m})\, y \geq 0$

3. Eliminate $\forall x, y$ by absolute positiveness criterion [Hong, Jakuš, *JAR '98*]:

Here: $a_\mathsf{s}\, b_\mathsf{m} + a_\mathsf{s}\, c_\mathsf{m} \geq 0 \wedge b_\mathsf{s}\, b_\mathsf{m} - b_\mathsf{m} \geq 0 \wedge b_\mathsf{s}\, c_\mathsf{m} - c_\mathsf{m} \geq 0$

Non-linear constraints, even for linear interpretations

Task: Show satisfiability of non-linear constraints over $\mathbb{N}$ ($\longrightarrow$ SMT solver!)

$\curvearrowright$ Prove termination of given term rewrite system

Extensions of Polynomial Interpretations

- Polynomials with negative coefficients and max-operator [Hirokawa, Middeldorp, *IC '07*; Fuhs et al, *SAT '07, RTA '08*]
  - can model behaviour of functions more closely:
    $[\mathsf{pred}](x_1) = \max(x_1 - 1, 0)$
  - automation via encoding to non-linear constraints, more complex Boolean structure

Extensions of Polynomial Interpretations

- Polynomials with negative coefficients and max-operator [Hirokawa, Middeldorp, *IC '07*; Fuhs et al, *SAT '07, RTA '08*]
  - can model behaviour of functions more closely: $[\mathsf{pred}](x_1) = \max(x_1 - 1, 0)$
  - automation via encoding to non-linear constraints, more complex Boolean structure
- Polynomials over $\mathbb{Q}^+$ and $\mathbb{R}^+$ [Lucas, *RAIRO '05*]
  - non-integer coefficients increase proving power
  - SMT-based automation [Fuhs et al, *AISC '08*; Zankl, Middeldorp, *LPAR '10*; Borralleras et al, *JAR '12*]

Extensions of Polynomial Interpretations

- Polynomials with negative coefficients and max-operator [Hirokawa, Middeldorp, *IC '07*; Fuhs et al, *SAT '07, RTA '08*]
  - can model behaviour of functions more closely: $[\mathsf{pred}](x_1) = \max(x_1 - 1, 0)$
  - automation via encoding to non-linear constraints, more complex Boolean structure
- Polynomials over $\mathbb{Q}^+$ and $\mathbb{R}^+$ [Lucas, *RAIRO '05*]
  - non-integer coefficients increase proving power
  - SMT-based automation [Fuhs et al, *AISC '08*; Zankl, Middeldorp, *LPAR '10*; Borralleras et al, *JAR '12*]
- Matrix interpretations [Endrullis, Waldmann, Zantema, *JAR '08*]
  - linear interpretation to vectors over $\mathbb{N}^k$, coefficients are matrices
  - useful for deeply nested terms
  - automation: constraints with more complex atoms
  - several flavours: plus-times-semiring, max-plus-semiring [Koprowski, Waldmann, *Acta Cyb. '09*], ...
  - generalisation to tuple interpretations [Yamada, *JAR '22*]

Extensions of Polynomial Interpretations

- Polynomials with negative coefficients and max-operator [Hirokawa, Middeldorp, *IC '07*; Fuhs et al, *SAT '07, RTA '08*]
  - can model behaviour of functions more closely: [pred]$(x_1) = \max(x_1 - 1, 0)$
  - automation via encoding to non-linear constraints, more complex Boolean structure
- Polynomials over $\mathbb{Q}^+$ and $\mathbb{R}^+$ [Lucas, *RAIRO '05*]
  - non-integer coefficients increase proving power
  - SMT-based automation [Fuhs et al, *AISC '08*; Zankl, Middeldorp, *LPAR '10*; Borralleras et al, *JAR '12*]
- Matrix interpretations [Endrullis, Waldmann, Zantema, *JAR '08*]
  - linear interpretation to vectors over $\mathbb{N}^k$, coefficients are matrices
  - useful for deeply nested terms
  - automation: constraints with more complex atoms
  - several flavours: plus-times-semiring, max-plus-semiring [Koprowski, Waldmann, *Acta Cyb. '09*], . . .
  - generalisation to tuple interpretations [Yamada, *JAR '22*]
- . . .

(SAT and) SMT Solving for Path Orders

Path orders: based on precedences on function symbols

- Knuth-Bendix Order [Knuth, Bendix, *CPAA '70*]
  $\longrightarrow$ polynomial time algorithm [Korovin, Voronkov, *IC '03*]
  $\longrightarrow$ SMT encoding [Zankl, Hirokawa, Middeldorp, *JAR '09*]

(SAT and) SMT Solving for Path Orders

Path orders: based on precedences on function symbols

- Knuth-Bendix Order [Knuth, Bendix, *CPAA '70*]
  $\longrightarrow$ polynomial time algorithm [Korovin, Voronkov, *IC '03*]
  $\longrightarrow$ SMT encoding [Zankl, Hirokawa, Middeldorp, *JAR '09*]

- Lexicographic Path Orders [Kamin, Lévy, *Unpublished Manuscript '80*]
  and Recursive Path Orders [Dershowitz, Manna, *CACM '79*; Dershowitz, *TCS '82*]
  $\longrightarrow$ SAT encoding [Codish et al, *JAR '11*]

(SAT and) SMT Solving for Path Orders

Path orders: based on precedences on function symbols

- Knuth-Bendix Order [Knuth, Bendix, *CPAA '70*]
  $\longrightarrow$ polynomial time algorithm [Korovin, Voronkov, *IC '03*]
  $\longrightarrow$ SMT encoding [Zankl, Hirokawa, Middeldorp, *JAR '09*]

- Lexicographic Path Orders [Kamin, Lévy, *Unpublished Manuscript '80*] and Recursive Path Orders [Dershowitz, Manna, *CACM '79*; Dershowitz, *TCS '82*]
  $\longrightarrow$ SAT encoding [Codish et al, *JAR '11*]

- Weighted Path Order [Yamada, Kusakari, Sakabe, *SCP '15*]
  $\longrightarrow$ SMT encoding

Further Techniques and Settings for TRSs

- Proving **non**-termination (an infinite run is possible) [Giesl, Thiemann, Schneider-Kamp, *FroCoS '05*; Payet, *TCS '08*; Zankl et al, *SOFSEM '10*; Emmes, Enger, Giesl, *IJCAR '12*; ...]

Further Techniques and Settings for TRSs

- Proving **non**-termination (an infinite run is possible) [Giesl, Thiemann, Schneider-Kamp, *FroCoS '05*; Payet, *TCS '08*; Zankl et al, *SOFSEM '10*; Emmes, Enger, Giesl, *IJCAR '12*; ...]
- Specific **rewrite strategies**: innermost, outermost, context-sensitive rewriting [Lucas, *ACM Comput. Surv. '20*], ...

Further Techniques and Settings for TRSs

- Proving **non**-termination (an infinite run is possible) [Giesl, Thiemann, Schneider-Kamp, *FroCoS '05*; Payet, *TCS '08*; Zankl et al, *SOFSEM '10*; Emmes, Enger, Giesl, *IJCAR '12*; ...]
- Specific **rewrite strategies**: innermost, outermost, context-sensitive rewriting [Lucas, *ACM Comput. Surv. '20*], ...
- **Higher-order** rewriting: functional variables, higher types, β-reduction

  $$\mathsf{map}(F, \mathsf{Cons}(x, xs)) \to \mathsf{Cons}(F(x), \mathsf{map}(F, xs))$$

  [Kop, *PhD thesis '12*]

Further Techniques and Settings for TRSs

- Proving **non**-termination (an infinite run is possible) [Giesl, Thiemann, Schneider-Kamp, *FroCoS '05*; Payet, *TCS '08*; Zankl et al, *SOFSEM '10*; Emmes, Enger, Giesl, *IJCAR '12*; . . .]
- Specific **rewrite strategies**: innermost, outermost, context-sensitive rewriting [Lucas, *ACM Comput. Surv. '20*], . . .
- **Higher-order** rewriting: functional variables, higher types, β-reduction

  $$\mathsf{map}(F, \mathsf{Cons}(x, xs)) \to \mathsf{Cons}(F(x), \mathsf{map}(F, xs))$$

  [Kop, *PhD thesis '12*]
- **Probabilistic** term rewriting: Positive/Strong Almost Sure Termination [Avanzini, Dal Lago, Yamada, *SCP '20*]

Further Techniques and Settings for TRSs

- Proving **non**-termination (an infinite run is possible) [Giesl, Thiemann, Schneider-Kamp, *FroCoS '05*; Payet, *TCS '08*; Zankl et al, *SOFSEM '10*; Emmes, Enger, Giesl, *IJCAR '12*; ...]
- Specific **rewrite strategies**: innermost, outermost, context-sensitive rewriting [Lucas, *ACM Comput. Surv. '20*], ...
- **Higher-order** rewriting: functional variables, higher types, β-reduction

  $$\mathsf{map}(F, \mathsf{Cons}(x, xs)) \to \mathsf{Cons}(F(x), \mathsf{map}(F, xs))$$

  [Kop, *PhD thesis '12*]
- **Probabilistic** term rewriting: Positive/Strong Almost Sure Termination [Avanzini, Dal Lago, Yamada, *SCP '20*]
- **Complexity analysis**
  [Hirokawa, Moser, *IJCAR '08*; Noschinski, Emmes, Giesl, *JAR '13*; ...]
  Can re-use termination machinery to infer and prove statements like "runtime complexity of this TRS is in $\mathcal{O}(n^3)$"
  $\longrightarrow$ more in Session 2!

SMT Solvers *from* Termination Analysis

Annual SMT-COMP, division QF_NIA (Quantifier-Free Non-linear Integer Arithmetic)

Year	Winner
2009	Barcelogic-QF_NIA
2010	MiniSmt
2011	AProVE
2012	*no QF_NIA*
2013	*no SMT-COMP*
2014	AProVE
2015	AProVE
2016	Yices
...	...

SMT Solvers *from* Termination Analysis

Annual SMT-COMP, division QF_NIA (Quantifier-Free Non-linear Integer Arithmetic)

Year	Winner
2009	Barcelogic-QF_NIA
2010	MiniSmt (spin-off of $\mathsf{T_TT_2}$)
2011	AProVE
2012	*no QF_NIA*
2013	*no SMT-COMP*
2014	AProVE
2015	AProVE
2016	Yices
...	...

$\Rightarrow$ Termination provers can also be successful SMT solvers!

SMT Solvers *from* Termination Analysis

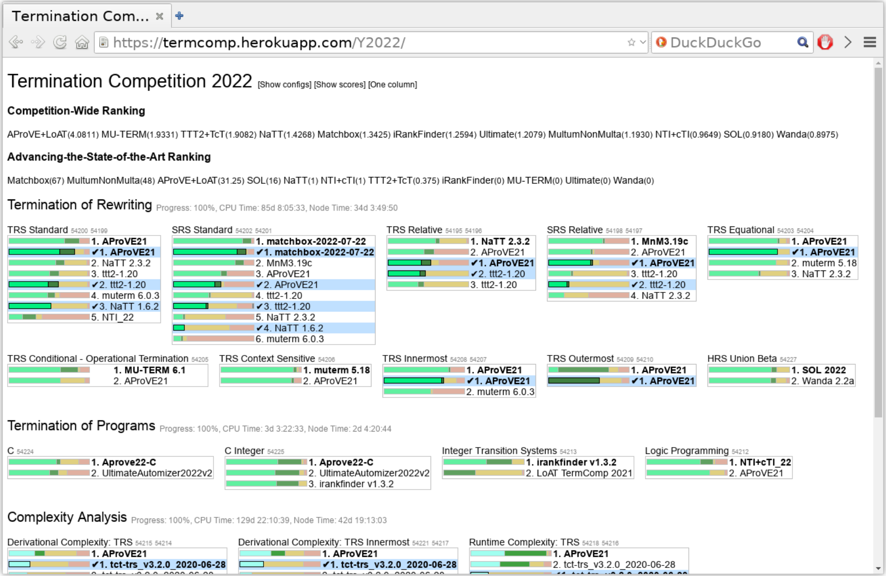
Annual SMT-COMP, division QF_NIA (Quantifier-Free Non-linear Integer Arithmetic)

Year	Winner
2009	Barcelogic-QF_NIA
2010	MiniSmt (spin-off of $\mathsf{T_TT_2}$)
2011	AProVE
2012	*no QF_NIA*
2013	*no SMT-COMP*
2014	AProVE
2015	AProVE
2016	Yices
...	...

⇒ Termination provers can also be successful SMT solvers!

(disclaimer: Z3 participated only *hors concours*)

The Termination Competition (termCOMP) (1/3)


Termination Com...

https://termcomp.herokuapp.com/Y2022/

DuckDuckGo

Termination Competition 2022 [Show configs] [Show scores] [One column]

Competition-Wide Ranking

AProVE+LoAT(4.0811) MU-TERM(1.9331) TTT2+TcT(1.9082) NaTT(1.4268) Matchbox(1.3425) iRankFinder(1.2594) Ultimate(1.2079) MultumNonMulta(1.1930) NTI+cTI(0.9649) SOL(0.9180) Wanda(0.8975)

Advancing-the-State-of-the-Art Ranking

Matchbox(67) MultumNonMulta(48) AProVE+LoAT(31.25) SOL(16) NaTT(1) NTI+cTI(1) TTT2+TcT(0.375) iRankFinder(0) MU-TERM(0) Ultimate(0) Wanda(0)

Termination of Rewriting Progress: 100%, CPU Time: 85d 8:05:33, Node Time: 34d 3:49:50

TRS Standard 54200 54199
1. AProVE21
✔1. AProVE21
2. NaTT 2.3.2
3. ttt2-1.20
✔2. ttt2-1.20
4. muterm 6.0.3
✔3. NaTT 1.6.2
5. NTI_22

SRS Standard 54202 54201
1. matchbox-2022-07-22
✔1. matchbox-2022-07-22
2. MnM3.19c
3. AProVE21
✔2. AProVE21
4. ttt2-1.20
✔3. ttt2-1.20
5. NaTT 2.3.2
✔4. NaTT 1.6.2
6. muterm 6.0.3

TRS Relative 54195 54196
1. NaTT 2.3.2
2. AProVE21
✔1. AProVE21
✔2. ttt2-1.20
3. ttt2-1.20

SRS Relative 54198 54197
1. MnM3.19c
2. AProVE21
✔1. AProVE21
3. ttt2-1.20
✔2. ttt2-1.20
4. NaTT 2.3.2

TRS Equational 54203 54204
1. AProVE21
✔1. AProVE21
2. muterm 5.18
3. NaTT 2.3.2

TRS Conditional - Operational Termination 54205
1. MU-TERM 6.1
2. AProVE21

TRS Context Sensitive 54206
1. muterm 5.18
2. AProVE21

TRS Innermost 54208 54207
1. AProVE21
✔1. AProVE21
2. muterm 6.0.3

TRS Outermost 54209 54210
1. AProVE21
✔1. AProVE21

HRS Union Beta 54227
1. SOL 2022
2. Wanda 2.2a

Termination of Programs Progress: 100%, CPU Time: 3d 3:22:33, Node Time: 2d 4:20:44

C 54224
1. Aprove22-C
2. UltimateAutomizer2022v2

C Integer 54225
1. Aprove22-C
2. UltimateAutomizer2022v2
3. irankfinder v1.3.2

Integer Transition Systems 54213
1. irankfinder v1.3.2
2. LoAT TermComp 2021

Logic Programming 54212
1. NTI+cTI_22
2. AProVE21

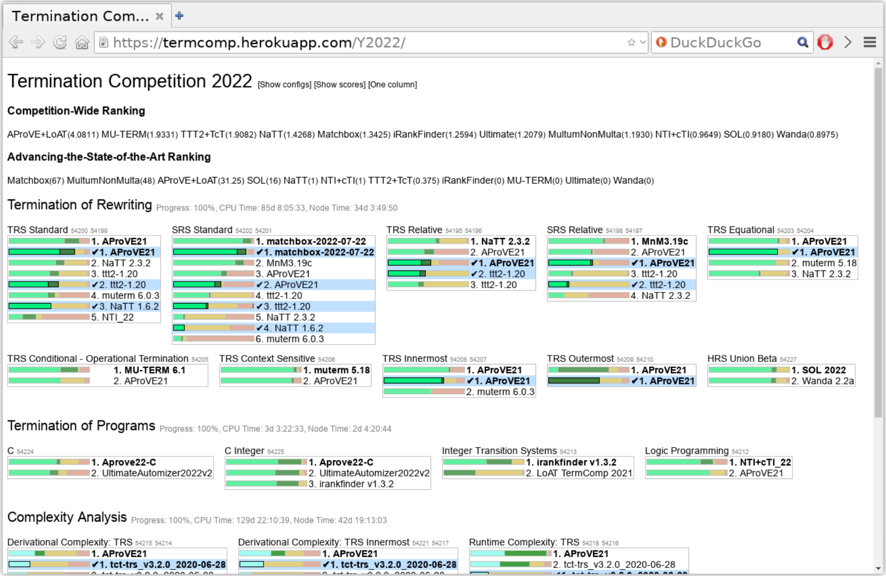
Complexity Analysis Progress: 100%, CPU Time: 129d 22:10:39, Node Time: 42d 19:13:03

Derivational Complexity: TRS 54215 54214
1. AProVE21
✔1. tct-trs_v3.2.0_2020-06-28

Derivational Complexity: TRS Innermost 54221 54217
1. AProVE21
✔1. tct-trs_v3.2.0_2020-06-28

Runtime Complexity: TRS 54218 54216
1. AProVE21
2. tct-trs_v3.2.0_2020-06-28

The Termination Competition (termCOMP) (1/3)



Termination Com... ✕ +

https://termcomp.herokuapp.com/Y2022/

DuckDuckGo

Termination Competition 2022 [Show configs] [Show scores] [One column]

Competition-Wide Ranking

AProVE+LoAT(4.0811) MU-TERM(1.9331) TTT2+TcT(1.9082) NaTT(1.4268) Matchbox(1.3425) iRankFinder(1.2594) Ultimate(1.2079) MultumNonMulta(1.1930) NTI+cTI(0.9649) SOL(0.9180) Wanda(0.8975)

Advancing-the-State-of-the-Art Ranking

Matchbox(67) MultumNonMulta(48) AProVE+LoAT(31.25) SOL(16) NaTT(1) NTI+cTI(1) TTT2+TcT(0.375) iRankFinder(0) MU-TERM(0) Ultimate(0) Wanda(0)

Termination of Rewriting Progress: 100%, CPU Time: 85d 8:05:33, Node Time: 34d 3:49:50

TRS Standard 54200 54199
1. AProVE21
✔1. AProVE21
2. NaTT 2.3.2
3. ttt2-1.20
✔2. ttt2-1.20
4. muterm 6.0.3
✔3. NaTT 1.6.2
5. NTI_22

SRS Standard 54202 54201
1. matchbox-2022-07-22
✔1. matchbox-2022-07-22
2. MnM3.19c
3. AProVE21
✔2. AProVE21
4. ttt2-1.20
✔3. ttt2-1.20
5. NaTT 2.3.2
✔4. NaTT 1.6.2
6. muterm 6.0.3

TRS Relative 54195 54196
1. NaTT 2.3.2
2. AProVE21
✔1. AProVE21
✔2. ttt2-1.20
3. ttt2-1.20

SRS Relative 54198 54197
1. MnM3.19c
2. AProVE21
✔1. AProVE21
3. ttt2-1.20
✔2. ttt2-1.20
4. NaTT 2.3.2

TRS Equational 54203 54204
1. AProVE21
✔1. AProVE21
2. muterm 5.18
3. NaTT 2.3.2

TRS Conditional - Operational Termination 54205
1. MU-TERM 6.1
2. AProVE21

TRS Context Sensitive 54206
1. muterm 5.18
2. AProVE21

TRS Innermost 54208 54207
1. AProVE21
✔1. AProVE21
2. muterm 6.0.3

TRS Outermost 54209 54210
1. AProVE21
✔1. AProVE21

HRS Union Beta 54227
1. SOL 2022
2. Wanda 2.2a

Termination of Programs Progress: 100%, CPU Time: 3d 3:22:33, Node Time: 2d 4:20:44

C 54224
1. Aprove22-C
2. UltimateAutomizer2022v2

C Integer 54225
1. Aprove22-C
2. UltimateAutomizer2022v2
3. irankfinder v1.3.2

Integer Transition Systems 54213
1. irankfinder v1.3.2
2. LoAT TermComp 2021

Logic Programming 54212
1. NTI+cTI_22
2. AProVE21

Complexity Analysis Progress: 100%, CPU Time: 129d 22:10:39, Node Time: 42d 19:13:03

Derivational Complexity: TRS 54215 54214
1. AProVE21
✔1. tct-trs_v3.2.0_2020-06-28

Derivational Complexity: TRS Innermost 54221 54217
1. AProVE21
✔1. tct-trs_v3.2.0_2020-06-28

Runtime Complexity: TRS 54218 54216
1. AProVE21
2. tct-trs_v3.2.0_2020-06-28

https://termination-portal.org/wiki/Termination_Competition

The Termination Competition (termCOMP) (2/3)

termCOMP 2022 participants:

- AProVE (RWTH Aachen, Birkbeck U London, U Innsbruck, ...)
- iRankFinder (UC Madrid)
- LoAT (RWTH Aachen)
- Matchbox (HTWK Leipzig)
- Mu-Term (UP Valencia)
- MultumNonMulta (BA Saarland)
- NaTT (AIST Tokyo)
- NTI+cTI (U Réunion)
- SOL (Gunma U)
- TcT (U Innsbruck, INRIA Sophia Antipolis)
- T_TT_2 (U Innsbruck)
- Ultimate Automizer (U Freiburg)
- Wanda (RU Nijmegen)

The Termination Competition (termCOMP) (3/3)

- Benchmark set: Termination Problem DataBase (TPDB)
  https://termination-portal.org/wiki/TPDB
  $\longrightarrow$ 1000s of termination and complexity problems

The Termination Competition (termCOMP) (3/3)

- Benchmark set: Termination Problem DataBase (TPDB)
  https://termination-portal.org/wiki/TPDB
  $\longrightarrow$ 1000s of termination and complexity problems
- Timeout: 300 seconds

The Termination Competition (termCOMP) (3/3)

- Benchmark set: Termination Problem DataBase (TPDB)
  https://termination-portal.org/wiki/TPDB
  $\longrightarrow$ 1000s of termination and complexity problems
- Timeout: 300 seconds
- Run on StarExec platform [Stump, Sutcliffe, Tinelli, *IJCAR '14*]

The Termination Competition (termCOMP) (3/3)

- Benchmark set: Termination Problem DataBase (TPDB)
  `https://termination-portal.org/wiki/TPDB`
  $\longrightarrow$ 1000s of termination and complexity problems
- Timeout: 300 seconds
- Run on StarExec platform [Stump, Sutcliffe, Tinelli, *IJCAR '14*]
- Categories for proving (non-)termination and for inferring upper/lower complexity bounds for different programming languages

The Termination Competition (termCOMP) (3/3)

- Benchmark set: Termination Problem DataBase (TPDB)
  https://termination-portal.org/wiki/TPDB
  $\longrightarrow$ 1000s of termination and complexity problems
- Timeout: 300 seconds
- Run on StarExec platform [Stump, Sutcliffe, Tinelli, *IJCAR '14*]
- Categories for proving (non-)termination and for inferring upper/lower complexity bounds for different programming languages
- Part of the Olympic Games at the Federated Logic Conference

Input for Automated Tools

Web interfaces available:

- AProVE: https://aprove.informatik.rwth-aachen.de/interface
- iRankFinder: http://irankfinder.loopkiller.com:8081/
- Mu-Term: http://zenon.dsic.upv.es/muterm/index.php/web-interface/
- $\mathsf{T_TT_2}$: http://colo6-c703.uibk.ac.at/ttt2/web/

Input for Automated Tools

Web interfaces available:

- AProVE: https://aprove.informatik.rwth-aachen.de/interface
- iRankFinder: http://irankfinder.loopkiller.com:8081/
- Mu-Term: http://zenon.dsic.upv.es/muterm/index.php/web-interface/
- $\mathsf{T_TT_2}$: http://colo6-c703.uibk.ac.at/ttt2/web/

Input format for termination of TRSs:

```
(VAR x y)
(RULES
  plus(0, y) -> y
  plus(s(x), y) -> s(plus(x, y))
)
```

I.2 Termination Analysis of Programs on Integers

Papers on termination of imperative programs often about **integers** as data

Papers on termination of imperative programs often about **integers** as data

Example (Imperative Program)

if $(\mathsf{x} \geq 0)$
  while $(\mathsf{x} \neq 0)$
    $\mathsf{x} = \mathsf{x} - 1;$

Does this program terminate?
(x ranges over $\mathbb{Z}$)

Papers on termination of imperative programs often about **integers** as data

Example (Imperative Program)

ℓ_0: **if** $(\mathsf{x} \geq 0)$
ℓ_1: **while** $(\mathsf{x} \neq 0)$
ℓ_2: $\mathsf{x} = \mathsf{x} - 1;$

Does this program terminate?
(x ranges over $\mathbb{Z}$)

Example (Equivalent Translation to an Integer Transition System, cf. [McCarthy, *CACM '60*])

$$
\begin{array}{lcll}
\ell_0(x) & \to & \ell_1(x) & [x \geq 0] \\
\ell_0(x) & \to & \ell_3(x) & [x < 0] \\
\ell_1(x) & \to & \ell_2(x) & [x \neq 0] \\
\ell_2(x) & \to & \ell_1(x-1) & \\
\ell_1(x) & \to & \ell_3(x) & [x = 0]
\end{array}
$$

Papers on termination of imperative programs often about **integers** as data

Example (Imperative Program)

ℓ_0: **if** $(\mathsf{x} \geq 0)$
ℓ_1: **while** $(\mathsf{x} \neq 0)$
ℓ_2: $\mathsf{x} = \mathsf{x} - 1;$

Does this program terminate?
(x ranges over $\mathbb{Z}$)

Example (Equivalent Translation to an Integer Transition System, cf. [McCarthy, *CACM '60*])

$$
\begin{array}{lcll}
\ell_0(x) & \to & \ell_1(x) & [x \geq 0] \\
\ell_0(x) & \to & \ell_3(x) & [x < 0] \\
\ell_1(x) & \to & \ell_2(x) & [x \neq 0] \\
\ell_2(x) & \to & \ell_1(x-1) & \\
\ell_1(x) & \to & \ell_3(x) & [x = 0]
\end{array}
$$

Oh no! $\ell_1(-1) \to \ell_2(-1) \to \ell_1(-2) \to \ell_2(-2) \to \ell_1(-3) \to \cdots$

Papers on termination of imperative programs often about **integers** as data

Example (Imperative Program)

ℓ_0: **if** (x ≥ 0)
ℓ_1: **while** (x $\neq 0$)
ℓ_2: x $=$ x $- 1$;

Does this program terminate?
(x ranges over $\mathbb{Z}$)

Example (Equivalent Translation to an Integer Transition System, cf. [McCarthy, *CACM '60*])

$$
\begin{array}{lcll}
\ell_0(x) & \to & \ell_1(x) & [x \geq 0] \\
\ell_0(x) & \to & \ell_3(x) & [x < 0] \\
\ell_1(x) & \to & \ell_2(x) & [x \neq 0] \\
\ell_2(x) & \to & \ell_1(x-1) & \\
\ell_1(x) & \to & \ell_3(x) & [x = 0]
\end{array}
$$

Oh no! $\ell_1(-1) \to \ell_2(-1) \to \ell_1(-2) \to \ell_2(-2) \to \ell_1(-3) \to \cdots$

$\Rightarrow$ **Restrict initial states** to $\ell_0(z)$ for $z \in \mathbb{Z}$

Papers on termination of imperative programs often about **integers** as data

Example (Imperative Program)

ℓ_0: **if** (x ≥ 0)
ℓ_1: **while** (x $\neq 0$)
ℓ_2: x $=$ x $- 1$;

Does this program terminate?
(x ranges over $\mathbb{Z}$)

Example (Equivalent Translation to an Integer Transition System, cf. [McCarthy, *CACM '60*])

$$
\begin{array}{lcll}
\ell_0(x) & \to & \ell_1(x) & [x \geq 0] \\
\ell_0(x) & \to & \ell_3(x) & [x < 0] \\
\ell_1(x) & \to & \ell_2(x) & [x \neq 0] \\
\ell_2(x) & \to & \ell_1(x-1) & \\
\ell_1(x) & \to & \ell_3(x) & [x = 0]
\end{array}
$$

Oh no! $\ell_1(-1) \to \ell_2(-1) \to \ell_1(-2) \to \ell_2(-2) \to \ell_1(-3) \to \cdots$

$\Rightarrow$ **Restrict initial states** to $\ell_0(z)$ for $z \in \mathbb{Z}$

$\Rightarrow$ Find **invariant** $x \geq 0$ at ℓ_1, ℓ_2 (exercise)

Papers on termination of imperative programs often about **integers** as data

Example (Imperative Program)

ℓ_0: **if** $(\mathsf{x} \geq 0)$
ℓ_1: **while** $(\mathsf{x} \neq 0)$
ℓ_2: $\mathsf{x} = \mathsf{x} - 1;$

Does this program terminate?
(x ranges over $\mathbb{Z}$)

Example (Equivalent Translation to an Integer Transition System, cf. [McCarthy, *CACM '60*])

$$
\begin{array}{lcll}
\ell_0(x) & \to & \ell_1(x) & [x \geq 0] \\
\ell_0(x) & \to & \ell_3(x) & [x < 0] \\
\ell_1(x) & \to & \ell_2(x) & [x \neq 0 \land x \geq 0] \\
\ell_2(x) & \to & \ell_1(x-1) & [x \geq 0] \\
\ell_1(x) & \to & \ell_3(x) & [x = 0 \land x \geq 0]
\end{array}
$$

Oh no! $\ell_1(-1) \to \ell_2(-1) \to \ell_1(-2) \to \ell_2(-2) \to \ell_1(-3) \to \cdots$

$\Rightarrow$ **Restrict initial states** to $\ell_0(z)$ for $z \in \mathbb{Z}$

$\Rightarrow$ Find **invariant** $x \geq 0$ at ℓ_1, ℓ_2 (exercise)

Proving Termination with Invariants

Example (Transition system with invariants)

$$\begin{array}{lcll}
\ell_0(x) & \to & \ell_1(x) & [x \geq 0] \\
\ell_1(x) & \to & \ell_2(x) & [x \neq 0 \wedge x \geq 0] \\
\ell_2(x) & \to & \ell_1(x-1) & [x \geq 0] \\
\ell_1(x) & \to & \ell_3(x) & [x = 0 \wedge x \geq 0]
\end{array}$$

Prove termination by ranking function $[\,\cdot\,]$ with $[\ell_0](x) = [\ell_1](x) = \cdots = x$

Proving Termination with Invariants

Example (Transition system with invariants)

$$
\begin{array}{lcll}
\ell_0(x) & \succsim & \ell_1(x) & [x \geq 0] \\
\ell_1(x) & \succsim & \ell_2(x) & [x \neq 0 \land x \geq 0] \\
\ell_2(x) & \succ & \ell_1(x-1) & [x \geq 0] \\
\ell_1(x) & \succsim & \ell_3(x) & [x = 0 \land x \geq 0]
\end{array}
$$

Prove termination by ranking function $[\,\cdot\,]$ with $[\ell_0](x) = [\ell_1](x) = \cdots = x$

Proving Termination with Invariants

Example (Transition system with invariants)

$$
\begin{array}{llll}
\ell_0(x) & \succsim & \ell_1(x) & [x \geq 0] \\
\ell_1(x) & \succsim & \ell_2(x) & [x \neq 0 \land x \geq 0] \\
\ell_2(x) & \succ & \ell_1(x-1) & [x \geq 0] \\
\ell_1(x) & \succsim & \ell_3(x) & [x = 0 \land x \geq 0]
\end{array}
$$

Prove termination by ranking function $[\,\cdot\,]$ with $[\ell_0](x) = [\ell_1](x) = \cdots = x$

Automate search using parametric ranking function:

$$[\ell_0](x) = a_0 + b_0 \cdot x, \quad [\ell_1](x) = a_1 + b_1 \cdot x, \quad \ldots$$

Proving Termination with Invariants

Example (Transition system with invariants)

$$\begin{array}{cccl}
\ell_0(x) & \succsim & \ell_1(x) & [x \geq 0] \\
\ell_1(x) & \succsim & \ell_2(x) & [x \neq 0 \wedge x \geq 0] \\
\ell_2(x) & \succ & \ell_1(x-1) & [x \geq 0] \\
\ell_1(x) & \succsim & \ell_3(x) & [x = 0 \wedge x \geq 0]
\end{array}$$

Prove termination by ranking function $[\,\cdot\,]$ with $[\ell_0](x) = [\ell_1](x) = \cdots = x$

Automate search using parametric ranking function:

$$[\ell_0](x) = a_0 + b_0 \cdot x, \quad [\ell_1](x) = a_1 + b_1 \cdot x, \quad \ldots$$

Constraints here:

$x \geq 0$	$\Rightarrow$	$a_2 + b_2 \cdot x > a_1 + b_1 \cdot (x-1)$	"decrease ..."
$x \geq 0$	$\Rightarrow$	$a_2 + b_2 \cdot x \geq 0$	"... against a bound"

Proving Termination with Invariants

Example (Transition system with invariants)

$$
\begin{array}{lcll}
\ell_0(x) & \succsim & \ell_1(x) & [x \geq 0] \\
\ell_1(x) & \succsim & \ell_2(x) & [x \neq 0 \land x \geq 0] \\
\ell_2(x) & \succ & \ell_1(x-1) & [x \geq 0] \\
\ell_1(x) & \succsim & \ell_3(x) & [x = 0 \land x \geq 0]
\end{array}
$$

Prove termination by ranking function $[\,\cdot\,]$ with $[\ell_0](x) = [\ell_1](x) = \cdots = x$

Automate search using parametric ranking function:

$$[\ell_0](x) = a_0 + b_0 \cdot x, \quad [\ell_1](x) = a_1 + b_1 \cdot x, \quad \ldots$$

Constraints here:

$$
\begin{array}{lcll}
x \geq 0 & \Rightarrow & a_2 + b_2 \cdot x > a_1 + b_1 \cdot (x-1) & \text{"decrease \ldots"} \\
x \geq 0 & \Rightarrow & a_2 + b_2 \cdot x \geq 0 & \text{"\ldots against a bound"}
\end{array}
$$

Use Farkas' Lemma to eliminate $\forall x$, solver for **linear** constraints gives model for a_i, b_i.

Proving Termination with Invariants

Example (Transition system with invariants)

$$
\begin{array}{llll}
\ell_0(x) & \succsim & \ell_1(x) & [x \geq 0] \\
\ell_1(x) & \succsim & \ell_2(x) & [x \neq 0 \land x \geq 0] \\
\ell_2(x) & \succ & \ell_1(x-1) & [x \geq 0] \\
\ell_1(x) & \succsim & \ell_3(x) & [x = 0 \land x \geq 0]
\end{array}
$$

Prove termination by ranking function $[\,\cdot\,]$ with $[\ell_0](x) = [\ell_1](x) = \cdots = x$

Automate search using parametric ranking function:

$$[\ell_0](x) = a_0 + b_0 \cdot x, \quad [\ell_1](x) = a_1 + b_1 \cdot x, \quad \ldots$$

Constraints here:

$$
\begin{array}{lll}
x \geq 0 & \Rightarrow & a_2 + b_2 \cdot x > a_1 + b_1 \cdot (x-1) \quad \text{“decrease ...”} \\
x \geq 0 & \Rightarrow & a_2 + b_2 \cdot x \geq 0 \quad \text{“... against a bound”}
\end{array}
$$

Use Farkas' Lemma to eliminate $\forall x$, solver for **linear** constraints gives model for a_i, b_i.

More: [Podelski, Rybalchenko, *VMCAI '04*, Alias et al, *SAS '10*]

Proving Termination with Invariants

Example (Transition system with invariants)

$$\begin{array}{lcll} \ell_0(x) & \rightarrow & \ell_1(x) & [x \geq 0] \\ \ell_1(x) & \rightarrow & \ell_2(x) & [x \neq 0 \land x \geq 0] \\ & & & \\ \ell_1(x) & \rightarrow & \ell_3(x) & [x = 0 \land x \geq 0] \end{array}$$

Prove termination by ranking function $[\,\cdot\,]$ with $[\ell_0](x) = [\ell_1](x) = \cdots = x$

Automate search using parametric ranking function:

$$[\ell_0](x) = a_0 + b_0 \cdot x, \quad [\ell_1](x) = a_1 + b_1 \cdot x, \quad \ldots$$

Constraints here:

$$\begin{array}{lcll} x \geq 0 & \Rightarrow & a_2 + b_2 \cdot x > a_1 + b_1 \cdot (x-1) & \text{“decrease \ldots”} \\ x \geq 0 & \Rightarrow & a_2 + b_2 \cdot x \geq 0 & \text{“\ldots against a bound”} \end{array}$$

Use Farkas' Lemma to eliminate $\forall x$, solver for **linear** constraints gives model for a_i, b_i.

More: [Podelski, Rybalchenko, *VMCAI '04*, Alias et al, *SAS '10*]

Searching for Invariants Using SMT

Termination prover needs to find invariants for programs on integers

Searching for Invariants Using SMT

Termination prover needs to find invariants for programs on integers

- Statically before the translation
  [Otto et al, *RTA '10*; Ströder et al, *JAR '17*, ...]
  $\longrightarrow$ abstract interpretation [Cousot, Cousot, *POPL '77*]
  $\longrightarrow$ more about this in a few minutes!

Searching for Invariants Using SMT

Termination prover needs to find invariants for programs on integers

- Statically before the translation
  [Otto et al, *RTA '10*; Ströder et al, *JAR '17*, ...]
  $\longrightarrow$ abstract interpretation [Cousot, Cousot, *POPL '77*]
  $\longrightarrow$ more about this in a few minutes!
- By counterexample-based reasoning + safety prover: **Terminator**
  [Cook, Podelski, Rybalchenko, *CAV '06, PLDI '06*]
  $\longrightarrow$ prove termination of single program **runs**
  $\longrightarrow$ termination argument often generalises

Searching for Invariants Using SMT

Termination prover needs to find invariants for programs on integers

- Statically before the translation
  [Otto et al, *RTA '10*; Ströder et al, *JAR '17*, . . .]
  $\longrightarrow$ abstract interpretation [Cousot, Cousot, *POPL '77*]
  $\longrightarrow$ more about this in a few minutes!
- By counterexample-based reasoning + safety prover: **Terminator**
  [Cook, Podelski, Rybalchenko, *CAV '06, PLDI '06*]
  $\longrightarrow$ prove termination of single program **runs**
  $\longrightarrow$ termination argument often generalises
- . . . also cooperating with removal of terminating **rules** (as for TRSs):
  T2 [Brockschmidt, Cook, Fuhs, *CAV '13*; Brockschmidt et al, *TACAS '16*]

Searching for Invariants Using SMT

Termination prover needs to find invariants for programs on integers

- Statically before the translation
  [Otto et al, *RTA '10*; Ströder et al, *JAR '17*, ...]
  $\longrightarrow$ abstract interpretation [Cousot, Cousot, *POPL '77*]
  $\longrightarrow$ more about this in a few minutes!
- By counterexample-based reasoning + safety prover: **Terminator**
  [Cook, Podelski, Rybalchenko, *CAV '06, PLDI '06*]
  $\longrightarrow$ prove termination of single program **runs**
  $\longrightarrow$ termination argument often generalises
- ... also cooperating with removal of terminating **rules** (as for TRSs):
  T2 [Brockschmidt, Cook, Fuhs, *CAV '13*; Brockschmidt et al, *TACAS '16*]
- Using Max-SMT
  [Larraz, Oliveras, Rodríguez-Carbonell, Rubio, *FMCAD '13*]

Searching for Invariants Using SMT

Termination prover needs to find invariants for programs on integers

- Statically before the translation
  [Otto et al, *RTA '10*; Ströder et al, *JAR '17*, ...]
  $\longrightarrow$ abstract interpretation [Cousot, Cousot, *POPL '77*]
  $\longrightarrow$ more about this in a few minutes!
- By counterexample-based reasoning + safety prover: **Terminator**
  [Cook, Podelski, Rybalchenko, *CAV '06, PLDI '06*]
  $\longrightarrow$ prove termination of single program **runs**
  $\longrightarrow$ termination argument often generalises
- ... also cooperating with removal of terminating **rules** (as for TRSs):
  T2 [Brockschmidt, Cook, Fuhs, *CAV '13*; Brockschmidt et al, *TACAS '16*]
- Using Max-SMT
  [Larraz, Oliveras, Rodríguez-Carbonell, Rubio, *FMCAD '13*]

Nowadays all SMT-based!

Extensions

- Proving **non**-termination (infinite run is possible **from initial states**) [Gupta et al, *POPL '08*, Brockschmidt et al, *FoVeOOS '11*, Chen et al, *TACAS '14*, Larraz et al, *CAV '14*, Cook et al, *FMCAD '14*, ...]

Extensions

- Proving **non**-termination (infinite run is possible **from initial states**) [Gupta et al, *POPL '08*, Brockschmidt et al, *FoVeOOS '11*, Chen et al, *TACAS '14*, Larraz et al, *CAV '14*, Cook et al, *FMCAD '14*, ...]
- Complexity bounds [Alias et al, *SAS '10*, Hoffmann, Shao, *JFP '15*, Brockschmidt et al, *TOPLAS '16*, ...]

Extensions

- Proving **non**-termination (infinite run is possible **from initial states**) [Gupta et al, *POPL '08*, Brockschmidt et al, *FoVeOOS '11*, Chen et al, *TACAS '14*, Larraz et al, *CAV '14*, Cook et al, *FMCAD '14*, ...]
- Complexity bounds [Alias et al, *SAS '10*, Hoffmann, Shao, *JFP '15*, Brockschmidt et al, *TOPLAS '16*, ...]
- CTL* model checking for **infinite** state systems based on termination and non-termination provers [Cook, Khlaaf, Piterman, *JACM '17*]

Extensions

- Proving **non**-termination (infinite run is possible **from initial states**)
  [Gupta et al, *POPL '08*, Brockschmidt et al, *FoVeOOS '11*, Chen et al, *TACAS '14*, Larraz et al, *CAV '14*, Cook et al, *FMCAD '14*, ...]

- Complexity bounds
  [Alias et al, *SAS '10*, Hoffmann, Shao, *JFP '15*, Brockschmidt et al, *TOPLAS '16*, ...]

- CTL* model checking for **infinite** state systems based on termination and non-termination provers
  [Cook, Khlaaf, Piterman, *JACM '17*]

- Beyond sequential programs on integers:
  - structs/classes [Berdine et al, *CAV '06*; Otto et al, *RTA '10*; ...]
  - arrays (pointer arithmetic) [Ströder et al, *JAR '17*, ...]
  - multi-threaded programs [Cook et al, *PLDI '07*, ...]
  - ...

Why Care about Termination of Term Rewriting?

- Termination needed by theorem provers

- Translate program P with inductive data structures (trees) to TRS, represent data structures as terms

  $\Rightarrow$ Termination of TRS implies termination of P

  - Logic programming: Prolog
    [van Raamsdonk, *ICLP '97*; Schneider-Kamp et al, *TOCL '09*; Giesl et al, *PPDP '12*]
  - (Lazy) functional programming: Haskell [Giesl et al, *TOPLAS '11*]
  - Object-oriented programming: Java [Otto et al, *RTA '10*]

Beyond Classic TRSs for Program Analysis

So far, so good ...
but do we *really* want to represent 1000000 as $\mathsf{s}(\mathsf{s}(\mathsf{s}(...)))$?!

Beyond Classic TRSs for Program Analysis

So far, so good ...
but do we *really* want to represent 1000000 as $\mathsf{s}(\mathsf{s}(\mathsf{s}(...)))$?!

Drawbacks:

Beyond Classic TRSs for Program Analysis

So far, so good ...
but do we *really* want to represent 1000000 as $\mathsf{s}(\mathsf{s}(\mathsf{s}(...)))$?!

Drawbacks:

- throws away domain knowledge about built-in data types like integers

Beyond Classic TRSs for Program Analysis

So far, so good ...
but do we *really* want to represent 1000000 as $\mathsf{s}(\mathsf{s}(\mathsf{s}(...)))$?!

Drawbacks:

- throws away domain knowledge about built-in data types like integers
- need to analyse recursive rules for minus, quot, ... over and over

Beyond Classic TRSs for Program Analysis

So far, so good ...
but do we *really* want to represent 1000000 as $\mathsf{s}(\mathsf{s}(\mathsf{s}(...)))$?!

Drawbacks:

- throws away domain knowledge about built-in data types like integers
- need to analyse recursive rules for minus, quot, ... over and over
- does not benefit from dedicated constraint solvers
  (e.g., SMT solvers) for arithmetic operations in programs

Beyond Classic TRSs for Program Analysis

So far, so good ...
but do we *really* want to represent 1000000 as $\mathsf{s}(\mathsf{s}(\mathsf{s}(...)))$?!

Drawbacks:

- throws away domain knowledge about built-in data types like integers
- need to analyse recursive rules for minus, quot, ... over and over
- does not benefit from dedicated constraint solvers
  (e.g., SMT solvers) for arithmetic operations in programs

Solution: use **constrained term rewriting**

Constrained Term Rewriting, What's That?

Term rewriting "with batteries included"

- first-order
- no fixed evaluation strategy
- no fixed order of rules to apply

Constrained Term Rewriting, What's That?

Term rewriting "with batteries included"

- first-order
- no fixed evaluation strategy
- no fixed order of rules to apply
- typed

Constrained Term Rewriting, What's That?

Term rewriting "with batteries included"

- first-order
- no fixed evaluation strategy
- no fixed order of rules to apply
- typed
- with pre-defined data structures (integers, arrays, bitvectors, ...), usually from SMT-LIB theories

Constrained Term Rewriting, What's That?

Term rewriting "with batteries included"

- first-order
- no fixed evaluation strategy
- no fixed order of rules to apply
- typed
- with pre-defined data structures (integers, arrays, bitvectors, ...), usually from SMT-LIB theories
- rewrite rules with SMT constraints

Constrained Term Rewriting, What's That?

Term rewriting "with batteries included"

- first-order
- no fixed evaluation strategy
- no fixed order of rules to apply
- typed
- with pre-defined data structures (integers, arrays, bitvectors, ...), usually from SMT-LIB theories
- rewrite rules with SMT constraints

$\Rightarrow$ Term rewriting + SMT solving for automated reasoning

Constrained Term Rewriting, What's That?

Term rewriting "with batteries included"

- first-order
- no fixed evaluation strategy
- no fixed order of rules to apply
- typed
- with pre-defined data structures (integers, arrays, bitvectors, ...), usually from SMT-LIB theories
- rewrite rules with SMT constraints

$\Rightarrow$ Term rewriting + SMT solving for automated reasoning

- General forms available, e.g., Logically Constrained TRSs [Kop, Nishida, *FroCoS '13*]

Constrained Term Rewriting, What's That?

Term rewriting "with batteries included"

- first-order
- no fixed evaluation strategy
- no fixed order of rules to apply
- typed
- with pre-defined data structures (integers, arrays, bitvectors, ...), usually from SMT-LIB theories
- rewrite rules with SMT constraints

$\Rightarrow$ Term rewriting + SMT solving for automated reasoning

- General forms available, e.g., Logically Constrained TRSs [Kop, Nishida, *FroCoS '13*]
- For program termination: use term rewriting with **integers** [Falke, Kapur, *CADE '09*; Fuhs et al, *RTA '09*; Giesl et al, *JAR '17*]

Constrained Rewriting by Example

Example (Constrained Rewrite System)

$$
\begin{array}{rcll}
\ell_0(n, r) & \rightarrow & \ell_1(n, r, \mathsf{Nil}) & \\
\ell_1(n, r, xs) & \rightarrow & \ell_1(n-1, r+1, \mathsf{Cons}(r, xs)) & [n > 0] \\
\ell_1(n, r, xs) & \rightarrow & \ell_2(xs) & [n = 0]
\end{array}
$$

Constrained Rewriting by Example

Example (Constrained Rewrite System)

$$
\begin{array}{rcll}
\ell_0(n, r) & \rightarrow & \ell_1(n, r, \mathsf{Nil}) & \\
\ell_1(n, r, xs) & \rightarrow & \ell_1(n-1, r+1, \mathsf{Cons}(r, xs)) & [n > 0] \\
\ell_1(n, r, xs) & \rightarrow & \ell_2(xs) & [n = 0]
\end{array}
$$

Possible rewrite sequence:

$$\ell_0(2, 7)$$

Constrained Rewriting by Example

Example (Constrained Rewrite System)

$$
\begin{array}{rcll}
\ell_0(n, r) & \to & \ell_1(n, r, \mathsf{Nil}) & \\
\ell_1(n, r, xs) & \to & \ell_1(n-1, r+1, \mathsf{Cons}(r, xs)) & [n > 0] \\
\ell_1(n, r, xs) & \to & \ell_2(xs) & [n = 0]
\end{array}
$$

Possible rewrite sequence:

$$
\begin{array}{l}
\ell_0(2, 7) \\
\to \ell_1(2, 7, \mathsf{Nil})
\end{array}
$$

Constrained Rewriting by Example

Example (Constrained Rewrite System)

$$
\begin{array}{rcll}
\ell_0(n, r) & \to & \ell_1(n, r, \mathsf{Nil}) & \\
\ell_1(n, r, xs) & \to & \ell_1(n-1, r+1, \mathsf{Cons}(r, xs)) & [n > 0] \\
\ell_1(n, r, xs) & \to & \ell_2(xs) & [n = 0]
\end{array}
$$

Possible rewrite sequence:

$$
\begin{array}{l}
\ \ \ \ell_0(2, 7) \\
\to \ell_1(2, 7, \mathsf{Nil}) \\
\to \ell_1(1, 8, \mathsf{Cons}(7, \mathsf{Nil}))
\end{array}
$$

Constrained Rewriting by Example

Example (Constrained Rewrite System)

$$
\begin{array}{rcll}
\ell_0(n, r) & \to & \ell_1(n, r, \mathsf{Nil}) & \\
\ell_1(n, r, xs) & \to & \ell_1(n-1, r+1, \mathsf{Cons}(r, xs)) & [n > 0] \\
\ell_1(n, r, xs) & \to & \ell_2(xs) & [n = 0]
\end{array}
$$

Possible rewrite sequence:

$$
\begin{array}{l}
\quad \ell_0(2, 7) \\
\to \ell_1(2, 7, \mathsf{Nil}) \\
\to \ell_1(1, 8, \mathsf{Cons}(7, \mathsf{Nil})) \\
\to \ell_1(0, 9, \mathsf{Cons}(8, \mathsf{Cons}(7, \mathsf{Nil})))
\end{array}
$$

Constrained Rewriting by Example

Example (Constrained Rewrite System)

$$
\begin{array}{rcll}
\ell_0(n, r) & \rightarrow & \ell_1(n, r, \mathsf{Nil}) & \\
\ell_1(n, r, xs) & \rightarrow & \ell_1(n-1, r+1, \mathsf{Cons}(r, xs)) & [n > 0] \\
\ell_1(n, r, xs) & \rightarrow & \ell_2(xs) & [n = 0]
\end{array}
$$

Possible rewrite sequence:

$$
\begin{array}{l}
\quad \ell_0(2, 7) \\
\rightarrow \ell_1(2, 7, \mathsf{Nil}) \\
\rightarrow \ell_1(1, 8, \mathsf{Cons}(7, \mathsf{Nil})) \\
\rightarrow \ell_1(0, 9, \mathsf{Cons}(8, \mathsf{Cons}(7, \mathsf{Nil}))) \\
\rightarrow \ell_2(\mathsf{Cons}(8, \mathsf{Cons}(7, \mathsf{Nil})))
\end{array}
$$

Constrained Rewriting by Example

Example (Constrained Rewrite System)

$$
\begin{array}{rcll}
\ell_0(n, r) & \to & \ell_1(n, r, \mathsf{Nil}) & \\
\ell_1(n, r, xs) & \to & \ell_1(n-1, r+1, \mathsf{Cons}(r, xs)) & [n > 0] \\
\ell_1(n, r, xs) & \to & \ell_2(xs) & [n = 0]
\end{array}
$$

Possible rewrite sequence:

$$
\begin{array}{l}
\ell_0(2, 7) \\
\to \ell_1(2, 7, \mathsf{Nil}) \\
\to \ell_1(1, 8, \mathsf{Cons}(7, \mathsf{Nil})) \\
\to \ell_1(0, 9, \mathsf{Cons}(8, \mathsf{Cons}(7, \mathsf{Nil}))) \\
\to \ell_2(\mathsf{Cons}(8, \mathsf{Cons}(7, \mathsf{Nil})))
\end{array}
$$

Here 7, 8, $\ldots$ are predefined constants.

Constrained Rewriting by Example

Example (Constrained Rewrite System)

$$
\begin{array}{rcll}
\ell_0(n, r) & \to & \ell_1(n, r, \mathsf{Nil}) & \\
\ell_1(n, r, xs) & \to & \ell_1(n-1, r+1, \mathsf{Cons}(r, xs)) & [n > 0] \\
\ell_1(n, r, xs) & \to & \ell_2(xs) & [n = 0]
\end{array}
$$

Possible rewrite sequence:

$$
\begin{array}{l}
\quad\ \ell_0(2, 7) \\
\to \ell_1(2, 7, \mathsf{Nil}) \\
\to \ell_1(1, 8, \mathsf{Cons}(7, \mathsf{Nil})) \\
\to \ell_1(0, 9, \mathsf{Cons}(8, \mathsf{Cons}(7, \mathsf{Nil}))) \\
\to \ell_2(\mathsf{Cons}(8, \mathsf{Cons}(7, \mathsf{Nil})))
\end{array}
$$

Here 7, 8, $\ldots$ are predefined constants.

Termination proof: reuse techniques for TRSs and integer programs

Conclusion: Termination Proving Back-Ends

- Automated termination analysis for term rewriting and for imperative programs developed in parallel over the last ~ 20 years

Conclusion: Termination Proving Back-Ends

- Automated termination analysis for term rewriting and for imperative programs developed in parallel over the last ~ 20 years
- Term rewriting: handles **inductive data structures** well

Conclusion: Termination Proving Back-Ends

- Automated termination analysis for term rewriting and for imperative programs developed in parallel over the last $\sim$ 20 years
- Term rewriting: handles **inductive data structures** well
- Imperative programs on integers: need to consider **reachability/safety** and **invariants**

Conclusion: Termination Proving Back-Ends

- Automated termination analysis for term rewriting and for imperative programs developed in parallel over the last $\sim$ 20 years
- Term rewriting: handles **inductive data structures** well
- Imperative programs on integers: need to consider **reachability/safety** and **invariants**
- Since a few years cross-fertilisation

Conclusion: Termination Proving Back-Ends

- Automated termination analysis for term rewriting and for imperative programs developed in parallel over the last $\sim$ 20 years
- Term rewriting: handles **inductive data structures** well
- Imperative programs on integers: need to consider **reachability/safety** and **invariants**
- Since a few years cross-fertilisation
- Constrained term rewriting: best of both worlds as back-end language

Conclusion: Termination Proving Back-Ends

- Automated termination analysis for term rewriting and for imperative programs developed in parallel over the last $\sim$ 20 years
- Term rewriting: handles **inductive data structures** well
- Imperative programs on integers: need to consider **reachability/safety** and **invariants**
- Since a few years cross-fertilisation
- Constrained term rewriting: best of both worlds as back-end language
- Proof search heavily relies on SMT solving for automation

Conclusion: Termination Proving Back-Ends

- Automated termination analysis for term rewriting and for imperative programs developed in parallel over the last $\sim$ 20 years
- Term rewriting: handles **inductive data structures** well
- Imperative programs on integers: need to consider **reachability/safety** and **invariants**
- Since a few years cross-fertilisation
- Constrained term rewriting: best of both worlds as back-end language
- Proof search heavily relies on SMT solving for automation
- Needs of termination analysis have also led to better SMT solvers

Conclusion: Termination Proving Back-Ends

- Automated termination analysis for term rewriting and for imperative programs developed in parallel over the last $\sim$ 20 years
- Term rewriting: handles **inductive data structures** well
- Imperative programs on integers: need to consider **reachability/safety** and **invariants**
- Since a few years cross-fertilisation
- Constrained term rewriting: best of both worlds as back-end language
- Proof search heavily relies on SMT solving for automation
- Needs of termination analysis have also led to better SMT solvers
- More information . . .

http://termination-portal.org

Conclusion: Termination Proving Back-Ends

- Automated termination analysis for term rewriting and for imperative programs developed in parallel over the last $\sim$ 20 years
- Term rewriting: handles **inductive data structures** well
- Imperative programs on integers: need to consider **reachability/safety** and **invariants**
- Since a few years cross-fertilisation
- Constrained term rewriting: best of both worlds as back-end language
- Proof search heavily relies on SMT solving for automation
- Needs of termination analysis have also led to better SMT solvers
- More information ...

http://termination-portal.org

Behind (almost) every successful termination prover ...

Conclusion: Termination Proving Back-Ends

- Automated termination analysis for term rewriting and for imperative programs developed in parallel over the last $\sim$ 20 years
- Term rewriting: handles **inductive data structures** well
- Imperative programs on integers: need to consider **reachability/safety** and **invariants**
- Since a few years cross-fertilisation
- Constrained term rewriting: best of both worlds as back-end language
- Proof search heavily relies on SMT solving for automation
- Needs of termination analysis have also led to better SMT solvers
- More information ...

http://termination-portal.org

Behind (almost) every successful termination prover ...

... there is a powerful SAT / SMT solver!

I.3 Termination Analysis of Java programs

From Program to Constrained Term Rewriting, high-level

- execute program **symbolically** from initial states of the program, handle language peculiarities here ($\longrightarrow$ Java: sharing, cyclicity analysis)

```
f : if ...
        ...
    else
        ...
        g : while ...
                ...
```

From Program to Constrained Term Rewriting, high-level

- execute program **symbolically** from initial states of the program, handle language peculiarities here ($\longrightarrow$ Java: sharing, cyclicity analysis)

```
f : if ...
        ...
    else
        ...
        g : while ...
                ...
```

init(...)

From Program to Constrained Term Rewriting, high-level

- execute program **symbolically** from initial states of the program, handle language peculiarities here ($\longrightarrow$ Java: sharing, cyclicity analysis)

```
f : if ...
        ...
    else
        ...
        g : while ...
                ...
```

$\mathsf{init}(\ldots)$

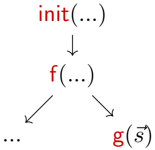
$\downarrow$

$\mathsf{f}(\ldots)$

From Program to Constrained Term Rewriting, high-level

- execute program **symbolically** from initial states of the program, handle language peculiarities here ($\longrightarrow$ Java: sharing, cyclicity analysis)

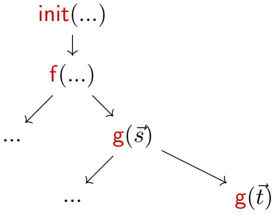
```
f : if ...
        ...
    else
        ...
        g : while ...
                ...
```



From Program to Constrained Term Rewriting, high-level

- execute program **symbolically** from initial states of the program, handle language peculiarities here ($\longrightarrow$ Java: sharing, cyclicity analysis)

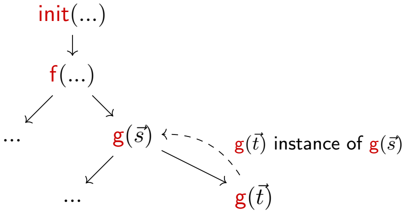
```
f : if ...
        ...
    else
        ...
        g : while ...
                ...
```



From Program to Constrained Term Rewriting, high-level

- execute program **symbolically** from initial states of the program, handle language peculiarities here (⟶ Java: sharing, cyclicity analysis)
- use **generalisation** of program states, get **over-approximation** of all possible program runs (≈ control-flow graph with extra info)
- closely related: Abstract Interpretation [Cousot and Cousot, *POPL '77*]

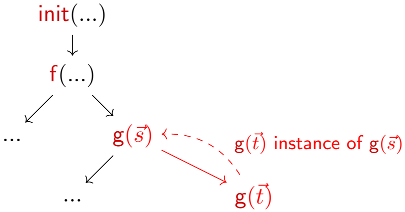
```
f : if ...
        ...
    else
        ...
        g : while ...
                ...
```



From Program to Constrained Term Rewriting, high-level

- execute program **symbolically** from initial states of the program, handle language peculiarities here (⟶ Java: sharing, cyclicity analysis)
- use **generalisation** of program states, get **over-approximation** of all possible program runs (≈ control-flow graph with extra info)
- closely related: Abstract Interpretation [Cousot and Cousot, *POPL '77*]
- **extract TRS** from cycles in the representation

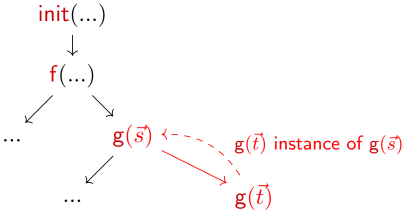
```
f : if ...
        ...
    else
        ...
        g : while ...
                  ...
```



From Program to Constrained Term Rewriting, high-level

- execute program **symbolically** from initial states of the program, handle language peculiarities here ($\longrightarrow$ Java: sharing, cyclicity analysis)
- use **generalisation** of program states, get **over-approximation** of all possible program runs ($\approx$ control-flow graph with extra info)
- closely related: Abstract Interpretation [Cousot and Cousot, *POPL '77*]
- **extract TRS** from cycles in the representation
- if TRS terminates
  $\Rightarrow$ any **concrete program execution** can use cycles only finitely often
  $\Rightarrow$ the program **must terminate**

```
f : if ...
        ...
    else
        ...
        g : while ...
                ...
```



Application: Termination Analysis of Programs

Recipe for proving program termination by reusing TRS termination provers

Application: Termination Analysis of Programs

Recipe for proving program termination by reusing TRS termination provers

- Decide on suitable symbolic representation of abstract program states (**abstract domain**)
  $\longrightarrow$ here: what data objects can we represent as terms?

Application: Termination Analysis of Programs

Recipe for proving program termination by reusing TRS termination provers

- Decide on suitable symbolic representation of abstract program states (**abstract domain**)
  $\longrightarrow$ here: what data objects can we represent as terms?
- Execute program **symbolically** from its initial states

Application: Termination Analysis of Programs

Recipe for proving program termination by reusing TRS termination provers

- Decide on suitable symbolic representation of abstract program states (**abstract domain**)
  $\longrightarrow$ here: what data objects can we represent as terms?
- Execute program **symbolically** from its initial states
- Use **generalisation** of program states to get closed finite representation (symbolic execution graph, abstract interpretation)

Application: Termination Analysis of Programs

Recipe for proving program termination by reusing TRS termination provers

- Decide on suitable symbolic representation of abstract program states (**abstract domain**)
  $\longrightarrow$ here: what data objects can we represent as terms?
- Execute program **symbolically** from its initial states
- Use **generalisation** of program states to get closed finite representation (symbolic execution graph, abstract interpretation)
- Extract **rewrite rules** that “over-approximate” program executions in strongly-connected components of graph

Application: Termination Analysis of Programs

Recipe for proving program termination by reusing TRS termination provers

- Decide on suitable symbolic representation of abstract program states (**abstract domain**)
  $\longrightarrow$ here: what data objects can we represent as terms?
- Execute program **symbolically** from its initial states
- Use **generalisation** of program states to get closed finite representation (symbolic execution graph, abstract interpretation)
- Extract **rewrite rules** that "over-approximate" program executions in strongly-connected components of graph
- Prove **termination** of these rewrite rules
  $\Rightarrow$ implies termination of program from initial states

Java Challenges

Java: object-oriented imperative language

- sharing and aliasing (several references to the same object)
- side effects
- cyclic data objects (e.g., `list.next == list`)
- object-orientation with inheritance
- ...

Java Example

```
public class MyInt {

  // only wrap a primitive int
  private int val;

  // count "num" up to the value in "limit"
  public static void count(MyInt num, MyInt limit) {
    if (num == null || limit == null) {
      return;
    }
    // introduce sharing
    MyInt copy = num;
    while (num.val < limit.val) {
      copy.val++;
    }
  }
}
```

Does **count** terminate for all inputs? Why (not)?

(Assume that **num** and **limit** are not references to the same object.)

Approach to Termination Analysis of Java

Tailor two-stage approach to Java [Otto et al, *RTA '10*]

Approach to Termination Analysis of Java

Tailor two-stage approach to Java [Otto et al, *RTA '10*]

Back-end: From rewrite system to termination proof

- Constrained term rewriting with integers [Giesl et al, *JAR '17*]
- Termination techniques for rewriting and for integers can be integrated

Approach to Termination Analysis of Java

Tailor two-stage approach to Java [Otto et al, *RTA '10*]

Back-end: From rewrite system to termination proof

- Constrained term rewriting with integers [Giesl et al, *JAR '17*]
- Termination techniques for rewriting and for integers can be integrated

Front-end: From Java to constrained rewrite system

- Build **symbolic execution graph** that over-approximates all runs of Java program (abstract interpretation)
- Symbolic execution graph has **invariants** for integers and heap object shape (trees?)
- Extract rewrite system from symbolic execution graph

Approach to Termination Analysis of Java

Tailor two-stage approach to Java [Otto et al, *RTA '10*]

Back-end: From rewrite system to termination proof

- Constrained term rewriting with integers [Giesl et al, *JAR '17*]
- Termination techniques for rewriting and for integers can be integrated

Front-end: From Java to constrained rewrite system

- Build **symbolic execution graph** that over-approximates all runs of Java program (abstract interpretation)
- Symbolic execution graph has **invariants** for integers and heap object shape (trees?)
- Extract rewrite system from symbolic execution graph

Implemented in the tool AProVE ($\longrightarrow$ web interface)

http://aprove.informatik.rwth-aachen.de/

Java: Source Code vs Bytecode

[Otto et al, *RTA '10*] describe their technique for **compiled** Java programs: **Java Bytecode**

Java: Source Code vs Bytecode

[Otto et al, *RTA '10*] describe their technique for **compiled** Java programs: **Java Bytecode**

- desugared machine code for a (virtual) stack machine, still has all the (relevant) information from source code
- input for Java interpreter and for many program analysis tools
- somewhat inconvenient for presentation, though ...

Java: Source Code vs Bytecode

[Otto et al, *RTA '10*] describe their technique for **cor**
programs: **Java Bytecode**

- desugared machine code for a (virtual) stack mac
  still has all the (relevant) information from sourc
- input for Java interpreter and for many program
- somewhat inconvenient for presentation, though

```
00: aload_0
01: ifnull 8
04: aload_1
05: ifnonnull 9
08: return
09: aload_0
10: astore_2
11: aload_0
12: getfield val
15: aload_1
16: getfield val
19: if_icmpge 35
22: aload_2
23: aload_2
24: getfield val
27: iconst_1
28: iadd
29: putfield val
32: goto 11
35: return
```

Java: Source Code vs Bytecode

[Otto et al, *RTA '10*] describe their technique for **compiled** Java programs: **Java Bytecode**

- desugared machine code for a (virtual) stack machine, still has all the (relevant) information from source code
- input for Java interpreter and for many program analysis tools
- somewhat inconvenient for presentation, though ...

Here: **Java source code**

Ingredients for the Abstract Domain

1. program counter value (line number)
2. values of variables (treating `int` as $\mathbb{Z}$)
3. over-approximating info on possible variable values
   - integers: use intervals, e.g. x $\in [4,\ 7]$ or y $\in [0,\ \infty)$
   - heap memory with objects, **no sharing** unless stated otherwise
   - `MyInt(?)`: maybe `null`, maybe a `MyInt` object

   Heap predicates:
   - Two references may be equal: $o_1 =^? o_2$

03	num : o_1, limit : o_2
o_1 : MyInt(?)	
o_2 : MyInt(val $= i_1$)	
i_1 : $[4, 80]$	

Ingredients for the Abstract Domain

1. program counter value (line number)
2. values of variables (treating `int` as $\mathbb{Z}$)
3. over-approximating info on possible variable values
   - integers: use intervals, e.g. x $\in [4,\ 7]$ or y $\in [0,\ \infty)$
   - heap memory with objects, **no sharing** unless stated otherwise
   - `MyInt(?)`: maybe `null`, maybe a `MyInt` object

Heap predicates:

- Two references may be equal: $o_1 =^? o_2$
- Two references may share: $o_1 \searrow\!\swarrow o_2$

`03` | `num` : o_1, `limit` : o_2
o_1 : `MyInt`$(?)$
o_2 : `MyInt`$($`val` $= i_1)$
i_1 : $[4, 80]$

Ingredients for the Abstract Domain

1. program counter value (line number)
2. values of variables (treating `int` as $\mathbb{Z}$)
3. over-approximating info on possible variable values
   - integers: use intervals, e.g. x $\in [4,\ 7]$ or y $\in [0,\ \infty)$
   - heap memory with objects, **no sharing** unless stated otherwise
   - `MyInt`(?): maybe `null`, maybe a `MyInt` object

   Heap predicates:

   - Two references may be equal: $o_1 =^? o_2$
   - Two references may share: $o_1 \searrow\!\swarrow o_2$
   - Reference may have cycles: $o_1\,!$

`03` | num : o_1, `limit` : o_2
o_1 : `MyInt`$(?)$
o_2 : `MyInt`(val $= i_1$)
i_1 : $[4, 80]$

Building the Symbolic Execution Graph

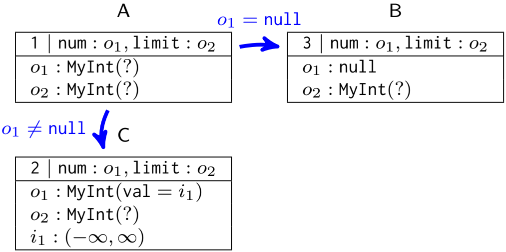
```
public class MyInt {
  private int val;
  static void count(MyInt num,
       MyInt limit) {
    if (num == null
        || limit == null)
      return;
    MyInt copy = num;
    while (num.val < limit.val)
      copy.val++;
} }
```

A

1	num : o_1, limit : o_2
o_1 : MyInt(?)	
o_2 : MyInt(?)	

Building the Symbolic Execution Graph

```
public class MyInt {
  private int val;
  static void count(MyInt num,
         MyInt limit) {
    if (num == null
        || limit == null)
      return;
    MyInt copy = num;
    while (num.val < limit.val)
      copy.val++;
} }
```

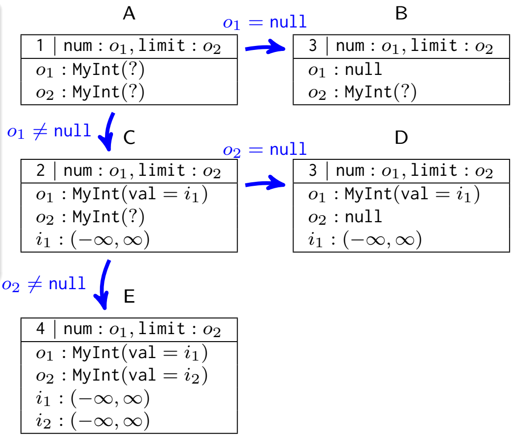


$$X \xrightarrow{cond} Y$$

means: refine X with $cond$, then evaluate to Y; here combined for brevity (narrowing)

Building the Symbolic Execution Graph

```
public class MyInt {
  private int val;
  static void count(MyInt num,
         MyInt limit) {
     if (num == null
         || limit == null)
       return;
     MyInt copy = num;
     while (num.val < limit.val)
       copy.val++;
} }
```

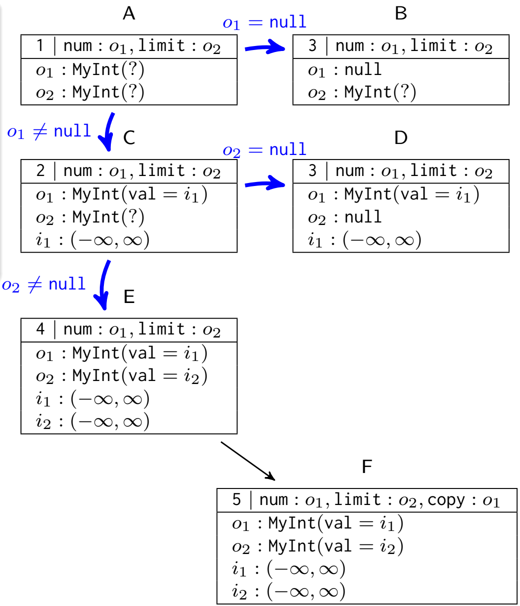


$$\mathrm{X} \xrightarrow{cond} \mathrm{Y}$$

means: refine X with $cond$, then evaluate to Y; here combined for brevity (narrowing)

Building the Symbolic Execution Graph

```
public class MyInt {
  private int val;
  static void count(MyInt num,
         MyInt limit) {
    if (num == null
        || limit == null)
      return;
    MyInt copy = num;
    while (num.val < limit.val)
      copy.val++;
} }
```

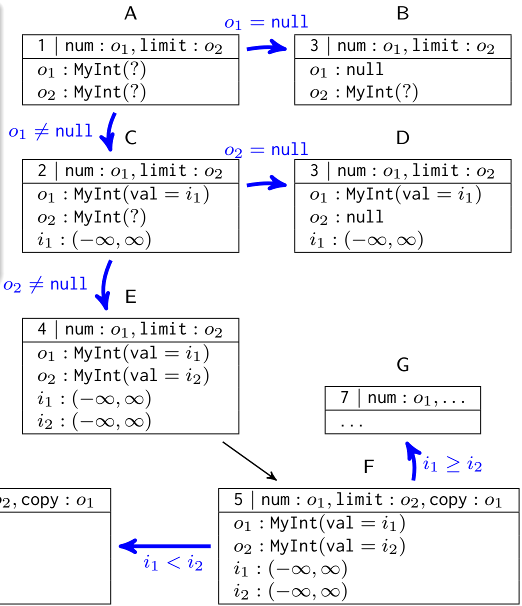


X ⟶ Y

means: evaluate X to Y

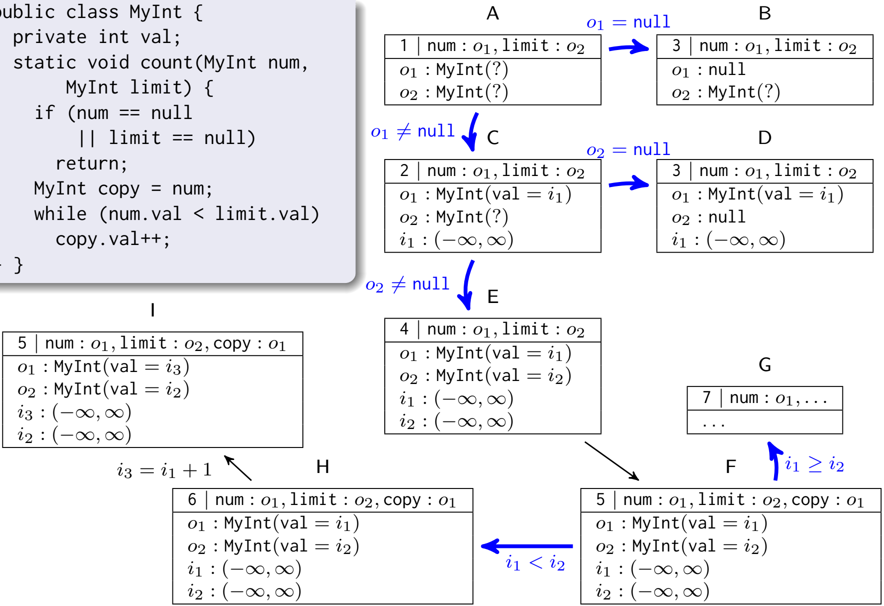
Building the Symbolic Execution Graph

```
   public class MyInt {
     private int val;
     static void count(MyInt num,
          MyInt limit) {
1:      if (num == null
2:          || limit == null)
3:        return;
4:      MyInt copy = num;
5:      while (num.val < limit.val)
6:        copy.val++;
7:  } }
```



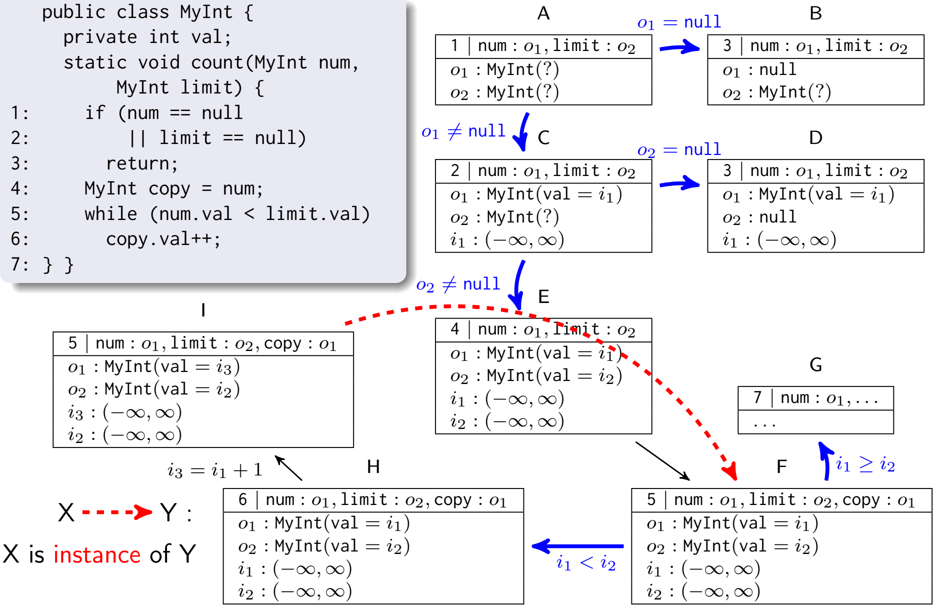
Building the Symbolic Execution Graph

```
public class MyInt {
  private int val;
  static void count(MyInt num,
       MyInt limit) {
    if (num == null
        || limit == null)
      return;
    MyInt copy = num;
    while (num.val < limit.val)
      copy.val++;
} }
```



Building the Symbolic Execution Graph

```
   public class MyInt {
     private int val;
     static void count(MyInt num,
          MyInt limit) {
1:      if (num == null
2:          || limit == null)
3:        return;
4:      MyInt copy = num;
5:      while (num.val < limit.val)
6:        copy.val++;
7: } }
```



Symbolic Execution Graphs

- symbolic over-approximation of all computations
  (abstract interpretation)
- expand nodes until all leaves correspond to program ends
- by suitable generalisation steps (widening),
  one can always get a **finite** symbolic execution graph
- state s_1 is instance of state s_2
  if all concrete states described by s_1 are also described by s_2

Symbolic Execution Graphs

- symbolic over-approximation of all computations
  (abstract interpretation)
- expand nodes until all leaves correspond to program ends
- by suitable generalisation steps (widening),
  one can always get a **finite** symbolic execution graph
- state s_1 is instance of state s_2
  if all concrete states described by s_1 are also described by s_2

Using Symbolic Execution Graphs for Termination Proofs

- every concrete Java computation corresponds to a **computation path**
  in the symbolic execution graph
- symbolic execution graph is called **terminating**
  iff it has no infinite computation path

Transformation of Objects to Terms (1/2)

Q

16 | num : o_1, limit : o_2, x : o_3, y : o_4, z : i_1
o_1 : MyInt(?)
o_2 : MyInt(val $= i_2$)
o_3 : null
o_4 : MyList(?)
o_4 !
i_1 : $[7, \infty)$
i_2 : $(-\infty, \infty)$

For every class C with n fields, introduce an n-ary function symbol C

- **term** for o_1: o_1
- **term** for o_2: MyInt(i_2)
- **term** for o_3: null
- **term** for o_4: x (new variable)
- **term** for i_1: i_1 with **side constraint** $i_1 \geq 7$
  (add invariant $i_1 \geq 7$ to constrained rewrite rules from state Q)

Transformation of Objects to Terms (2/2)

```
public class A {
  int a;
}

public class B extends A {
  int b;
}

...
A x = new A();
x.a = 1;

B y = new B();
y.a = 2;
y.b = 3;
```

Dealing with **subclasses**:

Transformation of Objects to Terms (2/2)

```
public class A {
  int a;
}

public class B extends A {
  int b;
}

...
A x = new A();
x.a = 1;

B y = new B();
y.a = 2;
y.b = 3;
```

Dealing with **subclasses**:

- for every class `C` with n fields, introduce $(n+1)$-ary function symbol C
- first argument: part of the object corresponding to subclasses of `C`
- **term** for `x`: $\mathsf{A}(\mathsf{eoc}, 1)$

  $\longrightarrow$ eoc for end of class
- **term** for `y`: $\mathsf{A}(\mathsf{B}(\mathsf{eoc}, 3), 2)$

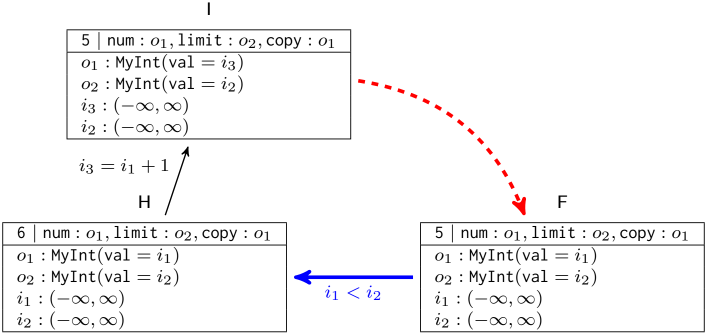
Transformation of Objects to Terms (2/2)

```
public class A {
  int a;
}

public class B extends A {
  int b;
}

...
A x = new A();
x.a = 1;

B y = new B();
y.a = 2;
y.b = 3;
```

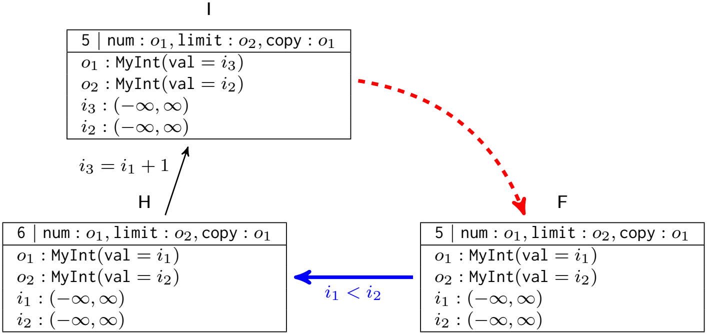
Dealing with **subclasses**:

- for every class `C` with n fields, introduce $(n+1)$-ary function symbol C
- first argument: part of the object corresponding to subclasses of `C`
- **term** for `x`: $\mathsf{jlO}(\mathsf{A}(\mathsf{eoc}, 1))$
  $\longrightarrow$ eoc for end of class
- **term** for `y`: $\mathsf{jlO}(\mathsf{A}(\mathsf{B}(\mathsf{eoc}, 3), 2))$
- every class extends `Object`!
  ($\longrightarrow$ jlO $\equiv$ `java.lang.Object`)

From the Symbolic Execution Graph to Terms and Rules



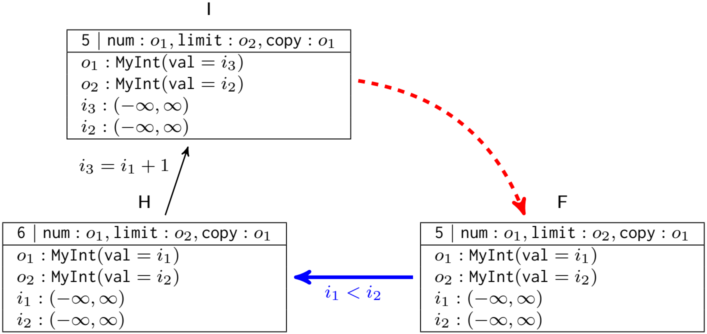
From the Symbolic Execution Graph to Terms and Rules



- State F: $\ell_F($ jIO(MyInt(eoc, i_1)), jIO(MyInt(eoc, i_2)) $)$

  State H: $\ell_H($ jIO(MyInt(eoc, i_1)), jIO(MyInt(eoc, i_2)) $)$

From the Symbolic Execution Graph to Terms and Rules

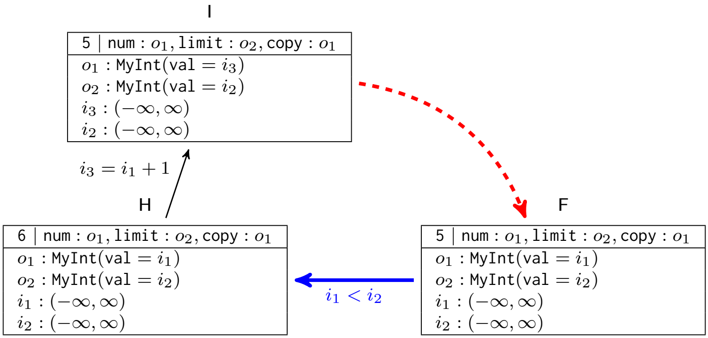


- State F: $\ell_F($ jlO(MyInt(eoc, i_1)), jlO(MyInt(eoc, i_2)) $)$

  $\longrightarrow$

  State H: $\ell_H($ jlO(MyInt(eoc, i_1)), jlO(MyInt(eoc, i_2)) $)$ $[i_1 < i_2]$

From the Symbolic Execution Graph to Terms and Rules



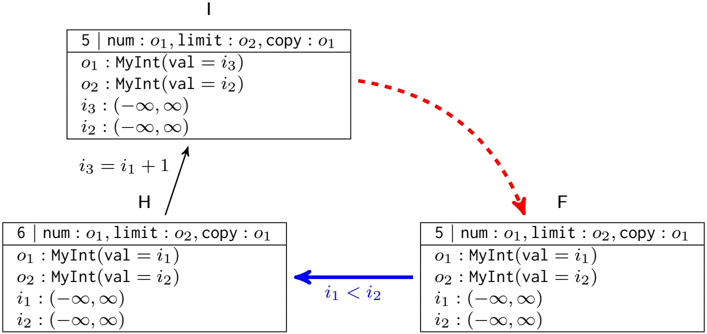
- State F: $\ell_F(\ \mathsf{jlO}(\mathsf{MyInt}(\mathsf{eoc}, i_1)),\ \ \mathsf{jlO}(\mathsf{MyInt}(\mathsf{eoc}, i_2))\ \ )$

  $\longrightarrow$

  State H: $\ell_H(\ \mathsf{jlO}(\mathsf{MyInt}(\mathsf{eoc}, i_1)),\ \ \mathsf{jlO}(\mathsf{MyInt}(\mathsf{eoc}, i_2))\ \ )$ $\quad [i_1 < i_2]$

- State H: $\ell_H(\ \mathsf{jlO}(\mathsf{MyInt}(\mathsf{eoc}, i_1)),\ \ \mathsf{jlO}(\mathsf{MyInt}(\mathsf{eoc}, i_2))\ \ )$

  State I: $\ell_F(\ \mathsf{jlO}(\mathsf{MyInt}(\mathsf{eoc}, i_1 + 1)),\ \ \mathsf{jlO}(\mathsf{MyInt}(\mathsf{eoc}, i_2))\ \ )$



- State F: $\ell_F(\ \mathsf{jlO}(\mathsf{MyInt}(\mathsf{eoc}, i_1)),\ \mathsf{jlO}(\mathsf{MyInt}(\mathsf{eoc}, i_2))\ )$

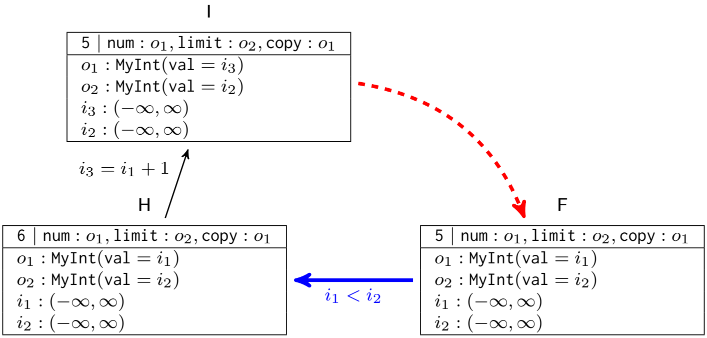
  $\longrightarrow$

  State H: $\ell_H(\ \mathsf{jlO}(\mathsf{MyInt}(\mathsf{eoc}, i_1)),\ \mathsf{jlO}(\mathsf{MyInt}(\mathsf{eoc}, i_2))\ )\quad [i_1 < i_2]$
- State H: $\ell_H(\ \mathsf{jlO}(\mathsf{MyInt}(\mathsf{eoc}, i_1)),\ \mathsf{jlO}(\mathsf{MyInt}(\mathsf{eoc}, i_2))\ )$

  $\longrightarrow$

  State I: $\ell_F(\ \mathsf{jlO}(\mathsf{MyInt}(\mathsf{eoc}, i_1 + 1)),\ \mathsf{jlO}(\mathsf{MyInt}(\mathsf{eoc}, i_2))\ )$

From the Symbolic Execution Graph to Terms and Rules



- State F: $\ell_F(\ \mathrm{jlO}(\mathrm{MyInt}(\mathrm{eoc}, i_1)),\ \mathrm{jlO}(\mathrm{MyInt}(\mathrm{eoc}, i_2))\ )$

  $\to$

  State H: $\ell_H(\ \mathrm{jlO}(\mathrm{MyInt}(\mathrm{eoc}, i_1)),\ \mathrm{jlO}(\mathrm{MyInt}(\mathrm{eoc}, i_2))\ )$ $[i_1 < i_2]$
- State H: $\ell_H(\ \mathrm{jlO}(\mathrm{MyInt}(\mathrm{eoc}, i_1)),\ \mathrm{jlO}(\mathrm{MyInt}(\mathrm{eoc}, i_2))\ )$

  $\to$

  State I: $\ell_F(\ \mathrm{jlO}(\mathrm{MyInt}(\mathrm{eoc}, i_1 + 1)),\ \mathrm{jlO}(\mathrm{MyInt}(\mathrm{eoc}, i_2))\ )$
- Termination easy to show (intuitively: $i_2 - i_1$ decreases against bound 0)

Extensions

- **modular** termination proofs and **recursion**
  [Brockschmidt et al, *RTA '11*]

Extensions

- **modular** termination proofs and **recursion** [Brockschmidt et al, *RTA '11*]
- proving **reachability** and **non-termination** (uses only symbolic execution graph) [Brockschmidt et al, *FoVeOOS '11*]

Extensions

- **modular** termination proofs and **recursion** [Brockschmidt et al, *RTA '11*]
- proving **reachability** and **non-termination** (uses only symbolic execution graph) [Brockschmidt et al, *FoVeOOS '11*]
- proving termination with **cyclic data objects** (preprocessing in symbolic execution graph) [Brockschmidt et al, *CAV '12*]

Extensions

- **modular** termination proofs and **recursion** [Brockschmidt et al, *RTA '11*]
- proving **reachability** and **non-termination** (uses only symbolic execution graph) [Brockschmidt et al, *FoVeOOS '11*]
- proving termination with **cyclic data objects** (preprocessing in symbolic execution graph) [Brockschmidt et al, *CAV '12*]
- proving upper bounds for **time complexity** (abstracts terms to numbers) [Frohn and Giesl, *iFM '17*]

From Java to C

- So far: Java as a memory-safe object-oriented language
  $\longrightarrow$ out-of-bounds memory accesses in Java: well-defined exceptions

From Java to C

- So far: Java as a memory-safe object-oriented language
  $\longrightarrow$ out-of-bounds memory accesses in Java: well-defined exceptions
- Now: C as a systems programming language with pointer arithmetic and **no** guarantees of memory safety
  $\longrightarrow$ out-of-bounds memory accesses in C: **undefined behaviour**

From Java to C

- So far: Java as a memory-safe object-oriented language
  $\longrightarrow$ out-of-bounds memory accesses in Java: well-defined exceptions
- Now: C as a systems programming language with pointer arithmetic and **no** guarantees of memory safety
  $\longrightarrow$ out-of-bounds memory accesses in C: **undefined behaviour**
  - replacing all files on the computer with cat GIFs

From Java to C

- So far: Java as a memory-safe object-oriented language
  $\longrightarrow$ out-of-bounds memory accesses in Java: well-defined exceptions
- Now: C as a systems programming language with pointer arithmetic and **no** guarantees of memory safety
  $\longrightarrow$ out-of-bounds memory accesses in C: **undefined behaviour**
  - replacing all files on the computer with cat GIFs
  - information leaks (Heartbleed)

From Java to C

- So far: Java as a memory-safe object-oriented language
  $\longrightarrow$ out-of-bounds memory accesses in Java: well-defined exceptions
- Now: C as a systems programming language with pointer arithmetic and **no** guarantees of memory safety
  $\longrightarrow$ out-of-bounds memory accesses in C: **undefined behaviour**
  - replacing all files on the computer with cat GIFs
  - information leaks (Heartbleed)
  - **non-termination**

From Java to C

- So far: Java as a memory-safe object-oriented language
  $\longrightarrow$ out-of-bounds memory accesses in Java: well-defined exceptions
- Now: C as a systems programming language with pointer arithmetic and **no** guarantees of memory safety
  $\longrightarrow$ out-of-bounds memory accesses in C: **undefined behaviour**
  - replacing all files on the computer with cat GIFs
  - information leaks (Heartbleed)
  - **non-termination**
  - ...

From Java to C

- So far: Java as a memory-safe object-oriented language
  $\longrightarrow$ out-of-bounds memory accesses in Java: well-defined exceptions
- Now: C as a systems programming language with pointer arithmetic and **no** guarantees of memory safety
  $\longrightarrow$ out-of-bounds memory accesses in C: **undefined behaviour**
  - replacing all files on the computer with cat GIFs
  - information leaks (Heartbleed)
  - **non-termination**
  - ...

$\Rightarrow$ C programs must be memory safe as a precondition for termination!

From Java to C

- So far: Java as a memory-safe object-oriented language
  $\longrightarrow$ out-of-bounds memory accesses in Java: well-defined exceptions
- Now: C as a systems programming language with pointer arithmetic and **no** guarantees of memory safety
  $\longrightarrow$ out-of-bounds memory accesses in C: **undefined behaviour**
  - replacing all files on the computer with cat GIFs
  - information leaks (Heartbleed)
  - **non-termination**
  - ...

$\Rightarrow$ C programs must be memory safe as a precondition for termination!

- Use case: programs on strings represented as char arrays whose last element has 0 as entry ("0-terminated strings")

From Java to C

- So far: Java as a memory-safe object-oriented language
  $\longrightarrow$ out-of-bounds memory accesses in Java: well-defined exceptions
- Now: C as a systems programming language with pointer arithmetic and **no** guarantees of memory safety
  $\longrightarrow$ out-of-bounds memory accesses in C: **undefined behaviour**
  - replacing all files on the computer with cat GIFs
  - information leaks (Heartbleed)
  - **non-termination**
  - ...

$\Rightarrow$ C programs must be memory safe as a precondition for termination!

- Use case: programs on strings represented as char arrays whose last element has 0 as entry ("0-terminated strings")
- Tailor two-stage approach to C [Ströder et al, *JAR '17*]

Motivation

Precondition: `str` points to allocated 0-terminated string

Is this program memory-safe and terminating?

```
int strlen(char* str) {
   char* s = str;
   while(*(++s));
   return s-str;
}
```

Motivation

Precondition: `str` points to allocated 0-terminated string

Is this program memory-safe and terminating?

```
int strlen(char* str) {
   char* s = str;
   while(*(++s));
   return s-str;
}
```

No memory access outside allocated memory!

Motivation

Precondition: `str` points to allocated 0-terminated string

Is this program memory-safe and terminating?

```
int strlen(char* str) {
   char* s = str;
   while(*(++s));
   return s-str;
}
```

No memory access outside allocated memory!

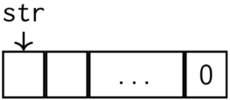
(precondition for termination)

Motivation

Precondition: `str` points to allocated 0-terminated string

Is this program memory-safe and terminating?

```
int strlen(char* str) {
   char* s = str;
   while(*(++s));
   return s-str;
}
```

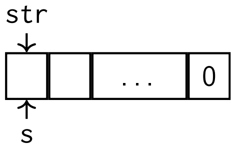


Motivation

Precondition: `str` points to allocated 0-terminated string

Is this program memory-safe and terminating?

```
int strlen(char* str) {
   char* s = str;
   while(*(++s));
   return s-str;
}
```

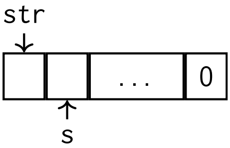


Motivation

Precondition: `str` points to allocated 0-terminated string

Is this program memory-safe and terminating?

```
int strlen(char* str) {
   char* s = str;
   while(*(++s));
   return s-str;
}
```

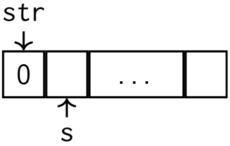


Motivation

Precondition: `str` points to allocated 0-terminated string

Is this program memory-safe and terminating?

```
int strlen(char* str) {
   char* s = str;
   while(*(++s));
   return s-str;
}
```

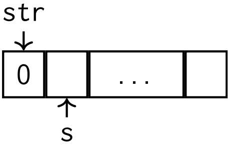


Motivation

Precondition: `str` points to allocated 0-terminated string

Is this program memory-safe and terminating? No!
(violation of memory safety)

```
int strlen(char* str) {
   char* s = str;
   while(*(++s));
   return s-str;
}
```

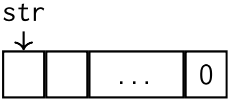


Motivation

Precondition: `str` points to allocated 0-terminated string

Is this program memory-safe and terminating?

```
int strlen(char* str) {
   char* s = str;
   while((*s)++);
   return s-str;
}
```

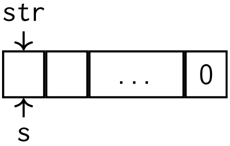


Motivation

Precondition: `str` points to allocated 0-terminated string

Is this program memory-safe and terminating?

```
int strlen(char* str) {
   char* s = str;
   while((*s)++);
   return s-str;
}
```

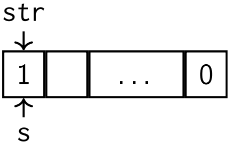


Motivation

Precondition: `str` points to allocated 0-terminated string

Is this program memory-safe and terminating?

```
int strlen(char* str) {
   char* s = str;
   while((*s)++);
   return s-str;
}
```

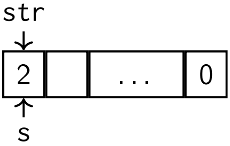


Motivation

Precondition: `str` points to allocated 0-terminated string

Is this program memory-safe and terminating?

```
int strlen(char* str) {
   char* s = str;
   while((*s)++);
   return s-str;
}
```

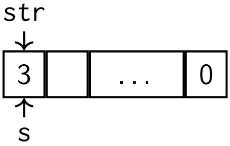


Motivation

Precondition: `str` points to allocated 0-terminated string

Is this program memory-safe and terminating?

```
int strlen(char* str) {
   char* s = str;
   while((*s)++);
   return s-str;
}
```

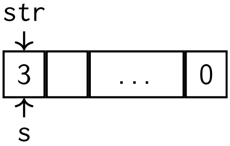


Motivation

Precondition: `str` points to allocated 0-terminated string

Is this program memory-safe and terminating? No!
(non-terminating)

```
int strlen(char* str) {
   char* s = str;
   while((*s)++);
   return s-str;
}
```

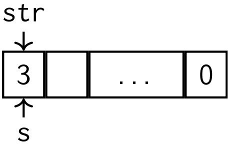


Motivation

Precondition: `str` points to allocated 0-terminated string

Is this program memory-safe and terminating? No!
(non-terminating – for unbounded integers)

```
int strlen(char* str) {
   char* s = str;
   while((*s)++);
   return s-str;
}
```

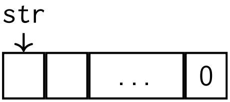


Motivation

Precondition: `str` points to allocated 0-terminated string

Is this program memory-safe and terminating?

```
int strlen(char* str) {
   char* s = str;
   while(*(s++));
   return s-str;
}
```

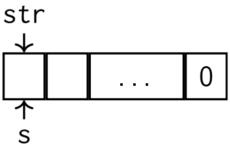


Motivation

Precondition: `str` points to allocated 0-terminated string

Is this program memory-safe and terminating?

```
int strlen(char* str) {
   char* s = str;
   while(*(s++));
   return s-str;
}
```

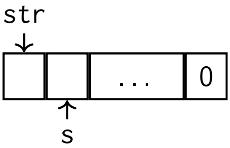


Motivation

Precondition: `str` points to allocated 0-terminated string

Is this program memory-safe and terminating?

```
int strlen(char* str) {
   char* s = str;
   while(*(s++));
   return s-str;
}
```

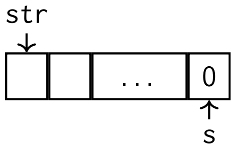


Motivation

Precondition: `str` points to allocated 0-terminated string

Is this program memory-safe and terminating?

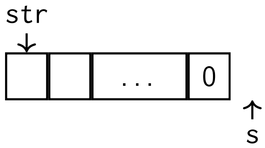
```
int strlen(char* str) {
   char* s = str;
   while(*(s++));
   return s-str;
}
```



Precondition: `str` points to allocated 0-terminated string

Is this program memory-safe and terminating?

```
int strlen(char* str) {
   char* s = str;
   while(*(s++));
   return s-str;
}
```

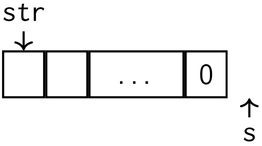


Motivation

Precondition: `str` points to allocated 0-terminated string

Is this program memory-safe and terminating? Yes! But...

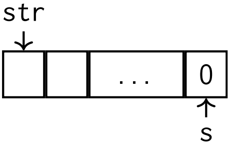
```
int strlen(char* str) {
   char* s = str;
   while(*(s++));
   return s-str;
}
```



Precondition: `str` points to allocated 0-terminated string

Is this program memory-safe and terminating? Yes!

```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```

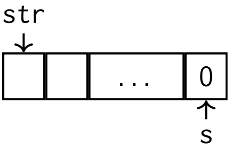


Motivation

Precondition: `str` points to allocated 0-terminated string

Is this program memory-safe and terminating? Yes!

```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```



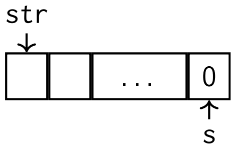
Bugs w.r.t. pointers are hard to recognise!

Motivation

Precondition: `str` points to allocated 0-terminated string

Is this program memory-safe and terminating? Yes!
How to prove this automatically?

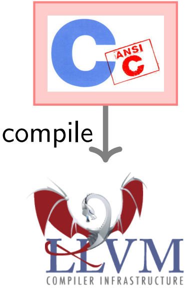
```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```



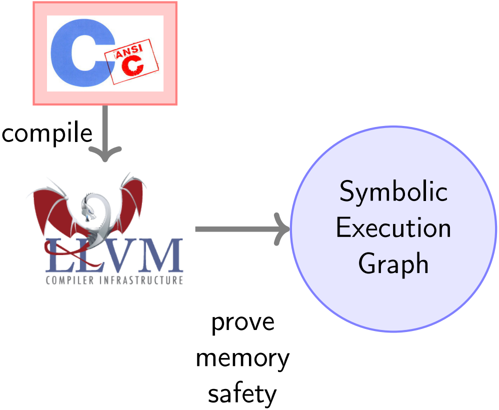
Bugs w.r.t. pointers are hard to recognise!


C
ANSI
C

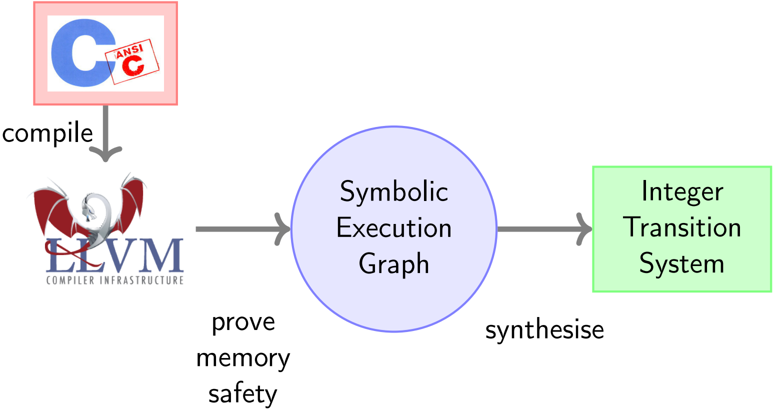
Overview



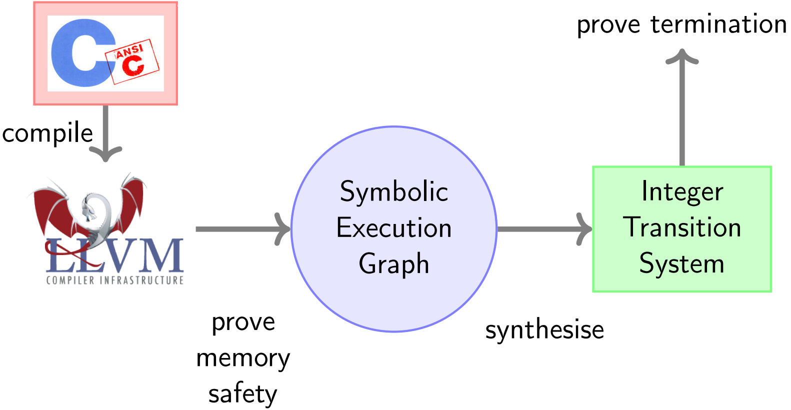
Overview


ANSI C
compile
LLVM
COMPILER INFRASTRUCTURE
prove memory safety
Symbolic Execution Graph

Overview

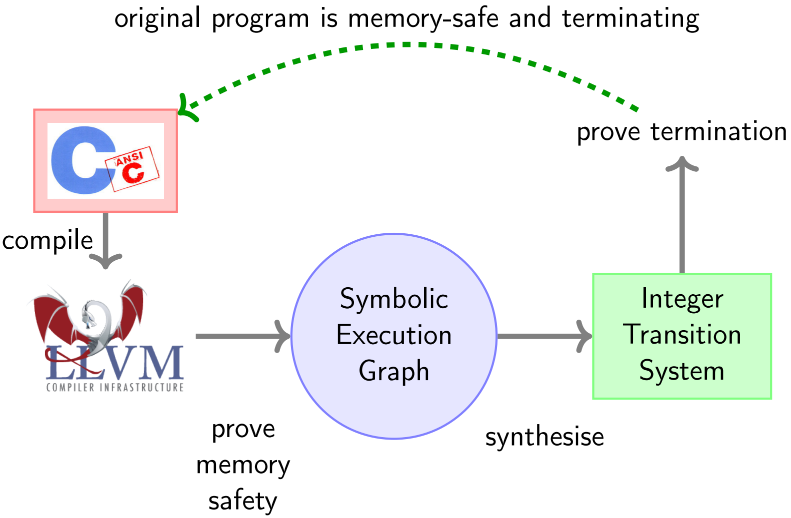

compile
Symbolic Execution Graph
Integer Transition System
prove memory safety
synthesise

Overview

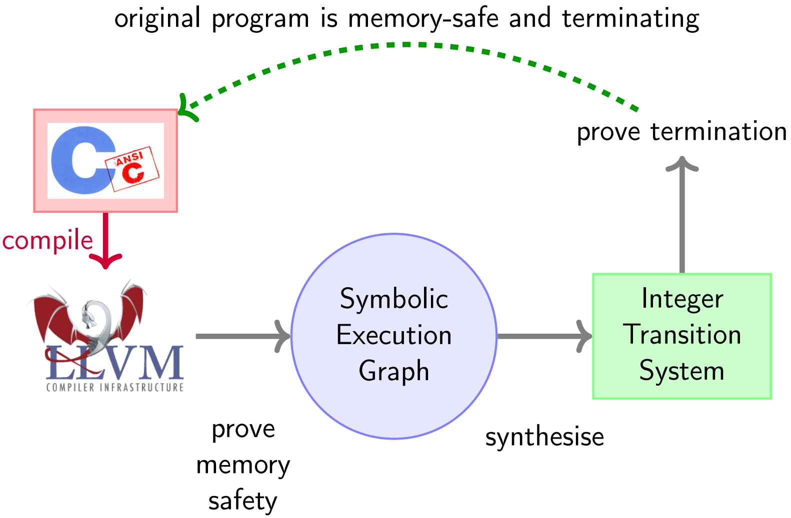


compile
COMPILER INFRASTRUCTURE
prove memory safety
Symbolic Execution Graph
synthesise
Integer Transition System
prove termination

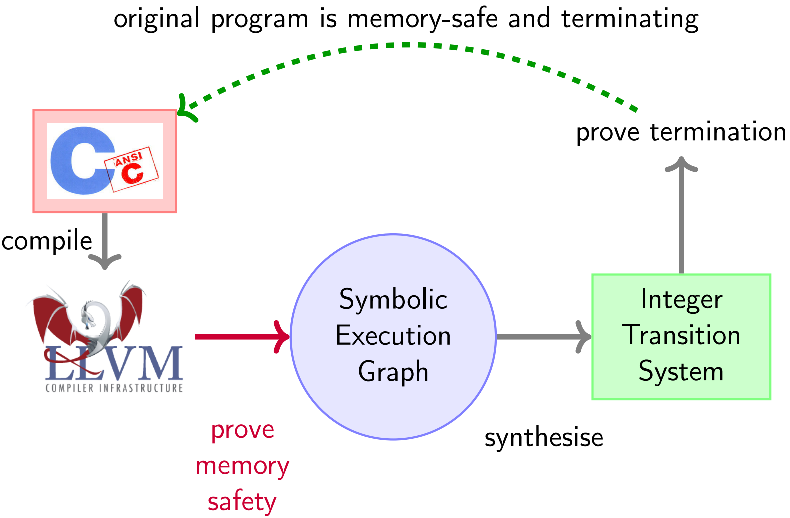
Overview


original program is memory-safe and terminating
prove termination
ANSI C
compile
LLVM
COMPILER INFRASTRUCTURE
Symbolic Execution Graph
Integer Transition System
prove memory safety
synthesise

Overview


original program is memory-safe and terminating
prove termination
ANSI
C
compile
LLVM
COMPILER INFRASTRUCTURE
Symbolic Execution Graph
Integer Transition System
prove memory safety
synthesise

Overview


original program is memory-safe and terminating
prove termination
compile
ANSI C
LLVM
COMPILER INFRASTRUCTURE
Symbolic Execution Graph
Integer Transition System
prove memory safety
synthesise

From Program to Symbolic Execution Graph (1/2)

- over-approximate operations

From Program to Symbolic Execution Graph (1/2)

- over-approximate operations
- inference rules for each instruction

From Program to Symbolic Execution Graph (1/2)

- over-approximate operations
- inference rules for each instruction
- refinement

From Program to Symbolic Execution Graph (1/2)

- over-approximate operations
- inference rules for each instruction
- refinement
- generalisation

From Program to Symbolic Execution Graph (1/2)

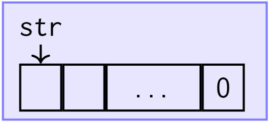
- over-approximate operations
- inference rules for each instruction
- refinement
- generalisation
- reduce reasoning to SMT

From Program to Symbolic Execution Graph (2/2)

```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```

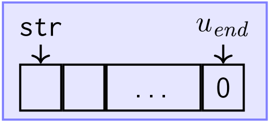
From Program to Symbolic Execution Graph (2/2)

```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```



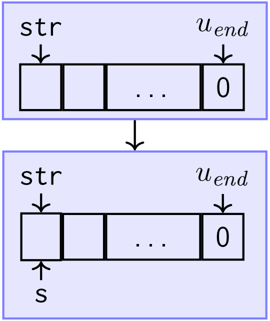
From Program to Symbolic Execution Graph (2/2)

```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```



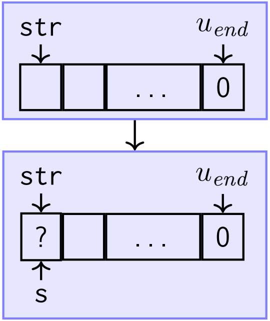
From Program to Symbolic Execution Graph (2/2)

```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```



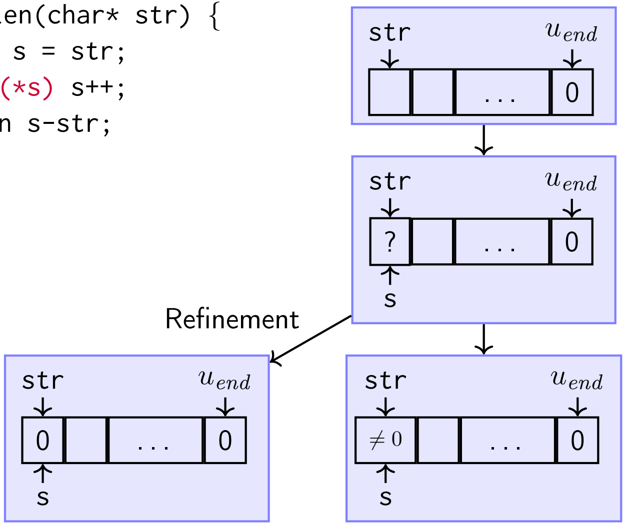
From Program to Symbolic Execution Graph (2/2)

```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```



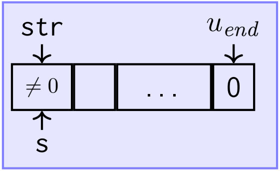
From Program to Symbolic Execution Graph (2/2)

```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```



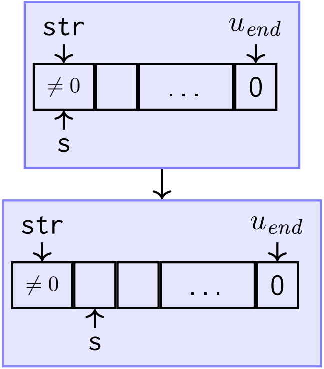
From Program to Symbolic Execution Graph (2/2)

```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```



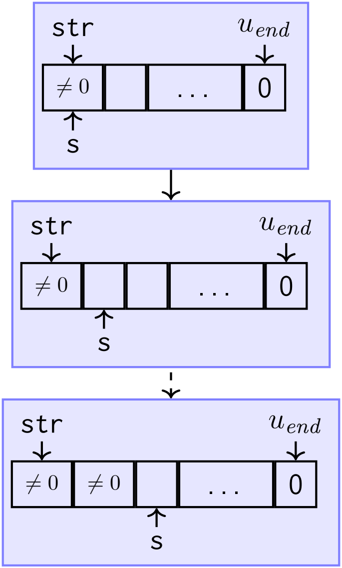
From Program to Symbolic Execution Graph (2/2)

```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```



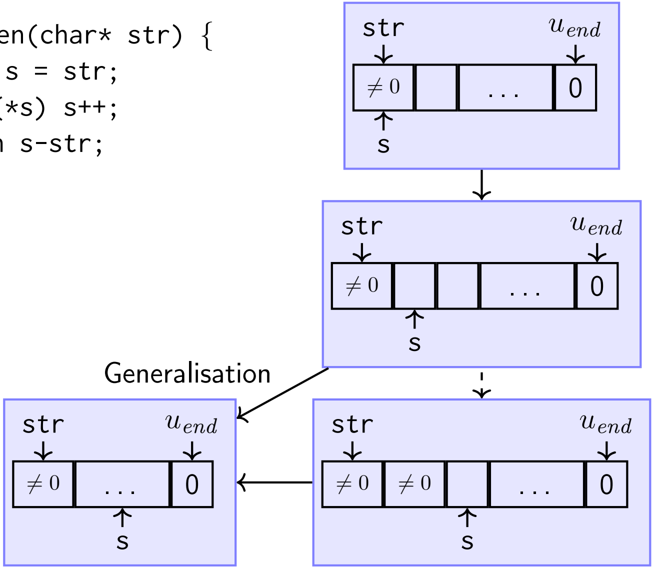
From Program to Symbolic Execution Graph (2/2)

```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```



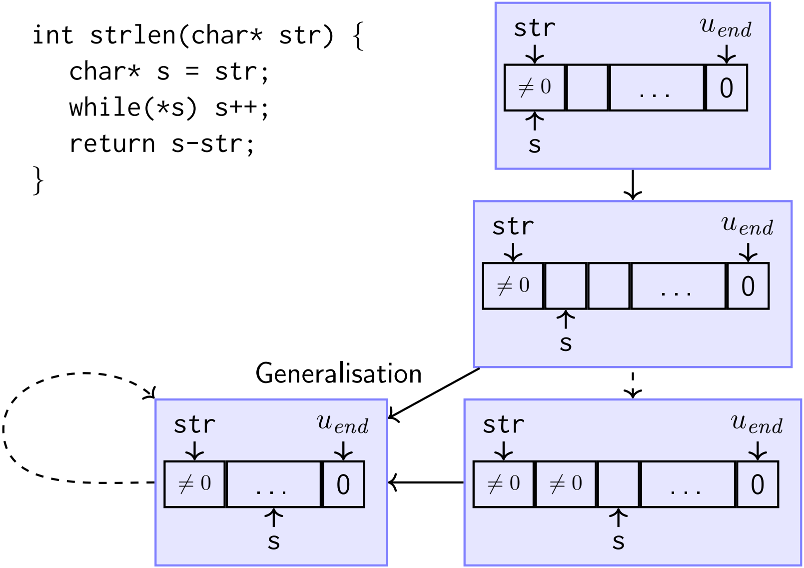
From Program to Symbolic Execution Graph (2/2)

```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```

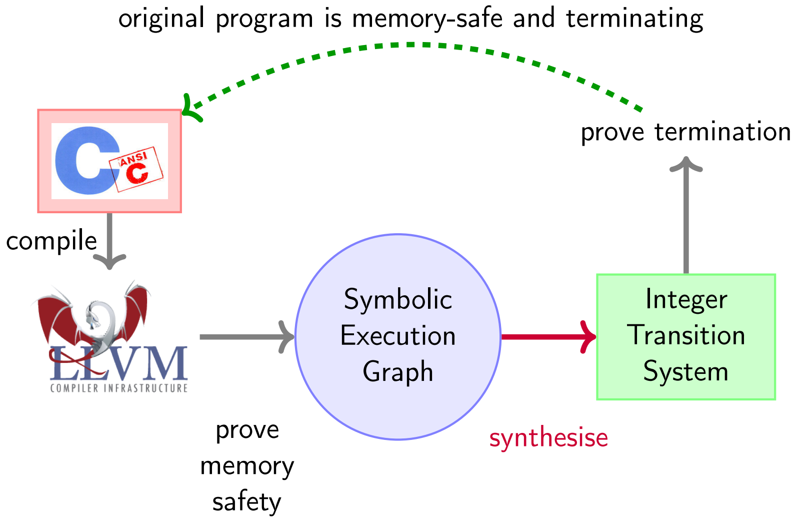


From Program to Symbolic Execution Graph (2/2)

```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```



Overview


original program is memory-safe and terminating
prove termination
compile
Symbolic
Execution
Graph
Integer
Transition
System
prove
memory
safety
synthesise

From Symb. Exec. Graph to Integer Transition Systems (1/3)

- Non-termination $\rightsquigarrow$ infinite run through graph

From Symb. Exec. Graph to Integer Transition Systems (1/3)

- Non-termination $\rightsquigarrow$ infinite run through graph
- Express graph traversal (SCCs)

From Symb. Exec. Graph to Integer Transition Systems (1/3)

- Non-termination $\rightsquigarrow$ infinite run through graph
- Express graph traversal (SCCs)

  by Integer Transition System (ITS)

From Symb. Exec. Graph to Integer Transition Systems (1/3)

- Non-termination $\rightsquigarrow$ infinite run through graph
- Express graph traversal (SCCs)

  by Integer Transition System (ITS)
- ITS terminating $\implies$ C program terminating

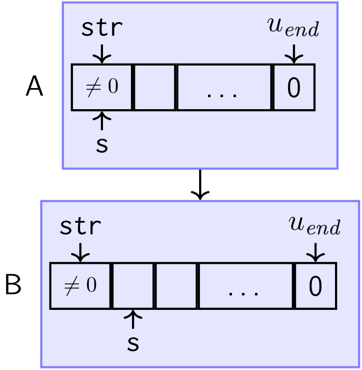
From Symb. Exec. Graph to Integer Transition Systems (2/3)

- Function symbols: abstract states

From Symb. Exec. Graph to Integer Transition Systems (2/3)

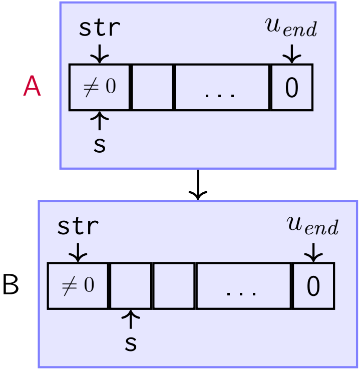
- Function symbols: abstract states
- Arguments: variables occurring in states

- Function symbols: abstract states
- Arguments: variables occurring in states



From Symb. Exec. Graph to Integer Transition Systems (2/3)

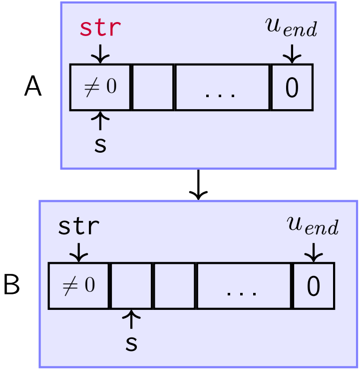
- Function symbols: abstract states
- Arguments: variables occurring in states



$\ell_{A}(\qquad\qquad)$

From Symb. Exec. Graph to Integer Transition Systems (2/3)

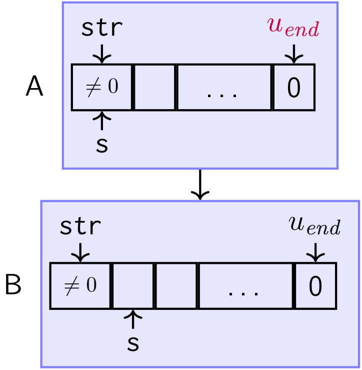
- Function symbols: abstract states
- Arguments: variables occurring in states



$\ell_A(\mathtt{str} \qquad)$

From Symb. Exec. Graph to Integer Transition Systems (2/3)

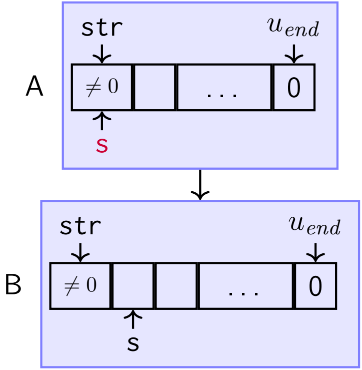
- Function symbols: abstract states
- Arguments: variables occurring in states



$\ell_A(\mathtt{str}, u_{end} \quad)$

From Symb. Exec. Graph to Integer Transition Systems (2/3)

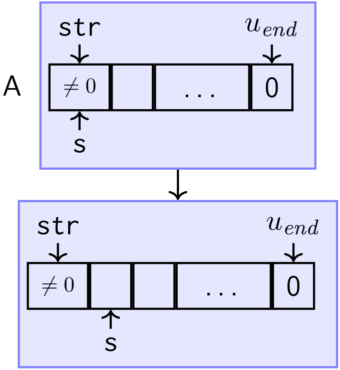
- Function symbols: abstract states
- Arguments: variables occurring in states



$\ell_A(\texttt{str}, u_{end}, \texttt{s})$

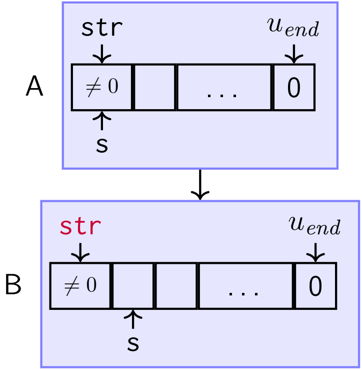
From Symb. Exec. Graph to Integer Transition Systems (2/3)

- Function symbols: abstract states
- Arguments: variables occurring in states



$$\ell_A(\texttt{str}, u_{end}, \texttt{s}) \quad \rightarrow \quad \ell_B(\qquad\qquad\qquad)$$

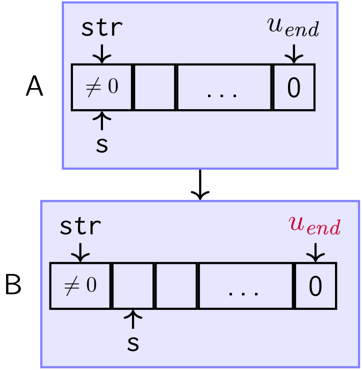
- Function symbols: abstract states
- Arguments: variables occurring in states



$$\ell_A(\texttt{str}, u_{end}, \texttt{s}) \quad \rightarrow \quad \ell_B(\texttt{str} \qquad\qquad)$$

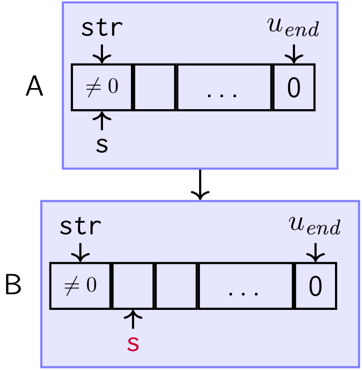
From Symb. Exec. Graph to Integer Transition Systems (2/3)

- Function symbols: abstract states
- Arguments: variables occurring in states



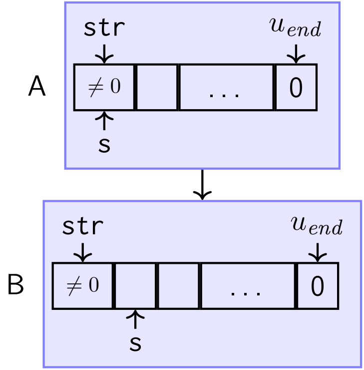
$$\ell_A(\mathtt{str}, u_{end}, \mathtt{s}) \quad \rightarrow \quad \ell_B(\mathtt{str}, u_{end} \qquad)$$

- Function symbols: abstract states
- Arguments: variables occurring in states



$$\ell_A(\mathtt{str}, u_{end}, \mathtt{s}) \quad \rightarrow \quad \ell_B(\mathtt{str}, u_{end}, \mathtt{s} + 1)$$

- Function symbols: abstract states
- Arguments: variables occurring in states



$$\ell_A(\mathtt{str}, u_{end}, \mathtt{s}) \xrightarrow{\mathtt{s} < u_{end}} \ell_B(\mathtt{str}, u_{end}, \mathtt{s} + 1)$$

Resulting ITS (after automated simplification):

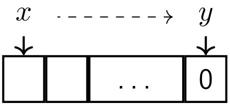
Resulting ITS (after automated simplification):

$$\ell(x, y) \xrightarrow{x<y} \ell(x+1, y)$$

From Symb. Exec. Graph to Integer Transition Systems (3/3)

Resulting ITS (after automated simplification):

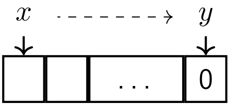
$$\ell(x,y) \xrightarrow{x<y} \ell(x+1,y)$$



From Symb. Exec. Graph to Integer Transition Systems (3/3)

Resulting ITS (after automated simplification):

$$\ell(x, y) \xrightarrow{x<y} \ell(x+1, y)$$

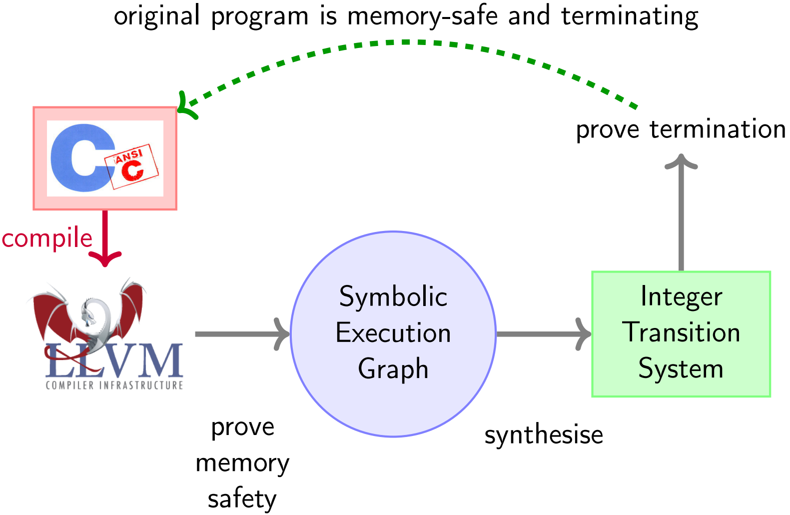


Automatic termination proof by any termination prover

Implementation: Analysis on LLVM Level

- So far: assume that LLVM bitcode is essentially “the same” as C code
- But: LLVM bitcode is much closer to assembly than C
- Let’s look at the details of the **actual** analysis

Overview


original program is memory-safe and terminating
prove termination
compile
ANSI C
LLVM
COMPILER INFRASTRUCTURE
Symbolic Execution Graph
Integer Transition System
prove memory safety
synthesise

The Low-Level Virtual Machine Framework

- LLVM used for compiler optimisation and verification

The Low-Level Virtual Machine Framework

- LLVM used for compiler optimisation and verification
- Close to assembly language

The Low-Level Virtual Machine Framework

- LLVM used for compiler optimisation and verification
- Close to assembly language
- Still structured: functions, data structures, type safety

The Low-Level Virtual Machine Framework

- LLVM used for compiler optimisation and verification
- Close to assembly language
- Still structured: functions, data structures, type safety
- Single Static Assignment (SSA)

The Low-Level Virtual Machine Framework

- LLVM used for compiler optimisation and verification
- Close to assembly language
- Still structured: functions, data structures, type safety
- Single Static Assignment (SSA)

- Caveat: user-defined data structures (structs) in LLVM are still work in progress for AProVE

From C to LLVM

Example C Program

```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```

From C to LLVM

LLVM Code (simplified)

```
define i32 strlen(i8* str) {

}
```

Example C Program

```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```

LLVM Code (simplified)

```
define i32 strlen(i8* str) {
 entry:
   0: c0 = load i8* str
```

Example C Program

```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```

```
 }
```

From C to LLVM

LLVM Code (simplified)

```
define i32 strlen(i8* str) {
 entry:
   0: c0 = load i8* str
   1: c0zero = icmp eq i8 c0, 0
```

Example C Program

```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```

```
 }
```

From C to LLVM

Example C Program

```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```

LLVM Code (simplified)

```
define i32 strlen(i8* str) {
 entry:
   0: c0 = load i8* str
   1: c0zero = icmp eq i8 c0, 0
   2: br i1 c0zero, label done, label loop
 loop:



 done:



}
```

From C to LLVM

Example C Program

```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```

LLVM Code (simplified)

```
define i32 strlen(i8* str) {
 entry:
   0: c0 = load i8* str
   1: c0zero = icmp eq i8 c0, 0
   2: br i1 c0zero, label done, label loop
 loop:
   0: olds = phi i8* [str,entry],[s,loop]




 done:




 }
```

From C to LLVM

Example C Program

```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```

LLVM Code (simplified)

```
define i32 strlen(i8* str) {
 entry:
   0: c0 = load i8* str
   1: c0zero = icmp eq i8 c0, 0
   2: br i1 c0zero, label done, label loop
 loop:
   0: olds = phi i8* [str,entry],[s,loop]
   1: s = getelementptr i8* olds, i32 1



 done:



}
```

Example C Program

```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```

LLVM Code (simplified)

```
define i32 strlen(i8* str) {
 entry:
   0: c0 = load i8* str
   1: c0zero = icmp eq i8 c0, 0
   2: br i1 c0zero, label done, label loop
 loop:
   0: olds = phi i8* [str,entry],[s,loop]
   1: s = getelementptr i8* olds, i32 1
   2: c = load i8* s



 done:




 }
```

From C to LLVM

Example C Program

```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```

LLVM Code (simplified)

```
define i32 strlen(i8* str) {
 entry:
   0: c0 = load i8* str
   1: c0zero = icmp eq i8 c0, 0
   2: br i1 c0zero, label done, label loop
 loop:
   0: olds = phi i8* [str,entry],[s,loop]
   1: s = getelementptr i8* olds, i32 1
   2: c = load i8* s
   3: czero = icmp eq i8 c, 0

 done:

}
```

From C to LLVM

Example C Program

```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```

LLVM Code (simplified)

```
define i32 strlen(i8* str) {
 entry:
   0: c0 = load i8* str
   1: c0zero = icmp eq i8 c0, 0
   2: br i1 c0zero, label done, label loop
 loop:
   0: olds = phi i8* [str,entry],[s,loop]
   1: s = getelementptr i8* olds, i32 1
   2: c = load i8* s
   3: czero = icmp eq i8 c, 0
   4: br i1 czero, label done, label loop
 done:




 }
```

From C to LLVM

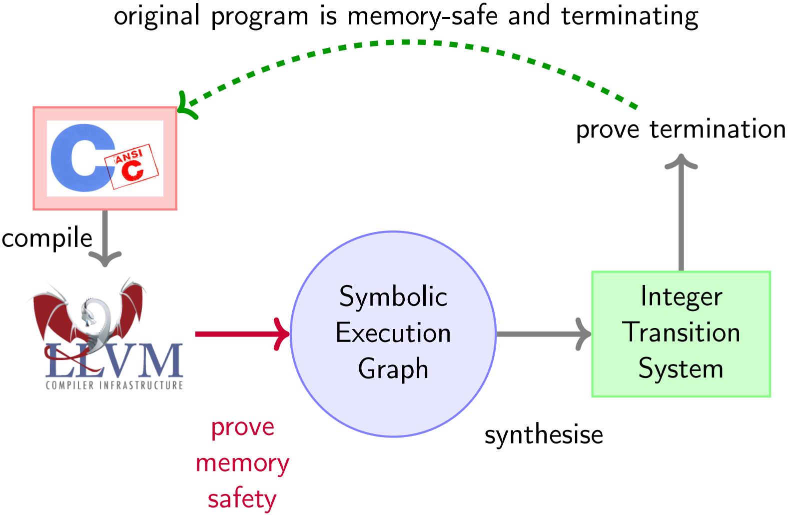
Example C Program

```
int strlen(char* str) {
   char* s = str;
   while(*s) s++;
   return s-str;
}
```

LLVM Code (simplified)

```
define i32 strlen(i8* str) {
 entry:
   0: c0 = load i8* str
   1: c0zero = icmp eq i8 c0, 0
   2: br i1 c0zero, label done, label loop
 loop:
   0: olds = phi i8* [str,entry],[s,loop]
   1: s = getelementptr i8* olds, i32 1
   2: c = load i8* s
   3: czero = icmp eq i8 c, 0
   4: br i1 czero, label done, label loop
 done:
   0: sfin = phi i8* [str,entry],[s,loop]
   1: sfinint = ptrtoint i8* sfin to i32
   2: strint = ptrtoint i8* str to i32
   3: size = sub i32 sfinint, strint
   4: ret i32 size
}
```

Overview


original program is memory-safe and terminating
prove termination
compile
ANSI C
LLVM
COMPILER INFRASTRUCTURE
Symbolic Execution Graph
Integer Transition System
prove memory safety
synthesise

From LLVM to Symbolic Execution Graph

Abstract domain:

From LLVM to Symbolic Execution Graph

Abstract domain:

- represent system configurations as states

From LLVM to Symbolic Execution Graph

Abstract domain:

- represent system configurations as states
- represent operations as edges

From LLVM to Symbolic Execution Graph

Abstract domain:

- represent system configurations as states
- represent operations as edges
- abstract states stand for sets of configurations

From LLVM to Symbolic Execution Graph

Abstract domain:

- represent system configurations as states
- represent operations as edges
- abstract states stand for sets of configurations

Initial State:

From LLVM to Symbolic Execution Graph

Abstract domain:

- represent system configurations as states
- represent operations as edges
- abstract states stand for sets of configurations
  - program position pos: previous block, current block, line number

Initial State:

From LLVM to Symbolic Execution Graph

Abstract domain:

- represent system configurations as states
- represent operations as edges
- abstract states stand for sets of configurations
  - program position pos: previous block, current block, line number

Initial State:

$pos = (\varepsilon, \texttt{entry}, 0)$

From LLVM to Symbolic Execution Graph

Abstract domain:

- represent system configurations as states
- represent operations as edges
- abstract states stand for sets of configurations
  - program position pos: previous block, current block, line number
  - allocation list AL

Initial State:

$pos = (\varepsilon, \texttt{entry}, 0)$

From LLVM to Symbolic Execution Graph

Abstract domain:

- represent system configurations as states
- represent operations as edges
- abstract states stand for sets of configurations
  - program position pos: previous block, current block, line number
  - allocation list AL

Initial State:

$pos = (\varepsilon, \texttt{entry}, 0)$
$AL = \{alloc(\texttt{str}, u_{end})\}$

From LLVM to Symbolic Execution Graph

Abstract domain:

- represent system configurations as states
- represent operations as edges
- abstract states stand for sets of configurations
  - program position pos: previous block, current block, line number
  - allocation list AL
  - points to map PT

Initial State:

$pos = (\varepsilon, \texttt{entry}, 0)$
$AL = \{alloc(\texttt{str}, u_{end})\}$

From LLVM to Symbolic Execution Graph

Abstract domain:

- represent system configurations as states
- represent operations as edges
- abstract states stand for sets of configurations
  - program position pos: previous block, current block, line number
  - allocation list AL
  - points to map PT

Initial State:

$pos = (\varepsilon, \texttt{entry}, 0)$
$AL = \{alloc(\texttt{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\texttt{i8}} 0\}$

From LLVM to Symbolic Execution Graph

Abstract domain:

- represent system configurations as states
- represent operations as edges
- abstract states stand for sets of configurations
  - program position pos: previous block, current block, line number
  - allocation list AL
  - points to map PT
  - knowledge base KB

Initial State:

$pos = (\varepsilon, \texttt{entry}, 0)$
$AL = \{alloc(\texttt{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\texttt{i8}} 0\}$

From LLVM to Symbolic Execution Graph

Abstract domain:

- represent system configurations as states
- represent operations as edges
- abstract states stand for sets of configurations
  - program position pos: previous block, current block, line number
  - allocation list AL
  - points to map PT
  - knowledge base KB

Initial State:

$pos = (\varepsilon, \texttt{entry}, 0)$
$AL = \{alloc(\texttt{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\texttt{i8}} 0\}$
$KB = \varnothing$

From LLVM to Symbolic Execution Graph

Abstract domain:

- represent system configurations as states
- represent operations as edges
- abstract states stand for sets of configurations
  - program position pos: previous block, current block, line number
  - allocation list AL
  - points to map PT
  - knowledge base KB

Initial State:

$pos = (\varepsilon, \texttt{entry}, 0)$
$AL = \{alloc(\texttt{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\texttt{i8}} 0\}$
$KB = \varnothing$

- formal semantics for states:
  Separation Logic [O'Hearn, Reynolds, Yang, *CSL '01*]

From LLVM to Symbolic Execution Graph

- over-approximate program states and operations

From LLVM to Symbolic Execution Graph

- over-approximate program states and operations
- inference rules for each instruction

From LLVM to Symbolic Execution Graph

- over-approximate program states and operations
- inference rules for each instruction
- refinement

From LLVM to Symbolic Execution Graph

- over-approximate program states and operations
- inference rules for each instruction
- refinement
- generalisation

From LLVM to Symbolic Execution Graph

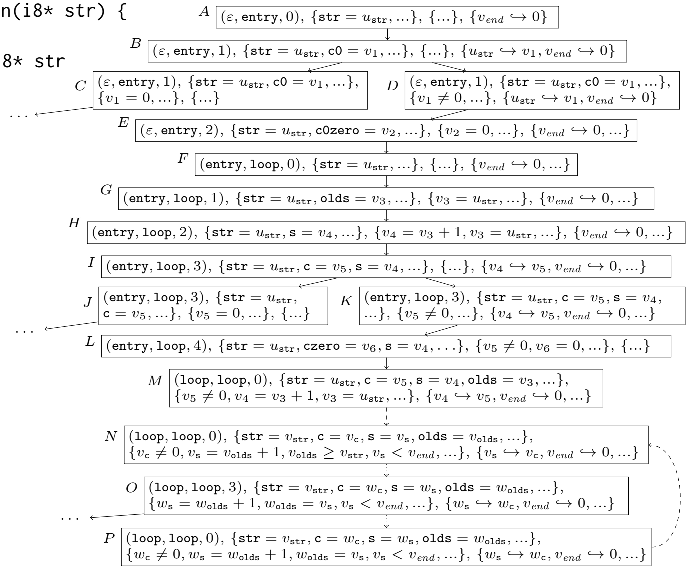
- over-approximate program states and operations
- inference rules for each instruction
- refinement
- generalisation
- automation via SMT solving (SAT Modulo Theories)

From LLVM to Symbolic Execution Graph

```
define i32 strlen(i8* str) {
entry:
  0: c0 = load i8* str
  ...
```

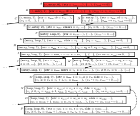
From LLVM to Symbolic Execution Graph

```
define i32 strlen(i8* str) {
entry:
  0: c0 = load i8* str
  ...
```



From LLVM to Symbolic Execution Graph

```
define i32 strlen(i8* str) {
entry:
  0: c0 = load i8* str
  ...
```

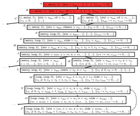


Initial state:

$$pos = (\varepsilon, \mathsf{entry}, 0)$$
$$AL = \{alloc(\mathsf{str}, u_{end})\}$$
$$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0\}$$
$$KB = \varnothing$$

From LLVM to Symbolic Execution Graph

```
define i32 strlen(i8* str) {
entry:
  0: c0 = load i8* str
  ...
```



Initial state:

$pos = (\varepsilon, \texttt{entry}, 0)$
$AL = \{alloc(\texttt{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\texttt{i8}} 0\}$
$KB = \varnothing$

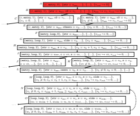
↓

$pos = (\varepsilon, \texttt{entry}, 1)$
$AL = \{alloc(\texttt{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\texttt{i8}} 0,$
$\texttt{str} \hookrightarrow_{\texttt{i8}} \texttt{c0}\}$
$KB = \varnothing$

Evaluation

From LLVM to Symbolic Execution Graph

```
define i32 strlen(i8* str) {
entry:
  0: c0 = load i8* str
  ...
```



Initial state:

$$pos = (\varepsilon, \mathsf{entry}, 0)$$
$$AL = \{alloc(\mathsf{str}, u_{end})\}$$
$$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0\}$$
$$KB = \varnothing$$

↓

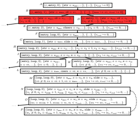
$$pos = (\varepsilon, \mathsf{entry}, 1)$$
$$AL = \{alloc(\mathsf{str}, u_{end})\}$$
$$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \; \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}\}$$
$$KB = \varnothing$$

Evaluation

Memory access: check allocation!

From LLVM to Symbolic Execution Graph

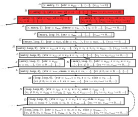
```
...
entry:
  0: c0 = load i8* str
  1: c0zero = icmp eq i8 c0, 0
  ...
```



$$pos = (\varepsilon, \texttt{entry}, 1)$$
$$AL = \{alloc(\texttt{str}, u_{end})\}$$
$$PT = \{u_{end} \hookrightarrow_{\texttt{i8}} 0, \;\; \texttt{str} \hookrightarrow_{\texttt{i8}} \texttt{c0}\}$$
$$KB = \varnothing$$

From LLVM to Symbolic Execution Graph

```
...
entry:
  0: c0 = load i8* str
  1: c0zero = icmp eq i8 c0, 0
  ...
```



$$\begin{aligned} pos &= (\varepsilon, \mathsf{entry}, 1) \\ AL &= \{alloc(\mathsf{str}, u_{end})\} \\ PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \\ &\qquad \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}\} \\ KB &= \varnothing \end{aligned}$$

$\mathtt{c0} = 0$ | $\mathtt{c0} \neq 0$

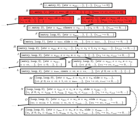
$$\begin{aligned} pos &= (\varepsilon, \mathsf{entry}, 1) \\ AL &= \{alloc(\mathsf{str}, u_{end})\} \\ PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \\ &\qquad \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}\} \\ KB &= \{ \qquad \} \end{aligned}$$

$$\begin{aligned} pos &= (\varepsilon, \mathsf{entry}, 1) \\ AL &= \{alloc(\mathsf{str}, u_{end})\} \\ PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \\ &\qquad \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}\} \\ KB &= \{ \qquad \} \end{aligned}$$

Refinement

From LLVM to Symbolic Execution Graph

```
...
entry:
  0: c0 = load i8* str
  1: c0zero = icmp eq i8 c0, 0
  ...
```



$$pos = (\varepsilon, \texttt{entry}, 1)$$
$$AL = \{alloc(\texttt{str}, u_{end})\}$$
$$PT = \{u_{end} \hookrightarrow_{\texttt{i8}} 0, \; \texttt{str} \hookrightarrow_{\texttt{i8}} \texttt{c0}\}$$
$$KB = \varnothing$$

$\texttt{c0} = 0$ | $\texttt{c0} \neq 0$

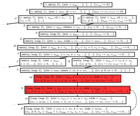
$$pos = (\varepsilon, \texttt{entry}, 1)$$
$$AL = \{alloc(\texttt{str}, u_{end})\}$$
$$PT = \{u_{end} \hookrightarrow_{\texttt{i8}} 0, \; \texttt{str} \hookrightarrow_{\texttt{i8}} \texttt{c0}\}$$
$$KB = \{\texttt{c0} = 0\}$$

$$pos = (\varepsilon, \texttt{entry}, 1)$$
$$AL = \{alloc(\texttt{str}, u_{end})\}$$
$$PT = \{u_{end} \hookrightarrow_{\texttt{i8}} 0, \; \texttt{str} \hookrightarrow_{\texttt{i8}} \texttt{c0}\}$$
$$KB = \{\texttt{c0} \neq 0\}$$

Refinement

From LLVM to Symbolic Execution Graph

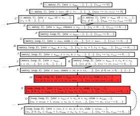
```
...
loop:
  0: olds = phi i8* [str,entry],[s,loop]
  1: s = getelementptr i8* olds, i32 1
  ...
```



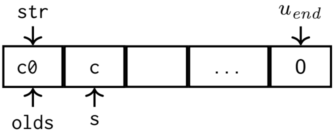
$$pos = (\mathsf{loop}, \mathsf{loop}, 0)$$
$$AL = \{alloc(\mathsf{str}, u_{end})\}$$
$$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}\}$$
$$KB = \{\mathsf{c} \neq 0, \mathsf{s} = \mathsf{olds} + 1, \mathsf{c0} \neq 0, \mathsf{olds} = \mathsf{str}\}$$

From LLVM to Symbolic Execution Graph

```
...
loop:
  0: olds = phi i8* [str,entry],[s,loop]
  1: s = getelementptr i8* olds, i32 1
  ...
```

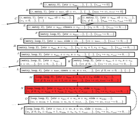


$$\begin{aligned} pos &= (\mathsf{loop}, \mathsf{loop}, 0) \\ AL &= \{alloc(\mathsf{str}, u_{end})\} \\ PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \\ &\quad\ \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}\} \\ KB &= \{\mathsf{c} \neq 0, \mathsf{s} = \mathsf{olds} + 1, \\ &\quad\ \mathtt{c0} \neq 0, \mathsf{olds} = \mathsf{str}\} \end{aligned}$$



From LLVM to Symbolic Execution Graph

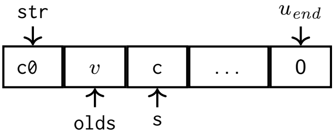
```
...
loop:
  0: olds = phi i8* [str,entry],[s,loop]
  1: s = getelementptr i8* olds, i32 1
  ...
```



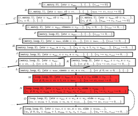
$$
\begin{aligned}
pos &= (\mathtt{loop}, \mathtt{loop}, 0)\\
AL &= \{alloc(\mathtt{str}, u_{end})\}\\
PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,\\
&\qquad \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathtt{s} \hookrightarrow_{\mathtt{i8}} \mathtt{c}\}\\
KB &= \{\mathtt{c} \neq 0, \mathtt{s} = \mathtt{olds} + 1,\\
&\qquad \mathtt{c0} \neq 0, \mathtt{olds} = \mathtt{str}\}
\end{aligned}
$$

...

$$
\begin{aligned}
pos &= (\mathtt{loop}, \mathtt{loop}, 0)\\
AL &= \{alloc(\mathtt{str}, u_{end})\}\\
PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,\\
&\qquad \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathtt{s} \hookrightarrow_{\mathtt{i8}} \mathtt{c},\\
&\qquad \mathtt{olds} \hookrightarrow_{\mathtt{i8}} v\}\\
KB &= \{\mathtt{c} \neq 0, v \neq 0,\\
&\qquad \mathtt{s} = \mathtt{olds} + 1, \mathtt{c0} \neq 0,\\
&\qquad \mathtt{olds} = \mathtt{str} + 1\}
\end{aligned}
$$



```
...
loop:
  0: olds = phi i8* [str,entry],[s,loop]
  1: s = getelementptr i8* olds, i32 1
  ...
```



$$
\begin{aligned}
pos &= (\mathsf{loop}, \mathsf{loop}, 0)\\
AL &= \{alloc(\mathsf{str}, u_{end})\}\\
PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,\\
&\qquad \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}\}\\
KB &= \{\mathsf{c} \neq 0, \mathsf{s} = \mathsf{olds} + 1,\\
&\qquad \mathsf{c0} \neq 0, \mathsf{olds} = \mathsf{str}\}
\end{aligned}
$$

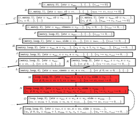
...

Generalisation

$$
\begin{aligned}
pos &= (\mathsf{loop}, \mathsf{loop}, 0)\\
AL &= \{alloc(\mathsf{str}, u_{end})\}\\
PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,\\
&\qquad \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c},\\
&\qquad \mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\}\\
KB &= \{\mathsf{c} \neq 0, v \neq 0,\\
&\qquad \mathsf{s} = \mathsf{olds} + 1, \mathsf{c0} \neq 0,\\
&\qquad \mathsf{olds} = \mathsf{str} + 1\}
\end{aligned}
$$

From LLVM to Symbolic Execution Graph

```
...
loop:
  0: olds = phi i8* [str,entry],[s,loop]
  1: s = getelementptr i8* olds, i32 1
  ...
```



$$\begin{aligned}
pos &= (\mathsf{loop}, \mathsf{loop}, 0)\\
AL &= \{alloc(\mathsf{str}, u_{end})\}\\
PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,\\
&\qquad \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}\}\\
KB &= \{\mathsf{c} \neq 0, \mathsf{s} = \mathsf{olds} + 1,\\
&\qquad \mathtt{c0} \neq 0, \mathsf{olds} = \mathsf{str}\}
\end{aligned}$$

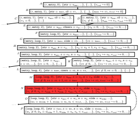
...

$$\begin{aligned}
pos &= (\mathsf{loop}, \mathsf{loop}, 0)\\
AL &= \{alloc(\mathsf{str}, u_{end})\}\\
PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,\\
&\qquad \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c},\\
&\qquad \mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\}\\
KB &= \{\mathsf{c} \neq 0, v \neq 0,\\
&\qquad \mathsf{s} = \mathsf{olds} + 1, \mathtt{c0} \neq 0,\\
&\qquad \mathsf{olds} = \mathsf{str} + 1\}
\end{aligned}$$

Generalisation
(to obtain finite graph)

From LLVM to Symbolic Execution Graph

```
...
loop:
  0: olds = phi i8* [str,entry],[s,loop]
  1: s = getelementptr i8* olds, i32 1
  ...
```



$$pos = (\mathsf{loop}, \mathsf{loop}, 0)$$
$$AL = \{alloc(\mathsf{str}, u_{end})\}$$
$$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}\}$$
$$KB = \{\mathsf{c} \neq 0, \mathsf{s} = \mathsf{olds} + 1, \mathsf{c0} \neq 0, \mathsf{olds} = \mathsf{str}\}$$

...

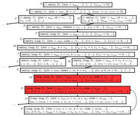
$$pos = (\mathsf{loop}, \mathsf{loop}, 0)$$
$$AL = \{alloc(\mathsf{str}, u_{end})\}$$
$$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}, \mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\}$$
$$KB = \{\mathsf{c} \neq 0, v \neq 0, \mathsf{s} = \mathsf{olds} + 1, \mathsf{c0} \neq 0, \mathsf{olds} = \mathsf{str} + 1\}$$

Generalisation

$$pos = (\mathsf{loop}, \mathsf{loop}, 0)$$

From LLVM to Symbolic Execution Graph

```
...
loop:
  0: olds = phi i8* [str,entry],[s,loop]
  1: s = getelementptr i8* olds, i32 1
  ...
```



$$pos = (\mathsf{loop}, \mathsf{loop}, 0)$$
$$AL = \{alloc(\mathsf{str}, u_{end})\}$$
$$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}\}$$
$$KB = \{\mathsf{c} \neq 0, \mathsf{s} = \mathsf{olds} + 1, \mathsf{c0} \neq 0, \mathsf{olds} = \mathsf{str}\}$$

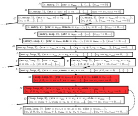
...

$$pos = (\mathsf{loop}, \mathsf{loop}, 0)$$
$$AL = \{alloc(\mathsf{str}, u_{end})\}$$
$$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}, \mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\}$$
$$KB = \{\mathsf{c} \neq 0, v \neq 0, \mathsf{s} = \mathsf{olds} + 1, \mathsf{c0} \neq 0, \mathsf{olds} = \mathsf{str} + 1\}$$

Generalisation

$$pos = (\mathsf{loop}, \mathsf{loop}, 0)$$
$$AL = \{alloc(\mathsf{str}, u_{end})\}$$

```
...
loop:
  0: olds = phi i8* [str,entry],[s,loop]
  1: s = getelementptr i8* olds, i32 1
  ...
```



$pos = (\mathsf{loop}, \mathsf{loop}, 0)$
$AL = \{alloc(\mathsf{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}\}$
$KB = \{\mathsf{c} \neq 0, \mathsf{s} = \mathsf{olds} + 1, \mathtt{c0} \neq 0, \mathsf{olds} = \mathsf{str}\}$

. . .

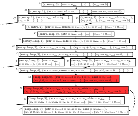
$pos = (\mathsf{loop}, \mathsf{loop}, 0)$
$AL = \{alloc(\mathsf{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}, \mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\}$
$KB = \{\mathsf{c} \neq 0, v \neq 0, \mathsf{s} = \mathsf{olds} + 1, \mathtt{c0} \neq 0, \mathsf{olds} = \mathsf{str} + 1\}$

Generalisation

$pos = (\mathsf{loop}, \mathsf{loop}, 0)$
$AL = \{alloc(\mathsf{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \quad \}$

From LLVM to Symbolic Execution Graph

```
...
loop:
  0: olds = phi i8* [str,entry],[s,loop]
  1: s = getelementptr i8* olds, i32 1
  ...
```



$pos = (\texttt{loop}, \texttt{loop}, 0)$
$AL = \{alloc(\texttt{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\texttt{i8}} 0, \texttt{str} \hookrightarrow_{\texttt{i8}} \texttt{c0}, \texttt{s} \hookrightarrow_{\texttt{i8}} \texttt{c}\}$
$KB = \{\texttt{c} \neq 0, \texttt{s} = \texttt{olds} + 1, \texttt{c0} \neq 0, \texttt{olds} = \texttt{str}\}$

...

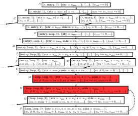
$pos = (\texttt{loop}, \texttt{loop}, 0)$
$AL = \{alloc(\texttt{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\texttt{i8}} 0, \texttt{str} \hookrightarrow_{\texttt{i8}} \texttt{c0}, \texttt{s} \hookrightarrow_{\texttt{i8}} \texttt{c}, \texttt{olds} \hookrightarrow_{\texttt{i8}} v\}$
$KB = \{\texttt{c} \neq 0, v \neq 0, \texttt{s} = \texttt{olds} + 1, \texttt{c0} \neq 0, \texttt{olds} = \texttt{str} + 1\}$

Generalisation

$pos = (\texttt{loop}, \texttt{loop}, 0)$
$AL = \{alloc(\texttt{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\texttt{i8}} 0, \texttt{str} \hookrightarrow_{\texttt{i8}} \texttt{c0}, \}$

From LLVM to Symbolic Execution Graph

```
...
loop:
  0: olds = phi i8* [str,entry],[s,loop]
  1: s = getelementptr i8* olds, i32 1
  ...
```



$pos = (\mathsf{loop}, \mathsf{loop}, 0)$
$AL = \{alloc(\mathsf{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathsf{i8}} 0, \mathsf{str} \hookrightarrow_{\mathsf{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathsf{i8}} \mathsf{c}\}$
$KB = \{\mathsf{c} \neq 0, \mathsf{s} = \mathsf{olds} + 1, \mathsf{c0} \neq 0, \mathsf{olds} = \mathsf{str}\}$

...

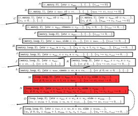
$pos = (\mathsf{loop}, \mathsf{loop}, 0)$
$AL = \{alloc(\mathsf{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathsf{i8}} 0, \mathsf{str} \hookrightarrow_{\mathsf{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathsf{i8}} \mathsf{c}, \mathsf{olds} \hookrightarrow_{\mathsf{i8}} v\}$
$KB = \{\mathsf{c} \neq 0, v \neq 0, \mathsf{s} = \mathsf{olds} + 1, \mathsf{c0} \neq 0, \mathsf{olds} = \mathsf{str} + 1\}$

Generalisation

$pos = (\mathsf{loop}, \mathsf{loop}, 0)$
$AL = \{alloc(\mathsf{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathsf{i8}} 0, \mathsf{str} \hookrightarrow_{\mathsf{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathsf{i8}} \mathsf{c}, \}$

From LLVM to Symbolic Execution Graph

```
...
loop:
  0: olds = phi i8* [str,entry],[s,loop]
  1: s = getelementptr i8* olds, i32 1
  ...
```



$$\begin{aligned} pos &= (\mathsf{loop}, \mathsf{loop}, 0) \\ AL &= \{alloc(\mathsf{str}, u_{end})\} \\ PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \\ &\quad\; \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}\} \\ KB &= \{\mathsf{c} \neq 0, \mathsf{s} = \mathsf{olds} + 1, \\ &\quad\; \mathtt{c0} \neq 0, \mathsf{olds} = \mathsf{str}\} \end{aligned}$$

...

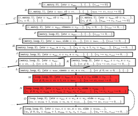
$$\begin{aligned} pos &= (\mathsf{loop}, \mathsf{loop}, 0) \\ AL &= \{alloc(\mathsf{str}, u_{end})\} \\ PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \\ &\quad\; \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}, \\ &\quad\; \mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\} \\ KB &= \{\mathsf{c} \neq 0, v \neq 0, \\ &\quad\; \mathsf{s} = \mathsf{olds} + 1, \mathtt{c0} \neq 0, \\ &\quad\; \mathsf{olds} = \mathsf{str} + 1\} \end{aligned}$$

Generalisation

$$\begin{aligned} pos &= (\mathsf{loop}, \mathsf{loop}, 0) \\ AL &= \{alloc(\mathsf{str}, u_{end})\} \\ PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \\ &\quad\; \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}, \\ &\quad\; \mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\} \end{aligned}$$

From LLVM to Symbolic Execution Graph

```
...
loop:
  0: olds = phi i8* [str,entry],[s,loop]
  1: s = getelementptr i8* olds, i32 1
  ...
```



$pos = (\mathtt{loop}, \mathtt{loop}, 0)$
$AL = \{alloc(\mathtt{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathtt{s} \hookrightarrow_{\mathtt{i8}} \mathtt{c}\}$
$KB = \{\mathtt{c} \neq 0, \mathtt{s} = \mathtt{olds} + 1, \mathtt{c0} \neq 0, \mathtt{olds} = \mathtt{str}\}$

...

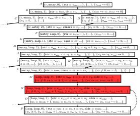
$pos = (\mathtt{loop}, \mathtt{loop}, 0)$
$AL = \{alloc(\mathtt{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathtt{s} \hookrightarrow_{\mathtt{i8}} \mathtt{c}, \mathtt{olds} \hookrightarrow_{\mathtt{i8}} v\}$
$KB = \{\mathtt{c} \neq 0, v \neq 0, \mathtt{s} = \mathtt{olds} + 1, \mathtt{c0} \neq 0, \mathtt{olds} = \mathtt{str} + 1\}$

Generalisation

$pos = (\mathtt{loop}, \mathtt{loop}, 0)$
$AL = \{alloc(\mathtt{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathtt{s} \hookrightarrow_{\mathtt{i8}} \mathtt{c}, \mathtt{olds} \hookrightarrow_{\mathtt{i8}} v\}$
$KB = \{\mathtt{c} \neq 0, \}$

From LLVM to Symbolic Execution Graph

```
...
loop:
  0: olds = phi i8* [str,entry],[s,loop]
  1: s = getelementptr i8* olds, i32 1
  ...
```



$$
\begin{aligned}
pos &= (\mathsf{loop}, \mathsf{loop}, 0)\\
AL &= \{alloc(\mathsf{str}, u_{end})\}\\
PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,\\
&\qquad \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}\}\\
KB &= \{\mathsf{c} \neq 0, \mathsf{s} = \mathsf{olds} + 1,\\
&\qquad \mathsf{c0} \neq 0, \mathsf{olds} = \mathsf{str}\}
\end{aligned}
$$

...

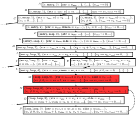
$$
\begin{aligned}
pos &= (\mathsf{loop}, \mathsf{loop}, 0)\\
AL &= \{alloc(\mathsf{str}, u_{end})\}\\
PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,\\
&\qquad \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c},\\
&\qquad \mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\}\\
KB &= \{\mathsf{c} \neq 0, v \neq 0,\\
&\qquad \mathsf{s} = \mathsf{olds} + 1, \mathsf{c0} \neq 0,\\
&\qquad \mathsf{olds} = \mathsf{str} + 1\}
\end{aligned}
$$

Generalisation

$$
\begin{aligned}
pos &= (\mathsf{loop}, \mathsf{loop}, 0)\\
AL &= \{alloc(\mathsf{str}, u_{end})\}\\
PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,\\
&\qquad \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c},\\
&\qquad \mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\}\\
KB &= \{\mathsf{c} \neq 0, v \neq 0,\\
&\qquad \}
\end{aligned}
$$

From LLVM to Symbolic Execution Graph

```
...
loop:
  0: olds = phi i8* [str,entry],[s,loop]
  1: s = getelementptr i8* olds, i32 1
  ...
```



$$
\begin{aligned}
pos &= (\mathsf{loop}, \mathsf{loop}, 0)\\
AL &= \{alloc(\mathsf{str}, u_{end})\}\\
PT &= \{u_{end} \hookrightarrow_{\mathsf{i8}} 0,\\
&\qquad \mathsf{str} \hookrightarrow_{\mathsf{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathsf{i8}} \mathsf{c}\}\\
KB &= \{\mathsf{c} \neq 0, \mathsf{s} = \mathsf{olds} + 1,\\
&\qquad \mathsf{c0} \neq 0, \mathsf{olds} = \mathsf{str}\}
\end{aligned}
$$

...

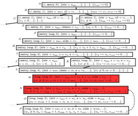
$$
\begin{aligned}
pos &= (\mathsf{loop}, \mathsf{loop}, 0)\\
AL &= \{alloc(\mathsf{str}, u_{end})\}\\
PT &= \{u_{end} \hookrightarrow_{\mathsf{i8}} 0,\\
&\qquad \mathsf{str} \hookrightarrow_{\mathsf{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathsf{i8}} \mathsf{c},\\
&\qquad \mathsf{olds} \hookrightarrow_{\mathsf{i8}} v\}\\
KB &= \{\mathsf{c} \neq 0, v \neq 0,\\
&\qquad \mathsf{s} = \mathsf{olds} + 1, \mathsf{c0} \neq 0,\\
&\qquad \mathsf{olds} = \mathsf{str} + 1\}
\end{aligned}
$$

Generalisation

$$
\begin{aligned}
pos &= (\mathsf{loop}, \mathsf{loop}, 0)\\
AL &= \{alloc(\mathsf{str}, u_{end})\}\\
PT &= \{u_{end} \hookrightarrow_{\mathsf{i8}} 0,\\
&\qquad \mathsf{str} \hookrightarrow_{\mathsf{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathsf{i8}} \mathsf{c},\\
&\qquad \mathsf{olds} \hookrightarrow_{\mathsf{i8}} v\}\\
KB &= \{\mathsf{c} \neq 0, v \neq 0,\\
&\qquad \mathsf{s} = \mathsf{olds} + 1,\\
&\qquad \}
\end{aligned}
$$

From LLVM to Symbolic Execution Graph

```
...
loop:
  0: olds = phi i8* [str,entry],[s,loop]
  1: s = getelementptr i8* olds, i32 1
  ...
```



$$\begin{aligned} pos &= (\mathsf{loop}, \mathsf{loop}, 0) \\ AL &= \{alloc(\mathsf{str}, u_{end})\} \\ PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \\ &\quad \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}\} \\ KB &= \{\mathsf{c} \neq 0, \mathsf{s} = \mathsf{olds} + 1, \\ &\quad \mathtt{c0} \neq 0, \mathsf{olds} = \mathsf{str}\} \end{aligned}$$

...

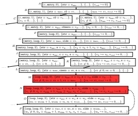
$$\begin{aligned} pos &= (\mathsf{loop}, \mathsf{loop}, 0) \\ AL &= \{alloc(\mathsf{str}, u_{end})\} \\ PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \\ &\quad \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}, \\ &\quad \mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\} \\ KB &= \{\mathsf{c} \neq 0, v \neq 0, \\ &\quad \mathsf{s} = \mathsf{olds} + 1, \mathtt{c0} \neq 0, \\ &\quad \mathsf{olds} = \mathsf{str} + 1\} \end{aligned}$$

Generalisation

$$\begin{aligned} pos &= (\mathsf{loop}, \mathsf{loop}, 0) \\ AL &= \{alloc(\mathsf{str}, u_{end})\} \\ PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \\ &\quad \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}, \\ &\quad \mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\} \\ KB &= \{\mathsf{c} \neq 0, v \neq 0, \\ &\quad \mathsf{s} = \mathsf{olds} + 1, \mathtt{c0} \neq 0, \\ &\quad \} \end{aligned}$$

From LLVM to Symbolic Execution Graph

```
...
loop:
  0: olds = phi i8* [str,entry],[s,loop]
  1: s = getelementptr i8* olds, i32 1
  ...
```



$pos = (\mathsf{loop}, \mathsf{loop}, 0)$
$AL = \{alloc(\mathsf{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathtt{c}\}$
$KB = \{\mathtt{c} \neq 0, \mathsf{s} = \mathsf{olds} + 1, \mathtt{c0} \neq 0, \mathsf{olds} = \mathsf{str}\}$

...

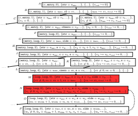
$pos = (\mathsf{loop}, \mathsf{loop}, 0)$
$AL = \{alloc(\mathsf{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathtt{c}, \mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\}$
$KB = \{\mathtt{c} \neq 0, v \neq 0, \mathsf{s} = \mathsf{olds} + 1, \mathtt{c0} \neq 0, \mathsf{olds} = \mathsf{str} + 1\}$

Generalisation

$pos = (\mathsf{loop}, \mathsf{loop}, 0)$
$AL = \{alloc(\mathsf{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathtt{c}, \mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\}$
$KB = \{\mathtt{c} \neq 0, v \neq 0, \mathsf{s} = \mathsf{olds} + 1, \mathtt{c0} \neq 0\}$

From LLVM to Symbolic Execution Graph

```
...
loop:
  0: olds = phi i8* [str,entry],[s,loop]
  1: s = getelementptr i8* olds, i32 1
  ...
```



$pos = (\mathsf{loop}, \mathsf{loop}, 0)$
$AL = \{alloc(\mathsf{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}\}$
$KB = \{\mathsf{c} \neq 0, \mathsf{s} = \mathsf{olds} + 1, \mathsf{c0} \neq 0, \mathsf{olds} = \mathsf{str}\}$

$$x = y \iff x \geq y \wedge x \leq y$$

...

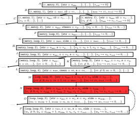
Generalisation

$pos = (\mathsf{loop}, \mathsf{loop}, 0)$
$AL = \{alloc(\mathsf{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}, \mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\}$
$KB = \{\mathsf{c} \neq 0, v \neq 0, \mathsf{s} = \mathsf{olds} + 1, \mathsf{c0} \neq 0, \mathsf{olds} = \mathsf{str} + 1\}$

$pos = (\mathsf{loop}, \mathsf{loop}, 0)$
$AL = \{alloc(\mathsf{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}, \mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\}$
$KB = \{\mathsf{c} \neq 0, v \neq 0, \mathsf{s} = \mathsf{olds} + 1, \mathsf{c0} \neq 0, \}$

From LLVM to Symbolic Execution Graph

```
...
loop:
  0: olds = phi i8* [str,entry],[s,loop]
  1: s = getelementptr i8* olds, i32 1
  ...
```



$pos = (\mathsf{loop}, \mathsf{loop}, 0)$
$AL = \{alloc(\mathsf{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}\}$
$KB = \{\mathsf{c} \neq 0, \mathsf{s} = \mathsf{olds} + 1, \mathtt{c0} \neq 0, \mathsf{olds} = \mathsf{str}\}$

...

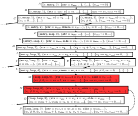
$pos = (\mathsf{loop}, \mathsf{loop}, 0)$
$AL = \{alloc(\mathsf{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}, \mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\}$
$KB = \{\mathsf{c} \neq 0, v \neq 0, \mathsf{s} = \mathsf{olds} + 1, \mathtt{c0} \neq 0, \mathsf{olds} = \mathsf{str} + 1\}$

Generalisation

$pos = (\mathsf{loop}, \mathsf{loop}, 0)$
$AL = \{alloc(\mathsf{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}, \mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\}$
$KB = \{\mathsf{c} \neq 0, v \neq 0, \mathsf{s} = \mathsf{olds} + 1, \mathtt{c0} \neq 0, \mathsf{olds} \geq \mathsf{str}, \}$

From LLVM to Symbolic Execution Graph

```
...
loop:
  0: olds = phi i8* [str,entry],[s,loop]
  1: s = getelementptr i8* olds, i32 1
  ...
```



$pos = (\texttt{loop}, \texttt{loop}, 0)$
$AL = \{alloc(\texttt{str}, u_{end})\}$

$x_1 \hookrightarrow_{\texttt{ty}} y_1 \wedge$
$x_2 \hookrightarrow_{\texttt{ty}} y_2 \wedge$
$y_1 \neq y_2$

ation

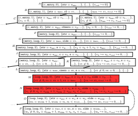
$pos = (\texttt{loop}, \texttt{loop},$
$AL = \{alloc(\texttt{str}, u$
$PT = \{u_{end} \hookrightarrow_{\texttt{i8}} 0,$
$\texttt{str} \hookrightarrow_{\texttt{i8}} \texttt{c0}, \texttt{s} \hookrightarrow_{\texttt{i8}} \texttt{c},$
$\texttt{olds} \hookrightarrow_{\texttt{i8}} v\}$
$KB = \{\texttt{c} \neq 0, v \neq 0,$
$\texttt{s} = \texttt{olds} + 1, \texttt{c0} \neq 0,$
$\texttt{olds} = \texttt{str} + 1\}$

$\rightarrow$

$PT = \{u_{end} \hookrightarrow_{\texttt{i8}} 0,$
$\texttt{str} \hookrightarrow_{\texttt{i8}} \texttt{c0}, \texttt{s} \hookrightarrow_{\texttt{i8}} \texttt{c},$
$\texttt{olds} \hookrightarrow_{\texttt{i8}} v\}$
$KB = \{\texttt{c} \neq 0, v \neq 0,$
$\texttt{s} = \texttt{olds} + 1, \texttt{c0} \neq 0,$
$\texttt{olds} \geq \texttt{str}, \quad \}$

From LLVM to Symbolic Execution Graph

```
...
loop:
  0: olds = phi i8* [str,entry],[s,loop]
  1: s = getelementptr i8* olds, i32 1
  ...
```



$pos = (\mathsf{loop}, \mathsf{loop}, 0)$
$AL = \{alloc(\mathsf{str}, u_{end})\}$

$$x_1 \hookrightarrow_{\mathtt{ty}} y_1 \wedge$$
$$x_2 \hookrightarrow_{\mathtt{ty}} y_2 \wedge \quad \implies \quad x_1 \neq x_2$$
$$y_1 \neq y_2$$

ation

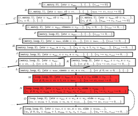
$pos = (\mathsf{loop}, \mathsf{loop},$
$AL = \{alloc(\mathsf{str}, u$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,$
$\mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c},$
$\mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\}$
$KB = \{\mathsf{c} \neq 0, v \neq 0,$
$\mathsf{s} = \mathsf{olds} + 1, \mathsf{c0} \neq 0,$
$\mathsf{olds} = \mathsf{str} + 1\}$

$\rightarrow$

$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,$
$\mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c},$
$\mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\}$
$KB = \{\mathsf{c} \neq 0, v \neq 0,$
$\mathsf{s} = \mathsf{olds} + 1, \mathsf{c0} \neq 0,$
$\mathsf{olds} \geq \mathsf{str}, \qquad \}$

From LLVM to Symbolic Execution Graph

```
...
loop:
  0: olds = phi i8* [str,entry],[s,loop]
  1: s = getelementptr i8* olds, i32 1
  ...
```



$pos = (\mathsf{loop}, \mathsf{loop}, 0)$
$AL = \{alloc(\mathsf{str}, u_{end})\}$

$$x_1 \hookrightarrow_{\mathtt{ty}} y_1 \wedge x_2 \hookrightarrow_{\mathtt{ty}} y_2 \wedge y_1 \neq y_2 \implies x_1 \neq x_2$$

Check whether $x_1 < x_2$ or $x_1 > x_2$ holds!

ation

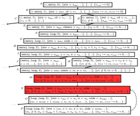
$pos = (\mathsf{loop}, \mathsf{loop},$
$AL = \{alloc(\mathsf{str}, u$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,$
$\mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c},$
$\mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\}$
$KB = \{\mathsf{c} \neq 0, v \neq 0,$
$\mathsf{s} = \mathsf{olds} + 1, \mathsf{c0} \neq 0,$
$\mathsf{olds} = \mathsf{str} + 1\}$

$\rightarrow$

$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,$
$\mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c},$
$\mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\}$
$KB = \{\mathsf{c} \neq 0, v \neq 0,$
$\mathsf{s} = \mathsf{olds} + 1, \mathsf{c0} \neq 0,$
$\mathsf{olds} \geq \mathsf{str}, \quad \}$

From LLVM to Symbolic Execution Graph

```
...
loop:
  0: olds = phi i8* [str,entry],[s,loop]
  1: s = getelementptr i8* olds, i32 1
  ...
```



$pos = (\mathsf{loop}, \mathsf{loop}, 0)$
$AL = \{alloc(\mathsf{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}\}$
$KB = \{\mathsf{c} \neq 0, \mathsf{s} = \mathsf{olds} + 1, \mathtt{c0} \neq 0, \mathsf{olds} = \mathsf{str}\}$

...

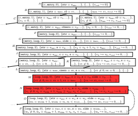
$pos = (\mathsf{loop}, \mathsf{loop}, 0)$
$AL = \{alloc(\mathsf{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}, \mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\}$
$KB = \{\mathsf{c} \neq 0, v \neq 0, \mathsf{s} = \mathsf{olds} + 1, \mathtt{c0} \neq 0, \mathsf{olds} = \mathsf{str} + 1\}$

Generalisation

$pos = (\mathsf{loop}, \mathsf{loop}, 0)$
$AL = \{alloc(\mathsf{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c}, \mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\}$
$KB = \{\mathsf{c} \neq 0, v \neq 0, \mathsf{s} = \mathsf{olds} + 1, \mathtt{c0} \neq 0, \mathsf{olds} \geq \mathsf{str}, \mathsf{s} \neq u_{end}\}$

From LLVM to Symbolic Execution Graph

```
...
loop:
  0: olds = phi i8* [str,entry],[s,loop]
  1: s = getelementptr i8* olds, i32 1
  ...
```



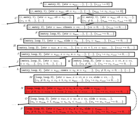
$pos = (\mathtt{loop}, \mathtt{loop}, 0)$
$AL = \{alloc(\mathtt{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathtt{s} \hookrightarrow_{\mathtt{i8}} \mathtt{c}\}$
$KB = \{\mathtt{c} \neq 0, \mathtt{s} = \mathtt{olds} + 1, \mathtt{c0} \neq 0, \mathtt{olds} = \mathtt{str}\}$

...

Generalisation

$pos = (\mathtt{loop}, \mathtt{loop}, 0)$
$AL = \{alloc(\mathtt{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathtt{s} \hookrightarrow_{\mathtt{i8}} \mathtt{c}, \mathtt{olds} \hookrightarrow_{\mathtt{i8}} v\}$
$KB = \{\mathtt{c} \neq 0, v \neq 0, \mathtt{s} = \mathtt{olds} + 1, \mathtt{c0} \neq 0, \mathtt{olds} = \mathtt{str} + 1\}$

$pos = (\mathtt{loop}, \mathtt{loop}, 0)$
$AL = \{alloc(\mathtt{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathtt{s} \hookrightarrow_{\mathtt{i8}} \mathtt{c}, \mathtt{olds} \hookrightarrow_{\mathtt{i8}} v\}$
$KB = \{\mathtt{c} \neq 0, v \neq 0, \mathtt{s} = \mathtt{olds} + 1, \mathtt{c0} \neq 0, \mathtt{olds} \geq \mathtt{str}, \mathtt{s} < u_{end}\}$



$$
\begin{aligned}
pos &= (\mathtt{loop}, \mathtt{loop}, 0)\\
AL &= \{alloc(\mathsf{str}, u_{end})\}\\
PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,\\
&\qquad \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c},\\
&\qquad \mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\}\\
KB &= \{\mathsf{c} \neq 0, v \neq 0,\\
&\qquad \mathsf{s} = \mathsf{olds} + 1, \mathsf{c0} \neq 0,\\
&\qquad \mathsf{olds} \geq \mathsf{str}, \mathsf{s} < u_{end}\}
\end{aligned}
$$

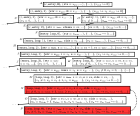
↓

...

↓

$$
\begin{aligned}
pos &= (\mathtt{loop}, \mathtt{loop}, 0)\\
AL &= \{alloc(\mathsf{str}, u_{end})\}\\
PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,\\
&\qquad \mathsf{str} \hookrightarrow_{\mathtt{i8}} \mathsf{c0}, \mathsf{s} \hookrightarrow_{\mathtt{i8}} \mathsf{c},\\
&\qquad \mathsf{olds} \hookrightarrow_{\mathtt{i8}} v\}\\
KB &= \{\mathsf{c} \neq 0, v \neq 0,\\
&\qquad \mathsf{s} = \mathsf{olds} + 1, \mathsf{c0} \neq 0,\\
&\qquad \mathsf{olds} \geq \mathsf{str}, \mathsf{s} < u_{end}\}
\end{aligned}
$$

From LLVM to Symbolic Execution Graph



$$
\begin{aligned}
pos &= (\mathtt{loop}, \mathtt{loop}, 0)\\
AL &= \{alloc(\mathtt{str}, u_{end})\}\\
PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,\\
&\qquad \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathtt{s} \hookrightarrow_{\mathtt{i8}} \mathtt{c},\\
&\qquad \mathtt{olds} \hookrightarrow_{\mathtt{i8}} v\}\\
KB &= \{\mathtt{c} \neq 0, v \neq 0,\\
&\qquad \mathtt{s} = \mathtt{olds} + 1, \mathtt{c0} \neq 0,\\
&\qquad \mathtt{olds} \geq \mathtt{str}, \mathtt{s} < u_{end}\}
\end{aligned}
$$

$\downarrow$

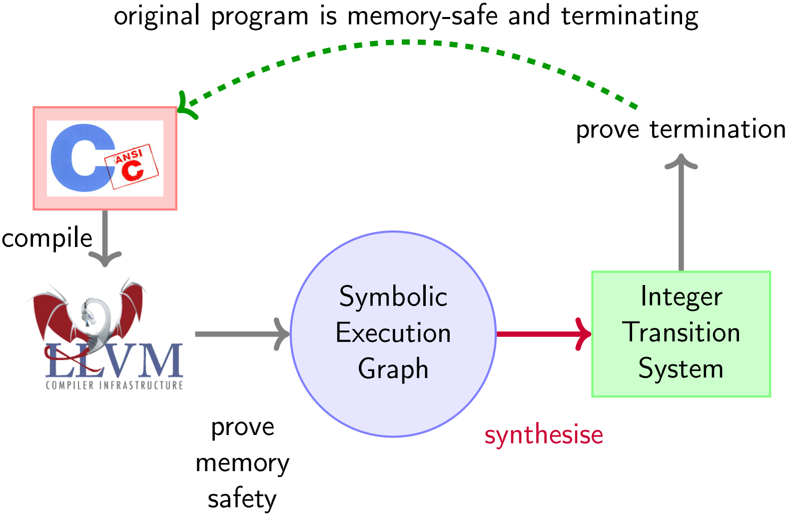
$\cdots$

$\downarrow$

$$
\begin{aligned}
pos &= (\mathtt{loop}, \mathtt{loop}, 0)\\
AL &= \{alloc(\mathtt{str}, u_{end})\}\\
PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,\\
&\qquad \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}, \mathtt{s} \hookrightarrow_{\mathtt{i8}} \mathtt{c},\\
&\qquad \mathtt{olds} \hookrightarrow_{\mathtt{i8}} v\}\\
KB &= \{\mathtt{c} \neq 0, v \neq 0,\\
&\qquad \mathtt{s} = \mathtt{olds} + 1, \mathtt{c0} \neq 0,\\
&\qquad \mathtt{olds} \geq \mathtt{str}, \mathtt{s} < u_{end}\}
\end{aligned}
$$

Generalisation

Overview


original program is memory-safe and terminating
prove termination
ANSI C
compile
LLVM
COMPILER INFRASTRUCTURE
Symbolic Execution Graph
Integer Transition System
prove memory safety
synthesise

From Symb. Exec. Graph to Integer Transition Systems (1/3)

- Non-termination $\rightsquigarrow$ infinite run through graph
- Express graph traversal (strongly connected components)

  by Integer Transition System (ITS)
- ITS terminating $\implies$ C program terminating

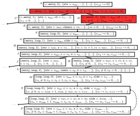
From Symb. Exec. Graph to Integer Transition Systems (2/3)

- Function symbols: abstract states

From Symb. Exec. Graph to Integer Transition Systems (2/3)

- Function symbols: abstract states
- Arguments: variables occurring in states

- Function symbols: abstract states
- Arguments: variables occurring in states



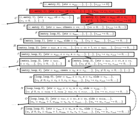
B

$$\begin{aligned} pos &= (\varepsilon, \mathtt{entry}, 1) \\ AL &= \{alloc(\mathtt{str}, u_{end})\} \\ PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \\ &\quad\ \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}\} \\ KB &= \varnothing \end{aligned}$$

D

$$\begin{aligned} pos &= (\varepsilon, \mathtt{entry}, 1) \\ AL &= \{alloc(\mathtt{str}, u_{end})\} \\ PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \\ &\quad\ \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}\} \\ KB &= \{\mathtt{c0} \neq 0\} \end{aligned}$$

- Function symbols: abstract states
- Arguments: variables occurring in states



B

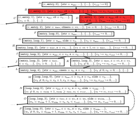
$$\begin{array}{l} pos = (\varepsilon, \texttt{entry}, 1) \\ AL = \{alloc(\texttt{str}, u_{end})\} \\ PT = \{u_{end} \hookrightarrow_{\texttt{i8}} 0, \\ \qquad\quad \texttt{str} \hookrightarrow_{\texttt{i8}} \texttt{c0}\} \\ KB = \varnothing \end{array}$$

D

$$\begin{array}{l} pos = (\varepsilon, \texttt{entry}, 1) \\ AL = \{alloc(\texttt{str}, u_{end})\} \\ PT = \{u_{end} \hookrightarrow_{\texttt{i8}} 0, \\ \qquad\quad \texttt{str} \hookrightarrow_{\texttt{i8}} \texttt{c0}\} \\ KB = \{\texttt{c0} \neq 0\} \end{array}$$

$\ell_{\mathsf{B}}(\qquad\qquad)$

- Function symbols: abstract states
- Arguments: variables occurring in states



B

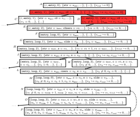
$pos = (\varepsilon, \texttt{entry}, 1)$
$AL = \{alloc(\texttt{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\texttt{i8}} 0,$
$\texttt{str} \hookrightarrow_{\texttt{i8}} \texttt{c0}\}$
$KB = \varnothing$

D

$pos = (\varepsilon, \texttt{entry}, 1)$
$AL = \{alloc(\texttt{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\texttt{i8}} 0,$
$\texttt{str} \hookrightarrow_{\texttt{i8}} \texttt{c0}\}$
$KB = \{\texttt{c0} \neq 0\}$

$\ell_{\mathsf{B}}(\texttt{str} \qquad)$

- Function symbols: abstract states
- Arguments: variables occurring in states



B

$$
\begin{aligned}
pos &= (\varepsilon, \mathsf{entry}, 1)\\
AL &= \{alloc(\mathsf{str}, u_{end})\}\\
PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,\\
&\qquad \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}\}\\
KB &= \varnothing
\end{aligned}
$$

↓

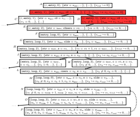
D

$$
\begin{aligned}
pos &= (\varepsilon, \mathsf{entry}, 1)\\
AL &= \{alloc(\mathsf{str}, u_{end})\}\\
PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,\\
&\qquad \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}\}\\
KB &= \{\mathtt{c0} \neq 0\}
\end{aligned}
$$

$$\ell_{\mathsf{B}}(\mathsf{str}, u_{end} \qquad)$$

From Symb. Exec. Graph to Integer Transition Systems (2/3)

- Function symbols: abstract states
- Arguments: variables occurring in states



B

$$\begin{aligned} pos &= (\varepsilon, \mathsf{entry}, 1) \\ AL &= \{alloc(\mathsf{str}, u_{end})\} \\ PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \\ &\qquad \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}\} \\ KB &= \varnothing \end{aligned}$$

↓

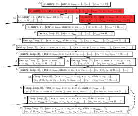
D

$$\begin{aligned} pos &= (\varepsilon, \mathsf{entry}, 1) \\ AL &= \{alloc(\mathsf{str}, u_{end})\} \\ PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \\ &\qquad \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}\} \\ KB &= \{\mathtt{c0} \neq 0\} \end{aligned}$$

$$\ell_{\mathsf{B}}(\mathtt{str}, u_{end}, \mathtt{c0})$$

From Symb. Exec. Graph to Integer Transition Systems (2/3)

- Function symbols: abstract states
- Arguments: variables occurring in states



B

$$
\begin{aligned}
pos &= (\varepsilon, \mathtt{entry}, 1)\\
AL &= \{alloc(\mathtt{str}, u_{end})\}\\
PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,\\
&\qquad \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}\}\\
KB &= \varnothing
\end{aligned}
$$

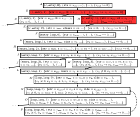
↓

D

$$
\begin{aligned}
pos &= (\varepsilon, \mathtt{entry}, 1)\\
AL &= \{alloc(\mathtt{str}, u_{end})\}\\
PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,\\
&\qquad \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}\}\\
KB &= \{\mathtt{c0} \neq 0\}
\end{aligned}
$$

$$\ell_{\mathsf{B}}(\mathtt{str}, u_{end}, \mathtt{c0}) \longrightarrow \ell_{\mathsf{D}}(\qquad\qquad)$$

- Function symbols: abstract states
- Arguments: variables occurring in states



B

$$\begin{aligned} pos &= (\varepsilon, \mathtt{entry}, 1) \\ AL &= \{alloc(\mathtt{str}, u_{end})\} \\ PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \\ &\quad\ \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}\} \\ KB &= \varnothing \end{aligned}$$

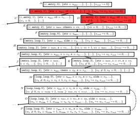
D

$$\begin{aligned} pos &= (\varepsilon, \mathtt{entry}, 1) \\ AL &= \{alloc(\mathtt{str}, u_{end})\} \\ PT &= \{u_{end} \hookrightarrow_{\mathtt{i8}} 0, \\ &\quad\ \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}\} \\ KB &= \{\mathtt{c0} \neq 0\} \end{aligned}$$

$$\ell_{\mathsf{B}}(\mathtt{str}, u_{end}, \mathtt{c0}) \longrightarrow \ell_{\mathsf{D}}(\mathtt{str} \qquad\qquad)$$

From Symb. Exec. Graph to Integer Transition Systems (2/3)

- Function symbols: abstract states
- Arguments: variables occurring in states



B

$$\begin{aligned} &pos = (\varepsilon, \mathtt{entry}, 1)\\ &AL = \{alloc(\mathtt{str}, u_{end})\}\\ &PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,\\ &\qquad\ \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}\}\\ &KB = \varnothing \end{aligned}$$

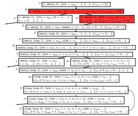
$\downarrow$

D

$$\begin{aligned} &pos = (\varepsilon, \mathtt{entry}, 1)\\ &AL = \{alloc(\mathtt{str}, u_{end})\}\\ &PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,\\ &\qquad\ \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}\}\\ &KB = \{\mathtt{c0} \neq 0\} \end{aligned}$$

$$\ell_{\mathsf{B}}(\mathtt{str}, u_{end}, \mathtt{c0}) \longrightarrow \ell_{\mathsf{D}}(\mathtt{str}, u_{end} \quad)$$

- Function symbols: abstract states
- Arguments: variables occurring in states



B

$pos = (\varepsilon, \mathtt{entry}, 1)$
$AL = \{alloc(\mathtt{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,$
$\quad \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}\}$
$KB = \varnothing$

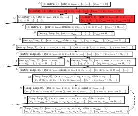
↓

D

$pos = (\varepsilon, \mathtt{entry}, 1)$
$AL = \{alloc(\mathtt{str}, u_{end})\}$
$PT = \{u_{end} \hookrightarrow_{\mathtt{i8}} 0,$
$\quad \mathtt{str} \hookrightarrow_{\mathtt{i8}} \mathtt{c0}\}$
$KB = \{\mathtt{c0} \neq 0\}$

$$\ell_{\mathsf{B}}(\mathtt{str}, u_{end}, \mathtt{c0}) \longrightarrow \ell_{\mathsf{D}}(\mathtt{str}, u_{end}, \mathtt{c0})$$

- Function symbols: abstract states
- Arguments: variables occurring in states



B

$$\begin{aligned} pos &= (\varepsilon, \texttt{entry}, 1) \\ AL &= \{alloc(\texttt{str}, u_{end})\} \\ PT &= \{u_{end} \hookrightarrow_{\texttt{i8}} 0, \\ &\qquad \texttt{str} \hookrightarrow_{\texttt{i8}} \texttt{c0}\} \\ KB &= \varnothing \end{aligned}$$

↓

D

$$\begin{aligned} pos &= (\varepsilon, \texttt{entry}, 1) \\ AL &= \{alloc(\texttt{str}, u_{end})\} \\ PT &= \{u_{end} \hookrightarrow_{\texttt{i8}} 0, \\ &\qquad \texttt{str} \hookrightarrow_{\texttt{i8}} \texttt{c0}\} \\ KB &= \{\texttt{c0} \neq 0\} \end{aligned}$$

$$\ell_{\mathsf{B}}(\texttt{str}, u_{end}, \texttt{c0}) \xrightarrow{\texttt{c0} \neq 0} \ell_{\mathsf{D}}(\texttt{str}, u_{end}, \texttt{c0})$$

From Symb. Exec. Graph to Integer Transition Systems (3/3)

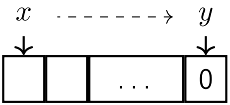
Resulting ITS (after automated simplification):

Resulting ITS (after automated simplification):

$$\ell(x, y) \quad \xrightarrow{x<y} \quad \ell(x+1, y)$$

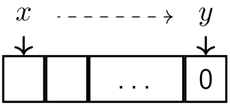
Resulting ITS (after automated simplification):

$$\ell(x, y) \xrightarrow{x<y} \ell(x+1, y)$$



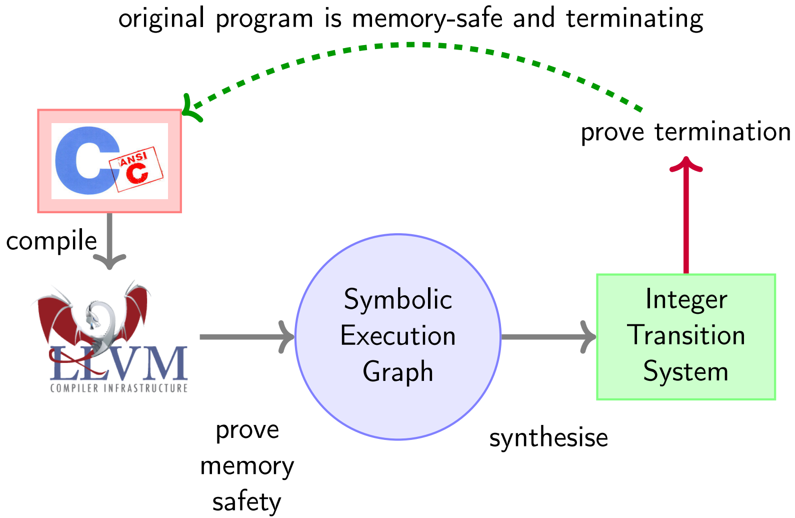
Resulting ITS (after automated simplification):

$$\ell(x, y) \xrightarrow{x<y} \ell(x+1, y)$$



Automatic termination proof by any termination prover

Overview



original program is memory-safe and terminating
prove termination
ANSI C
compile
LLVM
COMPILER INFRASTRUCTURE
Symbolic Execution Graph
Integer Transition System
prove memory safety
synthesise

Experimental Results

- implemented in AProVE
  http://aprove.informatik.rwth-aachen.de/

Experimental Results

- implemented in AProVE
  http://aprove.informatik.rwth-aachen.de/
- demo category of SV-COMP 2014 (TACAS):
  https://sv-comp.sosy-lab.org/

Experimental Results

- implemented in AProVE
  http://aprove.informatik.rwth-aachen.de/
- demo category of SV-COMP 2014 (TACAS):
  https://sv-comp.sosy-lab.org/
  5 participants, most points for AProVE

Experimental Results

- implemented in AProVE
  http://aprove.informatik.rwth-aachen.de/
- demo category of SV-COMP 2014 (TACAS):
  https://sv-comp.sosy-lab.org/
  5 participants, most points for AProVE
- C category of termCOMP 2014 (IJCAR):

Experimental Results

- implemented in AProVE
  http://aprove.informatik.rwth-aachen.de/
- demo category of SV-COMP 2014 (TACAS):
  https://sv-comp.sosy-lab.org/
  5 participants, most points for AProVE
- C category of termCOMP 2014 (IJCAR):
  3 participants, AProVE winner

Experimental Results

- implemented in AProVE
  http://aprove.informatik.rwth-aachen.de/
- demo category of SV-COMP 2014 (TACAS):
  https://sv-comp.sosy-lab.org/
  5 participants, most points for AProVE
- C category of termCOMP 2014 (IJCAR):
  3 participants, AProVE winner

Experimental Results

- implemented in AProVE
  http://aprove.informatik.rwth-aachen.de/
- demo category of SV-COMP 2014 (TACAS):
  https://sv-comp.sosy-lab.org/
  5 participants, most points for AProVE
- C category of termCOMP 2014 (IJCAR):
  3 participants, AProVE winner
- termination category of SV-COMP 2015 (TACAS):
  6 participants, AProVE winner
- termination category of SV-COMP 2016 (TACAS):
  3 participants, AProVE winner

. . .

Experimental Results

- implemented in AProVE
  http://aprove.informatik.rwth-aachen.de/
- demo category of SV-COMP 2014 (TACAS):
  https://sv-comp.sosy-lab.org/
  5 participants, most points for AProVE

- C category of termCOMP 2014 (IJCAR):
  3 participants, AProVE winner
- termination category of SV-COMP 2015 (TACAS):
  6 participants, AProVE winner
- termination category of SV-COMP 2016 (TACAS):
  3 participants, AProVE winner

. . .

- SV-COMP 2022 (TACAS): 3 participants, AProVE second (after UltimateAutomizer)
- termCOMP 2022 (IJCAR): 2 participants, AProVE winner

Extensions

Beyond `strlen`:

- support `malloc` + `free`

Extensions

Beyond `strlen`:

- support `malloc` + `free`
- improved generalisation heuristic, can handle `strcpy`

Extensions

Beyond `strlen`:

- support `malloc` + `free`
- improved generalisation heuristic, can handle `strcpy`
- function calls (also recursive)

Extensions

Beyond `strlen`:

- support `malloc` + `free`
- improved generalisation heuristic, can handle `strcpy`
- function calls (also recursive)
- soundness proved wrt formal Vellvm semantics
  from [Zhao et al, *POPL '12*]

Extensions

Beyond `strlen`:

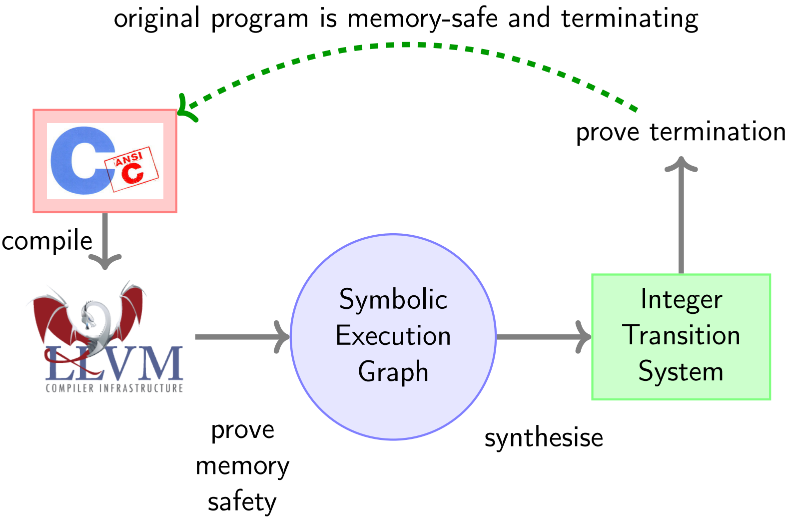
- support `malloc` + `free`
- improved generalisation heuristic, can handle `strcpy`
- function calls (also recursive)
- soundness proved wrt formal Vellvm semantics
  from [Zhao et al, *POPL '12*]
- non-termination analysis [Hensel, Mensendiek, Giesl, *TACAS '22*]

Extensions

Beyond `strlen`:

- support `malloc` + `free`
- improved generalisation heuristic, can handle `strcpy`
- function calls (also recursive)
- soundness proved wrt formal Vellvm semantics
  from [Zhao et al, *POPL '12*]
- non-termination analysis [Hensel, Mensendiek, Giesl, *TACAS '22*]
- termination and complexity wrt bitvector semantics (so far: `int` $= \mathbb{Z}$)
  [Hensel et al, *JLAMP '22*]

Conclusion: Termination of C / LLVM programs



Front-Ends for Haskell and Prolog

Haskell [Giesl et al, *TOPLAS '11*]

- lazy evaluation
- polymorphic types
- higher-order

Front-Ends for Haskell and Prolog

Haskell [Giesl et al, *TOPLAS '11*]

- lazy evaluation
- polymorphic types
- higher-order

⇒ abstract domain: a single term; extract (non-constrained) TRS

Front-Ends for Haskell and Prolog

Haskell [Giesl et al, *TOPLAS '11*]

- lazy evaluation
- polymorphic types
- higher-order

⇒ abstract domain: a single term; extract (non-constrained) TRS

Prolog [Schneider-Kamp et al, *TOCL '09*; Giesl et al, *PPDP '12*]

- backtracking
- uses unification instead of matching
- extra-logical language features (e.g., cut)

Front-Ends for Haskell and Prolog

Haskell [Giesl et al, *TOPLAS '11*]

- lazy evaluation
- polymorphic types
- higher-order

⇒ abstract domain: a single term; extract (non-constrained) TRS

Prolog [Schneider-Kamp et al, *TOCL '09*; Giesl et al, *PPDP '12*]

- backtracking
- uses unification instead of matching
- extra-logical language features (e.g., cut)

⇒ abstract domain based on equivalent **linear** Prolog semantics [Ströder et al, *LOPSTR '11*], tracks which variables are for ground terms vs arbitrary terms

Conclusion: Termination Analysis for Programs

- Termination proving for TRSs and ITSs driven by SMT solvers

Conclusion: Termination Analysis for Programs

- Termination proving for TRSs and ITSs driven by SMT solvers
- Constrained rewriting: Term rewriting + pre-defined primitive data structures

Conclusion: Termination Analysis for Programs

- Termination proving for TRSs and ITSs driven by SMT solvers
- Constrained rewriting: Term rewriting + pre-defined primitive data structures
- Common theme for analysis of program termination by (constrained) rewriting:
  - handle language specifics in **front-end**
  - transitions between program states become (constrained) rewrite rules for **termination back-end**

Conclusion: Termination Analysis for Programs

- Termination proving for TRSs and ITSs driven by SMT solvers
- Constrained rewriting: Term rewriting + pre-defined primitive data structures
- Common theme for analysis of program termination by (constrained) rewriting:
  - handle language specifics in **front-end**
  - transitions between program states become (constrained) rewrite rules for **termination back-end**
- Works across paradigms: Java, C, Haskell, Prolog

Outlook: Complexity Analysis

Given: Program P.

Session 1: Does P terminate at all?

Session 2: How many steps may P take until it terminates?

II.1 Complexity Analysis for Programs on Integers

What Do You Mean by Complexity?

Literature uses many alternative names:

- (Computational/Algorithmic) complexity analysis
- (Computational) cost analysis
- Resource analysis
- Static profiling
- ...

Resource:

- Number of evaluation steps
- Number of network requests
- Peak memory use
- Battery power
- ...

Given: Program P.

Task: Provide **upper/lower bounds** on the resource use of running P as a function of the input (size) **in the worst case**

Why Care About Computational Cost, Anyway?

- **Mobile devices**: Bound energy usage

Why Care About Computational Cost, Anyway?

- **Mobile devices**: Bound energy usage
- **Security**: Denial of Service attacks

Why Care About Computational Cost, Anyway?

- **Mobile devices**: Bound energy usage
- **Security**: Denial of Service attacks

  $\longrightarrow$ related DARPA project: *Space/Time Analysis for Cybersecurity*

  https://www.darpa.mil/program/space-time-analysis-for-cybersecurity

Why Care About Computational Cost, Anyway?

- **Mobile devices**: Bound energy usage
- **Security**: Denial of Service attacks

  → related DARPA project: *Space/Time Analysis for Cybersecurity*
  https://www.darpa.mil/program/space-time-analysis-for-cybersecurity
- **Embedded devices**: Bound memory usage

Why Care About Computational Cost, Anyway?

- **Mobile devices**: Bound energy usage
- **Security**: Denial of Service attacks

  $\longrightarrow$ related DARPA project: *Space/Time Analysis for Cybersecurity*
  https://www.darpa.mil/program/space-time-analysis-for-cybersecurity
- **Embedded devices**: Bound memory usage
- **Specifications**: What guarantees can we make to the API's user?

Why Care About Computational Cost, Anyway?

- **Mobile devices**: Bound energy usage
- **Security**: Denial of Service attacks
  $\longrightarrow$ related DARPA project: *Space/Time Analysis for Cybersecurity*
  https://www.darpa.mil/program/space-time-analysis-for-cybersecurity
- **Embedded devices**: Bound memory usage
- **Specifications**: What guarantees can we make to the API's user?
  "The size, isEmpty, get, set, iterator, and listIterator operations run in constant time. The add operation runs in amortized constant time, that is, adding n elements requires O(n) time. All of the other operations run in linear time (roughly speaking)."
  https://docs.oracle.com/javase/8/docs/api/java/util/ArrayList.html
  $\longrightarrow$ computational cost as a non-functional requirement!

Why Care About Computational Cost, Anyway?

- **Mobile devices**: Bound energy usage
- **Security**: Denial of Service attacks

  $\longrightarrow$ related DARPA project: *Space/Time Analysis for Cybersecurity*

  https://www.darpa.mil/program/space-time-analysis-for-cybersecurity
- **Embedded devices**: Bound memory usage
- **Specifications**: What guarantees can we make to the API's user?

  "The size, isEmpty, get, set, iterator, and listIterator operations run in constant time. The add operation runs in amortized constant time, that is, adding n elements requires O(n) time. All of the other operations run in linear time (roughly speaking)."

  https://docs.oracle.com/javase/8/docs/api/java/util/ArrayList.html

  $\longrightarrow$ computational cost as a non-functional requirement!
- **Profiling**:

  Which parts of the code need most runtime as inputs grow larger?

Why Care About Computational Cost, Anyway?

- **Mobile devices**: Bound energy usage
- **Security**: Denial of Service attacks
  $\longrightarrow$ related DARPA project: *Space/Time Analysis for Cybersecurity*
  https://www.darpa.mil/program/space-time-analysis-for-cybersecurity
- **Embedded devices**: Bound memory usage
- **Specifications**: What guarantees can we make to the API's user?
  "The size, isEmpty, get, set, iterator, and listIterator operations run in constant time. The add operation runs in amortized constant time, that is, adding n elements requires O(n) time. All of the other operations run in linear time (roughly speaking)."
  https://docs.oracle.com/javase/8/docs/api/java/util/ArrayList.html
  $\longrightarrow$ computational cost as a non-functional requirement!
- **Profiling**:
  Which parts of the code need most runtime as inputs grow larger?
- **Smart contracts**: Bound execution cost (as "gas", i.e., money)

Why Care About Computational Cost, Anyway?

- **Mobile devices**: Bound energy usage
- **Security**: Denial of Service attacks
  $\longrightarrow$ related DARPA project: *Space/Time Analysis for Cybersecurity*
  https://www.darpa.mil/program/space-time-analysis-for-cybersecurity
- **Embedded devices**: Bound memory usage
- **Specifications**: What guarantees can we make to the API's user?
  "The size, isEmpty, get, set, iterator, and listIterator operations run in constant time. The add operation runs in amortized constant time, that is, adding n elements requires O(n) time. All of the other operations run in linear time (roughly speaking)."
  https://docs.oracle.com/javase/8/docs/api/java/util/ArrayList.html
  $\longrightarrow$ computational cost as a non-functional requirement!
- **Profiling**:
  Which parts of the code need most runtime as inputs grow larger?
- **Smart contracts**: Bound execution cost (as "gas", i.e., money)
- More: see Section 1.1.2 of PhD thesis by Alicia Merayo Corcoba[1]

[1] A. Merayo Corcoba: *Resource analysis of integer and abstract programs*, PhD thesis, U Complutense Madrid, 2022

Show Me Some Examples!

Question: Write a Python function that returns the sum $1 + 2 + \cdots + n$.

Show Me Some Examples!

Question: Write a Python function that returns the sum $1 + 2 + \cdots + n$.

```
def sum1(n):
  r = 0
  i = 1
  while i <= n:
    r = r + i
    i = i + 1
  return r
```

Show Me Some Examples!

Question: Write a Python function that returns the sum $1 + 2 + \cdots + n$.

```
def sum1(n):
  r = 0
  i = 1
  while i <= n:
    r = r + i
    i = i + 1
  return r
```

$\mathcal{O}(n)$

Show Me Some Examples!

Question: Write a Python function that returns the sum $1 + 2 + \cdots + n$.

```
def sum1(n):
  r = 0
  i = 1
  while i <= n:
    r = r + i
    i = i + 1
  return r
```

$\mathcal{O}(n)$

runtime in $\mathcal{O}(f(n))$ means:

- the program needs at most about $f(n)$ steps for an input of "size" n
- the runtime is "of order $f(n)$"

Show Me Some Examples!

Question: Write a Python function that returns the sum $1 + 2 + \cdots + n$.

```
def sum1(n):
  r = 0
  i = 1
  while i <= n:
    r = r + i
    i = i + 1
  return r
```

$\mathcal{O}(n)$

```
def sum2(n):
  r = 0
  i = 1
  while i <= n:
    r = r + i

  return r
```

runtime in $\mathcal{O}(f(n))$ means:

- the program needs at most about $f(n)$ steps for an input of "size" n
- the runtime is "of order $f(n)$"

Show Me Some Examples!

Question: Write a Python function that returns the sum $1 + 2 + \cdots + n$.

```
def sum1(n):
  r = 0
  i = 1
  while i <= n:
    r = r + i
    i = i + 1
  return r
```

$\mathcal{O}(n)$

```
def sum2(n):
  r = 0
  i = 1
  while i <= n:
    r = r + i

  return r
```

$\mathcal{O}(\infty)$

runtime in $\mathcal{O}(f(n))$ means:

- the program needs at most about $f(n)$ steps for an input of "size" n
- the runtime is "of order $f(n)$"

Show Me Some Examples!

Question: Write a Python function that returns the sum $1 + 2 + \cdots + n$.

```python
def sum1(n):
  r = 0
  i = 1
  while i <= n:
    r = r + i
    i = i + 1
  return r
```

$\mathcal{O}(n)$

```python
def sum2(n):
  r = 0
  i = 1
  while i <= n:
    r = r + i

  return r
```

$\mathcal{O}(\infty)$

```python
def sum3(n):
  r = 0
  i = 1
  while i <= n:
    j = 0
    while j < i:
      r = r + 1
      j = j + 1
    i = i + 1
  return r
```

runtime in $\mathcal{O}(f(n))$ means:

- the program needs at most about $f(n)$ steps for an input of "size" n
- the runtime is "of order $f(n)$"

Show Me Some Examples!

Question: Write a Python function that returns the sum $1 + 2 + \cdots + n$.

```
def sum1(n):
  r = 0
  i = 1
  while i <= n:
    r = r + i
    i = i + 1
  return r
```

$\mathcal{O}(n)$

```
def sum2(n):
  r = 0
  i = 1
  while i <= n:
    r = r + i

  return r
```

$\mathcal{O}(\infty)$

```
def sum3(n):
  r = 0
  i = 1
  while i <= n:
    j = 0
    while j < i:
      r = r + 1
      j = j + 1
    i = i + 1
  return r
```

$\mathcal{O}(n^2)$

runtime in $\mathcal{O}(f(n))$ means:

- the program needs at most about $f(n)$ steps for an input of "size" n
- the runtime is "of order $f(n)$"

Show Me Some Examples!

Question: Write a Python function that returns the sum $1 + 2 + \cdots + n$.

```
def sum1(n):
  r = 0
  i = 1
  while i <= n:
    r = r + i
    i = i + 1
  return r
```

$\mathcal{O}(n)$

```
def sum2(n):
  r = 0
  i = 1
  while i <= n:
    r = r + i

  return r
```

$\mathcal{O}(\infty)$

```
def sum3(n):
  r = 0
  i = 1
  while i <= n:
    j = 0
    while j < i:
      r = r + 1
      j = j + 1
    i = i + 1
  return r
```

$\mathcal{O}(n^2)$

runtime in $\mathcal{O}(f(n))$ means:

- the program needs at most about $f(n)$ steps for an input of "size" n
- the runtime is "of order $f(n)$"

```
def sum4(n):
  return n*(n+1)//2
```

Show Me Some Examples!

Question: Write a Python function that returns the sum $1 + 2 + \cdots + n$.

```
def sum1(n):
    r = 0
    i = 1
    while i <= n:
        r = r + i
        i = i + 1
    return r
```

$\mathcal{O}(n)$

```
def sum2(n):
    r = 0
    i = 1
    while i <= n:
        r = r + i

    return r
```

$\mathcal{O}(\infty)$

```
def sum3(n):
    r = 0
    i = 1
    while i <= n:
        j = 0
        while j < i:
            r = r + 1
            j = j + 1
        i = i + 1
    return r
```

$\mathcal{O}(n^2)$

runtime in $\mathcal{O}(f(n))$ means:

- the program needs at most about $f(n)$ steps for an input of "size" n
- the runtime is "of order $f(n)$"

```
def sum4(n):
    return n*(n+1)//2
```

$\mathcal{O}(1)$

Is There a Tool that Finds such Bounds Automatically?

- Fully automatic open-source tool KoAT:

  https://github.com/s-falke/kittel-koat

Is There a Tool that Finds such Bounds Automatically?

- Fully automatic open-source tool KoAT:

  `https://github.com/s-falke/kittel-koat`

- Journal paper about the automated analysis implemented in KoAT:

  M. Brockschmidt, F. Emmes, S. Falke, C. Fuhs, J. Giesl,
  Analyzing runtime and size complexity of integer programs
  ACM Transactions on Programming Languages and Systems 38 (4), pp. 1 – 50, 2016.

Is There a Tool that Finds such Bounds Automatically?

- Fully automatic open-source tool KoAT:

  `https://github.com/s-falke/kittel-koat`

- Journal paper about the automated analysis implemented in KoAT:

  M. Brockschmidt, F. Emmes, S. Falke, C. Fuhs, J. Giesl,
  Analyzing runtime and size complexity of integer programs
  ACM Transactions on Programming Languages and Systems 38 (4),
  pp. 1 – 50, 2016.

- Experiments:

`http://aprove.informatik.rwth-aachen.de/eval/IntegerComplexity-Journal`

How Can We Make the Computer Do the Work for Us?

Idea: **Countdown**.

For each loop find a **ranking function** f on the variables:

expression that gets smaller each time round the loop, but never reaches 0.

How Can We Make the Computer Do the Work for Us?

Idea: **Countdown**.

For each loop find a **ranking function** f on the variables:

expression that gets smaller each time round the loop, but never reaches 0.

$\Rightarrow$ Gives us a bound on the number of times we go through the loop

How Can We Make the Computer Do the Work for Us?

Idea: **Countdown**.

For each loop find a **ranking function** f on the variables:
expression that gets smaller each time round the loop, but never reaches 0.

$\Rightarrow$ Gives us a bound on the number of times we go through the loop

Termination analysis tools find ranking functions automatically!

How Can We Make the Computer Do the Work for Us?

Idea: **Countdown**.

For each loop find a **ranking function** f on the variables:
expression that gets smaller each time round the loop, but never reaches 0.

⇒ Gives us a bound on the number of times we go through the loop

Termination analysis tools find ranking functions automatically!

```
def twoLoops1(x, z):
  while x > 0:
    x = x - 1


  while z > 0:
    z = z - 1
```

How Can We Make the Computer Do the Work for Us?

Idea: **Countdown**.

For each loop find a **ranking function** f on the variables:
expression that gets smaller each time round the loop, but never reaches 0.

⇒ Gives us a bound on the number of times we go through the loop

Termination analysis tools find ranking functions automatically!

```
def twoLoops1(x, z):
  while x > 0:
    x = x - 1


  while z > 0:
    z = z - 1
```

Loop 1: ranking function x

How Can We Make the Computer Do the Work for Us?

Idea: **Countdown**.

For each loop find a **ranking function** f on the variables:
expression that gets smaller each time round the loop, but never reaches 0.

⇒ Gives us a bound on the number of times we go through the loop

Termination analysis tools find ranking functions automatically!

```
def twoLoops1(x, z):
  while x > 0:
    x = x - 1


  while z > 0:
    z = z - 1
```

Loop 1: ranking function x
Loop 2: ranking function z

How Can We Make the Computer Do the Work for Us?

Idea: **Countdown**.

For each loop find a **ranking function** f on the variables:
expression that gets smaller each time round the loop, but never reaches 0.

⇒ Gives us a bound on the number of times we go through the loop

Termination analysis tools find ranking functions automatically!

```
def twoLoops1(x, z):
  while x > 0:
    x = x - 1


  while z > 0:
    z = z - 1
```

Loop 1: ranking function x
Loop 2: ranking function z

⇒ runtime in $\mathcal{O}(x + z)$

How Can We Make the Computer Do the Work for Us?

Idea: **Countdown**.

For each loop find a **ranking function** f on the variables:
expression that gets smaller each time round the loop, but never reaches 0.

⇒ Gives us a bound on the number of times we go through the loop

Termination analysis tools find ranking functions automatically!

```
def twoLoops1(x, z):
  while x > 0:
    x = x - 1

  while z > 0:
    z = z - 1
```

```
def twoLoops2(x, z):
  while x > 0:
    x = x - 1
    z = z + x
  while z > 0:
    z = z - 1
```

Loop 1: ranking function x

Loop 2: ranking function z

⇒ runtime in $\mathcal{O}(x + z)$

How Can We Make the Computer Do the Work for Us?

Idea: **Countdown**.

For each loop find a **ranking function** f on the variables:
expression that gets smaller each time round the loop, but never reaches 0.

$\Rightarrow$ Gives us a bound on the number of times we go through the loop

Termination analysis tools find ranking functions automatically!

```
def twoLoops1(x, z):
  while x > 0:
    x = x - 1

  while z > 0:
    z = z - 1
```

```
def twoLoops2(x, z):
  while x > 0:
    x = x - 1
    z = z + x
  while z > 0:
    z = z - 1
```

Loop 1: ranking function x
Loop 2: ranking function z
$\Rightarrow$ runtime in $\mathcal{O}(x + z)$

Loop 1: ranking function x

How Can We Make the Computer Do the Work for Us?

Idea: **Countdown**.

For each loop find a **ranking function** f on the variables:
expression that gets smaller each time round the loop, but never reaches 0.

⇒ Gives us a bound on the number of times we go through the loop

Termination analysis tools find ranking functions automatically!

```
def twoLoops1(x, z):
  while x > 0:
    x = x - 1

  while z > 0:
    z = z - 1
```

```
def twoLoops2(x, z):
  while x > 0:
    x = x - 1
    z = z + x
  while z > 0:
    z = z - 1
```

Loop 1: ranking function x
Loop 2: ranking function z

⇒ runtime in $\mathcal{O}(x + z)$

Loop 1: ranking function x
Loop 2: ranking function z

How Can We Make the Computer Do the Work for Us?

Idea: **Countdown**.

For each loop find a **ranking function** f on the variables:
expression that gets smaller each time round the loop, but never reaches 0.

$\Rightarrow$ Gives us a bound on the number of times we go through the loop

Termination analysis tools find ranking functions automatically!

```
def twoLoops1(x, z):
  while x > 0:
    x = x - 1

  while z > 0:
    z = z - 1
```

```
def twoLoops2(x, z):
  while x > 0:
    x = x - 1
    z = z + x
  while z > 0:
    z = z - 1
```

Loop 1: ranking function x
Loop 2: ranking function z

$\Rightarrow$ runtime in $\mathcal{O}(x + z)$

Loop 1: ranking function x
Loop 2: ranking function z

$\Rightarrow$ runtime in

How Can We Make the Computer Do the Work for Us?

Idea: **Countdown**.

For each loop find a **ranking function** f on the variables:
expression that gets smaller each time round the loop, but never reaches 0.

⇒ Gives us a bound on the number of times we go through the loop

Termination analysis tools find ranking functions automatically!

```
def twoLoops1(x, z):
  while x > 0:
    x = x - 1

  while z > 0:
    z = z - 1
```

```
def twoLoops2(x, z):
  while x > 0:
    x = x - 1
    z = z + x
  while z > 0:
    z = z - 1
```

Loop 1: ranking function x
Loop 2: ranking function z

⇒ runtime in $\mathcal{O}(x + z)$

Loop 1: ranking function x
Loop 2: ranking function z

⇒ runtime in ... oops.

How Can We Make the Computer Do the Work for Us?

Idea: **Countdown**.

For each loop find a **ranking function** f on the variables:
expression that gets smaller each time round the loop, but never reaches 0.

$\Rightarrow$ Gives us a bound on the number of times we go through the loop

Termination analysis tools find ranking functions automatically!

```
def twoLoops1(x, z):
  while x > 0:
    x = x - 1

  while z > 0:
    z = z - 1
```

```
def twoLoops2(x, z):
  while x > 0:
    x = x - 1
    z = z + x
  while z > 0:
    z = z - 1
```

Loop 1: ranking function x
Loop 2: ranking function z
$\Rightarrow$ runtime in $\mathcal{O}(x + z)$

Loop 1: ranking function x
Loop 2: ranking function z
$\Rightarrow$ runtime in ... oops.
Best runtime bound: $\mathcal{O}(x^2 + z)$

How Can we Fix our Approach?

```
def twoLoops2(x, z):
  while x > 0:
    x = x - 1
    z = z + x
  while z > 0:
    z = z - 1
```

Loop 1: ranking function $f_1(x, z) = x$

Loop 2: ranking function $f_2(x, z) = z$

How Can we Fix our Approach?

```
def twoLoops2(x, z):
  while x > 0:
    x = x - 1
    z = z + x
  while z > 0:
    z = z - 1
```

Loop 1: ranking function $f_1(x, z) = x$

Loop 2: ranking function $f_2(x, z) = z$

Problem:
Loop 1 writes to z. In Loop 2, z is much larger than its initial value z_0!

How Can we Fix our Approach?

```
def twoLoops2(x, z):
  while x > 0:
    x = x - 1
    z = z + x
  while z > 0:
    z = z - 1
```

Loop 1: ranking function $f_1(x, z) = x$

Loop 2: ranking function $f_2(x, z) = z$

Problem:
Loop 1 writes to z. In Loop 2, z is much larger than its initial value z_0!
Now an oracle tells us:

How Can we Fix our Approach?

```
def twoLoops2(x, z):
  while x > 0:
    x = x - 1
    z = z + x
  while z > 0:
    z = z - 1
```

Loop 1: ranking function $f_1(x, z) = x$

Loop 2: ranking function $f_2(x, z) = z$

Problem:

Loop 1 writes to z. In Loop 2, z is much larger than its initial value z_0!

Now an oracle tells us:

Oh, when you reach Loop 2, z is at most $z_0 + x_0^2$, and x is 0.

How Can we Fix our Approach?

```
def twoLoops2(x, z):
  while x > 0:
    x = x - 1
    z = z + x

  while z > 0:
    z = z - 1
```

Loop 1: ranking function $f_1(x, z) = x$

Loop 2: ranking function $f_2(x, z) = z$

Problem:

Loop 1 writes to z. In Loop 2, z is much larger than its initial value z_0!

Now an oracle tells us:

Oh, when you reach Loop 2, z is at most $z_0 + x_0^2$, and x is 0.

So:

1. we can make at most $f_2(x, z) = z$ steps in Loop 2

How Can we Fix our Approach?

```
def twoLoops2(x, z):
  while x > 0:
    x = x - 1
    z = z + x

  while z > 0:
    z = z - 1
```

Loop 1: ranking function $f_1(x, z) = x$

Loop 2: ranking function $f_2(x, z) = z$

Problem:

Loop 1 writes to z. In Loop 2, z is much larger than its initial value z_0!

Now an oracle tells us:

Oh, when you reach Loop 2, z is at most $z_0 + x_0^2$, and x is 0.

So:

1. we can make at most $f_2(x, z) = z$ steps in Loop 2
2. when we enter Loop 2, we know $z \leq z_0 + x_0^2$ and $x = 0$

How Can we Fix our Approach?

```
def twoLoops2(x, z):
  while x > 0:
    x = x - 1
    z = z + x
  while z > 0:
    z = z - 1
```

Loop 1: ranking function $f_1(x, z) = x$

Loop 2: ranking function $f_2(x, z) = z$

Problem:

Loop 1 writes to z. In Loop 2, z is much larger than its initial value z_0!

Now an oracle tells us:

Oh, when you reach Loop 2, z is at most $z_0 + x_0^2$, and x is 0.

So:

1. we can make at most $f_2(x, z) = z$ steps in Loop 2
2. when we enter Loop 2, we know $z \leq z_0 + x_0^2$ and $x = 0$

$$\Rightarrow f_2(0, z_0 + x_0^2) = z_0 + x_0^2$$

How Can we Fix our Approach?

```
def twoLoops2(x, z):
  while x > 0:
    x = x - 1
    z = z + x

  while z > 0:
    z = z - 1
```

Loop 1: ranking function $f_1(x, z) = x$

Loop 2: ranking function $f_2(x, z) = z$

Problem:

Loop 1 writes to z. In Loop 2, z is much larger than its initial value z_0!

Now an oracle tells us:

Oh, when you reach Loop 2, z is at most $z_0 + x_0^2$, and x is 0.

So:

1. we can make at most $f_2(x, z) = z$ steps in Loop 2
2. when we enter Loop 2, we know $z \leq z_0 + x_0^2$ and $x = 0$

$\Rightarrow$ $f_2(0, z_0 + x_0^2) = z_0 + x_0^2$ gives runtime bound for Loop 2: $\mathcal{O}(z_0 + x_0^2)$

How Can we Fix our Approach?

```
def twoLoops2(x, z):
  while x > 0:
    x = x - 1
    z = z + x
  while z > 0:
    z = z - 1
```

Loop 1: ranking function $f_1(x, z) = x$

Loop 2: ranking function $f_2(x, z) = z$

Problem:

Loop 1 writes to z. In Loop 2, z is much larger than its initial value z_0!

Now an oracle tells us:

Oh, when you reach Loop 2, z is at most $z_0 + x_0^2$, and x is 0.

So:

1. we can make at most $f_2(x, z) = z$ steps in Loop 2
2. when we enter Loop 2, we know $z \leq z_0 + x_0^2$ and $x = 0$

$\Rightarrow$ $f_2(0, z_0 + x_0^2) = z_0 + x_0^2$ gives runtime bound for Loop 2: $\mathcal{O}(z_0 + x_0^2)$

Data size influences runtime.

How Can We Build such an Oracle for Size Bounds?

```
def twoLoops2(x, z):
  while x > 0:
    x = x - 1
    z = z + x
  # (*)
  while z > 0:
    z = z - 1
```

Loop 1: ranking function $f_1(x, z) = x$

Loop 2: ranking function $f_2(x, z) = z$

How Can We Build such an Oracle for Size Bounds?

```
def twoLoops2(x, z):
  while x > 0:
    x = x - 1
    z = z + x
  # (*)
  while z > 0:
    z = z - 1
```

Loop 1: ranking function $f_1(x, z) = x$

Loop 2: ranking function $f_2(x, z) = z$

Wanted: automatic oracle to tell how big z can be at (*).

How Can We Build such an Oracle for Size Bounds?

```
def twoLoops2(x, z):
  while x > 0:
    x = x - 1
    z = z + x
  # (*)
  while z > 0:
    z = z - 1
```

Loop 1: ranking function $f_1(x, z) = x$

Loop 2: ranking function $f_2(x, z) = z$

Wanted: automatic oracle to tell how big z can be at (*).

We know:

1. each time round Loop 1, x goes down by 1, from x_0 until 0

How Can We Build such an Oracle for Size Bounds?

```
def twoLoops2(x, z):
  while x > 0:
    x = x - 1
    z = z + x
  # (*)
  while z > 0:
    z = z - 1
```

Loop 1: ranking function $f_1(x, z) = x$

Loop 2: ranking function $f_2(x, z) = z$

Wanted: automatic oracle to tell how big z can be at (*).

We know:

1. each time round Loop 1, x goes down by 1, from x_0 until 0
   $\Rightarrow$ in Loop 1: $x \leq x_0$

How Can We Build such an Oracle for Size Bounds?

```
def twoLoops2(x, z):
  while x > 0:
    x = x - 1
    z = z + x
  # (*)
  while z > 0:
    z = z - 1
```

Loop 1: ranking function $f_1(x, z) = x$

Loop 2: ranking function $f_2(x, z) = z$

Wanted: automatic oracle to tell how big z can be at (*).

We know:

1. each time round Loop 1, x goes down by 1, from x_0 until 0
   $\Rightarrow$ in Loop 1: $x \leq x_0$
2. each time round Loop 1, z goes up by x ($\leq x_0$)

How Can We Build such an Oracle for Size Bounds?

```
def twoLoops2(x, z):
  while x > 0:
    x = x - 1
    z = z + x
  # (*)
  while z > 0:
    z = z - 1
```

Loop 1: ranking function $f_1(x, z) = x$

Loop 2: ranking function $f_2(x, z) = z$

Wanted: automatic oracle to tell how big z can be at (*).

We know:

1. each time round Loop 1, x goes down by 1, from x_0 until 0
   $\Rightarrow$ in Loop 1: $x \leq x_0$
2. each time round Loop 1, z goes up by x ($\leq x_0$)
3. we run through Loop 1 at most $f_1(x_0, z_0) = x_0$ times

How Can We Build such an Oracle for Size Bounds?

```
def twoLoops2(x, z):
  while x > 0:
    x = x - 1
    z = z + x
  # (*)
  while z > 0:
    z = z - 1
```

Loop 1: ranking function $f_1(x, z) = x$

Loop 2: ranking function $f_2(x, z) = z$

Wanted: automatic oracle to tell how big z can be at (*).

We know:

1. each time round Loop 1, x goes down by 1, from x_0 until 0
   $\Rightarrow$ in Loop 1: $x \leq x_0$
2. each time round Loop 1, z goes up by x ($\leq x_0$)
3. we run through Loop 1 at most $f_1(x_0, z_0) = x_0$ times

$\Rightarrow$ at (*), z will be at most $z_0 + x_0 \cdot x_0 \;=\; z_0 + x_0^2$!

How Can We Build such an Oracle for Size Bounds?

```
def twoLoops2(x, z):
  while x > 0:
    x = x - 1
    z = z + x
  # (*)
  while z > 0:
    z = z - 1
```

Loop 1: ranking function $f_1(x, z) = x$

Loop 2: ranking function $f_2(x, z) = z$

Wanted: automatic oracle to tell how big z can be at (*).

We know:

1. each time round Loop 1, x goes down by 1, from x_0 until 0
   $\Rightarrow$ in Loop 1: $x \leq x_0$
2. each time round Loop 1, z goes up by x $(\leq x_0)$
3. we run through Loop 1 at most $f_1(x_0, z_0) = x_0$ times

$\Rightarrow$ at (*), z will be at most $z_0 + x_0 \cdot x_0 \; = \; z_0 + x_0^2$!

Runtime influences data size.

Show Me More!

Example (List program)

Input: List x

ℓ_0: List y = null

ℓ_1: **while** x ≠ null **do**

  y = **new** List(x.val, y)

  x = x.next

 done

 List z = y

ℓ_2: **while** z ≠ null **do**

  List u = z.next

ℓ_3: **while** u ≠ null **do**

   z.val += u.val

   u = u.next

  done

  z = z.next

 done

Show Me More!

Example (List program)

```
Input: List x
ℓ0: List y = null
ℓ1: while x ≠ null do
        y = new List(x.val, y)
        x = x.next
    done
    List z = y
ℓ2: while z ≠ null do
        List u = z.next
ℓ3:     while u ≠ null do
            z.val += u.val
            u = u.next
        done
        z = z.next
    done
```

$x = [3, 1, 5] \quad \curvearrowright$

$y = [5, 1, 3] \quad \curvearrowright$

$z = [5 + 1 + 3,\ 1 + 3,\ 3]$

Show Me More!

Example (List program)

Input: List x

ℓ_0: List y = null

ℓ_1: **while** x ≠ null **do**

  y = **new** List(x.val, y)

  x = x.next

done

List z = y

ℓ_2: **while** z ≠ null **do**

  List u = z.next

ℓ_3: **while** u ≠ null **do**

    z.val += u.val

    u = u.next

  done

  z = z.next

done

Example (Integer abstraction)

Input: int x

ℓ_0: int y = 0

ℓ_1: **while** x > 0 **do**

  y = y + 1

  x = x − 1

done

int z = y

ℓ_2: **while** z > 0 **do**

  int u = z − 1

ℓ_3: **while** u > 0 **do**

    skip

    u = u − 1

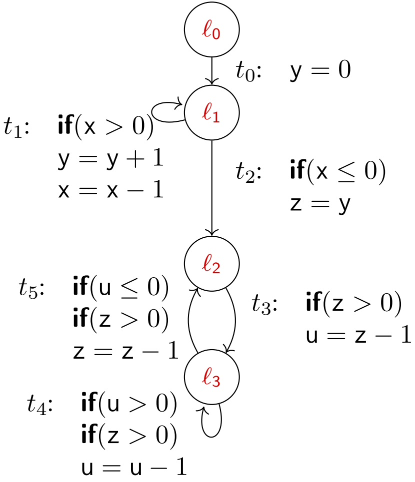
  done

  z = z − 1

done

Show Me More!

Control flow graph:



Example (Integer abstraction)

Input: `int x`

ℓ_0: `int` y = 0

ℓ_1: **while** x > 0 **do**

    y = y + 1

    x = x − 1

  done

  `int` z = y

ℓ_2: **while** z > 0 **do**

    `int` u = z − 1

ℓ_3:   **while** u > 0 **do**

      skip

      u = u − 1

    done

    z = z − 1

  done

What Does the Problem Look Like?

- **Programs** as Integer Transition Systems:
  - Locations $\mathcal{L}$: ℓ_0 start
  - Variables $\mathcal{V}$
  - Transitions $\mathcal{T}$: Formula over pre- $(x, y, \ldots)$, post-variables $(x', y', \ldots)$

    e.g., $t_5 \ = \ (\ell_3,\ u \leq 0 \wedge z > 0 \wedge z' = z - 1,\ \ell_2)$

    for $\ell_3(u, x, y, z) \longrightarrow \ell_2(u', x', y', z')\ [u \leq 0 \wedge z > 0 \wedge z' = z - 1 \wedge u' = u \wedge x' = x \wedge y' = y]$

What Do the Problem and the Solution Look Like?

- **Programs** as Integer Transition Systems:
  - Locations $\mathcal{L}$: ℓ_0 start
  - Variables $\mathcal{V}$
  - Transitions $\mathcal{T}$: Formula over pre- $(x, y, \ldots)$, post-variables $(x', y', \ldots)$

    e.g., $t_5 \;=\; (\ell_3,\; u \leq 0 \land z > 0 \land z' = z - 1,\; \ell_2)$

    for $\ell_3(u, x, y, z) \longrightarrow \ell_2(u', x', y', z')$ $[u \leq 0 \land z > 0 \land z' = z - 1 \land u' = u \land x' = x \land y' = y]$

- **Runtime complexity**:
  - $\mathcal{R}(t)$ upper bound on number of uses of $t \in \mathcal{T}$ in execution
  - $\mathcal{R}(t)$ monotonic function in $\mathcal{V}$, e.g. $|x|^2 + |y| + 1$
  - $\mathcal{R}(t)$ expresses bound in *input values*

What Do the Problem and the Solution Look Like?

- **Programs** as Integer Transition Systems:
  - Locations $\mathcal{L}$: ℓ_0 start
  - Variables $\mathcal{V}$
  - Transitions $\mathcal{T}$: Formula over pre- $(x, y, \ldots)$, post-variables $(x', y', \ldots)$

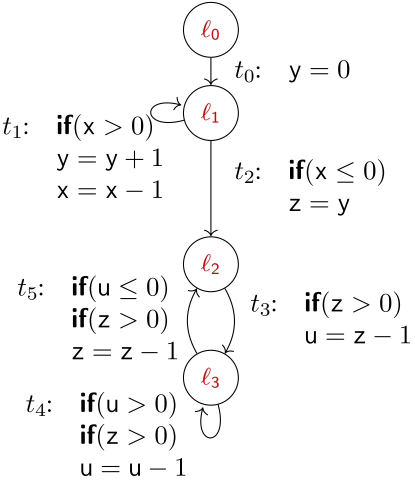
    e.g., $t_5 = (\ell_3,\ u \leq 0 \wedge z > 0 \wedge z' = z - 1,\ \ell_2)$

    for $\ell_3(u, x, y, z) \longrightarrow \ell_2(u', x', y', z')\ [u \leq 0 \wedge z > 0 \wedge z' = z - 1 \wedge u' = u \wedge x' = x \wedge y' = y]$

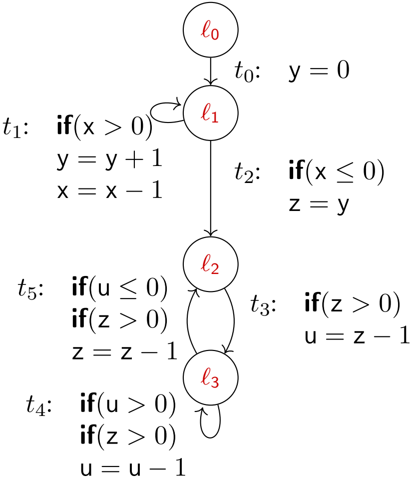
- **Runtime complexity**:
  - $\mathcal{R}(t)$ upper bound on number of uses of $t \in \mathcal{T}$ in execution
  - $\mathcal{R}(t)$ monotonic function in $\mathcal{V}$, e.g. $|x|^2 + |y| + 1$
  - $\mathcal{R}(t)$ expresses bound in *input values*

- **Size complexity**:
  - $\mathcal{S}(t, v')$ upper bound on size of $v \in \mathcal{V}$ after using $t \in \mathcal{T}$
  - $\mathcal{S}(t, v')$ monotonic function in $\mathcal{V}$
  - $\mathcal{S}(t, v')$ expresses bound in *input values*

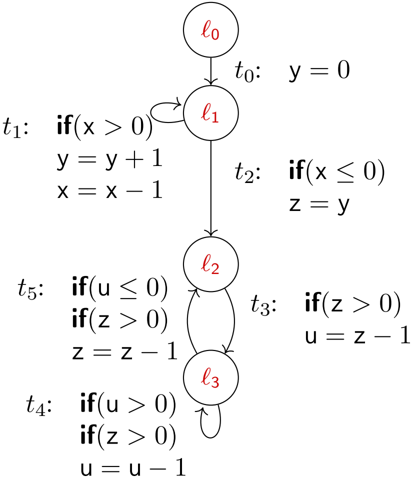
And in the Example?



And in the Example?



Goal: find complexity bounds w.r.t. the *sizes* of the input variables



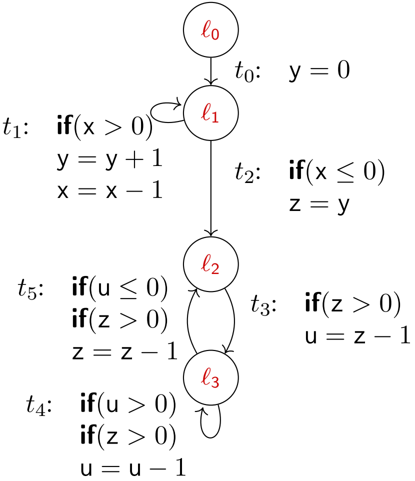
Goal: find complexity bounds w.r.t. the *sizes* of the input variables

- Runtime bound function $\mathcal{R}(t)$:

  bound on number of times that transition t occurs in executions

  e.g., $\mathcal{R}(t_1) = |x|$,
  $\mathcal{R}(t_4) = |x| + |x|^2$

And in the Example?



Goal: find complexity bounds w.r.t. the *sizes* of the input variables

- Runtime bound function $\mathcal{R}(t)$:

  bound on number of times that transition t occurs in executions

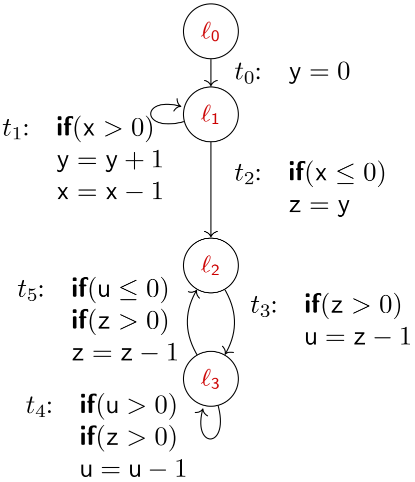
  e.g., $\mathcal{R}(t_1) = |\mathsf{x}|$,
  $\mathcal{R}(t_4) = |\mathsf{x}| + |\mathsf{x}|^2$

- Size bound function $\mathcal{S}(t, v')$:

  bound on $|v|$ after using transition t in program executions

  e.g. $\mathcal{S}(t_1, \mathsf{y}') = |\mathsf{x}|$

And in the Example?



Goal: find complexity bounds w.r.t. the *sizes* of the input variables

- Runtime bound function $\mathcal{R}(t)$:

  bound on number of times that transition t occurs in executions

  e.g., $\mathcal{R}(t_1) = |\mathsf{x}|$,
  $\mathcal{R}(t_4) = |\mathsf{x}| + |\mathsf{x}|^2$

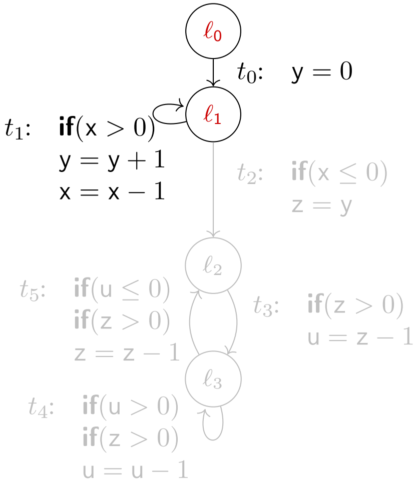
- Size bound function $\mathcal{S}(t, v')$:

  bound on $|v|$ after using transition t in program executions

  e.g. $\mathcal{S}(t_1, \mathsf{y}') = |\mathsf{x}|$

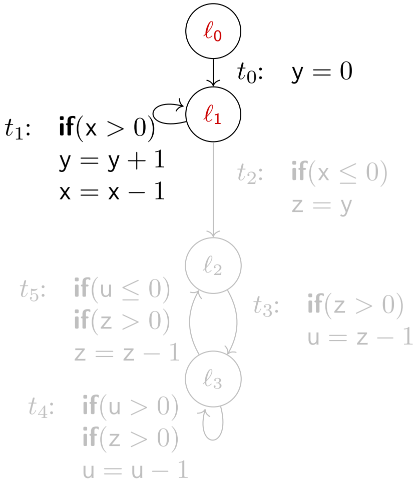
Overall runtime is bounded by $\mathcal{R}(t_1) + \ldots + \mathcal{R}(t_5) = 3 + 4 \cdot |\mathsf{x}| + |\mathsf{x}|^2$.

How Do You Know?



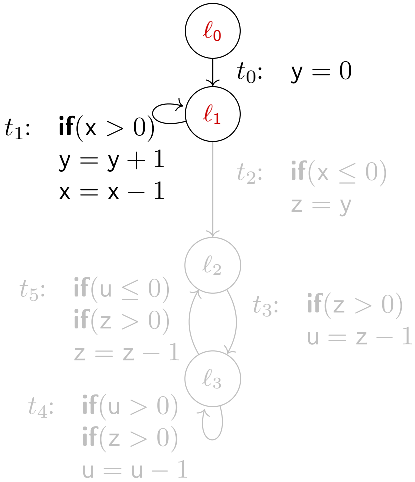
ℓ_0
t_0: y = 0
ℓ_1
t_1: **if**(x > 0)
y = y + 1
x = x − 1
t_2: **if**(x ≤ 0)
z = y
ℓ_2
t_3: **if**(z > 0)
u = z − 1
t_5: **if**(u ≤ 0)
if(z > 0)
z = z − 1
ℓ_3
t_4: **if**(u > 0)
if(z > 0)
u = u − 1

Runtime Bounds I (PRFs)



Polynomial ranking function (PRF):
$\mathcal{P} : \mathcal{L} \to \mathbb{Z}[\mathcal{V}]$ with

1. **no increase**
   No transition increases
2. **decrease**
   At least one decreases
3. **bounded**
   Bounded from below by 1



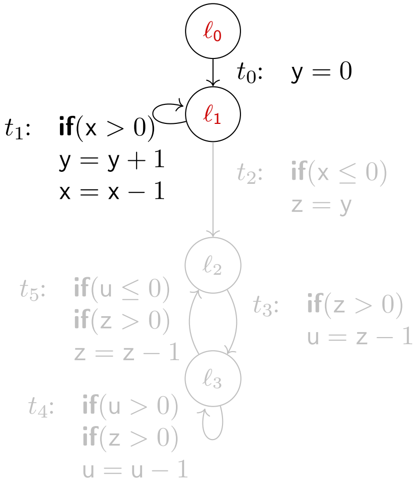
Polynomial ranking function (PRF):
$\mathcal{P} : \mathcal{L} \to \mathbb{Z}[\mathcal{V}]$ with

1. **no increase**
   No transition increases
2. **decrease**
   At least one decreases
3. **bounded**
   Bounded from below by 1

Example (PRF I)

$$\mathcal{P}_1(\ell) = x \quad \text{for all } \ell \in \mathcal{L}$$

Runtime Bounds I (PRFs)



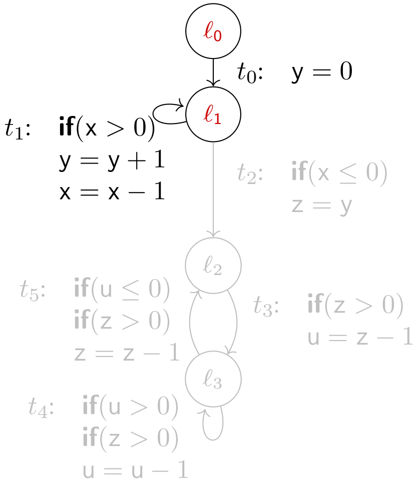
Polynomial ranking function (PRF):
$\mathcal{P} : \mathcal{L} \rightarrow \mathbb{Z}[\mathcal{V}]$ with

1. **no increase**
   No transition increases
2. **decrease**
   At least one decreases
3. **bounded**
   Bounded from below by 1

Example (PRF I)

$$\mathcal{P}_1(\ell) = x \quad \text{for all } \ell \in \mathcal{L}$$

no increase on any transition
t_1 **decreases**, **bounded**

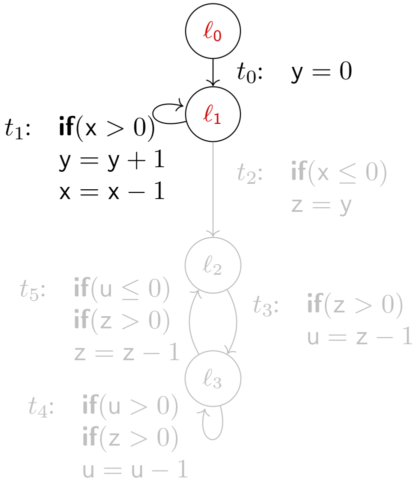


Polynomial ranking function (PRF): $\mathcal{P} : \mathcal{L} \to \mathbb{Z}[\mathcal{V}]$ with

1. **no increase**
   No transition increases
2. **decrease**
   At least one decreases
3. **bounded**
   Bounded from below by 1

Key idea: **decreasing** t used at most $\mathcal{P}(\ell_0)$ times

Runtime Bounds I (PRFs for Complexity)



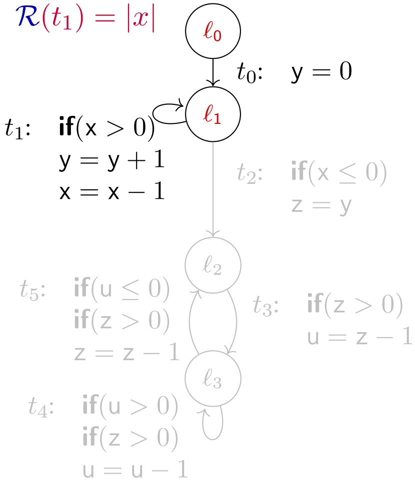
Polynomial ranking function (PRF):
$\mathcal{P} : \mathcal{L} \to \mathbb{Z}[\mathcal{V}]$ with

1. **no increase**
   No transition increases
2. **decrease**
   At least one decreases
3. **bounded**
   Bounded from below by 1

Key idea: **decreasing** t used at most $\mathcal{P}(\ell_0)$ times

$$\hookrightarrow \mathcal{R}(t) \le [\mathcal{P}(\ell_0)]$$

$[-] \equiv$ "make monotonic (on $\mathbb{N}$)"



Polynomial ranking function (PRF):
$\mathcal{P} : \mathcal{L} \to \mathbb{Z}[\mathcal{V}]$ with

1. **no increase**
   No transition increases
2. **decrease**
   At least one decreases
3. **bounded**
   Bounded from below by 1

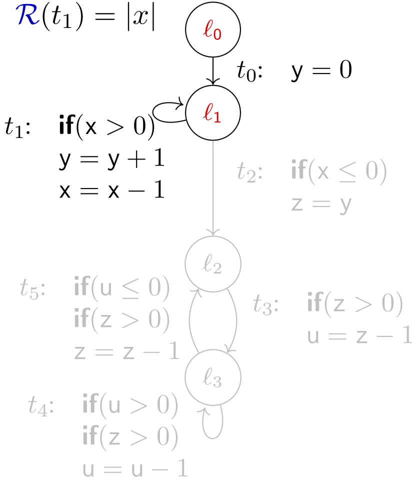
Key idea: **decreasing** t used at most $\mathcal{P}(\ell_0)$ times

$$\hookrightarrow \mathcal{R}(t) \leq [\mathcal{P}(\ell_0)]$$

$[\,-\,] \equiv$ “make monotonic (on $\mathbb{N}$)”

$\mathcal{R}(t_0) = 1$

$\mathcal{R}(t_1) = |x|$



Polynomial ranking function (PRF):
$\mathcal{P} : \mathcal{L} \to \mathbb{Z}[\mathcal{V}]$ with

1. **no increase**
   No transition increases
2. **decrease**
   At least one decreases
3. **bounded**
   Bounded from below by 1

Example (PRF II)

$$\mathcal{P}_2(\ell_0) = 1$$

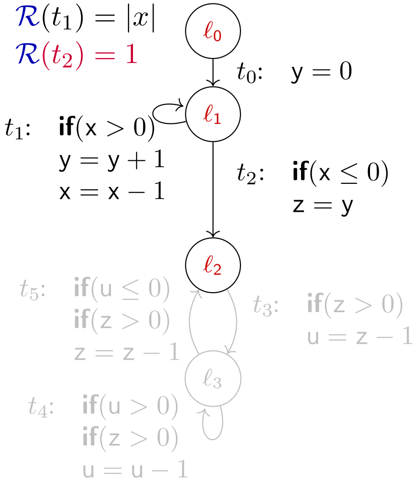
$$\mathcal{P}_2(\ell) = 0 \quad \text{for all } \ell \in \mathcal{L} \setminus \{\ell_0\}$$

no increase on any transition

t_0 **decreases**, **bounded**

Runtime Bounds I (PRFs for Complexity)

$\mathcal{R}(t_0) = 1$
$\mathcal{R}(t_1) = |x|$
$\mathcal{R}(t_2) = 1$



Polynomial ranking function (PRF):
$\mathcal{P} : \mathcal{L} \to \mathbb{Z}[\mathcal{V}]$ with

1. **no increase**
   No transition increases
2. **decrease**
   At least one decreases
3. **bounded**
   Bounded from below by 1

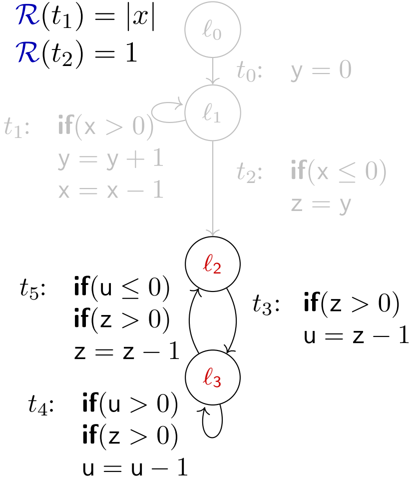
Example (PRF III)

$$\mathcal{P}_3(\ell) = 1 \quad \text{for all } \ell \in \{\ell_0, \ell_1\}$$
$$\mathcal{P}_3(\ell) = 0 \quad \text{for all } \ell \in \{\ell_2, \ell_3\}$$

no increase on any transition
t_2 **decreases**, **bounded**

Size Bounds

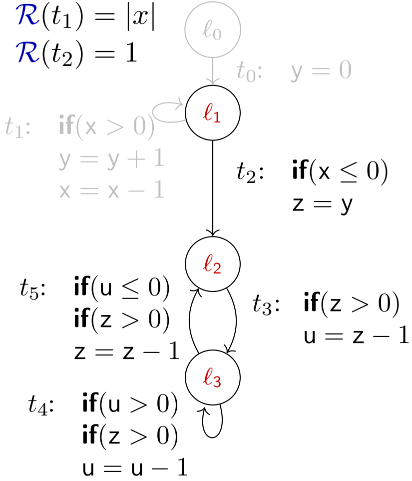
$\mathcal{R}(t_0) = 1$
$\mathcal{R}(t_1) = |x|$
$\mathcal{R}(t_2) = 1$



Second loop depends on z

Size Bounds

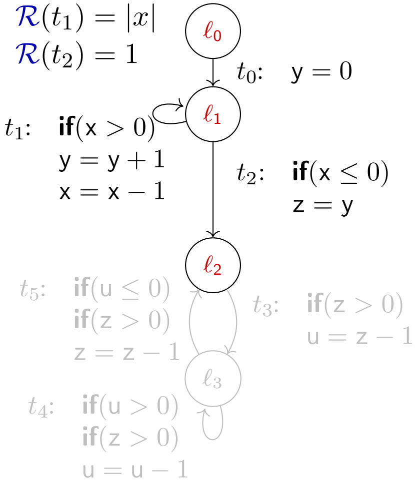
$\mathcal{R}(t_0) = 1$
$\mathcal{R}(t_1) = |x|$
$\mathcal{R}(t_2) = 1$



Second loop depends on z
$\hookrightarrow$ Compute $\mathcal{S}(t_2, z')$

Size Bounds

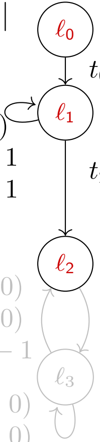
$\mathcal{R}(t_0) = 1$
$\mathcal{R}(t_1) = |x|$
$\mathcal{R}(t_2) = 1$



Second loop depends on z
$\hookrightarrow$ Compute $\mathcal{S}(t_2, z')$
... which depends on y after t_0, t_1

Size Bounds: Local

$\mathcal{R}(t_0) = 1$
$\mathcal{R}(t_1) = |x|$
$\mathcal{R}(t_2) = 1$



t_0: $\mathsf{y} = 0$

t_1: **if**$(\mathsf{x} > 0)$
$\mathsf{y} = \mathsf{y} + 1$
$\mathsf{x} = \mathsf{x} - 1$

t_2: **if**$(\mathsf{x} \leq 0)$
$\mathsf{z} = \mathsf{y}$

t_5: **if**$(\mathsf{u} \leq 0)$
if$(\mathsf{z} > 0)$
$\mathsf{z} = \mathsf{z} - 1$

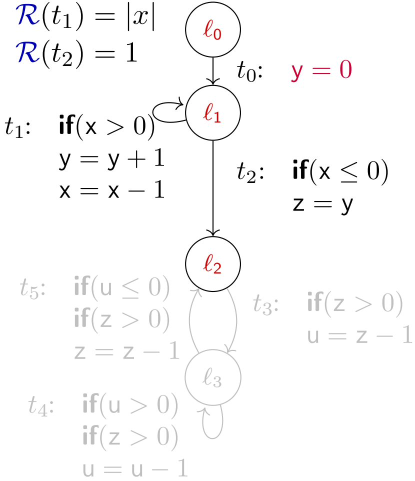
t_3: **if**$(\mathsf{z} > 0)$
$\mathsf{u} = \mathsf{z} - 1$

t_4: **if**$(\mathsf{u} > 0)$
if$(\mathsf{z} > 0)$
$\mathsf{u} = \mathsf{u} - 1$

Result Variable Graph:

Size Bounds: Local

$\mathcal{R}(t_0) = 1$
$\mathcal{R}(t_1) = |x|$
$\mathcal{R}(t_2) = 1$



$0 \geq |t_0, \mathsf{y}'|$

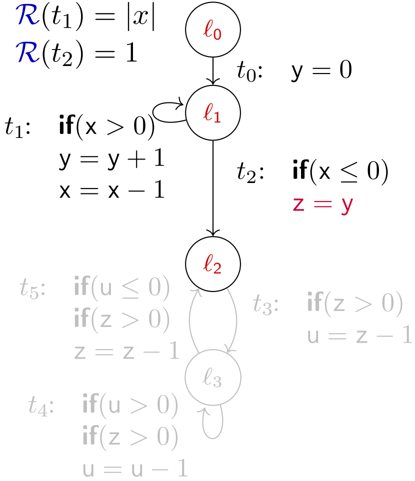
Result Variable Graph:

- Nodes $|t, v'|$, labels $S_l(t, v')$
  Change of v in *one use* of t:

$$t \implies S_l(t, v')(\mathcal{V}) \geq v'$$

Size Bounds: Local

$\mathcal{R}(t_0) = 1$
$\mathcal{R}(t_1) = |x|$
$\mathcal{R}(t_2) = 1$



$0 \geq |t_0, y'|$

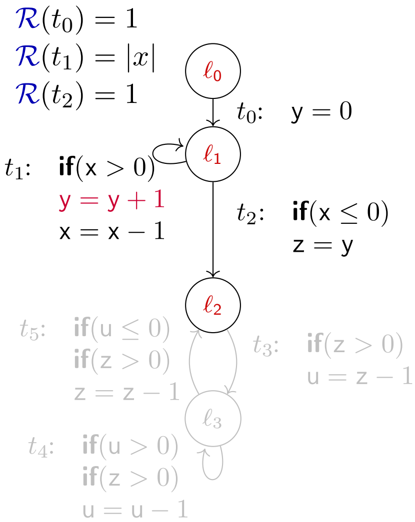
$|y| \geq |t_2, z'|$

Result Variable Graph:

- Nodes $|t, v'|$, labels $S_l(t, v')$
  Change of v in *one use* of t:

$$t \implies S_l(t, v')(\mathcal{V}) \geq v'$$

Size Bounds: Local



$$0 \geq |t_0, y'|$$

$$|y| + 1 \geq |t_1, y'|$$

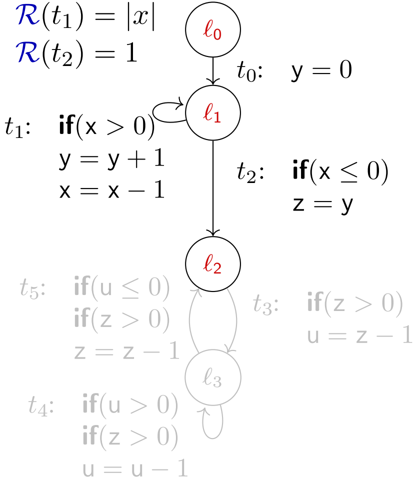
$$|y| \geq |t_2, z'|$$

Result Variable Graph:

- Nodes $|t, v'|$, labels $S_l(t, v')$
  Change of v in *one use* of t:

$$t \implies S_l(t, v')(\mathcal{V}) \geq v'$$

$\mathcal{R}(t_0) = 1$
$\mathcal{R}(t_1) = |x|$
$\mathcal{R}(t_2) = 1$



$$0 \geq |t_0, \mathsf{y}'|$$

$$|\mathsf{y}| + 1 \geq |t_1, \mathsf{y}'|$$

$$|\mathsf{y}| \geq |t_2, \mathsf{z}'|$$

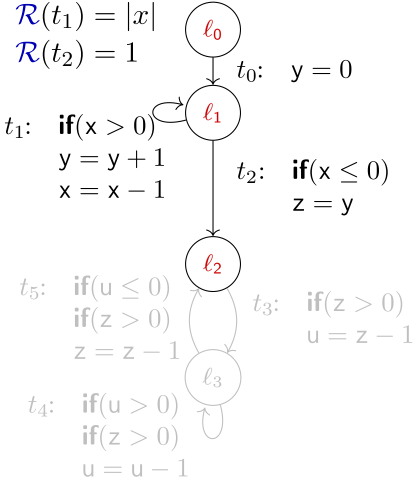
Result Variable Graph:

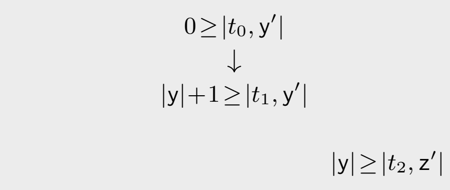
- Nodes $|t, v'|$, labels $S_l(t, v')$
  Change of v in *one use* of t:

$$t \implies S_l(t, v')(\mathcal{V}) \geq v'$$

- Edges:
  Flow of information

$\mathcal{R}(t_0) = 1$
$\mathcal{R}(t_1) = |x|$
$\mathcal{R}(t_2) = 1$





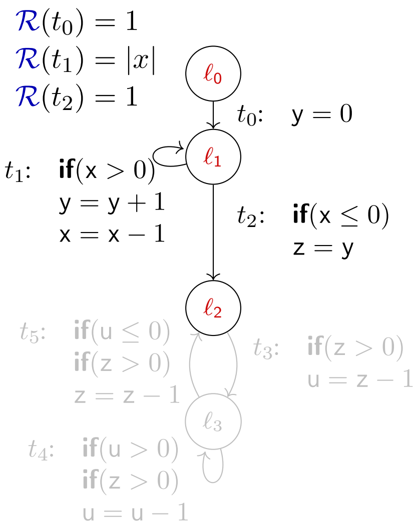
Result Variable Graph:

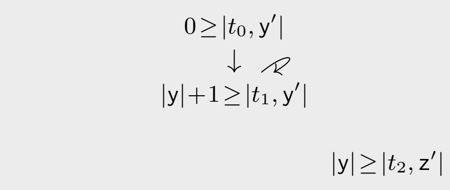
- Nodes $|t, v'|$, labels $S_l(t, v')$
  Change of v in *one use* of t:

$$t \implies S_l(t, v')(\mathcal{V}) \geq v'$$

- Edges:
  Flow of information

Size Bounds: Local





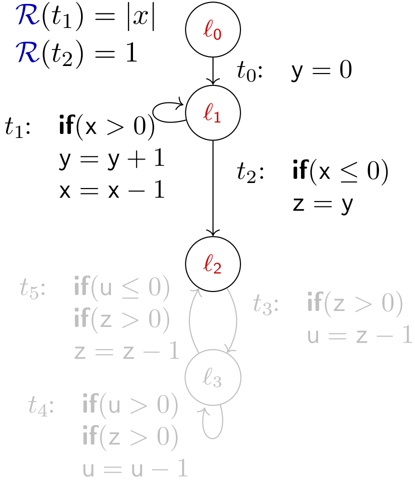
Result Variable Graph:

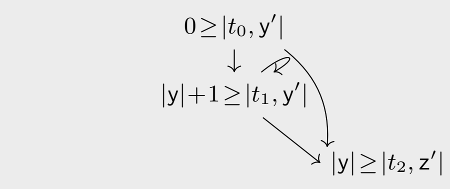
- Nodes $|t, v'|$, labels $S_l(t, v')$
  Change of v in *one use* of t:

$$t \implies S_l(t, v')(\mathcal{V}) \geq v'$$

- Edges:
  Flow of information

$\mathcal{R}(t_0) = 1$
$\mathcal{R}(t_1) = |x|$
$\mathcal{R}(t_2) = 1$





Result Variable Graph:

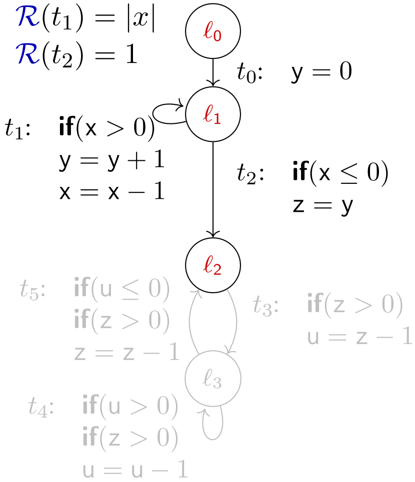
- Nodes $|t, v'|$, labels $S_l(t, v')$
  Change of v in *one use* of t:

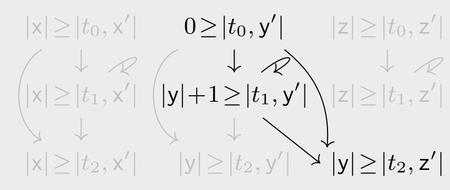
$$t \implies S_l(t, v')(\mathcal{V}) \geq v'$$

- Edges:
  Flow of information

Size Bounds: Local

$\mathcal{R}(t_0) = 1$
$\mathcal{R}(t_1) = |x|$
$\mathcal{R}(t_2) = 1$





Result Variable Graph:

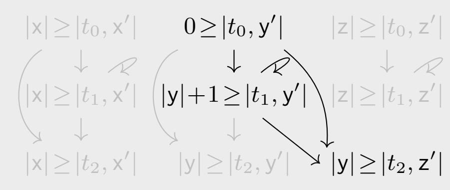
- Nodes $|t, v'|$, labels $S_l(t, v')$
  Change of v in *one use* of t:

$$t \implies S_l(t, v')(\mathcal{V}) \geq v'$$

- Edges:
  Flow of information

Size Bounds: Global

$\mathcal{R}(t_0) = 1$
$\mathcal{R}(t_1) = |x|$
$\mathcal{R}(t_2) = 1$



Result Variable Graph:

- Nodes $|t, v'|$, labels $S_l(t, v')$
  Change of v in *one use* of t:

$$t \implies S_l(t, v')(\mathcal{V}) \geq v'$$

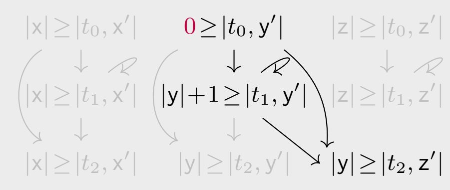
- Edges:
  Flow of information

Computing $\mathcal{S}(t, v')$:

Size Bounds: Global

$\mathcal{R}(t_0) = 1$
$\mathcal{R}(t_1) = |x|$
$\mathcal{R}(t_2) = 1$

$\mathcal{S}(t_0, y') = 0$



Result Variable Graph:

- Nodes $|t, v'|$, labels $S_l(t, v')$
  Change of v in *one use* of t:

$$t \implies S_l(t, v')(\mathcal{V}) \geq v'$$

- Edges:
  Flow of information

Computing $\mathcal{S}(t, v')$:

- No cycles: $\mathcal{S}_l$

Size Bounds: Global

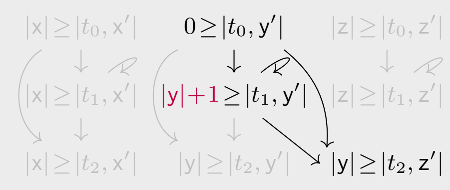
$\mathcal{R}(t_0) = 1$

$\mathcal{R}(t_1) = |x|$

$\mathcal{R}(t_2) = 1$

$\mathcal{S}(t_0, y') = 0$

$\mathcal{S}(t_1, y') = |x|$



Result Variable Graph:

- Nodes $|t, v'|$, labels $S_l(t, v')$
  Change of v in *one use* of t:

$$t \implies S_l(t, v')(\mathcal{V}) \geq v'$$

- Edges:
  Flow of information

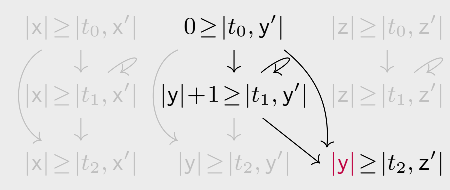
Computing $\mathcal{S}(t, v')$:

- No cycles: $\mathcal{S}_l$
- Cycles: Combine $\mathcal{R}$, $\mathcal{S}_l$
  - if $\mathcal{S}_l \approx v + c$, $c \in \mathbb{Z}$:
    $\mathcal{S}(t, v') = \mathcal{S}(\tilde{t}, v') + \mathcal{R}(t) \cdot c$
    $\tilde{t}$ predecessor of t

$\mathcal{R}(t_0) = 1$ $\quad$ $\mathcal{S}(t_0, y') = 0$

$\mathcal{R}(t_1) = |x|$ $\quad$ $\mathcal{S}(t_1, y') = |x|$

$\mathcal{R}(t_2) = 1$ $\quad$ $\mathcal{S}(t_2, z') = |x|$



Result Variable Graph:

- Nodes $|t, v'|$, labels $S_l(t, v')$
  Change of v in *one use* of t:

$$t \implies S_l(t, v')(\mathcal{V}) \geq v'$$

- Edges:
  Flow of information

Computing $\mathcal{S}(t, v')$:

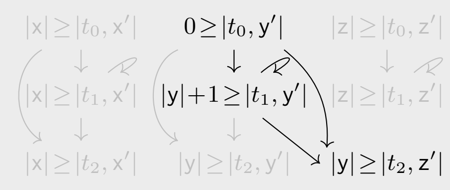
- No cycles: $\mathcal{S}_l$ (+ propagation)
- Cycles: Combine $\mathcal{R}$, $\mathcal{S}_l$
  - if $\mathcal{S}_l \approx v + c$, $c \in \mathbb{Z}$:
    $\mathcal{S}(t, v') = \mathcal{S}(\tilde{t}, v') + \mathcal{R}(t) \cdot c$
    $\tilde{t}$ predecessor of t

Size Bounds: Global

$\mathcal{R}(t_0) = 1$ $\qquad$ $\mathcal{S}(t_0, y') = 0$

$\mathcal{R}(t_1) = |x|$ $\qquad$ $\mathcal{S}(t_1, y') = |x|$

$\mathcal{R}(t_2) = 1$ $\qquad$ $\mathcal{S}(t_2, z') = |x|$



Result Variable Graph:

- Nodes $|t, v'|$, labels $S_l(t, v')$
  Change of v in *one use* of t:

$$t \implies S_l(t, v')(\mathcal{V}) \geq v'$$

- Edges:
  Flow of information

Computing $\mathcal{S}(t, v')$:

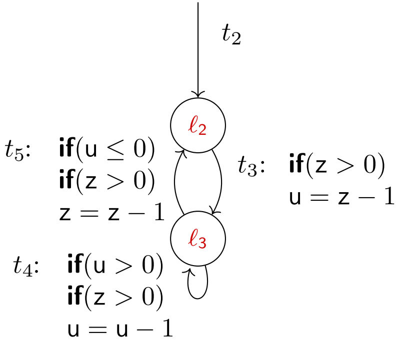
- No cycles: $\mathcal{S}_l$ (+ propagation)
- Cycles: Combine $\mathcal{R}$, $\mathcal{S}_l$
  - if $\mathcal{S}_l \approx v + c$, $c \in \mathbb{Z}$:
    $\mathcal{S}(t, v') = \mathcal{S}(\tilde{t}, v') + \mathcal{R}(t) \cdot c$
    $\tilde{t}$ predecessor of t
  - More complex: See paper

Runtime Bounds II: Modularity

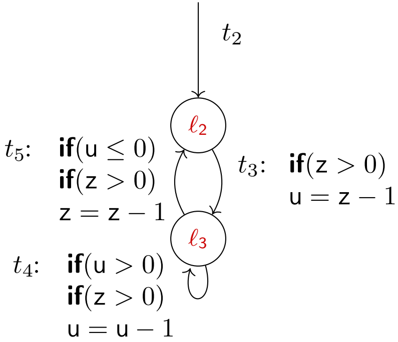
$\mathcal{R}(t_0) = 1$ $\qquad$ $\mathcal{S}(t_0, y') = 0$

$\mathcal{R}(t_1) = |x|$ $\qquad$ $\mathcal{S}(t_1, y') = |x|$

$\mathcal{R}(t_2) = 1$ $\qquad$ $\mathcal{S}(t_2, z') = |x|$



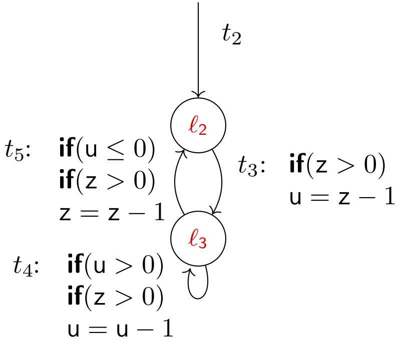
$\mathcal{R}(t_0) = 1$ $\mathcal{S}(t_0, y') = 0$
$\mathcal{R}(t_1) = |x|$ $\mathcal{S}(t_1, y') = |x|$
$\mathcal{R}(t_2) = 1$ $\mathcal{S}(t_2, z') = |x|$



Example (PRF IV)

Consider only $\mathcal{T}_1 = \{t_3, t_4, t_5\}$

$\mathcal{R}(t_0) = 1$ $\mathcal{S}(t_0, y') = 0$
$\mathcal{R}(t_1) = |x|$ $\mathcal{S}(t_1, y') = |x|$
$\mathcal{R}(t_2) = 1$ $\mathcal{S}(t_2, z') = |x|$



Example (PRF IV)

Consider only $\mathcal{T}_1 = \{t_3, t_4, t_5\}$

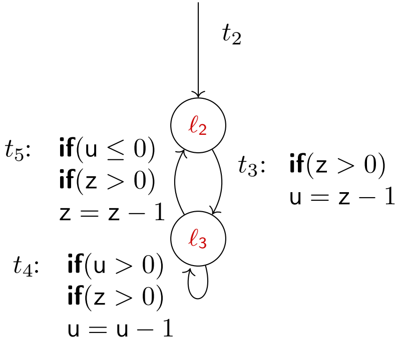
$$\mathcal{P}_4(\ell_2) = \mathcal{P}_4(\ell_3) = z$$

no increase on transitions $\mathcal{T}_1$
t_5 **decreases, bounded**

$\mathcal{R}(t_0) = 1$ $\qquad$ $\mathcal{S}(t_0, y') = 0$

$\mathcal{R}(t_1) = |x|$ $\qquad$ $\mathcal{S}(t_1, y') = |x|$

$\mathcal{R}(t_2) = 1$ $\qquad$ $\mathcal{S}(t_2, z') = |x|$



Example (PRF IV)

Consider only $\mathcal{T}_1 = \{t_3, t_4, t_5\}$

$$\mathcal{P}_4(\ell_2) = \mathcal{P}_4(\ell_3) = z$$

no increase on transitions $\mathcal{T}_1$

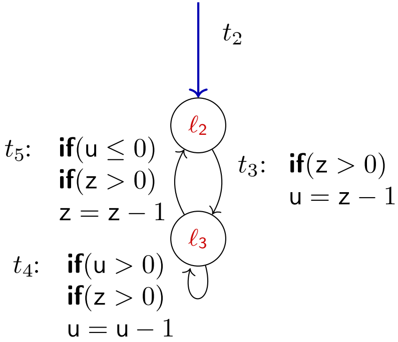
t_5 **decreases**, **bounded**

$\hookrightarrow$ **When** $\mathcal{T}_1$ reached, then z **steps**:

$\mathcal{R}(t_0) = 1$ $\quad$ $\mathcal{S}(t_0, y') = 0$

$\mathcal{R}(t_1) = |x|$ $\quad$ $\mathcal{S}(t_1, y') = |x|$

$\mathcal{R}(t_2) = 1$ $\quad$ $\mathcal{S}(t_2, z') = |x|$



Example (PRF IV)

Consider only $\mathcal{T}_1 = \{t_3, t_4, t_5\}$

$$\mathcal{P}_4(\ell_2) = \mathcal{P}_4(\ell_3) = z$$

no increase on transitions $\mathcal{T}_1$

t_5 **decreases**, **bounded**

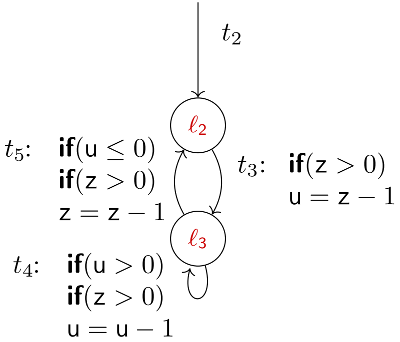
$\hookrightarrow$ **When** $\mathcal{T}_1$ reached, then z **steps**:

$\mathcal{T}_1$ reached $\mathcal{R}(t_2) = 1$ time

$\mathcal{R}(t_0) = 1$ $\mathcal{S}(t_0, y') = 0$

$\mathcal{R}(t_1) = |x|$ $\mathcal{S}(t_1, y') = |x|$

$\mathcal{R}(t_2) = 1$ $\mathcal{S}(t_2, z') = |x|$



Example (PRF IV)

Consider only $\mathcal{T}_1 = \{t_3, t_4, t_5\}$

$$\mathcal{P}_4(\ell_2) = \mathcal{P}_4(\ell_3) = z$$

no increase on transitions $\mathcal{T}_1$

t_5 **decreases**, **bounded**

$\hookrightarrow$ **When** $\mathcal{T}_1$ reached, then z **steps**:

$\mathcal{T}_1$ reached $\mathcal{R}(t_2) = 1$ time

z has size $\mathcal{S}(t_2, y') = |x|$

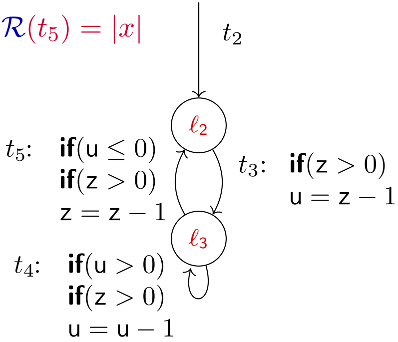
Runtime Bounds II: Modularity

$\mathcal{R}(t_0) = 1$ $\quad\quad$ $\mathcal{S}(t_0, y') = 0$

$\mathcal{R}(t_1) = |x|$ $\quad\quad$ $\mathcal{S}(t_1, y') = |x|$

$\mathcal{R}(t_2) = 1$ $\quad\quad$ $\mathcal{S}(t_2, z') = |x|$

$\mathcal{R}(t_5) = |x|$



Example (PRF IV)

Consider only $\mathcal{T}_1 = \{t_3, t_4, t_5\}$

$$\mathcal{P}_4(\ell_2) = \mathcal{P}_4(\ell_3) = z$$

no increase on transitions $\mathcal{T}_1$

t_5 **decreases**, **bounded**

$\hookrightarrow$ **When** $\mathcal{T}_1$ reached, then z **steps**:

$\mathcal{T}_1$ reached $\mathcal{R}(t_2) = 1$ time

z has size $\mathcal{S}(t_2, y') = |x|$

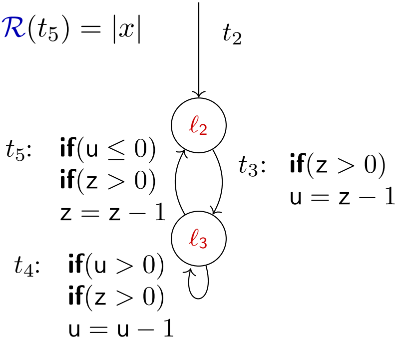
$$\hookrightarrow \mathcal{R}(t_5) = \mathcal{R}(t_2) \cdot \mathcal{S}(t_2, y') = 1 \cdot |x|$$

$\mathcal{R}(t_0) = 1$ $\quad\mathcal{S}(t_0, y') = 0$

$\mathcal{R}(t_1) = |x|$ $\quad\mathcal{S}(t_1, y') = |x|$

$\mathcal{R}(t_2) = 1$ $\quad\mathcal{S}(t_2, z') = |x|$

$\mathcal{R}(t_5) = |x|$



Example (PRF V)

Consider only $\mathcal{T}_2 = \{t_3, t_4\}$

$$\mathcal{P}_4(\ell_2) = 1 \quad \mathcal{P}_4(\ell_3) = 0$$

no increase on transitions $\mathcal{T}_2$

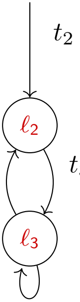
t_3 **decreases**, **bounded**

$\mathcal{R}(t_0) = 1$ $\quad$ $\mathcal{S}(t_0, y') = 0$

$\mathcal{R}(t_1) = |x|$ $\quad$ $\mathcal{S}(t_1, y') = |x|$

$\mathcal{R}(t_2) = 1$ $\quad$ $\mathcal{S}(t_2, z') = |x|$

$\mathcal{R}(t_5) = |x|$



t_5: **if**(u ≤ 0)
if(z > 0)
z $=$ z $- 1$

t_3: **if**(z > 0)
u $=$ z $- 1$

t_4: **if**(u > 0)
if(z > 0)
u $=$ u $- 1$

Example (PRF V)

Consider only $\mathcal{T}_2 = \{t_3, t_4\}$

$$\mathcal{P}_4(\ell_2) = 1 \quad \mathcal{P}_4(\ell_3) = 0$$

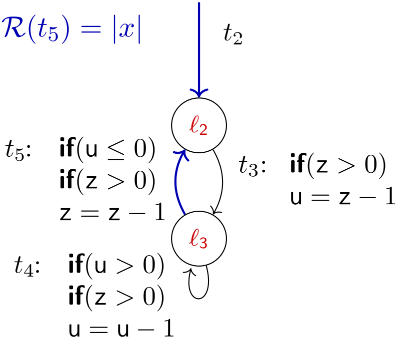
no increase on transitions $\mathcal{T}_2$
t_3 **decreases**, **bounded**

$\hookrightarrow$ **When** $\mathcal{T}_2$ reached, then 1 **step**:

Runtime Bounds II: Modularity

$\mathcal{R}(t_0) = 1$ $\qquad \mathcal{S}(t_0, y') = 0$
$\mathcal{R}(t_1) = |x|$ $\qquad \mathcal{S}(t_1, y') = |x|$
$\mathcal{R}(t_2) = 1$ $\qquad \mathcal{S}(t_2, z') = |x|$

$\mathcal{R}(t_5) = |x|$



Example (PRF V)

Consider only $\mathcal{T}_2 = \{t_3, t_4\}$

$$\mathcal{P}_4(\ell_2) = 1 \quad \mathcal{P}_4(\ell_3) = 0$$

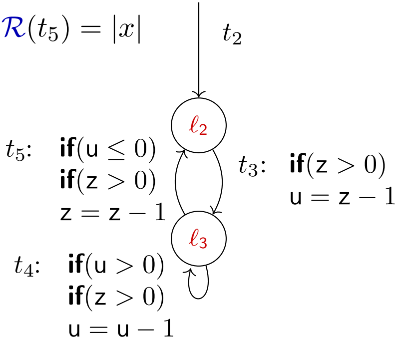
no increase on transitions $\mathcal{T}_2$
t_3 **decreases**, **bounded**

$\hookrightarrow$ **When** $\mathcal{T}_2$ reached, then 1 **step**:

$\mathcal{T}_2$ reached
$\mathcal{R}(t_2) = 1$ time and
$\mathcal{R}(t_5) = |x|$ times

$\mathcal{R}(t_0) = 1$ $\mathcal{S}(t_0, y') = 0$
$\mathcal{R}(t_1) = |x|$ $\mathcal{S}(t_1, y') = |x|$
$\mathcal{R}(t_2) = 1$ $\mathcal{S}(t_2, z') = |x|$
$\mathcal{R}(t_3) = |x| + 1$

$\mathcal{R}(t_5) = |x|$



Example (PRF V)

Consider only $\mathcal{T}_2 = \{t_3, t_4\}$

$$\mathcal{P}_4(\ell_2) = 1 \quad \mathcal{P}_4(\ell_3) = 0$$

no increase on transitions $\mathcal{T}_2$
t_3 **decreases**, **bounded**

$\hookrightarrow$ **When** $\mathcal{T}_2$ reached, then 1 **step**:

$\mathcal{T}_2$ reached
$\mathcal{R}(t_2) = 1$ time and
$\mathcal{R}(t_5) = |x|$ times

$$\hookrightarrow \mathcal{R}(t_3) = \mathcal{R}(t_2) \cdot 1 + \mathcal{R}(t_5) \cdot 1$$
$$= 1 \cdot 1 + |x| \cdot 1$$

$\mathcal{R}(t_0) = 1$

$\mathcal{R}(t_1) = |x|$

$\mathcal{R}(t_2) = 1$

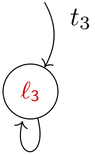
$\mathcal{R}(t_3) = |x| + 1$

$\mathcal{R}(t_5) = |x|$

$\mathcal{S}(t_0, y') = 0$

$\mathcal{S}(t_1, y') = |x|$

$\mathcal{S}(t_2, z') = |x|$



t_4: **if**(u > 0)
if(z > 0)
u $=$ u $- 1$

Example (PRF VI)

Consider only $\mathcal{T}_3 = \{t_4\}$

$$\mathcal{P}_5(\ell_3) = u$$

no increase on transitions $\mathcal{T}_3$

t_4 **decreases**, **bounded**

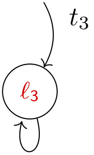
$\mathcal{R}(t_0) = 1$ $\quad$ $\mathcal{S}(t_0, y') = 0$

$\mathcal{R}(t_1) = |x|$ $\quad$ $\mathcal{S}(t_1, y') = |x|$

$\mathcal{R}(t_2) = 1$ $\quad$ $\mathcal{S}(t_2, z') = |x|$

$\mathcal{R}(t_3) = |x| + 1$

$\mathcal{R}(t_5) = |x|$



t_4: **if**(u $>$ 0)
if(z $>$ 0)
u $=$ u $-$ 1

Example (PRF VI)

Consider only $\mathcal{T}_3 = \{t_4\}$

$$\mathcal{P}_5(\ell_3) = u$$

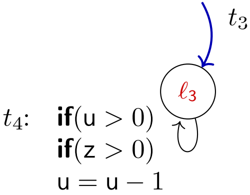
no increase on transitions $\mathcal{T}_3$
t_4 **decreases**, **bounded**

$\hookrightarrow$ **When** $\mathcal{T}_3$ reached, then u **steps**:

Runtime Bounds II: Modularity

$\mathcal{R}(t_0) = 1$ $\qquad \mathcal{S}(t_0, y') = 0$
$\mathcal{R}(t_1) = |x|$ $\qquad \mathcal{S}(t_1, y') = |x|$
$\mathcal{R}(t_2) = 1$ $\qquad \mathcal{S}(t_2, z') = |x|$
$\mathcal{R}(t_3) = |x| + 1$

$\mathcal{R}(t_5) = |x|$



Example (PRF VI)

Consider only $\mathcal{T}_3 = \{t_4\}$

$$\mathcal{P}_5(\ell_3) = u$$

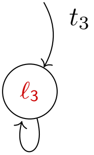
no increase on transitions $\mathcal{T}_3$
t_4 **decreases**, **bounded**

$\hookrightarrow$ **When** $\mathcal{T}_3$ reached, then u **steps**:

$\mathcal{T}_3$ reached $\mathcal{R}(t_3) = |x| + 1$ times

$\mathcal{R}(t_0) = 1$ $\mathcal{S}(t_0, y') = 0$
$\mathcal{R}(t_1) = |x|$ $\mathcal{S}(t_1, y') = |x|$
$\mathcal{R}(t_2) = 1$ $\mathcal{S}(t_2, z') = |x|$
$\mathcal{R}(t_3) = |x| + 1$

$\mathcal{R}(t_5) = |x|$



t_4: **if**(u > 0)
if(z > 0)
u $=$ u $- 1$

Example (PRF VI)

Consider only $\mathcal{T}_3 = \{t_4\}$

$$\mathcal{P}_5(\ell_3) = u$$

no increase on transitions $\mathcal{T}_3$
t_4 **decreases**, **bounded**

$\hookrightarrow$ **When** $\mathcal{T}_3$ reached, then u **steps**:

$\mathcal{T}_3$ reached $\mathcal{R}(t_3) = |x| + 1$ times

u has size $\mathcal{S}(t_3, u')$

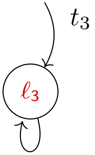
$\mathcal{R}(t_0) = 1$ $\quad\mathcal{S}(t_0, y') = 0$

$\mathcal{R}(t_1) = |x|$ $\quad\mathcal{S}(t_1, y') = |x|$

$\mathcal{R}(t_2) = 1$ $\quad\mathcal{S}(t_2, z') = |x|$

$\mathcal{R}(t_3) = |x| + 1$ $\quad\mathcal{S}(t_3, u') = |x|$

$\mathcal{R}(t_5) = |x|$



t_4: **if**(u > 0)
if(z > 0)
u $=$ u $- 1$

Example (PRF VI)

Consider only $\mathcal{T}_3 = \{t_4\}$

$$\mathcal{P}_5(\ell_3) = u$$

no increase on transitions $\mathcal{T}_3$
t_4 **decreases**, **bounded**

$\hookrightarrow$ **When** $\mathcal{T}_3$ reached, then u **steps**:

$\mathcal{T}_3$ reached $\mathcal{R}(t_3) = |x| + 1$ times

u has size $\mathcal{S}(t_3, u') = |x|$

$\mathcal{R}(t_0) = 1$ $\quad$ $\mathcal{S}(t_0, y') = 0$

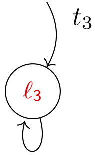
$\mathcal{R}(t_1) = |x|$ $\quad$ $\mathcal{S}(t_1, y') = |x|$

$\mathcal{R}(t_2) = 1$ $\quad$ $\mathcal{S}(t_2, z') = |x|$

$\mathcal{R}(t_3) = |x| + 1$ $\quad$ $\mathcal{S}(t_3, u') = |x|$

$\mathcal{R}(t_4) = |x|^2 + |x|$

$\mathcal{R}(t_5) = |x|$



t_4: **if**(u $>$ 0)
if(z $>$ 0)
u $=$ u $-$ 1

Example (PRF VI)

Consider only $\mathcal{T}_3 = \{t_4\}$

$$\mathcal{P}_5(\ell_3) = u$$

no increase on transitions $\mathcal{T}_3$
t_4 **decreases**, **bounded**

$\hookrightarrow$ **When** $\mathcal{T}_3$ reached, then u **steps**:

$\mathcal{T}_3$ reached $\mathcal{R}(t_3) = |x| + 1$ times

u has size $\mathcal{S}(t_3, u') = |x|$

$$\hookrightarrow \mathcal{R}(t_4) = \mathcal{R}(t_3) \cdot \mathcal{S}(t_3, u')$$
$$= (|x| + 1) \cdot |x|$$

TimeBounds: Procedure

TimeBounds($\mathcal{R}, \mathcal{S}$)

Input: Runtime bounds $\mathcal{R}$, Size bounds $\mathcal{S}$

$\mathcal{T}' \leftarrow \{t \in \mathcal{T} \mid \mathcal{R}(t) \text{ unbounded}\}$

$\mathcal{P} \leftarrow \text{synthPRF}(\mathcal{T}')$

$\mathcal{L}_\downarrow \leftarrow \text{entryLocations}(\mathcal{T}')$

$\mathcal{T}_\ell \leftarrow \text{leadingTo}(\ell, \mathcal{T} \setminus \mathcal{T}')$

$\mathcal{R}' \leftarrow \mathcal{R}$

for all $t \in \mathcal{T}'$ decreasing under $\mathcal{P}$ **do**

$\mathcal{R}'(t) \leftarrow \sum_{\ell \in \mathcal{L}_\downarrow, \tilde{t} \in \mathcal{T}_\ell} \mathcal{R}(\tilde{t}) \cdot [\mathcal{P}(\ell)](\mathcal{S}(\tilde{t}, v_1'), \ldots, \mathcal{S}(\tilde{t}, v_n'))$

end for

Output: $\mathcal{R}'$

SizeBoundsTriv$(\mathcal{R}, \mathcal{S}, C)$

Input: Runtime bounds $\mathcal{R}$, Size bounds $\mathcal{S}$, $C = \{|t, v'|\}$

$$\mathcal{T}_t \leftarrow \mathsf{leadingTo}(t, \mathcal{T})$$
$$\mathcal{S}' \leftarrow \mathcal{S}$$
$$\mathcal{S}'(t, v') \leftarrow \max\{\mathcal{S}_l(t, v')(\mathcal{S}(\tilde{t}, v'_1), \ldots, \mathcal{S}(\tilde{t}, v'_n)) \mid \tilde{t} \in \mathcal{T}_t\}$$

Output: $\mathcal{S}'$

SizeBounds: Procedure

SizeBoundsTriv($\mathcal{R}, \mathcal{S}, C$)

Input: Runtime bounds $\mathcal{R}$, Size bounds $\mathcal{S}$, $C = \{|t, v'|\}$

$$\mathcal{T}_t \leftarrow \text{leadingTo}(t, \mathcal{T})$$

$$\mathcal{S}' \leftarrow \mathcal{S}$$

$$\mathcal{S}'(t, v') \leftarrow \max\{\mathcal{S}_l(t, v')(\mathcal{S}(\tilde{t}, v'_1), \ldots, \mathcal{S}(\tilde{t}, v'_n)) \mid \tilde{t} \in \mathcal{T}_t\}$$

Output: $\mathcal{S}'$

SizeBoundsNonTriv($\mathcal{R}, \mathcal{S}, C$)

Case C non-trivial Strongly Connected Component: See paper

AlternatingCompl: Overall Procedure

AlternatingCompl($\mathcal{T}, \mathcal{V}$)

Input: Program of transitions $\mathcal{T}$, variables $\mathcal{V}$

```
  R ← unboundedTimeCompl(T)
  S ← unboundedSizeCompl(T, V)
  while R, S have unbounded elements do
    R ← TimeBounds(R, S)
    for all C SCC of RVG(T, V) do
      S ← SizeBounds(R, S, C)
    end for
  end while
```

Output: $\mathcal{R}$, $\mathcal{S}$

Are There Other Techniques and Tools?

- Using techniques from termination proving: ABC[2], AProVE, CoFloCo[3], COSTA/PUBS[4], Loopus[5], Rank[6], TcT[7], ...

---

[2] R. Blanc, T. Henzinger, L. Kovács: *ABC: Algebraic Bound Computation for Loops*, LPAR (Dakar) '10

[3] A. Flores-Montoya and R. Hähnle: *Resource Analysis of Complex Programs with Cost Equations*, APLAS '14

[4] E. Albert, P. Arenas, S. Genaim, G. Puebla, D.Zanardini: *Cost analysis of object-oriented bytecode programs*, TCS '12

[5] M. Sinn, F. Zuleger, H. Veith: *A Simple and Scalable Static Analysis for Bound Analysis and Amortized Complexity Analysis*, CAV '14

[6] C. Alias, A. Darte, P. Feautrier, L. Gonnord: *Multi-dimensional Rankings, Program Termination, and Complexity Bounds of Flowchart Programs*, SAS '10

[7] M. Avanzini, G. Moser, M. Schaper: *TcT: Tyrolean Complexity Tool*, TACAS '16

Are There Other Techniques and Tools?

- Using techniques from termination proving: ABC[2], AProVE, CoFloCo[3], COSTA/PUBS[4], Loopus[5], Rank[6], TcT[7], ...
- Using invariant generation: SPEED[8]

---

[2] R. Blanc, T. Henzinger, L. Kovács: *ABC: Algebraic Bound Computation for Loops*, LPAR (Dakar) '10

[3] A. Flores-Montoya and R. Hähnle: *Resource Analysis of Complex Programs with Cost Equations*, APLAS '14

[4] E. Albert, P. Arenas, S. Genaim, G. Puebla, D.Zanardini: *Cost analysis of object-oriented bytecode programs*, TCS '12

[5] M. Sinn, F. Zuleger, H. Veith: *A Simple and Scalable Static Analysis for Bound Analysis and Amortized Complexity Analysis*, CAV '14

[6] C. Alias, A. Darte, P. Feautrier, L. Gonnord: *Multi-dimensional Rankings, Program Termination, and Complexity Bounds of Flowchart Programs*, SAS '10

[7] M. Avanzini, G. Moser, M. Schaper: *TcT: Tyrolean Complexity Tool*, TACAS '16

[8] S. Gulwani, K. Mehro, T. Chilimbi: *SPEED: precise and efficient static estimation of program computational complexity*, POPL '09

Are There Other Techniques and Tools?

- Using techniques from termination proving: ABC[2], AProVE, CoFloCo[3], COSTA/PUBS[4], Loopus[5], Rank[6], TcT[7], ...
- Using invariant generation: SPEED[8]
- Using type-based amortised analysis:[9] RAML[10], ...

[2] R. Blanc, T. Henzinger, L. Kovács: *ABC: Algebraic Bound Computation for Loops*, LPAR (Dakar) '10

[3] A. Flores-Montoya and R. Hähnle: *Resource Analysis of Complex Programs with Cost Equations*, APLAS '14

[4] E. Albert, P. Arenas, S. Genaim, G. Puebla, D.Zanardini: *Cost analysis of object-oriented bytecode programs*, TCS '12

[5] M. Sinn, F. Zuleger, H. Veith: *A Simple and Scalable Static Analysis for Bound Analysis and Amortized Complexity Analysis*, CAV '14

[6] C. Alias, A. Darte, P. Feautrier, L. Gonnord: *Multi-dimensional Rankings, Program Termination, and Complexity Bounds of Flowchart Programs*, SAS '10

[7] M. Avanzini, G. Moser, M. Schaper: *TcT: Tyrolean Complexity Tool*, TACAS '16

[8] S. Gulwani, K. Mehro, T. Chilimbi: *SPEED: precise and efficient static estimation of program computational complexity*, POPL '09

[9] J. Hoffmann, S. Jost: *Two decades of automatic amortized resource analysis*, MSCS '22

[10] J. Hoffmann, K. Aehlig, M. Hofmann: *Resource Aware ML*, CAV '12

Did You Ever Test That?

Prototype: KoAT, using Microsoft's SMT solver Z3 (Z3 on github: https://github.com/Z3Prover/z3) to find PRFs, size bounds, ...

Did You Ever Test That?

Prototype: KoAT, using Microsoft's SMT solver Z3 (Z3 on github: https://github.com/Z3Prover/z3) to find PRFs, size bounds, ...

682 examples, taken from

- prior evaluations (of ABC, Loopus, PUBS/COSTA, Rank, SPEED)
- termination benchmarks (of T2, AProVE)
- examples from our article describing the techniques

Did You Ever Test That?

Prototype: KoAT, using Microsoft's SMT solver Z3 (Z3 on github: https://github.com/Z3Prover/z3) to find PRFs, size bounds, ...

682 examples, taken from

- prior evaluations (of ABC, Loopus, PUBS/COSTA, Rank, SPEED)
- termination benchmarks (of T2, AProVE)
- examples from our article describing the techniques

Tool	1	$\log n$	n	$n \log n$	n^2	n^3	$n^{>3}$	EXP	No res.	Time
KoAT	131	0	167	0	78	7	3	18	285	0.7 s
CoFloCo	117	0	153	0	66	9	2	0	342	1.3 s
Loopus	117	0	130	0	49	5	5	0	383	0.2 s
KoAT-TACAS'14	118	0	127	0	50	0	3	0	391	1.1 s
PUBS	109	4	127	6	24	8	0	7	404	0.8 s
Rank	56	0	16	0	8	1	0	0	608	0.1 s

- timeout 60 s
- *Time* is average runtime for successful proof

Which Tool Should I Be Using, Then?

Comparing KoAT directly to other tools (wrt asymptotic bounds)

Compared tool	more precise	less precise
CoFloCo	31	80
KoAT-TACAS'14	0	118
PUBS	46	134
Loopus	16	117
Rank	5	327

$\Rightarrow$ each tool has its own strengths and weaknesses

So, Is That Everything?

Extensions implemented:

- Recursion (beyond tail recursion)

So, Is That Everything?

Extensions implemented:

- Recursion (beyond tail recursion)
- Exponential data (e.g., **while** $\mathsf{x} > 0$ **do** $\mathsf{y} = 2 \cdot \mathsf{y}$; $\mathsf{x} - -$; **done**)

So, Is That Everything?

Extensions implemented:

- Recursion (beyond tail recursion)
- Exponential data (e.g., **while** x > 0 **do** y $= 2 \cdot$ y; x $--$; **done**)
- Exponential calls (e.g., $f(n) = f(n-1) + f(n-2)$)

So, Is That Everything?

Extensions implemented:

- Recursion (beyond tail recursion)
- Exponential data (e.g., **while** x > 0 **do** y $= 2 \cdot$ y; x $- -$; **done**)
- Exponential calls (e.g., $f(n) = f(n-1) + f(n-2)$)
- Methods handled independently, composing results at call sites

So, Is That Everything?

Extensions implemented:

- Recursion (beyond tail recursion)
- Exponential data (e.g., **while** x > 0 **do** y $= 2 \cdot$ y; x $- -$; **done**)
- Exponential calls (e.g., $f(n) = f(n-1) + f(n-2)$)
- Methods handled independently, composing results at call sites
- Other cost measures (e.g., network traffic, energy usage, ...)
  $\longrightarrow$ annotate transitions with *cost* of transition
  (so far: each transition costs 1)

So, Is That Everything?

Extensions implemented:

- Recursion (beyond tail recursion)
- Exponential data (e.g., **while** x > 0 **do** y $= 2 \cdot$ y; x $--$; **done**)
- Exponential calls (e.g., $f(n) = f(n-1) + f(n-2)$)
- Methods handled independently, composing results at call sites
- Other cost measures (e.g., network traffic, energy usage, . . .)
  $\longrightarrow$ annotate transitions with *cost* of transition
  (so far: each transition costs 1)

http://aprove.informatik.rwth-aachen.de/eval/IntegerComplexity-Journal

Where Can I Learn More? Current Developments

- Precise handling of loops with computable complexity in the KoAT approach[11]

[11] N. Lommen, F. Meyer, J. Giesl: *Automatic Complexity Analysis of Integer Programs via Triangular Weakly Non-Linear Loops*, IJCAR '22

Where Can I Learn More? Current Developments

- Precise handling of loops with computable complexity in the KoAT approach[11]
- Inference of **lower** bounds for worst-case runtime complexity[12]: LoAT[13]

[11] N. Lommen, F. Meyer, J. Giesl: *Automatic Complexity Analysis of Integer Programs via Triangular Weakly Non-Linear Loops*, IJCAR '22

[12] F. Frohn, M. Naaf, M. Brockschmidt, J. Giesl: *Inferring Lower Runtime Bounds for Integer Programs*, TOPLAS '20

[13] F. Frohn, J. Giesl: *Proving Non-Termination and Lower Runtime Bounds with LoAT (System Description)*, IJCAR '22

Where Can I Learn More? Current Developments

- Precise handling of loops with computable complexity in the KoAT approach[11]
- Inference of **lower** bounds for worst-case runtime complexity[12]: LoAT[13]
- Cost analysis for Java programs via Integer Transition Systems[14]

---

[11] N. Lommen, F. Meyer, J. Giesl: *Automatic Complexity Analysis of Integer Programs via Triangular Weakly Non-Linear Loops*, IJCAR '22
[12] F. Frohn, M. Naaf, M. Brockschmidt, J. Giesl: *Inferring Lower Runtime Bounds for Integer Programs*, TOPLAS '20
[13] F. Frohn, J. Giesl: *Proving Non-Termination and Lower Runtime Bounds with LoAT (System Description)*, IJCAR '22
[14] F. Frohn, J. Giesl: *Complexity Analysis for Java with AProVE*, iFM '17

Where Can I Learn More? Current Developments

- Precise handling of loops with computable complexity in the KoAT approach[11]
- Inference of **lower** bounds for worst-case runtime complexity[12]: LoAT[13]
- Cost analysis for Java programs via Integer Transition Systems[14]
- Cost analysis for **probabilistic** programs[15][16][17]

---

[11] N. Lommen, F. Meyer, J. Giesl: *Automatic Complexity Analysis of Integer Programs via Triangular Weakly Non-Linear Loops*, IJCAR '22
[12] F. Frohn, M. Naaf, M. Brockschmidt, J. Giesl: *Inferring Lower Runtime Bounds for Integer Programs*, TOPLAS '20
[13] F. Frohn, J. Giesl: *Proving Non-Termination and Lower Runtime Bounds with LoAT (System Description)*, IJCAR '22
[14] F. Frohn, J. Giesl: *Complexity Analysis for Java with AProVE*, iFM '17
[15] P. Wang, H. Fu, A. Goharshady, K. Chatterjee, X. Qin, W. Shi: *Cost analysis of nondeterministic probabilistic programs*, PLDI '19
[16] F. Meyer, M. Hark, J. Giesl: *Inferring Expected Runtimes of Probabilistic Integer Programs Using Expected Sizes*, TACAS '21
[17] L. Leutgeb, G. Moser, F. Zuleger: *Automated Expected Amortised Cost Analysis of Probabilistic Data Structures*, CAV '22

Complexity of Integer Programs: What to Take Home?

Key insights:

- Data size influences runtime
- Runtime influences data size
- *Other influences minor*

Complexity of Integer Programs: What to Take Home?

Key insights:

- Data size influences runtime
- Runtime influences data size
- *Other influences minor*

Solution:

- Alternating size/runtime analysis
- Modularity by using *only* these results

II.2 Complexity Analysis for Term Rewriting

What is *Term Rewriting*?

(1) Core functional programming language
without many restrictions (and features) of “real” FP:

What is *Term Rewriting*?

(1) Core functional programming language

without many restrictions (and features) of “real” FP:

- first-order (usually)
- no fixed evaluation strategy
- untyped
- no pre-defined data structures (integers, arrays, ...)

What is *Term Rewriting*?

(1) Core functional programming language

without many restrictions (and features) of "real" FP:

- first-order (usually)
- no fixed evaluation strategy
- untyped
- no pre-defined data structures (integers, arrays, ...)

(2) Syntactic approach for reasoning in equational first-order logic

What is *Term Rewriting*?

(1) Core functional programming language

without many restrictions (and features) of "real" FP:

- first-order (usually)
- no fixed evaluation strategy
- untyped
- no pre-defined data structures (integers, arrays, ...)

(2) Syntactic approach for reasoning in equational first-order logic

Example (Term Rewrite System (TRS) $\mathcal{R}$)

$$\mathsf{double}(\mathsf{0}) \to \mathsf{0}$$

$$\mathsf{double}(\mathsf{s}(x)) \to \mathsf{s}(\mathsf{s}(\mathsf{double}(x)))$$

What is *Term Rewriting*?

(1) Core functional programming language

without many restrictions (and features) of "real" FP:

- first-order (usually)
- no fixed evaluation strategy
- untyped
- no pre-defined data structures (integers, arrays, ...)

(2) Syntactic approach for reasoning in equational first-order logic

Example (Term Rewrite System (TRS) $\mathcal{R}$)

$$\mathsf{double}(\mathsf{0}) \to \mathsf{0}$$

$$\mathsf{double}(\mathsf{s}(x)) \to \mathsf{s}(\mathsf{s}(\mathsf{double}(x)))$$

Compute "double of 3 is 6":

$$\mathsf{double}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{0}))))$$

What is *Term Rewriting*?

(1) Core functional programming language

without many restrictions (and features) of "real" FP:

- first-order (usually)
- no fixed evaluation strategy
- untyped
- no pre-defined data structures (integers, arrays, ...)

(2) Syntactic approach for reasoning in equational first-order logic

Example (Term Rewrite System (TRS) $\mathcal{R}$)

$$\mathsf{double}(\mathsf{0}) \to \mathsf{0}$$

$$\mathsf{double}(\mathsf{s}(x)) \to \mathsf{s}(\mathsf{s}(\mathsf{double}(x)))$$

Compute "double of 3 is 6":

$$\begin{array}{ll} & \mathsf{double}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{0})))) \\ \to_{\mathcal{R}} & \mathsf{s}(\mathsf{s}(\mathsf{double}(\mathsf{s}(\mathsf{s}(\mathsf{0}))))) \end{array}$$

What is *Term Rewriting*?

(1) Core functional programming language

without many restrictions (and features) of "real" FP:

- first-order (usually)
- no fixed evaluation strategy
- untyped
- no pre-defined data structures (integers, arrays, ...)

(2) Syntactic approach for reasoning in equational first-order logic

Example (Term Rewrite System (TRS) $\mathcal{R}$)

$$\mathsf{double}(0) \to 0$$

$$\mathsf{double}(\mathsf{s}(x)) \to \mathsf{s}(\mathsf{s}(\mathsf{double}(x)))$$

Compute "double of 3 is 6":

$$\begin{aligned} & \mathsf{double}(\mathsf{s}(\mathsf{s}(\mathsf{s}(0)))) \\ \to_{\mathcal{R}} \; & \mathsf{s}(\mathsf{s}(\mathsf{double}(\mathsf{s}(\mathsf{s}(0))))) \\ \to_{\mathcal{R}} \; & \mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{double}(\mathsf{s}(0)))))) \end{aligned}$$

What is *Term Rewriting*?

(1) Core functional programming language
without many restrictions (and features) of "real" FP:

- first-order (usually)
- no fixed evaluation strategy
- untyped
- no pre-defined data structures (integers, arrays, ...)

(2) Syntactic approach for reasoning in equational first-order logic

Example (Term Rewrite System (TRS) $\mathcal{R}$)

$$\mathsf{double}(\mathsf{0}) \to \mathsf{0}$$

$$\mathsf{double}(\mathsf{s}(x)) \to \mathsf{s}(\mathsf{s}(\mathsf{double}(x)))$$

Compute "double of 3 is 6":

$$\begin{array}{ll} & \mathsf{double}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{0})))) \\ \to_{\mathcal{R}} & \mathsf{s}(\mathsf{s}(\mathsf{double}(\mathsf{s}(\mathsf{s}(\mathsf{0}))))) \\ \to_{\mathcal{R}} & \mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{double}(\mathsf{s}(\mathsf{0})))))) \\ \to_{\mathcal{R}} & \mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{double}(\mathsf{0}))))))) \end{array}$$

What is *Term Rewriting*?

(1) Core functional programming language
without many restrictions (and features) of "real" FP:

- first-order (usually)
- no fixed evaluation strategy
- untyped
- no pre-defined data structures (integers, arrays, ...)

(2) Syntactic approach for reasoning in equational first-order logic

Example (Term Rewrite System (TRS) $\mathcal{R}$)

$$\mathsf{double}(\mathsf{0}) \to \mathsf{0}$$

$$\mathsf{double}(\mathsf{s}(x)) \to \mathsf{s}(\mathsf{s}(\mathsf{double}(x)))$$

Compute "double of 3 is 6":

$$\begin{array}{ll} & \mathsf{double}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{0})))) \\ \to_{\mathcal{R}} & \mathsf{s}(\mathsf{s}(\mathsf{double}(\mathsf{s}(\mathsf{s}(\mathsf{0}))))) \\ \to_{\mathcal{R}} & \mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{double}(\mathsf{s}(\mathsf{0})))))) \\ \to_{\mathcal{R}} & \mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{double}(\mathsf{0}))))))) \\ \to_{\mathcal{R}} & \mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{0})))))) \end{array}$$

What is *Term Rewriting*?

(1) Core functional programming language
without many restrictions (and features) of "real" FP:

- first-order (usually)
- no fixed evaluation strategy
- untyped
- no pre-defined data structures (integers, arrays, ...)

(2) Syntactic approach for reasoning in equational first-order logic

Example (Term Rewrite System (TRS) $\mathcal{R}$)

$$\mathsf{double}(\mathsf{0}) \to \mathsf{0}$$

$$\mathsf{double}(\mathsf{s}(x)) \to \mathsf{s}(\mathsf{s}(\mathsf{double}(x)))$$

Compute "double of 3 is 6":

$$\begin{aligned} & \mathsf{double}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{0})))) \\ \to_{\mathcal{R}} \quad & \mathsf{s}(\mathsf{s}(\mathsf{double}(\mathsf{s}(\mathsf{s}(\mathsf{0}))))) \\ \to_{\mathcal{R}} \quad & \mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{double}(\mathsf{s}(\mathsf{0})))))) \\ \to_{\mathcal{R}} \quad & \mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{double}(\mathsf{0}))))))) \\ \to_{\mathcal{R}} \quad & \mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{0})))))) \end{aligned}$$

in 4 steps with $\to_{\mathcal{R}}$

What is *Term Rewriting*?

(1) Core functional programming language
without many restrictions (and features) of "real" FP:

- first-order (usually)
- no fixed evaluation strategy
- untyped
- no pre-defined data structures (integers, arrays, ...)

(2) Syntactic approach for reasoning in equational first-order logic

Example (Term Rewrite System (TRS) $\mathcal{R}$)

$$\mathsf{double}(0) \to 0$$

$$\mathsf{double}(\mathsf{s}(x)) \to \mathsf{s}(\mathsf{s}(\mathsf{double}(x)))$$

Compute "double of 3 is 6":

$$\begin{array}{ll} & \mathsf{double}(\mathsf{s}^3(0)) \\ \to_{\mathcal{R}} & \mathsf{s}^2(\mathsf{double}(\mathsf{s}^2(0))) \\ \to_{\mathcal{R}} & \mathsf{s}^4(\mathsf{double}(\mathsf{s}(0))) \\ \to_{\mathcal{R}} & \mathsf{s}^6(\mathsf{double}(0)) \\ \to_{\mathcal{R}} & \mathsf{s}^6(0) \end{array}$$

in 4 steps with $\to_{\mathcal{R}}$

What is *Complexity* of Term Rewriting?

Given: TRS $\mathcal{R}$ (e.g., $\{$ double(0) $\to$ 0, double(s(x)) $\to$ s(s(double(x))) $\}$)

What is *Complexity* of Term Rewriting?

Given: TRS $\mathcal{R}$ (e.g., $\{\ \mathsf{double}(\mathsf{0}) \to \mathsf{0},\ \mathsf{double}(\mathsf{s}(x)) \to \mathsf{s}(\mathsf{s}(\mathsf{double}(x)))\ \}$)

Question: How long can a $\to_{\mathcal{R}}$ sequence from a term of size n become?

(worst case)

What is *Complexity* of Term Rewriting?

Given: TRS $\mathcal{R}$ (e.g., $\{$ double(0) $\to$ 0, double(s(x)) $\to$ s(s(double(x))) $\}$)

Question: How long can a $\to_{\mathcal{R}}$ sequence from a term of size n become? (worst case)

Here: Does $\mathcal{R}$ have complexity $\Theta(n)$?

What is *Complexity* of Term Rewriting?

Given: TRS $\mathcal{R}$ (e.g., $\{$ double(0) $\to$ 0, double(s(x)) $\to$ s(s(double(x))) $\}$)

Question: How long can a $\to_{\mathcal{R}}$ sequence from a term of size n become?
(worst case)

Here: Does $\mathcal{R}$ have complexity $\Theta(n)$?

(1) **Yes!**

What is *Complexity* of Term Rewriting?

Given: TRS $\mathcal{R}$ (e.g., $\{$ $\mathsf{double}(\mathsf{0}) \to \mathsf{0}$, $\mathsf{double}(\mathsf{s}(x)) \to \mathsf{s}(\mathsf{s}(\mathsf{double}(x)))$ $\}$)

Question: How long can a $\to_{\mathcal{R}}$ sequence from a term of size n become? (worst case)

Here: Does $\mathcal{R}$ have complexity $\Theta(n)$?

(1) **Yes!**

$$\mathsf{double}(\mathsf{s}^{n-2}(\mathsf{0})) \to_{\mathcal{R}}^{n-1} \mathsf{s}^{2n-4}(\mathsf{0})$$

What is *Complexity* of Term Rewriting?

Given: TRS $\mathcal{R}$ (e.g., $\{$ double(0) $\to$ 0, double(s(x)) $\to$ s(s(double(x))) $\}$)

Question: How long can a $\to_{\mathcal{R}}$ sequence from a term of size n become?

(worst case)

Here: Does $\mathcal{R}$ have complexity $\Theta(n)$?

(1) **Yes!**

$$\mathsf{double}(\mathsf{s}^{n-2}(\mathsf{0})) \to_{\mathcal{R}}^{n-1} \mathsf{s}^{2n-4}(\mathsf{0})$$

- **basic terms** $f(t_1, \ldots, t_n)$ with t_i constructor terms allow only n steps

What is *Complexity* of Term Rewriting?

Given: TRS $\mathcal{R}$ (e.g., $\{$ double(0) $\to$ 0, double(s(x)) $\to$ s(s(double(x))) $\}$)

Question: How long can a $\to_{\mathcal{R}}$ sequence from a term of size n become?

(worst case)

Here: Does $\mathcal{R}$ have complexity $\Theta(n)$?

(1) **Yes!**

$$\mathsf{double}(\mathsf{s}^{n-2}(\mathsf{0})) \to_{\mathcal{R}}^{n-1} \mathsf{s}^{2n-4}(\mathsf{0})$$

- **basic terms** $f(t_1, \ldots, t_n)$ with t_i constructor terms allow only n steps
- **runtime complexity** $\mathrm{rc}_{\mathcal{R}}(n)$: basic terms as start terms

What is *Complexity* of Term Rewriting?

Given: TRS $\mathcal{R}$ (e.g., $\{$ double(0) $\to$ 0, double(s(x)) $\to$ s(s(double(x))) $\}$)

Question: How long can a $\to_{\mathcal{R}}$ sequence from a term of size n become?

(worst case)

Here: Does $\mathcal{R}$ have complexity $\Theta(n)$?

(1) **Yes!**

$$\mathsf{double}(\mathsf{s}^{n-2}(\mathsf{0})) \to_{\mathcal{R}}^{n-1} \mathsf{s}^{2n-4}(\mathsf{0})$$

- **basic terms** $f(t_1, \ldots, t_n)$ with t_i constructor terms allow only n steps
- **runtime complexity** $\mathrm{rc}_{\mathcal{R}}(n)$: basic terms as start terms
- $\mathrm{rc}_{\mathcal{R}}(n)$ for **program analysis**

What is *Complexity* of Term Rewriting?

Given: TRS $\mathcal{R}$ (e.g., $\{$ $\mathsf{double}(\mathsf{0}) \to \mathsf{0}$, $\mathsf{double}(\mathsf{s}(x)) \to \mathsf{s}(\mathsf{s}(\mathsf{double}(x)))$ $\}$)

Question: How long can a $\to_{\mathcal{R}}$ sequence from a term of size n become? (worst case)

Here: Does $\mathcal{R}$ have complexity $\Theta(n)$?

(1) **Yes!**

$$\mathsf{double}(\mathsf{s}^{n-2}(\mathsf{0})) \to_{\mathcal{R}}^{n-1} \mathsf{s}^{2n-4}(\mathsf{0})$$

- **basic terms** $f(t_1, \ldots, t_n)$ with t_i constructor terms allow only n steps
- **runtime complexity** $\mathrm{rc}_{\mathcal{R}}(n)$: basic terms as start terms
- $\mathrm{rc}_{\mathcal{R}}(n)$ for **program analysis**

(2) **No!**

What is *Complexity* of Term Rewriting?

Given: TRS $\mathcal{R}$ (e.g., { double(0) $\to$ 0, double(s(x)) $\to$ s(s(double(x))) })

Question: How long can a $\to_{\mathcal{R}}$ sequence from a term of size n become? (worst case)

Here: Does $\mathcal{R}$ have complexity $\Theta(n)$?

(1) **Yes!**

$$\mathsf{double}(\mathsf{s}^{n-2}(\mathsf{0})) \to_{\mathcal{R}}^{n-1} \mathsf{s}^{2n-4}(\mathsf{0})$$

- **basic terms** $f(t_1, \ldots, t_n)$ with t_i constructor terms allow only n steps
- **runtime complexity** $\mathrm{rc}_{\mathcal{R}}(n)$: basic terms as start terms
- $\mathrm{rc}_{\mathcal{R}}(n)$ for **program analysis**

(2) **No!**

$\mathsf{double}^3(\mathsf{s}(\mathsf{0})) \to_{\mathcal{R}}^{2} \mathsf{double}^2(\mathsf{s}^2(\mathsf{0})) \to_{\mathcal{R}}^{3} \mathsf{double}(\mathsf{s}^4(\mathsf{0})) \to_{\mathcal{R}}^{5} \mathsf{s}^8(\mathsf{0})$ in 10 steps

What is *Complexity* of Term Rewriting?

Given: TRS $\mathcal{R}$ (e.g., $\{$ double(0) $\to$ 0, double(s(x)) $\to$ s(s(double(x))) $\}$)

Question: How long can a $\to_{\mathcal{R}}$ sequence from a term of size n become? (worst case)

Here: Does $\mathcal{R}$ have complexity $\Theta(n)$?

(1) **Yes!**

$$\mathsf{double}(\mathsf{s}^{n-2}(\mathsf{0})) \to_{\mathcal{R}}^{n-1} \mathsf{s}^{2n-4}(\mathsf{0})$$

- **basic terms** $f(t_1, \ldots, t_n)$ with t_i constructor terms allow only n steps
- **runtime complexity** $\mathrm{rc}_{\mathcal{R}}(n)$: basic terms as start terms
- $\mathrm{rc}_{\mathcal{R}}(n)$ for **program analysis**

(2) **No!**

$\mathsf{double}^3(\mathsf{s}(\mathsf{0})) \to_{\mathcal{R}}^{2} \mathsf{double}^2(\mathsf{s}^2(\mathsf{0})) \to_{\mathcal{R}}^{3} \mathsf{double}(\mathsf{s}^4(\mathsf{0})) \to_{\mathcal{R}}^{5} \mathsf{s}^8(\mathsf{0})$ in 10 steps

- $\mathsf{double}^{n-2}(\mathsf{s}(\mathsf{0}))$ allows $\Theta(2^n)$ many steps to $\mathsf{s}^{2^{n-2}}(\mathsf{0})$

What is *Complexity* of Term Rewriting?

Given: TRS $\mathcal{R}$ (e.g., $\{$ $\mathsf{double}(\mathsf{0}) \to \mathsf{0}$, $\mathsf{double}(\mathsf{s}(x)) \to \mathsf{s}(\mathsf{s}(\mathsf{double}(x)))$ $\}$)

Question: How long can a $\to_{\mathcal{R}}$ sequence from a term of size n become? (worst case)

Here: Does $\mathcal{R}$ have complexity $\Theta(n)$?

(1) **Yes!**

$$\mathsf{double}(\mathsf{s}^{n-2}(\mathsf{0})) \to_{\mathcal{R}}^{n-1} \mathsf{s}^{2n-4}(\mathsf{0})$$

- **basic terms** $f(t_1, \ldots, t_n)$ with t_i constructor terms allow only n steps
- **runtime complexity** $\mathrm{rc}_{\mathcal{R}}(n)$: basic terms as start terms
- $\mathrm{rc}_{\mathcal{R}}(n)$ for **program analysis**

(2) **No!**

$\mathsf{double}^3(\mathsf{s}(\mathsf{0})) \to_{\mathcal{R}}^{2} \mathsf{double}^2(\mathsf{s}^2(\mathsf{0})) \to_{\mathcal{R}}^{3} \mathsf{double}(\mathsf{s}^4(\mathsf{0})) \to_{\mathcal{R}}^{5} \mathsf{s}^8(\mathsf{0})$ in 10 steps

- $\mathsf{double}^{n-2}(\mathsf{s}(\mathsf{0}))$ allows $\Theta(2^n)$ many steps to $\mathsf{s}^{2^{n-2}}(\mathsf{0})$
- **derivational complexity** $\mathrm{dc}_{\mathcal{R}}(n)$: no restrictions on start terms

What is *Complexity* of Term Rewriting?

Given: TRS $\mathcal{R}$ (e.g., $\{$ double(0) $\to$ 0, double(s(x)) $\to$ s(s(double(x))) $\}$)

Question: How long can a $\to_{\mathcal{R}}$ sequence from a term of size n become? (worst case)

Here: Does $\mathcal{R}$ have complexity $\Theta(n)$?

(1) **Yes!**

$$\mathsf{double}(\mathsf{s}^{n-2}(\mathsf{0})) \to_{\mathcal{R}}^{n-1} \mathsf{s}^{2n-4}(\mathsf{0})$$

- **basic terms** $f(t_1, \ldots, t_n)$ with t_i constructor terms allow only n steps
- **runtime complexity** $\mathrm{rc}_{\mathcal{R}}(n)$: basic terms as start terms
- $\mathrm{rc}_{\mathcal{R}}(n)$ for **program analysis**

(2) **No!**

$\mathsf{double}^3(\mathsf{s}(\mathsf{0})) \to_{\mathcal{R}}^{2} \mathsf{double}^2(\mathsf{s}^2(\mathsf{0})) \to_{\mathcal{R}}^{3} \mathsf{double}(\mathsf{s}^4(\mathsf{0})) \to_{\mathcal{R}}^{5} \mathsf{s}^8(\mathsf{0})$ in 10 steps

- $\mathsf{double}^{n-2}(\mathsf{s}(\mathsf{0}))$ allows $\Theta(2^n)$ many steps to $\mathsf{s}^{2^{n-2}}(\mathsf{0})$
- **derivational complexity** $\mathrm{dc}_{\mathcal{R}}(n)$: no restrictions on start terms
- $\mathrm{dc}_{\mathcal{R}}(n)$ for **equational reasoning**: cost of solving the word problem $\mathcal{E} \models s \equiv t$ by rewriting s and t via an equivalent convergent TRS $\mathcal{R}_{\mathcal{E}}$

Complexity Analysis for TRSs: Overview

1. Introduction
2. Automatically Finding Upper Bounds
3. Automatically Finding Lower Bounds
4. Transformational Techniques
5. Analysing Program Complexity via TRS Complexity
6. Current Developments

A Short Timeline (1/2)

1989: Derivational complexity introduced, linked to termination proofs[18]

[18] D. Hofbauer, C. Lautemann: *Termination proofs and the length of derivations*, RTA '89

A Short Timeline (1/2)

1989: Derivational complexity introduced, linked to termination proofs[18]

2001: Techniques for polynomial upper complexity bounds[19]

---

[18] D. Hofbauer, C. Lautemann: *Termination proofs and the length of derivations*, RTA '89

[19] G. Bonfante, A. Cichon, J. Marion, and H. Touzet: *Algorithms with polynomial interpretation termination proof*, JFP '01

A Short Timeline (1/2)

1989: Derivational complexity introduced, linked to termination proofs[18]

2001: Techniques for polynomial upper complexity bounds[19]

2008: Runtime complexity introduced with first analysis techniques[20]

---

[18] D. Hofbauer, C. Lautemann: *Termination proofs and the length of derivations*, RTA '89

[19] G. Bonfante, A. Cichon, J. Marion, and H. Touzet: *Algorithms with polynomial interpretation termination proof*, JFP '01

[20] N. Hirokawa, G. Moser: *Automated complexity analysis based on the dependency pair method*, IJCAR '08

A Short Timeline (1/2)

1989: Derivational complexity introduced, linked to termination proofs[18]

2001: Techniques for polynomial upper complexity bounds[19]

2008: Runtime complexity introduced with first analysis techniques[20]

2008: First automated tools to find complexity bounds: TcT[21], CaT[22]

---

[18] D. Hofbauer, C. Lautemann: *Termination proofs and the length of derivations*, RTA '89

[19] G. Bonfante, A. Cichon, J. Marion, and H. Touzet: *Algorithms with polynomial interpretation termination proof*, JFP '01

[20] N. Hirokawa, G. Moser: *Automated complexity analysis based on the dependency pair method*, IJCAR '08

[21] M. Avanzini, G. Moser, M. Schaper: *TcT: Tyrolean Complexity Tool*, TACAS '16, https://tcs-informatik.uibk.ac.at/tools/tct/

[22] M. Korp, C. Sternagel, H. Zankl, A. Middeldorp: *Tyrolean Termination Tool 2*, RTA '09, http://cl-informatik.uibk.ac.at/software/cat/

A Short Timeline (1/2)

1989: Derivational complexity introduced, linked to termination proofs[18]

2001: Techniques for polynomial upper complexity bounds[19]

2008: Runtime complexity introduced with first analysis techniques[20]

2008: First automated tools to find complexity bounds: TcT[21], CaT[22]

2008: First complexity analysis categories in the Termination Competition

http://termination-portal.org/wiki/Termination_Competition

---

[18] D. Hofbauer, C. Lautemann: *Termination proofs and the length of derivations*, RTA '89

[19] G. Bonfante, A. Cichon, J. Marion, and H. Touzet: *Algorithms with polynomial interpretation termination proof*, JFP '01

[20] N. Hirokawa, G. Moser: *Automated complexity analysis based on the dependency pair method*, IJCAR '08

[21] M. Avanzini, G. Moser, M. Schaper: *TcT: Tyrolean Complexity Tool*, TACAS '16, https://tcs-informatik.uibk.ac.at/tools/tct/

[22] M. Korp, C. Sternagel, H. Zankl, A. Middeldorp: *Tyrolean Termination Tool 2*, RTA '09, http://cl-informatik.uibk.ac.at/software/cat/

A Short Timeline (1/2)

1989: Derivational complexity introduced, linked to termination proofs[18]

2001: Techniques for polynomial upper complexity bounds[19]

2008: Runtime complexity introduced with first analysis techniques[20]

2008: First automated tools to find complexity bounds: TcT[21], CaT[22]

2008: First complexity analysis categories in the Termination Competition

http://termination-portal.org/wiki/Termination_Competition

...

---

[18] D. Hofbauer, C. Lautemann: *Termination proofs and the length of derivations*, RTA '89

[19] G. Bonfante, A. Cichon, J. Marion, and H. Touzet: *Algorithms with polynomial interpretation termination proof*, JFP '01

[20] N. Hirokawa, G. Moser: *Automated complexity analysis based on the dependency pair method*, IJCAR '08

[21] M. Avanzini, G. Moser, M. Schaper: *TcT: Tyrolean Complexity Tool*, TACAS '16, https://tcs-informatik.uibk.ac.at/tools/tct/

[22] M. Korp, C. Sternagel, H. Zankl, A. Middeldorp: *Tyrolean Termination Tool 2*, RTA '09, http://cl-informatik.uibk.ac.at/software/cat/

A Short Timeline (2/2)

...

2022: Termination Competition 2022 with complexity analysis tools AProVE[23], TcT in August 2022

https://termcomp.github.io/Y2022

[23] J. Giesl, C. Aschermann, M. Brockschmidt, F. Emmes, F. Frohn, C. Fuhs, J. Hensel, C. Otto, M. Plücker, P. Schneider-Kamp, T. Ströder, S. Swiderski, R. Thiemann: *Analyzing Program Termination and Complexity Automatically with AProVE*, JAR '17, http://aprove.informatik.rwth-aachen.de/

Some Definitions

Definition (Derivation Height dh)

For a term $t \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ and a relation $\longrightarrow$, the **derivation height** is:

$$\mathrm{dh}(t, \longrightarrow) \;=\; \sup \{\, n \mid \exists t'.\, t \longrightarrow^{n} t' \,\}$$

If t starts an infinite $\longrightarrow$-sequence, we set $\mathrm{dh}(t, \longrightarrow) = \omega$.

Some Definitions

Definition (Derivation Height dh)

For a term $t \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ and a relation $\longrightarrow$, the **derivation height** is:

$$\mathrm{dh}(t, \longrightarrow) \;=\; \sup \{\, n \mid \exists t'.\, t \longrightarrow^{n} t' \,\}$$

If t starts an infinite $\longrightarrow$-sequence, we set $\mathrm{dh}(t, \longrightarrow) = \omega$.

$\mathrm{dh}(t, \longrightarrow)$: length of the longest $\longrightarrow$-sequence from t.

Some Definitions

Definition (Derivation Height dh)

For a term $t \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ and a relation $\rightarrow$, the **derivation height** is:

$$\mathrm{dh}(t, \rightarrow) \;=\; \sup \{\, n \mid \exists t'.\, t \rightarrow^{n} t' \,\}$$

If t starts an infinite $\rightarrow$-sequence, we set $\mathrm{dh}(t, \rightarrow) = \omega$.

$\mathrm{dh}(t, \rightarrow)$: length of the longest $\rightarrow$-sequence from t.

Example: $\mathrm{dh}(\,\mathsf{double}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{0})))),\ \rightarrow_{\mathcal{R}}\,) = 4$

Some Definitions

Definition (Derivation Height dh)

For a term $t \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ and a relation $\longrightarrow$, the **derivation height** is:

$$\mathrm{dh}(t, \longrightarrow) \;=\; \sup \{\, n \mid \exists t'.\, t \longrightarrow^{n} t' \,\}$$

If t starts an infinite $\longrightarrow$-sequence, we set $\mathrm{dh}(t, \longrightarrow) = \omega$.

$\mathrm{dh}(t, \longrightarrow)$: length of the longest $\longrightarrow$-sequence from t.

Example: $\mathrm{dh}(\,\mathsf{double}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{0})))),\ \longrightarrow_{\mathcal{R}}\,) = 4$

Definition (Derivational Complexity dc)

For a TRS $\mathcal{R}$, the **derivational complexity** is:

$$\mathrm{dc}_{\mathcal{R}}(n) \;=\; \sup \{\, \mathrm{dh}(t, \longrightarrow_{\mathcal{R}}) \mid t \in \mathcal{T}(\mathcal{F}, \mathcal{V}), |t| \leq n \,\}$$

Some Definitions

Definition (Derivation Height dh)

For a term $t \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ and a relation $\longrightarrow$, the **derivation height** is:

$$\mathrm{dh}(t, \longrightarrow) \;=\; \sup \{\, n \mid \exists t'.\, t \longrightarrow^{n} t' \,\}$$

If t starts an infinite $\longrightarrow$-sequence, we set $\mathrm{dh}(t, \longrightarrow) = \omega$.

$\mathrm{dh}(t, \longrightarrow)$: length of the longest $\longrightarrow$-sequence from t.

Example: $\mathrm{dh}(\, \mathsf{double}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{0})))),\ \longrightarrow_{\mathcal{R}}\,) = 4$

Definition (Derivational Complexity dc)

For a TRS $\mathcal{R}$, the **derivational complexity** is:

$$\mathrm{dc}_{\mathcal{R}}(n) \;=\; \sup \{\, \mathrm{dh}(t, \longrightarrow_{\mathcal{R}}) \mid t \in \mathcal{T}(\mathcal{F}, \mathcal{V}), |t| \leq n \,\}$$

$\mathrm{dc}_{\mathcal{R}}(n)$: length of the longest $\longrightarrow_{\mathcal{R}}$-sequence from a term of size at most n

Some Definitions

Definition (Derivation Height dh)

For a term $t \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ and a relation $\longrightarrow$, the **derivation height** is:

$$\mathrm{dh}(t, \longrightarrow) \;=\; \sup \{\, n \mid \exists t'.\, t \longrightarrow^{n} t' \,\}$$

If t starts an infinite $\longrightarrow$-sequence, we set $\mathrm{dh}(t, \longrightarrow) = \omega$.

$\mathrm{dh}(t, \longrightarrow)$: length of the longest $\longrightarrow$-sequence from t.

Example: $\mathrm{dh}(\, \mathsf{double}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{0})))),\ \longrightarrow_{\mathcal{R}}\,) = 4$

Definition (Derivational Complexity dc)

For a TRS $\mathcal{R}$, the **derivational complexity** is:

$$\mathrm{dc}_{\mathcal{R}}(n) \;=\; \sup \{\, \mathrm{dh}(t, \longrightarrow_{\mathcal{R}}) \mid t \in \mathcal{T}(\mathcal{F}, \mathcal{V}), |t| \leq n \,\}$$

$\mathrm{dc}_{\mathcal{R}}(n)$: length of the longest $\longrightarrow_{\mathcal{R}}$-sequence from a term of size at most n

Example: For $\mathcal{R}$ for double, we have $\mathrm{dc}_{\mathcal{R}}(n) \in \Theta(2^n)$.

Upper Bounds

The Bad News for automation:

Upper Bounds

The Bad News for automation:

For a given TRS $\mathcal{R}$, the following questions are undecidable:

- $\mathrm{dc}_{\mathcal{R}}(n) = \omega$ for some n? ($\longrightarrow$ termination!)

Upper Bounds

The Bad News for automation:

For a given TRS $\mathcal{R}$, the following questions are undecidable:

- $\mathrm{dc}_{\mathcal{R}}(n) = \omega$ for some n? ($\longrightarrow$ termination!)
- $\mathrm{dc}_{\mathcal{R}}(n)$ polynomially bounded?[24]

[24] A. Schnabl and J. G. Simonsen: *The exact hardness of deciding derivational and runtime complexity*, CSL '11

Upper Bounds

The Bad News for automation:

For a given TRS $\mathcal{R}$, the following questions are undecidable:

- $\mathrm{dc}_{\mathcal{R}}(n) = \omega$ for some n? ($\longrightarrow$ termination!)
- $\mathrm{dc}_{\mathcal{R}}(n)$ polynomially bounded?[24]

Goal: find **approximations** for derivational complexity

Initial focus: find upper bounds

$$\mathrm{dc}_{\mathcal{R}}(n) \in \mathcal{O}(...)$$

[24] A. Schnabl and J. G. Simonsen: *The exact hardness of deciding derivational and runtime complexity*, CSL '11

Derivational Complexity from Polynomial Interpretations (1/2)

Example (double)

$$\begin{aligned} \mathsf{double}(\mathsf{0}) &\to \mathsf{0} \\ \mathsf{double}(\mathsf{s}(x)) &\to \mathsf{s}(\mathsf{s}(\mathsf{double}(x))) \end{aligned}$$

Derivational Complexity from Polynomial Interpretations (1/2)

Example (double)

$$\begin{aligned} \mathsf{double}(\mathsf{0}) &\succ \mathsf{0} \\ \mathsf{double}(\mathsf{s}(x)) &\succ \mathsf{s}(\mathsf{s}(\mathsf{double}(x))) \end{aligned}$$

Show $\mathrm{dc}_{\mathcal{R}}(n) < \omega$ by **termination proof** with reduction order $\succ$ on terms.

Derivational Complexity from Polynomial Interpretations (1/2)

Example (double)

$$\begin{aligned} \mathsf{double}(\mathsf{0}) &\succ \mathsf{0} \\ \mathsf{double}(\mathsf{s}(x)) &\succ \mathsf{s}(\mathsf{s}(\mathsf{double}(x))) \end{aligned}$$

Show $\mathrm{dc}_{\mathcal{R}}(n) < \omega$ by **termination proof** with reduction order $\succ$ on terms.
Get $\succ$ via **polynomial interpretation**[25] $[\,\cdot\,]$ over $\mathbb{N}$: $\ell \succ r \iff [\ell] \succ [r]$

[25] D. Lankford: *Canonical algebraic simplification in computational logic*, U Texas '75

Derivational Complexity from Polynomial Interpretations (1/2)

Example (double)

$$\begin{aligned} \mathsf{double}(\mathsf{0}) &\succ \mathsf{0} \\ \mathsf{double}(\mathsf{s}(x)) &\succ \mathsf{s}(\mathsf{s}(\mathsf{double}(x))) \end{aligned}$$

Show $\mathrm{dc}_{\mathcal{R}}(n) < \omega$ by **termination proof** with reduction order $\succ$ on terms.
Get $\succ$ via **polynomial interpretation**[25] $[\cdot]$ over $\mathbb{N}$: $\ell \succ r \iff [\ell] \succ [r]$

Example: $[\mathsf{double}](x) = 3 \cdot x, \quad [\mathsf{s}](x) = x + 1, \quad [\mathsf{0}] = 1$

[25] D. Lankford: *Canonical algebraic simplification in computational logic*, U Texas '75

Derivational Complexity from Polynomial Interpretations (1/2)

Example (double)

$$\begin{aligned} \mathsf{double}(\mathsf{0}) &\succ \mathsf{0} \\ \mathsf{double}(\mathsf{s}(x)) &\succ \mathsf{s}(\mathsf{s}(\mathsf{double}(x))) \end{aligned}$$

Show $\mathrm{dc}_{\mathcal{R}}(n) < \omega$ by **termination proof** with reduction order $\succ$ on terms.
Get $\succ$ via **polynomial interpretation**[25] $[\,\cdot\,]$ over $\mathbb{N}$: $\ell \succ r \iff [\ell] \succ [r]$

Example: $[\mathsf{double}](x) = 3 \cdot x$, $[\mathsf{s}](x) = x + 1$, $[\mathsf{0}] = 1$

Extend to terms:

- $[x] = x$
- $[f(t_1, \ldots, t_n)] = [f]([t_1], \ldots, [t_n])$

[25] D. Lankford: *Canonical algebraic simplification in computational logic*, U Texas '75

Example (double)

double(0)	$\succ$	0		3	$>$	1
double(s(x))	$\succ$	s(s(double(x)))		$3 \cdot x + 3$	$>$	$3 \cdot x + 2$

Show $\mathrm{dc}_{\mathcal{R}}(n) < \omega$ by **termination proof** with reduction order $\succ$ on terms.
Get $\succ$ via **polynomial interpretation**[25] $[\cdot]$ over $\mathbb{N}$: $\ell \succ r \iff [\ell] \succ [r]$

Example: $[\mathsf{double}](x) = 3 \cdot x, \quad [\mathsf{s}](x) = x + 1, \quad [\mathsf{0}] = 1$

Extend to terms:

- $[x] = x$
- $[f(t_1, \ldots, t_n)] = [f]([t_1], \ldots, [t_n])$

[25] D. Lankford: *Canonical algebraic simplification in computational logic*, U Texas '75

Derivational Complexity from Polynomial Interpretations (1/2)

Example (double)

$$\begin{array}{rcl|rcl} \mathsf{double}(\mathsf{0}) & \succ & \mathsf{0} & 3 & > & 1 \\ \mathsf{double}(\mathsf{s}(x)) & \succ & \mathsf{s}(\mathsf{s}(\mathsf{double}(x))) & 3 \cdot x + 3 & > & 3 \cdot x + 2 \end{array}$$

Show $\mathrm{dc}_{\mathcal{R}}(n) < \omega$ by **termination proof** with reduction order $\succ$ on terms.
Get $\succ$ via **polynomial interpretation**[25] $[\,\cdot\,]$ over $\mathbb{N}$: $\ell \succ r \iff [\ell] \succ [r]$

Example: $[\mathsf{double}](x) = 3 \cdot x$, $[\mathsf{s}](x) = x + 1$, $[\mathsf{0}] = 1$

Extend to terms:

- $[x] = x$
- $[f(t_1, \ldots, t_n)] = [f]([t_1], \ldots, [t_n])$

Automated search for $[\,\cdot\,]$ via SAT[26] or SMT[27] solving

[25] D. Lankford: *Canonical algebraic simplification in computational logic*, U Texas '75
[26] C. Fuhs, J. Giesl, A. Middeldorp, P. Schneider-Kamp, R. Thiemann, H. Zankl: *SAT solving for termination analysis with polynomial interpretations*, SAT '07
[27] C. Borralleras, S. Lucas, A. Oliveras, E. Rodríguez-Carbonell, A. Rubio: *SAT modulo linear arithmetic for solving polynomial constraints*, JAR '12

Derivational Complexity from Polynomial Interpretations (2/2)

Example (double)

$\mathsf{double}(\mathsf{0})$	$\succ$	$\mathsf{0}$		3	$>$	1
$\mathsf{double}(\mathsf{s}(x))$	$\succ$	$\mathsf{s}(\mathsf{s}(\mathsf{double}(x)))$		$3 \cdot x + 3$	$>$	$3 \cdot x + 2$

Example: $[\mathsf{double}](x) = 3 \cdot x, \qquad [\mathsf{s}](x) = x + 1, \qquad [\mathsf{0}] = 1$

This proves more than just termination. . .

Example (double)

$$\begin{array}{rcl} \mathsf{double}(\mathsf{0}) & \succ & \mathsf{0} \\ \mathsf{double}(\mathsf{s}(x)) & \succ & \mathsf{s}(\mathsf{s}(\mathsf{double}(x))) \end{array} \quad\Bigg|\quad \begin{array}{rcl} 3 & > & 1 \\ 3 \cdot x + 3 & > & 3 \cdot x + 2 \end{array}$$

Example: $[\mathsf{double}](x) = 3 \cdot x, \quad [\mathsf{s}](x) = x + 1, \quad [\mathsf{0}] = 1$

This proves more than just termination. . .

Theorem (Upper bounds for $\mathrm{dc}_{\mathcal{R}}(n)$ from polynomial interpretations[28])

- *Termination proof for TRS $\mathcal{R}$ with **polynomial** interpretation*

$$\Rightarrow \mathrm{dc}_{\mathcal{R}}(n) \in 2^{2^{\mathcal{O}(n)}}$$

[28] D. Hofbauer, C. Lautemann: *Termination proofs and the length of derivations*, RTA '89

Example (double)

$$\begin{array}{rcl} \mathsf{double}(\mathsf{0}) & \succ & \mathsf{0} \\ \mathsf{double}(\mathsf{s}(x)) & \succ & \mathsf{s}(\mathsf{s}(\mathsf{double}(x))) \end{array} \quad \Bigg| \quad \begin{array}{rcl} 3 & > & 1 \\ 3 \cdot x + 3 & > & 3 \cdot x + 2 \end{array}$$

Example: $[\mathsf{double}](x) = 3 \cdot x, \quad [\mathsf{s}](x) = x + 1, \quad [\mathsf{0}] = 1$

This proves more than just termination...

Theorem (Upper bounds for $\mathrm{dc}_{\mathcal{R}}(n)$ from polynomial interpretations[28])

- *Termination proof for TRS $\mathcal{R}$ with **polynomial** interpretation*
  $\Rightarrow \mathrm{dc}_{\mathcal{R}}(n) \in 2^{2^{\mathcal{O}(n)}}$
- *Termination proof for TRS $\mathcal{R}$ with **linear polynomial** interpretation*
  $\Rightarrow \mathrm{dc}_{\mathcal{R}}(n) \in 2^{\mathcal{O}(n)}$

[28] D. Hofbauer, C. Lautemann: *Termination proofs and the length of derivations*, RTA '89

Derivational Complexity from Termination Proofs (1/2)

Termination proof for TRS $\mathcal{R}$ with ...

- matchbounds[29] $\Rightarrow \mathrm{dc}_{\mathcal{R}}(n) \in \mathcal{O}(n)$
- arctic matrix interpretations[30] $\Rightarrow \mathrm{dc}_{\mathcal{R}}(n) \in \mathcal{O}(n)$

---

[29] A. Geser, D. Hofbauer, J. Waldmann: *Match-bounded string rewriting systems*, AAECC '04

[30] A. Koprowski, J. Waldmann: *Max/plus tree automata for termination of term rewriting*, Acta Cyb. '09

Derivational Complexity from Termination Proofs (1/2)

Termination proof for TRS $\mathcal{R}$ with ...

- matchbounds[29] $\Rightarrow \mathrm{dc}_{\mathcal{R}}(n) \in \mathcal{O}(n)$
- arctic matrix interpretations[30] $\Rightarrow \mathrm{dc}_{\mathcal{R}}(n) \in \mathcal{O}(n)$
- triangular matrix interpretation[31] $\Rightarrow \mathrm{dc}_{\mathcal{R}}(n)$ is at most polynomial
- matrix interpretation of spectral radius[32] ≤ 1
  $\Rightarrow \mathrm{dc}_{\mathcal{R}}(n)$ is at most polynomial

---

[29] A. Geser, D. Hofbauer, J. Waldmann: *Match-bounded string rewriting systems*, AAECC '04

[30] A. Koprowski, J. Waldmann: *Max/plus tree automata for termination of term rewriting*, Acta Cyb. '09

[31] G. Moser, A. Schnabl, J. Waldmann: *Complexity analysis of term rewriting based on matrix and context dependent interpretations*, FSTTCS '08

[32] F. Neurauter, H. Zankl, A. Middeldorp: *Revisiting matrix interpretations for polynomial derivational complexity of term rewriting*, LPAR (Yogyakarta) '10

Derivational Complexity from Termination Proofs (1/2)

Termination proof for TRS $\mathcal{R}$ with ...

- matchbounds[29] $\Rightarrow \mathrm{dc}_{\mathcal{R}}(n) \in \mathcal{O}(n)$
- arctic matrix interpretations[30] $\Rightarrow \mathrm{dc}_{\mathcal{R}}(n) \in \mathcal{O}(n)$
- triangular matrix interpretation[31] $\Rightarrow \mathrm{dc}_{\mathcal{R}}(n)$ is at most polynomial
- matrix interpretation of spectral radius[32] ≤ 1
  $\Rightarrow \mathrm{dc}_{\mathcal{R}}(n)$ is at most polynomial
- standard matrix interpretation[33] $\Rightarrow \mathrm{dc}_{\mathcal{R}}(n)$ is at most exponential

---

[29] A. Geser, D. Hofbauer, J. Waldmann: *Match-bounded string rewriting systems*, AAECC '04

[30] A. Koprowski, J. Waldmann: *Max/plus tree automata for termination of term rewriting*, Acta Cyb. '09

[31] G. Moser, A. Schnabl, J. Waldmann: *Complexity analysis of term rewriting based on matrix and context dependent interpretations*, FSTTCS '08

[32] F. Neurauter, H. Zankl, A. Middeldorp: *Revisiting matrix interpretations for polynomial derivational complexity of term rewriting*, LPAR (Yogyakarta) '10

[33] J. Endrullis, J. Waldmann, and H. Zantema: *Matrix interpretations for proving termination of term rewriting*, JAR '08

Derivational Complexity from Termination Proofs (2/2)

Termination proof for TRS $\mathcal{R}$ with ...

- lexicographic path order[34] $\Rightarrow \mathrm{dc}_{\mathcal{R}}(n)$ is at most multiple recursive[35]

[34] S. Kamin, J.-J. Lévy: *Two generalizations of the recursive path ordering*, U Illinois '80
[35] A. Weiermann: *Termination proofs for term rewriting systems by lexicographic path orderings imply multiply recursive derivation lengths*, TCS '95

Derivational Complexity from Termination Proofs (2/2)

Termination proof for TRS $\mathcal{R}$ with ...

- lexicographic path order[34] $\Rightarrow \mathrm{dc}_{\mathcal{R}}(n)$ is at most multiple recursive[35]
- Dependency Pairs method[36] with dependency graphs and usable rules $\Rightarrow \mathrm{dc}_{\mathcal{R}}(n)$ is at most primitive recursive[37]

---

[34] S. Kamin, J.-J. Lévy: *Two generalizations of the recursive path ordering*, U Illinois '80
[35] A. Weiermann: *Termination proofs for term rewriting systems by lexicographic path orderings imply multiply recursive derivation lengths*, TCS '95
[36] T. Arts, J. Giesl: *Termination of term rewriting using dependency pairs*, TCS '00
[37] G. Moser, A. Schnabl: *The derivational complexity induced by the dependency pair method*, LMCS '11

Derivational Complexity from Termination Proofs (2/2)

Termination proof for TRS $\mathcal{R}$ with ...

- lexicographic path order[34] $\Rightarrow \mathrm{dc}_{\mathcal{R}}(n)$ is at most multiple recursive[35]
- Dependency Pairs method[36] with dependency graphs and usable rules $\Rightarrow \mathrm{dc}_{\mathcal{R}}(n)$ is at most primitive recursive[37]
- Dependency Pairs framework[38][39] with dependency graphs, reduction pairs, subterm criterion $\Rightarrow \mathrm{dc}_{\mathcal{R}}(n)$ is at most multiple recursive[40]

---

[34] S. Kamin, J.-J. Lévy: *Two generalizations of the recursive path ordering*, U Illinois '80
[35] A. Weiermann: *Termination proofs for term rewriting systems by lexicographic path orderings imply multiply recursive derivation lengths*, TCS '95
[36] T. Arts, J. Giesl: *Termination of term rewriting using dependency pairs*, TCS '00
[37] G. Moser, A. Schnabl: *The derivational complexity induced by the dependency pair method*, LMCS '11
[38] J. Giesl, R. Thiemann, P. Schneider-Kamp, S. Falke: *Mechanizing and improving dependency pairs*, JAR '06
[39] N. Hirokawa and A. Middeldorp: *Tyrolean Termination Tool: Techniques and features*, IC '07
[40] G. Moser, A. Schnabl: *Termination proofs in the dependency pair framework may induce multiple recursive derivational complexity*, RTA '11

Runtime Complexity

- So far: upper bounds for derivational complexity

Runtime Complexity

- So far: upper bounds for derivational complexity
- But: derivational complexity counter-intuitive, often infeasible

Runtime Complexity

- So far: upper bounds for derivational complexity
- But: derivational complexity counter-intuitive, often infeasible
- Wanted: complexity of evaluation of double **on data**: $\mathsf{double}(\mathsf{s}^n(0))$

Runtime Complexity

- So far: upper bounds for derivational complexity
- But: derivational complexity counter-intuitive, often infeasible
- Wanted: complexity of evaluation of double **on data**: double(s^n(0))

Definition (Basic Term[41])

For defined symbols $\mathcal{D}$ and constructor symbols $\mathcal{C}$, the term

$$f(t_1, \ldots, t_n)$$

is in the set $\mathcal{T}_{\text{basic}}$ of **basic terms** iff $f \in \mathcal{D}$ and $t_1, \ldots, t_n \in \mathcal{T}(\mathcal{C}, \mathcal{V})$.

[41] N. Hirokawa, G. Moser: *Automated complexity analysis based on the dependency pair method*, IJCAR '08

Runtime Complexity

- So far: upper bounds for derivational complexity
- But: derivational complexity counter-intuitive, often infeasible
- Wanted: complexity of evaluation of double **on data**: double($\mathsf{s}^n(0)$)

Definition (Basic Term[41])

For defined symbols $\mathcal{D}$ and constructor symbols $\mathcal{C}$, the term

$$f(t_1, \ldots, t_n)$$

is in the set $\mathcal{T}_{\text{basic}}$ of **basic terms** iff $f \in \mathcal{D}$ and $t_1, \ldots, t_n \in \mathcal{T}(\mathcal{C}, \mathcal{V})$.

Definition (Runtime Complexity rc[41])

For a TRS $\mathcal{R}$, the **runtime complexity** is:

$$\mathrm{rc}_{\mathcal{R}}(n) \;=\; \sup \{ \, \mathrm{dh}(t, \to_{\mathcal{R}}) \mid t \in \mathcal{T}_{\text{basic}}, |t| \leq n \, \}$$

[41] N. Hirokawa, G. Moser: *Automated complexity analysis based on the dependency pair method*, IJCAR '08

Runtime Complexity

- So far: upper bounds for derivational complexity
- But: derivational complexity counter-intuitive, often infeasible
- Wanted: complexity of evaluation of double **on data**: $\mathsf{double}(\mathsf{s}^n(\mathsf{0}))$

Definition (Basic Term[41])

For defined symbols $\mathcal{D}$ and constructor symbols $\mathcal{C}$, the term

$$f(t_1, \ldots, t_n)$$

is in the set $\mathcal{T}_{\mathrm{basic}}$ of **basic terms** iff $f \in \mathcal{D}$ and $t_1, \ldots, t_n \in \mathcal{T}(\mathcal{C}, \mathcal{V})$.

Definition (Runtime Complexity rc[41])

For a TRS $\mathcal{R}$, the **runtime complexity** is:

$$\mathrm{rc}_{\mathcal{R}}(n) \quad = \quad \sup \{ \, \mathrm{dh}(t, \to_{\mathcal{R}}) \mid t \in \mathcal{T}_{\mathrm{basic}}, |t| \leq n \, \}$$

$\mathrm{rc}_{\mathcal{R}}(n)$: like derivational complexity... but for basic terms only!

---

[41] N. Hirokawa, G. Moser: *Automated complexity analysis based on the dependency pair method*, IJCAR '08

Runtime Complexity from Polynomial Interpretations

Polynomial interpretations can induce upper bounds to runtime complexity:[42]

Definition (Strongly linear polynomial, restricted interpretation)

- Polynomial p is **strongly linear** iff $p(x_1, \ldots, x_n) = x_1 + \cdots + x_n + a$ for some $a \in \mathbb{N}$.
- Polynomial interpretation $[\,\cdot\,]$ is **restricted** iff for all constructor symbols f, $[f](x_1, \ldots, x_n)$ is strongly linear.

Idea: $[t] \leq c \cdot |t|$ for fixed $c \in \mathbb{N}$.

[42] G. Bonfante, A. Cichon, J. Marion, H. Touzet: *Algorithms with polynomial interpretation termination proof*, JFP '01

Runtime Complexity from Polynomial Interpretations

Polynomial interpretations can induce upper bounds to runtime complexity:[42]

Definition (Strongly linear polynomial, restricted interpretation)

- Polynomial p is **strongly linear** iff $p(x_1, \ldots, x_n) = x_1 + \cdots + x_n + a$ for some $a \in \mathbb{N}$.
- Polynomial interpretation $[\,\cdot\,]$ is **restricted** iff for all constructor symbols f, $[f](x_1, \ldots, x_n)$ is strongly linear.

Idea: $[t] \leq c \cdot |t|$ for fixed $c \in \mathbb{N}$.

Theorem (Upper bounds for $\mathrm{rc}_{\mathcal{R}}(n)$ from restricted interpretations)

*Termination proof for TRS $\mathcal{R}$ with **restricted** interpretation $[\,\cdot\,]$ of degree at most d for $[f]$* $\Rightarrow \mathrm{rc}_{\mathcal{R}}(n) \in \mathcal{O}(n^d)$

[42] G. Bonfante, A. Cichon, J. Marion, H. Touzet: *Algorithms with polynomial interpretation termination proof*, JFP '01

Runtime Complexity from Polynomial Interpretations

Polynomial interpretations can induce upper bounds to runtime complexity:[42]

Definition (Strongly linear polynomial, restricted interpretation)

- Polynomial p is **strongly linear** iff $p(x_1, \ldots, x_n) = x_1 + \cdots + x_n + a$ for some $a \in \mathbb{N}$.
- Polynomial interpretation $[\,\cdot\,]$ is **restricted** iff for all constructor symbols f, $[f](x_1, \ldots, x_n)$ is strongly linear.

Idea: $[t] \leq c \cdot |t|$ for fixed $c \in \mathbb{N}$.

Theorem (Upper bounds for $\mathrm{rc}_{\mathcal{R}}(n)$ from restricted interpretations)

*Termination proof for TRS $\mathcal{R}$ with **restricted** interpretation $[\,\cdot\,]$ of degree at most d for $[f]$* $\Rightarrow \mathrm{rc}_{\mathcal{R}}(n) \in \mathcal{O}(n^d)$

Example: $[\mathsf{double}](x) = 3 \cdot x$, $[\mathsf{s}](x) = x + 1$, $[\mathsf{0}] = 1$ is restricted, degree 1

$\Rightarrow \mathrm{rc}_{\mathcal{R}}(n) \in \mathcal{O}(n)$ for TRS $\mathcal{R}$ for double

[42] G. Bonfante, A. Cichon, J. Marion, H. Touzet: *Algorithms with polynomial interpretation termination proof*, JFP '01

Dependency Tuples for *Innermost* Runtime Complexity irc

Here: innermost rewriting ($\approx$ call-by-value)

Example (reverse)

$\mathsf{app}(\mathsf{nil}, y) \to y$	$\mathsf{app}(\mathsf{add}(n, x), y) \to \mathsf{add}(n, \mathsf{app}(x, y))$
$\mathsf{reverse}(\mathsf{nil}) \to \mathsf{nil}$	$\mathsf{reverse}(\mathsf{add}(n, x)) \to \mathsf{app}(\mathsf{reverse}(x), \mathsf{add}(n, \mathsf{nil}))$

Dependency Tuples for *Innermost* Runtime Complexity irc

Here: innermost rewriting ($\approx$ call-by-value)

Example (reverse)

$\mathsf{app}(\mathsf{nil}, y) \rightarrow y$	$\mathsf{app}(\mathsf{add}(n, x), y) \rightarrow \mathsf{add}(n, \mathsf{app}(x, y))$
$\mathsf{reverse}(\mathsf{nil}) \rightarrow \mathsf{nil}$	$\mathsf{reverse}(\mathsf{add}(n, x)) \rightarrow \mathsf{app}(\mathsf{reverse}(x), \mathsf{add}(n, \mathsf{nil}))$

For rule $\ell \longrightarrow r$, eval of ℓ costs 1 + eval of all function calls in r **together**:

[43] L. Noschinski, F. Emmes, J. Giesl: *Analyzing innermost runtime complexity of term rewriting by dependency pairs*, JAR '13

Dependency Tuples for *Innermost* Runtime Complexity irc

Here: innermost rewriting (≈ call-by-value)

Example (reverse)

$$\mathsf{app}(\mathsf{nil}, y) \to y \qquad \mathsf{app}(\mathsf{add}(n, x), y) \to \mathsf{add}(n, \mathsf{app}(x, y))$$
$$\mathsf{reverse}(\mathsf{nil}) \to \mathsf{nil} \qquad \mathsf{reverse}(\mathsf{add}(n, x)) \to \mathsf{app}(\mathsf{reverse}(x), \mathsf{add}(n, \mathsf{nil}))$$

For rule $\ell \to r$, eval of ℓ costs 1 + eval of all function calls in r **together**:

Example (Dependency Tuples[43] for reverse)

$$\begin{aligned}
\mathsf{app}^\sharp(\mathsf{nil}, y) &\to \mathsf{Com}_0 \\
\mathsf{app}^\sharp(\mathsf{add}(n, x), y) &\to \mathsf{Com}_1(\mathsf{app}^\sharp(x, y)) \\
\mathsf{reverse}^\sharp(\mathsf{nil}) &\to \mathsf{Com}_0 \\
\mathsf{reverse}^\sharp(\mathsf{add}(n, x)) &\to \mathsf{Com}_2(\mathsf{app}^\sharp(\mathsf{reverse}(x), \mathsf{add}(n, \mathsf{nil})), \mathsf{reverse}^\sharp(x))
\end{aligned}$$

- Function calls to count marked with $\sharp$
- Compound symbols Com_k group function calls together

[43] L. Noschinski, F. Emmes, J. Giesl: *Analyzing innermost runtime complexity of term rewriting by dependency pairs*, JAR '13

Polynomial Interpretations for Dependency Tuples

Example (reverse, Dependency Tuples for reverse)

$$
\begin{aligned}
\mathsf{app}^\sharp(\mathsf{nil}, y) &\to \mathsf{Com}_0\\
\mathsf{app}^\sharp(\mathsf{add}(n, x), y) &\to \mathsf{Com}_1(\mathsf{app}^\sharp(x, y))\\
\mathsf{reverse}^\sharp(\mathsf{nil}) &\to \mathsf{Com}_0\\
\mathsf{reverse}^\sharp(\mathsf{add}(n, x)) &\to \mathsf{Com}_2(\mathsf{app}^\sharp(\mathsf{reverse}(x), \mathsf{add}(n, \mathsf{nil})), \mathsf{reverse}^\sharp(x))
\end{aligned}
$$

$\mathsf{app}(\mathsf{nil}, y) \to y$	$\mathsf{app}(\mathsf{add}(n, x), y) \to \mathsf{add}(n, \mathsf{app}(x, y))$
$\mathsf{reverse}(\mathsf{nil}) \to \mathsf{nil}$	$\mathsf{reverse}(\mathsf{add}(n, x)) \to \mathsf{app}(\mathsf{reverse}(x), \mathsf{add}(n, \mathsf{nil}))$

Polynomial Interpretations for Dependency Tuples

Example (reverse, Dependency Tuples for reverse)

$$
\begin{aligned}
\mathsf{app}^\sharp(\mathsf{nil}, y) &\to \mathsf{Com}_0\\
\mathsf{app}^\sharp(\mathsf{add}(n, x), y) &\to \mathsf{Com}_1(\mathsf{app}^\sharp(x, y))\\
\mathsf{reverse}^\sharp(\mathsf{nil}) &\to \mathsf{Com}_0\\
\mathsf{reverse}^\sharp(\mathsf{add}(n, x)) &\to \mathsf{Com}_2(\mathsf{app}^\sharp(\mathsf{reverse}(x), \mathsf{add}(n, \mathsf{nil})), \mathsf{reverse}^\sharp(x))
\end{aligned}
$$

$\mathsf{app}(\mathsf{nil}, y) \to y$	$\mathsf{app}(\mathsf{add}(n, x), y) \to \mathsf{add}(n, \mathsf{app}(x, y))$
$\mathsf{reverse}(\mathsf{nil}) \to \mathsf{nil}$	$\mathsf{reverse}(\mathsf{add}(n, x)) \to \mathsf{app}(\mathsf{reverse}(x), \mathsf{add}(n, \mathsf{nil}))$

Use interpretation $[\,\cdot\,]$ with $[\mathsf{Com}_k](x_1, \ldots, x_k) = x_1 + \cdots + x_k$ and

$[\mathsf{nil}] = 0$	$[\mathsf{add}](x_1, x_2) = x_2 + 1$ ($\leq$ restricted interpret.)
$[\mathsf{app}](x_1, x_2) = x_1 + x_2$	$[\mathsf{reverse}](x_1) = x_1$ (bounds helper fct. result size)
$[\mathsf{app}^\sharp](x_1, x_2) = x_1 + 1$	$[\mathsf{reverse}^\sharp](x_1) = x_1^2 + x_1 + 1$ (complexity of fct.)

to show $[\ell] \geq [r]$ for all rules and $[\ell] \geq 1 + [r]$ for all Dependency Tuples

Maximum degree of $[\,\cdot\,]$ is 2 $\Rightarrow \mathrm{irc}_{\mathcal{R}}(n) \in \mathcal{O}(n^2)$

Related Techniques

- Dependency Tuples are an adaptation of Dependency Pairs (DPs) from termination analysis to complexity analysis, allow for **incremental** complexity proofs with several techniques

Related Techniques

- Dependency Tuples are an adaptation of Dependency Pairs (DPs) from termination analysis to complexity analysis, allow for **incremental** complexity proofs with several techniques
- Further adaptation of DPs (incomparable): Weak (Innermost) Dependency Pairs for (innermost) runtime complexity[44]

[44] N. Hirokawa, G. Moser: *Automated complexity analysis based on the dependency pair method*, IJCAR '08

Related Techniques

- Dependency Tuples are an adaptation of Dependency Pairs (DPs) from termination analysis to complexity analysis, allow for **incremental** complexity proofs with several techniques
- Further adaptation of DPs (incomparable): Weak (Innermost) Dependency Pairs for (innermost) runtime complexity[44]
- Extensions by polynomial path orders[45], usable replacement maps[46], a combination framework for complexity analysis[47], ...

---

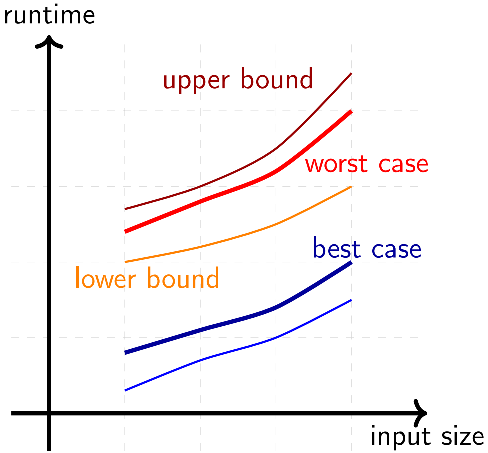
[44] N. Hirokawa, G. Moser: *Automated complexity analysis based on the dependency pair method*, IJCAR '08

[45] M. Avanzini, G. Moser: *Dependency pairs and polynomial path orders*, RTA '09

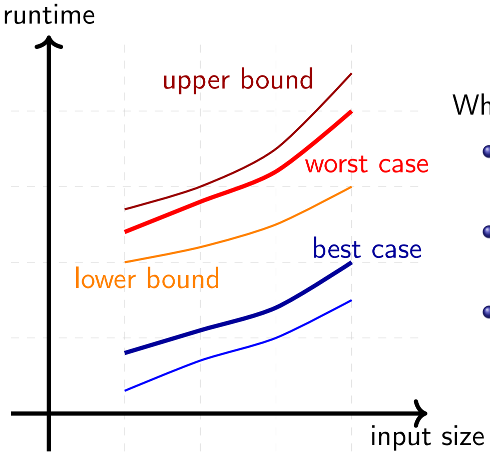
[46] N. Hirokawa, G. Moser: *Automated complexity analysis based on context-sensitive rewriting*, RTA-TLCA '14

[47] M. Avanzini, G. Moser: *A combination framework for complexity*, IC '16

How about Lower Bounds for Complexity?



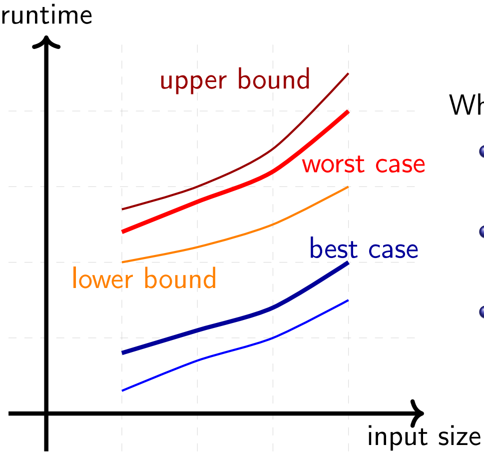
How about Lower Bounds for Complexity?



Why lower bounds?

- get **tight bounds** with upper bounds
- can indicate implementation bugs
- security: single query can trigger Denial of Service

How about Lower Bounds for Complexity?



Why lower bounds?

- get **tight bounds** with upper bounds
- can indicate implementation bugs
- security: single query can trigger Denial of Service

Here: Two techniques for finding lower bounds[48] inspired by proving **non-termination**

[48] F. Frohn, J. Giesl, J. Hensel, C. Aschermann, and T. Ströder: *Lower bounds for runtime complexity of term rewriting*, JAR '17

Finding Lower Bounds by Induction

(1) Induction technique, inspired by **non-looping** non-termination[49]

Finding Lower Bounds by Induction

(1) Induction technique, inspired by **non-looping** non-termination[49]

- Generate infinite family $\mathcal{T}_{\text{witness}}$ of basic terms as witnesses in

$$\forall n \in \mathbb{N}. \quad \exists t_n \in \mathcal{T}_{\text{witness}}. \quad |t_n| \leq q(n) \quad \wedge \quad \text{dh}(t_n, \to_{\mathcal{R}}) \geq p(n)$$

to conclude $\text{rc}_{\mathcal{R}}(n) \in \Omega(p'(n))$.

[49] F. Emmes, T. Enger, J. Giesl: *Proving non-looping non-termination automatically*, IJCAR '12

Finding Lower Bounds by Induction

(1) Induction technique, inspired by **non-looping** non-termination[49]

- Generate infinite family $\mathcal{T}_{\text{witness}}$ of basic terms as witnesses in

$$\forall n \in \mathbb{N}. \quad \exists t_n \in \mathcal{T}_{\text{witness}}. \quad |t_n| \leq q(n) \quad \wedge \quad \text{dh}(t_n, \to_{\mathcal{R}}) \geq p(n)$$

  to conclude $\text{rc}_{\mathcal{R}}(n) \in \Omega(p'(n))$.

- Constructor terms for arguments can be built recursively after type inference: $0, \mathsf{s}(0), \mathsf{s}(\mathsf{s}(0)), \ldots$ (here $q(n) = n + 1$, often linear)

[49] F. Emmes, T. Enger, J. Giesl: *Proving non-looping non-termination automatically*, IJCAR '12

Finding Lower Bounds by Induction

(1) Induction technique, inspired by **non-looping** non-termination[49]

- Generate infinite family $\mathcal{T}_{\text{witness}}$ of basic terms as witnesses in

$$\forall n \in \mathbb{N}. \quad \exists t_n \in \mathcal{T}_{\text{witness}}. \quad |t_n| \leq q(n) \quad \wedge \quad \text{dh}(t_n, \to_{\mathcal{R}}) \geq p(n)$$

  to conclude $\text{rc}_{\mathcal{R}}(n) \in \Omega(p'(n))$.
- Constructor terms for arguments can be built recursively after type inference: $0, \mathsf{s}(0), \mathsf{s}(\mathsf{s}(0)), \ldots$ (here $q(n) = n + 1$, often linear)
- Evaluate t_n by narrowing, get rewrite sequences with recursive calls

[49] F. Emmes, T. Enger, J. Giesl: *Proving non-looping non-termination automatically*, IJCAR '12

Finding Lower Bounds by Induction

(1) Induction technique, inspired by **non-looping** non-termination[49]

- Generate infinite family $\mathcal{T}_{\text{witness}}$ of basic terms as witnesses in

$$\forall n \in \mathbb{N}. \quad \exists t_n \in \mathcal{T}_{\text{witness}}. \quad |t_n| \leq q(n) \quad \wedge \quad \mathrm{dh}(t_n, \to_{\mathcal{R}}) \geq p(n)$$

  to conclude $\mathrm{rc}_{\mathcal{R}}(n) \in \Omega(p'(n))$.
- Constructor terms for arguments can be built recursively after type inference: $0, \mathsf{s}(0), \mathsf{s}(\mathsf{s}(0)), \ldots$ (here $q(n) = n + 1$, often linear)
- Evaluate t_n by narrowing, get rewrite sequences with recursive calls
- Speculate polynomial $p(n)$ based on values for $n = 0, 1, \ldots, k$

[49] F. Emmes, T. Enger, J. Giesl: *Proving non-looping non-termination automatically*, IJCAR '12

Finding Lower Bounds by Induction

(1) Induction technique, inspired by **non-looping** non-termination[49]

- Generate infinite family $\mathcal{T}_{\text{witness}}$ of basic terms as witnesses in

$$\forall n \in \mathbb{N}. \quad \exists t_n \in \mathcal{T}_{\text{witness}}. \quad |t_n| \leq q(n) \quad \wedge \quad \text{dh}(t_n, \rightarrow_{\mathcal{R}}) \geq p(n)$$

  to conclude $\text{rc}_{\mathcal{R}}(n) \in \Omega(p'(n))$.
- Constructor terms for arguments can be built recursively after type inference: $0, \mathsf{s}(0), \mathsf{s}(\mathsf{s}(0)), \ldots$ (here $q(n) = n + 1$, often linear)
- Evaluate t_n by narrowing, get rewrite sequences with recursive calls
- Speculate polynomial $p(n)$ based on values for $n = 0, 1, \ldots, k$
- Prove rewrite lemma $t_n \rightarrow_{\mathcal{R}}^{\geq p(n)} t'_n$ inductively

[49] F. Emmes, T. Enger, J. Giesl: *Proving non-looping non-termination automatically*, IJCAR '12

Finding Lower Bounds by Induction

(1) Induction technique, inspired by **non-looping** non-termination[49]

- Generate infinite family $\mathcal{T}_{\text{witness}}$ of basic terms as witnesses in

$$\forall n \in \mathbb{N}. \quad \exists t_n \in \mathcal{T}_{\text{witness}}. \quad |t_n| \leq q(n) \quad \wedge \quad \text{dh}(t_n, \to_{\mathcal{R}}) \geq p(n)$$

  to conclude $\text{rc}_{\mathcal{R}}(n) \in \Omega(p'(n))$.
- Constructor terms for arguments can be built recursively after type inference: $0, s(0), s(s(0)), \ldots$ (here $q(n) = n + 1$, often linear)
- Evaluate t_n by narrowing, get rewrite sequences with recursive calls
- Speculate polynomial $p(n)$ based on values for $n = 0, 1, \ldots, k$
- Prove rewrite lemma $t_n \to_{\mathcal{R}}^{\geq p(n)} t'_n$ inductively
- Get lower bound for $\text{rc}_{\mathcal{R}}(n)$ from $p(n)$ in rewrite lemma and $q(n)$

[49] F. Emmes, T. Enger, J. Giesl: *Proving non-looping non-termination automatically*, IJCAR '12

Finding Lower Bounds by Induction: Example

Example (quicksort)

$$
\begin{aligned}
\mathsf{qs}(\mathsf{nil}) &\to \mathsf{nil}\\
\mathsf{qs}(\mathsf{cons}(x, xs)) &\to \mathsf{qs}(\mathsf{low}(x, xs)) \mathbin{++} \mathsf{cons}(x, \mathsf{qs}(\mathsf{low}(x, xs)))\\
\mathsf{low}(x, \mathsf{nil}) &\to \mathsf{nil}\\
\mathsf{low}(x, \mathsf{cons}(y, ys)) &\to \mathsf{if}(x \leq y, x, \mathsf{cons}(y, ys))\\
\mathsf{if}(\mathsf{tt}, x, \mathsf{cons}(y, ys)) &\to \mathsf{low}(x, ys)\\
\mathsf{if}(\mathsf{ff}, x, \mathsf{cons}(y, ys)) &\to \mathsf{cons}(y, \mathsf{low}(x, ys))\\
&\ldots
\end{aligned}
$$

Finding Lower Bounds by Induction: Example

Example (quicksort)

$$
\begin{aligned}
\mathsf{qs}(\mathsf{nil}) &\to \mathsf{nil} \\
\mathsf{qs}(\mathsf{cons}(x, xs)) &\to \mathsf{qs}(\mathsf{low}(x, xs)) \mathbin{++} \mathsf{cons}(x, \mathsf{qs}(\mathsf{low}(x, xs))) \\
\mathsf{low}(x, \mathsf{nil}) &\to \mathsf{nil} \\
\mathsf{low}(x, \mathsf{cons}(y, ys)) &\to \mathsf{if}(x \leq y, x, \mathsf{cons}(y, ys)) \\
\mathsf{if}(\mathsf{tt}, x, \mathsf{cons}(y, ys)) &\to \mathsf{low}(x, ys) \\
\mathsf{if}(\mathsf{ff}, x, \mathsf{cons}(y, ys)) &\to \mathsf{cons}(y, \mathsf{low}(x, ys)) \\
&\ldots
\end{aligned}
$$

Speculate and prove rewrite lemma:

$$
\mathsf{qs}(\mathsf{cons}(\mathsf{zero}, \ldots, \mathsf{cons}(\mathsf{zero}, \mathsf{nil}))) \to^{3n^2+2n+1} \mathsf{cons}(\mathsf{zero}, \ldots, \mathsf{cons}(\mathsf{zero}, \mathsf{nil}))
$$

Finding Lower Bounds by Induction: Example

Example (quicksort)

$$
\begin{array}{rcl}
\mathsf{qs}(\mathsf{nil}) & \to & \mathsf{nil} \\
\mathsf{qs}(\mathsf{cons}(x, xs)) & \to & \mathsf{qs}(\mathsf{low}(x, xs)) \mathbin{++} \mathsf{cons}(x, \mathsf{qs}(\mathsf{low}(x, xs))) \\
\mathsf{low}(x, \mathsf{nil}) & \to & \mathsf{nil} \\
\mathsf{low}(x, \mathsf{cons}(y, ys)) & \to & \mathsf{if}(x \leq y, x, \mathsf{cons}(y, ys)) \\
\mathsf{if}(\mathsf{tt}, x, \mathsf{cons}(y, ys)) & \to & \mathsf{low}(x, ys) \\
\mathsf{if}(\mathsf{ff}, x, \mathsf{cons}(y, ys)) & \to & \mathsf{cons}(y, \mathsf{low}(x, ys)) \\
 & \ldots &
\end{array}
$$

Speculate and prove rewrite lemma:

$$
\begin{array}{r}
\mathsf{qs}(\mathsf{cons}(\mathsf{zero}, \ldots, \mathsf{cons}(\mathsf{zero}, \mathsf{nil}))) \to^{3n^2+2n+1} \mathsf{cons}(\mathsf{zero}, \ldots, \mathsf{cons}(\mathsf{zero}, \mathsf{nil})) \\
\mathsf{qs}(\mathsf{cons}^n(\mathsf{zero}, \mathsf{nil})) \to^{3n^2+2n+1} \mathsf{cons}(\mathsf{zero}, \ldots, \mathsf{cons}(\mathsf{zero}, \mathsf{nil}))
\end{array}
$$

Finding Lower Bounds by Induction: Example

Example (quicksort)

$$
\begin{aligned}
\mathsf{qs}(\mathsf{nil}) &\to \mathsf{nil}\\
\mathsf{qs}(\mathsf{cons}(x, xs)) &\to \mathsf{qs}(\mathsf{low}(x, xs)) \mathbin{++} \mathsf{cons}(x, \mathsf{qs}(\mathsf{low}(x, xs)))\\
\mathsf{low}(x, \mathsf{nil}) &\to \mathsf{nil}\\
\mathsf{low}(x, \mathsf{cons}(y, ys)) &\to \mathsf{if}(x \leq y, x, \mathsf{cons}(y, ys))\\
\mathsf{if}(\mathsf{tt}, x, \mathsf{cons}(y, ys)) &\to \mathsf{low}(x, ys)\\
\mathsf{if}(\mathsf{ff}, x, \mathsf{cons}(y, ys)) &\to \mathsf{cons}(y, \mathsf{low}(x, ys))\\
&\ldots
\end{aligned}
$$

Speculate and prove rewrite lemma:

$$
\begin{aligned}
\mathsf{qs}(\mathsf{cons}(\mathsf{zero}, \ldots, \mathsf{cons}(\mathsf{zero}, \mathsf{nil}))) &\to^{3n^2+2n+1} \mathsf{cons}(\mathsf{zero}, \ldots, \mathsf{cons}(\mathsf{zero}, \mathsf{nil}))\\
\mathsf{qs}(\mathsf{cons}^n(\mathsf{zero}, \mathsf{nil})) &\to^{3n^2+2n+1} \mathsf{cons}(\mathsf{zero}, \ldots, \mathsf{cons}(\mathsf{zero}, \mathsf{nil}))
\end{aligned}
$$

From $|\mathsf{qs}(\mathsf{cons}^n(\mathsf{zero}, \mathsf{nil}))| = 2n + 2$ we get

$$\mathrm{rc}_{\mathcal{R}}(2n + 2) \geq 3n^2 + 2n + 1$$

Finding Lower Bounds by Induction: Example

Example (quicksort)

$$
\begin{aligned}
\mathsf{qs}(\mathsf{nil}) &\to \mathsf{nil} \\
\mathsf{qs}(\mathsf{cons}(x, xs)) &\to \mathsf{qs}(\mathsf{low}(x, xs)) \mathbin{++} \mathsf{cons}(x, \mathsf{qs}(\mathsf{low}(x, xs))) \\
\mathsf{low}(x, \mathsf{nil}) &\to \mathsf{nil} \\
\mathsf{low}(x, \mathsf{cons}(y, ys)) &\to \mathsf{if}(x \leq y, x, \mathsf{cons}(y, ys)) \\
\mathsf{if}(\mathsf{tt}, x, \mathsf{cons}(y, ys)) &\to \mathsf{low}(x, ys) \\
\mathsf{if}(\mathsf{ff}, x, \mathsf{cons}(y, ys)) &\to \mathsf{cons}(y, \mathsf{low}(x, ys)) \\
&\ldots
\end{aligned}
$$

Speculate and prove rewrite lemma:

$$
\begin{aligned}
\mathsf{qs}(\mathsf{cons}(\mathsf{zero}, \ldots, \mathsf{cons}(\mathsf{zero}, \mathsf{nil}))) &\to^{3n^2+2n+1} \mathsf{cons}(\mathsf{zero}, \ldots, \mathsf{cons}(\mathsf{zero}, \mathsf{nil})) \\
\mathsf{qs}(\mathsf{cons}^n(\mathsf{zero}, \mathsf{nil})) &\to^{3n^2+2n+1} \mathsf{cons}(\mathsf{zero}, \ldots, \mathsf{cons}(\mathsf{zero}, \mathsf{nil}))
\end{aligned}
$$

From $|\mathsf{qs}(\mathsf{cons}^n(\mathsf{zero}, \mathsf{nil}))| = 2n + 2$ we get

$\mathrm{rc}_{\mathcal{R}}(2n+2) \geq 3n^2 + 2n + 1$ and $\mathrm{rc}_{\mathcal{R}}(n) \in \Omega(n^2)$.

Finding Linear Lower Bounds by Decreasing Loops

(2) Decreasing loops, inspired by **looping** non-termination with

$$s \to_{\mathcal{R}}^{+} C[s\sigma] \to_{\mathcal{R}}^{+} C[C\sigma[s\sigma^2]] \to_{\mathcal{R}}^{+} \cdots$$

Example: $\mathsf{f}(y) \to \mathsf{f}(\mathsf{s}(y))$ has loop $\mathsf{f}(y) \to_{\mathcal{R}}^{+} \mathsf{f}(\mathsf{s}(y))$ with $\sigma(y) = \mathsf{0}$.

Finding Linear Lower Bounds by Decreasing Loops

(2) Decreasing loops, inspired by **looping** non-termination with

$$s \to_{\mathcal{R}}^{+} C[s\sigma] \to_{\mathcal{R}}^{+} C[C\sigma[s\sigma^2]] \to_{\mathcal{R}}^{+} \cdots$$

Example: $\mathsf{f}(y) \to \mathsf{f}(\mathsf{s}(y))$ has loop $\mathsf{f}(y) \to_{\mathcal{R}}^{+} \mathsf{f}(\mathsf{s}(y))$ with $\sigma(y) = \mathsf{0}$.

Intuition for **linear** lower bounds:
some fixed context D is **removed** in an argument of recursive call, other arguments may grow, sequence can be repeated (loop)

Finding Linear Lower Bounds by Decreasing Loops

(2) Decreasing loops, inspired by **looping** non-termination with

$$s \to_{\mathcal{R}}^{+} C[s\sigma] \to_{\mathcal{R}}^{+} C[C\sigma[s\sigma^2]] \to_{\mathcal{R}}^{+} \cdots$$

Example: $\mathsf{f}(y) \to \mathsf{f}(\mathsf{s}(y))$ has loop $\mathsf{f}(y) \to_{\mathcal{R}}^{+} \mathsf{f}(\mathsf{s}(y))$ with $\sigma(y) = \mathsf{0}$.

Intuition for **linear** lower bounds:
some fixed context D is **removed** in an argument of recursive call, other arguments may grow, sequence can be repeated (loop)

Example: $\mathsf{plus}(\mathsf{s}(x), y) \to \mathsf{plus}(x, \mathsf{s}(y))$ has **decreasing** loop

$$\mathsf{plus}(\mathsf{s}(x), y) \to_{\mathcal{R}}^{+} \mathsf{plus}(x, \mathsf{s}(y)) \text{ with } D[x] = \mathsf{s}(x)$$

Finding Linear Lower Bounds by Decreasing Loops

(2) Decreasing loops, inspired by **looping** non-termination with

$$s \to_{\mathcal{R}}^{+} C[s\sigma] \to_{\mathcal{R}}^{+} C[C\sigma[s\sigma^2]] \to_{\mathcal{R}}^{+} \cdots$$

Example: $\mathsf{f}(y) \to \mathsf{f}(\mathsf{s}(y))$ has loop $\mathsf{f}(y) \to_{\mathcal{R}}^{+} \mathsf{f}(\mathsf{s}(y))$ with $\sigma(y) = \mathsf{0}$.

Intuition for **linear** lower bounds:
some fixed context D is **removed** in an argument of recursive call, other arguments may grow, sequence can be repeated (loop)

Example: $\mathsf{plus}(\mathsf{s}(x), y) \to \mathsf{plus}(x, \mathsf{s}(y))$ has **decreasing** loop

$$\mathsf{plus}(\mathsf{s}(x), y) \to_{\mathcal{R}}^{+} \mathsf{plus}(x, \mathsf{s}(y)) \text{ with } D[x] = \mathsf{s}(x)$$

for *base term* $s = \mathsf{plus}(x, y)$, *pumping substitution* $\theta = [x \mapsto \mathsf{s}(x)]$, and *result substitution* $\sigma = [y \mapsto \mathsf{s}(y)]$:

$$s\theta \to_{\mathcal{R}}^{+} C[s\sigma]$$

Implies $\mathrm{rc}(n) \in \Omega(n)$!

Finding Exponential Lower Bounds by Decreasing Loops

Exponential lower bounds: several "compatible" parallel recursive calls:

- **Example:** $\mathsf{fib}(\mathsf{s}(\mathsf{s}(n))) \to \mathsf{plus}(\mathsf{fib}(\mathsf{s}(n)), \mathsf{fib}(n))$ has 2 decreasing loops:

  $$\mathsf{fib}(\mathsf{s}(\mathsf{s}(n))) \to_{\mathcal{R}}^{+} C[\mathsf{fib}(\mathsf{s}(n))] \quad \text{and} \quad \mathsf{fib}(\mathsf{s}(\mathsf{s}(n))) \to_{\mathcal{R}}^{+} C[\mathsf{fib}(n)]$$

  Implies $\mathrm{rc}(n) \in \Omega(2^n)$!

Finding Exponential Lower Bounds by Decreasing Loops

Exponential lower bounds: several "compatible" parallel recursive calls:

- **Example:** $\mathsf{fib}(\mathsf{s}(\mathsf{s}(n))) \to \mathsf{plus}(\mathsf{fib}(\mathsf{s}(n)), \mathsf{fib}(n))$ has 2 decreasing loops:

  $$\mathsf{fib}(\mathsf{s}(\mathsf{s}(n))) \to_{\mathcal{R}}^{+} C[\mathsf{fib}(\mathsf{s}(n))] \quad \text{and} \quad \mathsf{fib}(\mathsf{s}(\mathsf{s}(n))) \to_{\mathcal{R}}^{+} C[\mathsf{fib}(n)]$$

  Implies $\mathrm{rc}(n) \in \Omega(2^n)$!

- **(Non-)Example:** $\mathsf{tr}(\mathsf{node}(x, y)) \to \mathsf{node}(\mathsf{tr}(x), \mathsf{tr}(y))$

  Has **linear** complexity. But:

  $$\mathsf{tr}(\mathsf{node}(x, y)) \to_{\mathcal{R}}^{+} C[\mathsf{tr}(x)] \quad \text{and} \quad \mathsf{tr}(\mathsf{node}(x, y)) \to_{\mathcal{R}}^{+} C[\mathsf{tr}(y)]$$

  are not compatible (their pumping substitutions do not commute).

Finding Exponential Lower Bounds by Decreasing Loops

Exponential lower bounds: several "compatible" parallel recursive calls:

- **Example:** $\mathsf{fib}(\mathsf{s}(\mathsf{s}(n))) \to \mathsf{plus}(\mathsf{fib}(\mathsf{s}(n)), \mathsf{fib}(n))$ has 2 decreasing loops:

  $$\mathsf{fib}(\mathsf{s}(\mathsf{s}(n))) \to_{\mathcal{R}}^{+} C[\mathsf{fib}(\mathsf{s}(n))] \quad \text{and} \quad \mathsf{fib}(\mathsf{s}(\mathsf{s}(n))) \to_{\mathcal{R}}^{+} C[\mathsf{fib}(n)]$$

  Implies $\mathrm{rc}(n) \in \Omega(2^n)$!

- **(Non-)Example:** $\mathsf{tr}(\mathsf{node}(x, y)) \to \mathsf{node}(\mathsf{tr}(x), \mathsf{tr}(y))$

  Has **linear** complexity. But:

  $$\mathsf{tr}(\mathsf{node}(x, y)) \to_{\mathcal{R}}^{+} C[\mathsf{tr}(x)] \quad \text{and} \quad \mathsf{tr}(\mathsf{node}(x, y)) \to_{\mathcal{R}}^{+} C[\mathsf{tr}(y)]$$

  are not compatible (their pumping substitutions do not commute).

Automation for decreasing loops: **narrowing**.

Lower Bounds: Induction Technique vs Decreasing Loops

Benefits of Induction Technique:

- Can find **non-linear** polynomial lower bounds
- Also works on non-left-linear TRSs

Lower Bounds: Induction Technique vs Decreasing Loops

Benefits of Induction Technique:

- Can find **non-linear** polynomial lower bounds
- Also works on non-left-linear TRSs

Benefits of Decreasing Loops:

- Does not rely as much on heuristics
- Computationally more lightweight

Lower Bounds: Induction Technique vs Decreasing Loops

Benefits of Induction Technique:

- Can find **non-linear** polynomial lower bounds
- Also works on non-left-linear TRSs

Benefits of Decreasing Loops:

- Does not rely as much on heuristics
- Computationally more lightweight

$\Rightarrow$ First try decreasing loops, then induction technique

Lower Bounds: Induction Technique vs Decreasing Loops

Benefits of Induction Technique:

- Can find **non-linear** polynomial lower bounds
- Also works on non-left-linear TRSs

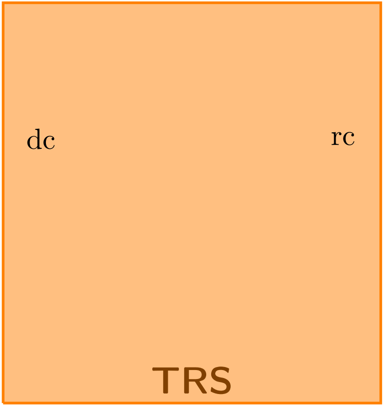
Benefits of Decreasing Loops:

- Does not rely as much on heuristics
- Computationally more lightweight

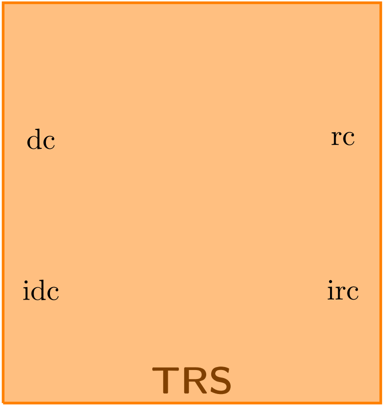
$\Rightarrow$ First try decreasing loops, then induction technique

Both techniques can be adapted to innermost runtime complexity!

A Landscape of Complexity Properties and Transformations

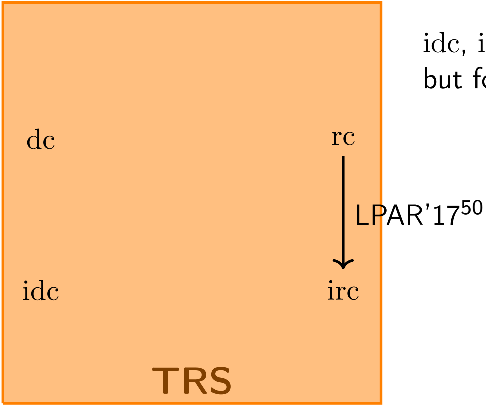


A Landscape of Complexity Properties and Transformations



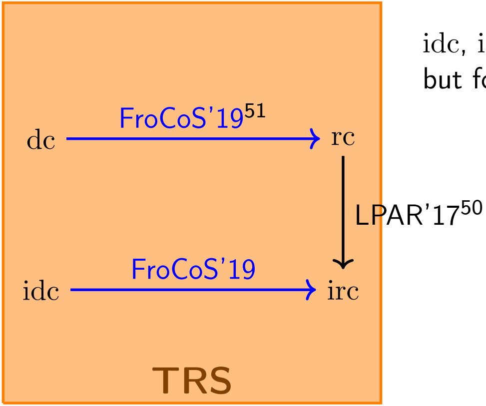
idc, irc: like dc, rc,
but for *innermost* rewriting

A Landscape of Complexity Properties and Transformations



idc, irc: like dc, rc,
but for *innermost* rewriting

[50] F. Frohn, J. Giesl: *Analyzing runtime complexity via innermost runtime complexity*, LPAR '17



idc, irc: like dc, rc,
but for *innermost* rewriting

[50] F. Frohn, J. Giesl: *Analyzing runtime complexity via innermost runtime complexity*, LPAR '17

[51] C. Fuhs: *Transforming Derivational Complexity of Term Rewriting to Runtime Complexity*, FroCoS '19

Transforming Derivational Complexity to Runtime Complexity

The big picture:

- **Have:** Tool for automated analysis of runtime complexity $\mathrm{rc}_{\mathcal{R}}$

Transforming Derivational Complexity to Runtime Complexity

The big picture:

- **Have:** Tool for automated analysis of runtime complexity $\mathrm{rc}_{\mathcal{R}}$
- **Want:** Tool for automated analysis of derivational complexity $\mathrm{dc}_{\mathcal{R}}$

Transforming Derivational Complexity to Runtime Complexity

The big picture:

- **Have:** Tool for automated analysis of runtime complexity $\mathrm{rc}_{\mathcal{R}}$
- **Want:** Tool for automated analysis of derivational complexity $\mathrm{dc}_{\mathcal{R}}$
- **Idea:**

  "$\mathrm{rc}_{\mathcal{R}}$ analysis tool + transformation on TRS $\mathcal{R}$ = $\mathrm{dc}_{\mathcal{R}}$ analysis tool"

Transforming Derivational Complexity to Runtime Complexity

The big picture:

- **Have:** Tool for automated analysis of runtime complexity $\mathrm{rc}_{\mathcal{R}}$
- **Want:** Tool for automated analysis of derivational complexity $\mathrm{dc}_{\mathcal{R}}$
- **Idea:**

  "$\mathrm{rc}_{\mathcal{R}}$ analysis tool + transformation on TRS $\mathcal{R}$ = $\mathrm{dc}_{\mathcal{R}}$ analysis tool"

- **Benefits:**
  - Get analysis of derivational complexity "for free"
  - Progress in runtime complexity analysis automatically improves derivational complexity analysis

From dc to rc: Results

- program transformation such that runtime complexity of transformed TRS is **identical** to derivational complexity of original TRS

From dc to rc: Results

- program transformation such that runtime complexity of transformed TRS is **identical** to derivational complexity of original TRS
- transformation correct also from idc to irc

From dc to rc: Results

- program transformation such that runtime complexity of transformed TRS is **identical** to derivational complexity of original TRS
- transformation correct also from idc to irc
- **implemented** in program analysis tool AProVE

From dc to rc: Results

- program transformation such that runtime complexity of transformed TRS is **identical** to derivational complexity of original TRS
- transformation correct also from idc to irc
- **implemented** in program analysis tool AProVE
- **evaluated** successfully on TPDB[52] relative to state of the art TcT

[52] Termination Problem DataBase, standard benchmark source for annual Termination Competition (termCOMP) with 1000s of problems, http://termination-portal.org/wiki/TPDB

From dc to rc: Transformation

Issue:

- Runtime complexity assumes **basic** terms as start terms
- We want to analyse complexity for **arbitrary** terms

From dc to rc: Transformation

Issue:

- Runtime complexity assumes **basic** terms as start terms
- We want to analyse complexity for **arbitrary** terms

Idea:

- Introduce constructor symbol c_f for defined symbol f

From dc to rc: Transformation

Issue:

- Runtime complexity assumes **basic** terms as start terms
- We want to analyse complexity for **arbitrary** terms

Idea:

- Introduce constructor symbol c_f for defined symbol f
- Add **generator rewrite rules** $\mathcal{G}$ to reconstruct arbitrary term with f from basic term with c_f

From dc to rc: Transformation

Issue:

- Runtime complexity assumes **basic** terms as start terms
- We want to analyse complexity for **arbitrary** terms

Idea:

- Introduce constructor symbol c_f for defined symbol f
- Add **generator rewrite rules** $\mathcal{G}$ to reconstruct arbitrary term with f from basic term with c_f

Represent

$t = \mathsf{double}(\mathsf{double}(\mathsf{double}(\mathsf{s}(0))))$

From dc to rc: Transformation

Issue:

- Runtime complexity assumes **basic** terms as start terms
- We want to analyse complexity for **arbitrary** terms

Idea:

- Introduce constructor symbol c_f for defined symbol f
- Add **generator rewrite rules** $\mathcal{G}$ to reconstruct arbitrary term with f from basic term with c_f

Represent

$$t = \mathsf{double}(\mathsf{double}(\mathsf{double}(\mathsf{s}(\mathsf{0}))))$$

by **basic variant**

$$\mathrm{bv}(t) = \mathsf{enc}_{\mathsf{double}}(\mathsf{c}_{\mathsf{double}}(\mathsf{c}_{\mathsf{double}}(\mathsf{s}(\mathsf{0}))))$$

From dc to rc: Transformation

Issue:

- Runtime complexity assumes **basic** terms as start terms
- We want to analyse complexity for **arbitrary** terms

Idea:

- Introduce constructor symbol c_f for defined symbol f
- Add **generator rewrite rules** $\mathcal{G}$ to reconstruct arbitrary term with f from basic term with c_f

Represent

$$t = \mathsf{double}(\mathsf{double}(\mathsf{double}(\mathsf{s}(\mathsf{0}))))$$

by **basic variant**

$$\mathrm{bv}(t) = \mathsf{enc}_{\mathsf{double}}(\mathsf{c}_{\mathsf{double}}(\mathsf{c}_{\mathsf{double}}(\mathsf{s}(\mathsf{0}))))$$

Example (Generator rules $\mathcal{G}$)

$$\begin{aligned}
\mathsf{enc}_{\mathsf{double}}(x) &\to \mathsf{double}(\mathsf{argenc}(x)) \\
\mathsf{enc}_{\mathsf{0}} &\to \mathsf{0} \\
\mathsf{enc}_{\mathsf{s}}(x) &\to \mathsf{s}(\mathsf{argenc}(x)) \\
\mathsf{argenc}(\mathsf{c}_{\mathsf{double}}(x)) &\to \mathsf{double}(\mathsf{argenc}(x)) \\
\mathsf{argenc}(\mathsf{0}) &\to \mathsf{0} \\
\mathsf{argenc}(\mathsf{s}(x)) &\to \mathsf{s}(\mathsf{argenc}(x))
\end{aligned}$$

From dc to rc: Transformation

Issue:

- Runtime complexity assumes **basic** terms as start terms
- We want to analyse complexity for **arbitrary** terms

Idea:

- Introduce constructor symbol c_f for defined symbol f
- Add **generator rewrite rules** $\mathcal{G}$ to reconstruct arbitrary term with f from basic term with c_f

Represent

$$t = \mathsf{double}(\mathsf{double}(\mathsf{double}(\mathsf{s}(0))))$$

by **basic variant**

$$\mathrm{bv}(t) = \mathsf{enc}_{\mathsf{double}}(\mathsf{c}_{\mathsf{double}}(\mathsf{c}_{\mathsf{double}}(\mathsf{s}(0))))$$

Then:

- $\mathrm{bv}(t)$ is **basic** term, size $|t|$

Example (Generator rules $\mathcal{G}$)

$$\begin{aligned}
\mathsf{enc}_{\mathsf{double}}(x) &\to \mathsf{double}(\mathsf{argenc}(x))\\
\mathsf{enc}_{0} &\to 0\\
\mathsf{enc}_{\mathsf{s}}(x) &\to \mathsf{s}(\mathsf{argenc}(x))\\
\mathsf{argenc}(\mathsf{c}_{\mathsf{double}}(x)) &\to \mathsf{double}(\mathsf{argenc}(x))\\
\mathsf{argenc}(0) &\to 0\\
\mathsf{argenc}(\mathsf{s}(x)) &\to \mathsf{s}(\mathsf{argenc}(x))
\end{aligned}$$

From dc to rc: Transformation

Issue:

- Runtime complexity assumes **basic** terms as start terms
- We want to analyse complexity for **arbitrary** terms

Idea:

- Introduce constructor symbol c_f for defined symbol f
- Add **generator rewrite rules** $\mathcal{G}$ to reconstruct arbitrary term with f from basic term with c_f

Represent

$$t = \mathsf{double}(\mathsf{double}(\mathsf{double}(\mathsf{s}(\mathsf{0}))))$$

by **basic variant**

$$\mathrm{bv}(t) = \mathsf{enc}_{\mathsf{double}}(\mathsf{c}_{\mathsf{double}}(\mathsf{c}_{\mathsf{double}}(\mathsf{s}(\mathsf{0}))))$$

Then:

- $\mathrm{bv}(t)$ is **basic** term, size $|t|$
- $\mathrm{bv}(t) \to_{\mathcal{G}}^{*} t$

Example (Generator rules $\mathcal{G}$)

$$\begin{aligned}
\mathsf{enc}_{\mathsf{double}}(x) &\to \mathsf{double}(\mathsf{argenc}(x))\\
\mathsf{enc}_{\mathsf{0}} &\to \mathsf{0}\\
\mathsf{enc}_{\mathsf{s}}(x) &\to \mathsf{s}(\mathsf{argenc}(x))\\
\mathsf{argenc}(\mathsf{c}_{\mathsf{double}}(x)) &\to \mathsf{double}(\mathsf{argenc}(x))\\
\mathsf{argenc}(\mathsf{0}) &\to \mathsf{0}\\
\mathsf{argenc}(\mathsf{s}(x)) &\to \mathsf{s}(\mathsf{argenc}(x))
\end{aligned}$$

General Case: Relative Rewriting

Issue:

- $\to_{\mathcal{R} \cup \mathcal{G}}$ has extra rewrite steps not present in $\to_{\mathcal{R}}$
- may change complexity

General Case: Relative Rewriting

Issue:

- $\to_{\mathcal{R}\cup\mathcal{G}}$ has extra rewrite steps not present in $\to_{\mathcal{R}}$
- may change complexity

Solution:

- add $\mathcal{G}$ as **relative** rewrite rules:
  $\to_{\mathcal{G}}$ steps are **not counted** for complexity analysis!
- transform $\mathcal{R}$ to $\mathcal{R}/\mathcal{G}$ ($\to_{\mathcal{R}}$ steps are counted, $\to_{\mathcal{G}}$ steps are not)

General Case: Relative Rewriting

Issue:

- $\rightarrow_{\mathcal{R} \cup \mathcal{G}}$ has extra rewrite steps not present in $\rightarrow_{\mathcal{R}}$
- may change complexity

Solution:

- add $\mathcal{G}$ as **relative** rewrite rules:
  $\rightarrow_{\mathcal{G}}$ steps are **not counted** for complexity analysis!
- transform $\mathcal{R}$ to $\mathcal{R}/\mathcal{G}$ ($\rightarrow_{\mathcal{R}}$ steps are counted, $\rightarrow_{\mathcal{G}}$ steps are not)
- more generally: transform $\mathcal{R}/\mathcal{S}$ to $\mathcal{R}/(\mathcal{S} \cup \mathcal{G})$
  (input may contain relative rules $\mathcal{S}$, too)

From dc to rc: Correctness

Theorem (Derivational Complexity via Runtime Complexity)

Let $\mathcal{R}/\mathcal{S}$ be a relative TRS, let $\mathcal{G}$ be the generator rules for $\mathcal{R}/\mathcal{S}$. Then

1. $\mathrm{dc}_{\mathcal{R}/\mathcal{S}}(n) = \mathrm{rc}_{\mathcal{R}/(\mathcal{S} \cup \mathcal{G})}(n)$ *(arbitrary rewrite strategies)*
2. $\mathrm{idc}_{\mathcal{R}/\mathcal{S}}(n) = \mathrm{irc}_{\mathcal{R}/(\mathcal{S} \cup \mathcal{G})}(n)$ *(innermost rewriting)*

Note: equalities hold also non-asymptotically!

From (i)dc to (i)rc: Experiments

Experiments on TPDB, compare with state of the art in TcT:

- upper bounds idc: both AProVE and TcT with transformation are stronger than standard TcT
- upper bounds dc: TcT stronger than AProVE and TcT with transformation, but AProVE still solves some new examples
- lower bounds idc and dc: heuristics do not seem to benefit much

From (i)dc to (i)rc: Experiments

Experiments on TPDB, compare with state of the art in TcT:

- upper bounds idc: both AProVE and TcT with transformation are stronger than standard TcT
- upper bounds dc: TcT stronger than AProVE and TcT with transformation, but AProVE still solves some new examples
- lower bounds idc and dc: heuristics do not seem to benefit much

$\Rightarrow$ Transformation-based approach should be part of the portfolio of analysis tools for derivational complexity

Derivational Complexity: Future Work

- **Possible applications**
  - compiler simplifications
  - SMT solver preprocessing

  Start terms may have nested defined symbols, so $\mathrm{dc}_{\mathcal{R}}$ is appropriate

- **Possible applications**
  - compiler simplifications
  - SMT solver preprocessing

  Start terms may have nested defined symbols, so $\mathrm{dc}_{\mathcal{R}}$ is appropriate

- Go **between** derivational and runtime complexity
  - So far: encode *full* term universe $\mathcal{T}$ via basic terms $\mathcal{T}_{\mathrm{basic}}$
  - Generalise: write relative rules to generate **arbitrary** set $\mathcal{U}$ of terms "between" basic and all terms ($\mathcal{T}_{\mathrm{basic}} \subseteq \mathcal{U} \subseteq \mathcal{T}$).

Derivational Complexity: Future Work

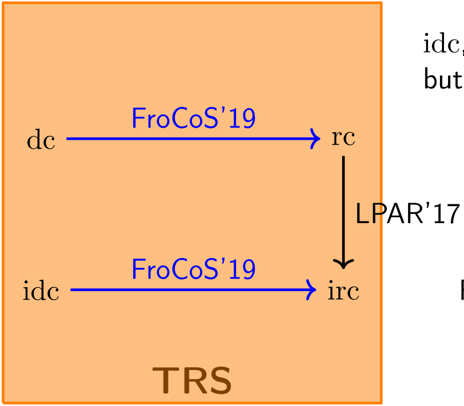
- **Possible applications**
  - compiler simplifications
  - SMT solver preprocessing

  Start terms may have nested defined symbols, so $\mathrm{dc}_{\mathcal{R}}$ is appropriate

- Go **between** derivational and runtime complexity
  - So far: encode *full* term universe $\mathcal{T}$ via basic terms $\mathcal{T}_{\mathrm{basic}}$
  - Generalise: write relative rules to generate **arbitrary** set $\mathcal{U}$ of terms "between" basic and all terms ($\mathcal{T}_{\mathrm{basic}} \subseteq \mathcal{U} \subseteq \mathcal{T}$).

- Want to adapt **techniques** from runtime complexity analysis to derivational complexity! How?
  - (Useful) adaptation of Dependency Pairs?
  - Abstractions to numbers?
  - ...

A Landscape of Complexity Properties and Transformations



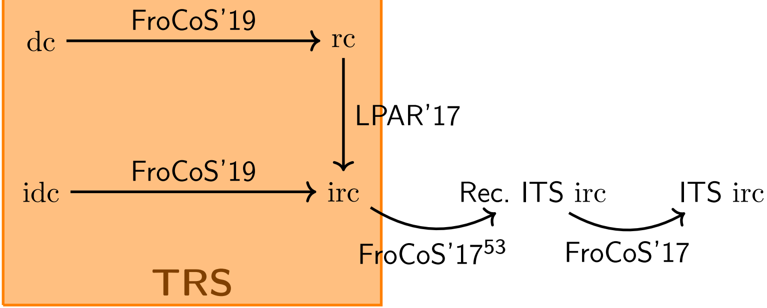
idc, irc: like dc, rc,
but for *innermost* rewriting

Rec. ITS irc

ITS irc

A Landscape of Complexity Properties and Transformations

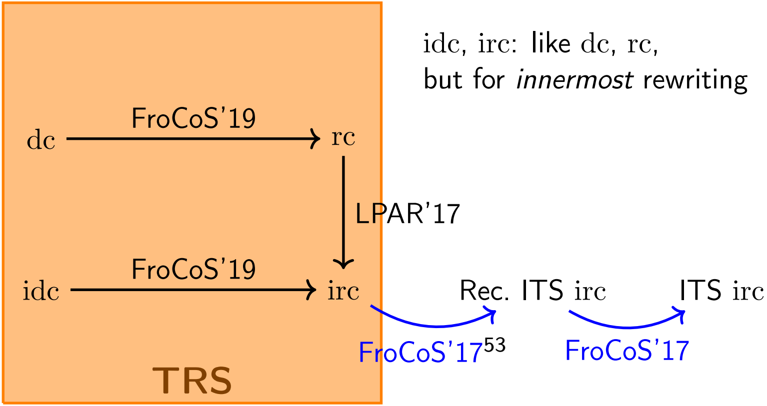
idc, irc: like dc, rc,
but for *innermost* rewriting



[53] M. Naaf, F. Frohn, M. Brockschmidt, C. Fuhs, J. Giesl: *Complexity analysis for term rewriting by integer transition systems*, FroCoS '17

A Landscape of Complexity Properties and Transformations

idc, irc: like dc, rc,
but for *innermost* rewriting



[53] M. Naaf, F. Frohn, M. Brockschmidt, C. Fuhs, J. Giesl: *Complexity analysis for term rewriting by integer transition systems*, FroCoS '17

Bottom-Up Complexity Analysis for Imperative Programs

Recently significant progress in complexity analysis tools for **Integer Transition Systems (ITSs)**:

- CoFloCo[54]
- KoAT[55]
- PUBS[56]

Goal: use these tools to find upper bounds for TRS complexity

[54] A. Flores-Montoya, R. Hähnle: *Resource analysis of complex programs with cost equations*, APLAS '14, https://github.com/aeflores/CoFloCo

[55] M. Brockschmidt, F. Emmes, S. Falke, C. Fuhs, J. Giesl: *Analyzing Runtime and Size Complexity of Integer Programs*, TOPLAS '16, https://github.com/s-falke/kittel-koat

[56] E. Albert, P. Arenas, S. Genaim, G. Puebla: *Closed-Form Upper Bounds in Static Cost Analysis*, JAR '11, https://costa.fdi.ucm.es/pubs/

Analysing irc of Insertion Sort by Hand: Bottom-Up

Example

$$
\begin{array}{rcl}
\mathsf{isort}(\mathsf{nil}, ys) & \longrightarrow & ys \\
\mathsf{isort}(\mathsf{cons}(x, xs), ys) & \longrightarrow & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) \\
\mathsf{insert}(x, \mathsf{nil}) & \longrightarrow & \mathsf{cons}(x, \mathsf{nil}) \\
\mathsf{insert}(x, \mathsf{cons}(y, ys)) & \longrightarrow & \mathsf{if}(\mathsf{gt}(x, y), x, \mathsf{cons}(y, ys)) \\
\mathsf{if}(\mathsf{true}, x, \mathsf{cons}(y, ys)) & \longrightarrow & \mathsf{cons}(y, \mathsf{insert}(x, ys)) \\
\mathsf{if}(\mathsf{false}, x, \mathsf{cons}(y, ys)) & \longrightarrow & \mathsf{cons}(x, \mathsf{cons}(y, ys)) \\
\mathsf{gt}(\mathsf{0}, y) & \stackrel{=}{\longrightarrow} & \mathsf{false} \\
\mathsf{gt}(\mathsf{s}(x), \mathsf{0}) & \stackrel{=}{\longrightarrow} & \mathsf{true} \\
\mathsf{gt}(\mathsf{s}(x), \mathsf{s}(y)) & \stackrel{=}{\longrightarrow} & \mathsf{gt}(x, y)
\end{array}
$$

Analysing irc of Insertion Sort by Hand: Bottom-Up

Example

$$
\begin{aligned}
\mathsf{isort}(\mathsf{nil}, ys) &\to ys \\
\mathsf{isort}(\mathsf{cons}(x, xs), ys) &\to \mathsf{isort}(xs, \mathsf{insert}(x, ys)) \\
\mathsf{insert}(x, \mathsf{nil}) &\to \mathsf{cons}(x, \mathsf{nil}) \\
\mathsf{insert}(x, \mathsf{cons}(y, ys)) &\to \mathsf{if}(\mathsf{gt}(x, y), x, \mathsf{cons}(y, ys)) \\
\mathsf{if}(\mathsf{true}, x, \mathsf{cons}(y, ys)) &\to \mathsf{cons}(y, \mathsf{insert}(x, ys)) \\
\mathsf{if}(\mathsf{false}, x, \mathsf{cons}(y, ys)) &\to \mathsf{cons}(x, \mathsf{cons}(y, ys)) \\
\mathsf{gt}(\mathsf{0}, y) &\xrightarrow{=} \mathsf{false} \\
\mathsf{gt}(\mathsf{s}(x), \mathsf{0}) &\xrightarrow{=} \mathsf{true} \\
\mathsf{gt}(\mathsf{s}(x), \mathsf{s}(y)) &\xrightarrow{=} \mathsf{gt}(x, y)
\end{aligned}
$$

Note: innermost reduction strategy

Analysing irc of Insertion Sort by Hand: Bottom-Up

Example

$$
\begin{aligned}
\mathsf{isort}(\mathsf{nil}, ys) &\to ys \\
\mathsf{isort}(\mathsf{cons}(x, xs), ys) &\to \mathsf{isort}(xs, \mathsf{insert}(x, ys)) \\
\mathsf{insert}(x, \mathsf{nil}) &\to \mathsf{cons}(x, \mathsf{nil}) \\
\mathsf{insert}(x, \mathsf{cons}(y, ys)) &\to \mathsf{if}(\mathsf{gt}(x, y), x, \mathsf{cons}(y, ys)) \\
\mathsf{if}(\mathsf{true}, x, \mathsf{cons}(y, ys)) &\to \mathsf{cons}(y, \mathsf{insert}(x, ys)) \\
\mathsf{if}(\mathsf{false}, x, \mathsf{cons}(y, ys)) &\to \mathsf{cons}(x, \mathsf{cons}(y, ys)) \\
\mathsf{gt}(0, y) &\xrightarrow{=} \mathsf{false} \\
\mathsf{gt}(\mathsf{s}(x), 0) &\xrightarrow{=} \mathsf{true} \\
\mathsf{gt}(\mathsf{s}(x), \mathsf{s}(y)) &\xrightarrow{=} \mathsf{gt}(x, y)
\end{aligned}
$$

- $\mathsf{rt}(\mathsf{gt}(x, y)) \in \mathcal{O}(1)$ ("$\xrightarrow{=}$" for relative rules)

Note: innermost reduction strategy

Analysing irc of Insertion Sort by Hand: Bottom-Up

Example

$$
\begin{array}{rcl}
\mathsf{isort}(\mathsf{nil}, ys) & \to & ys \\
\mathsf{isort}(\mathsf{cons}(x, xs), ys) & \to & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) \\
\mathsf{insert}(x, \mathsf{nil}) & \to & \mathsf{cons}(x, \mathsf{nil}) \\
\mathsf{insert}(x, \mathsf{cons}(y, ys)) & \to & \mathsf{if}(\mathsf{gt}(x, y), x, \mathsf{cons}(y, ys)) \\
\mathsf{if}(\mathsf{true}, x, \mathsf{cons}(y, ys)) & \to & \mathsf{cons}(y, \mathsf{insert}(x, ys)) \\
\mathsf{if}(\mathsf{false}, x, \mathsf{cons}(y, ys)) & \to & \mathsf{cons}(x, \mathsf{cons}(y, ys)) \\
\mathsf{gt}(0, y) & \stackrel{=}{\to} & \mathsf{false} \\
\mathsf{gt}(\mathsf{s}(x), 0) & \stackrel{=}{\to} & \mathsf{true} \\
\mathsf{gt}(\mathsf{s}(x), \mathsf{s}(y)) & \stackrel{=}{\to} & \mathsf{gt}(x, y)
\end{array}
$$

- $\mathsf{rt}(\mathsf{gt}(x, y)) \in \mathcal{O}(1)$ ("$\stackrel{=}{\to}$" for relative rules)
- $\mathsf{rt}(\mathsf{insert}(x, ys)) \in \mathcal{O}(\mathsf{length}(ys))$

Note: innermost reduction strategy

Analysing irc of Insertion Sort by Hand: Bottom-Up

Example

$$
\begin{array}{rcl}
\mathsf{isort}(\mathsf{nil}, ys) & \to & ys \\
\mathsf{isort}(\mathsf{cons}(x, xs), ys) & \to & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) \\
\mathsf{insert}(x, \mathsf{nil}) & \to & \mathsf{cons}(x, \mathsf{nil}) \\
\mathsf{insert}(x, \mathsf{cons}(y, ys)) & \to & \mathsf{if}(\mathsf{gt}(x, y), x, \mathsf{cons}(y, ys)) \\
\mathsf{if}(\mathsf{true}, x, \mathsf{cons}(y, ys)) & \to & \mathsf{cons}(y, \mathsf{insert}(x, ys)) \\
\mathsf{if}(\mathsf{false}, x, \mathsf{cons}(y, ys)) & \to & \mathsf{cons}(x, \mathsf{cons}(y, ys)) \\
\mathsf{gt}(\mathsf{0}, y) & \xrightarrow{=} & \mathsf{false} \\
\mathsf{gt}(\mathsf{s}(x), \mathsf{0}) & \xrightarrow{=} & \mathsf{true} \\
\mathsf{gt}(\mathsf{s}(x), \mathsf{s}(y)) & \xrightarrow{=} & \mathsf{gt}(x, y)
\end{array}
$$

- $\mathsf{rt}(\mathsf{gt}(x, y)) \in \mathcal{O}(1)$ (“$\xrightarrow{=}$” for relative rules)
- $\mathsf{rt}(\mathsf{insert}(x, ys)) \in \mathcal{O}(\mathsf{length}(ys))$
- $\mathsf{rt}(\mathsf{isort}(xs, ys)) \in \mathcal{O}(\mathsf{length}(xs) \cdot \ldots)$

Note: innermost reduction strategy

Analysing irc of Insertion Sort by Hand: Bottom-Up

Example

$$
\begin{array}{rcl}
\mathsf{isort}(\mathsf{nil}, ys) & \to & ys \\
\mathsf{isort}(\mathsf{cons}(x, xs), ys) & \to & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) \\
\mathsf{insert}(x, \mathsf{nil}) & \to & \mathsf{cons}(x, \mathsf{nil}) \\
\mathsf{insert}(x, \mathsf{cons}(y, ys)) & \to & \mathsf{if}(\mathsf{gt}(x, y), x, \mathsf{cons}(y, ys)) \\
\mathsf{if}(\mathsf{true}, x, \mathsf{cons}(y, ys)) & \to & \mathsf{cons}(y, \mathsf{insert}(x, ys)) \\
\mathsf{if}(\mathsf{false}, x, \mathsf{cons}(y, ys)) & \to & \mathsf{cons}(x, \mathsf{cons}(y, ys)) \\
\mathsf{gt}(\mathsf{0}, y) & \xrightarrow{=} & \mathsf{false} \\
\mathsf{gt}(\mathsf{s}(x), \mathsf{0}) & \xrightarrow{=} & \mathsf{true} \\
\mathsf{gt}(\mathsf{s}(x), \mathsf{s}(y)) & \xrightarrow{=} & \mathsf{gt}(x, y)
\end{array}
$$

- $\mathsf{rt}(\mathsf{gt}(x, y)) \in \mathcal{O}(1)$ ("$\xrightarrow{=}$" for relative rules)
- $\mathsf{rt}(\mathsf{insert}(x, ys)) \in \mathcal{O}(\mathsf{length}(ys))$
- $\mathsf{rt}(\mathsf{isort}(xs, ys)) \in \mathcal{O}(\mathsf{length}(xs) \cdot (\mathsf{length}(xs) + \mathsf{length}(ys)))$

Note: innermost reduction strategy

Using Dependency Tuples: Top-Down

Example

$$
\begin{aligned}
\mathsf{isort}(\mathsf{nil}, ys) &\longrightarrow ys \\
\mathsf{isort}(\mathsf{cons}(x, xs), ys) &\longrightarrow \mathsf{isort}(xs, \mathsf{insert}(x, ys)) \\
\mathsf{insert}(x, \mathsf{nil}) &\longrightarrow \mathsf{cons}(x, \mathsf{nil}) \\
\mathsf{insert}(x, \mathsf{cons}(y, ys)) &\longrightarrow \mathsf{if}(\mathsf{gt}(x, y), x, \mathsf{cons}(y, ys)) \\
\mathsf{if}(\mathsf{true}, x, \mathsf{cons}(y, ys)) &\longrightarrow \mathsf{cons}(y, \mathsf{insert}(x, ys)) \\
\mathsf{if}(\mathsf{false}, x, \mathsf{cons}(y, ys)) &\longrightarrow \mathsf{cons}(x, \mathsf{cons}(y, ys)) \\
\mathsf{gt}(\mathsf{0}, y) &\stackrel{=}{\longrightarrow} \mathsf{false} \\
\mathsf{gt}(\mathsf{s}(x), \mathsf{0}) &\stackrel{=}{\longrightarrow} \mathsf{true} \\
\mathsf{gt}(\mathsf{s}(x), \mathsf{s}(y)) &\stackrel{=}{\longrightarrow} \mathsf{gt}(x, y)
\end{aligned}
$$

- the recursive isort rule is at most applied linearly often

Using Dependency Tuples: Top-Down

Example

$$
\begin{aligned}
\mathsf{isort}(\mathsf{nil}, ys) &\to ys \\
\mathsf{isort}(\mathsf{cons}(x, xs), ys) &\to \mathsf{isort}(xs, \mathsf{insert}(x, ys)) \\
\mathsf{insert}(x, \mathsf{nil}) &\to \mathsf{cons}(x, \mathsf{nil}) \\
\mathsf{insert}(x, \mathsf{cons}(y, ys)) &\to \mathsf{if}(\mathsf{gt}(x, y), x, \mathsf{cons}(y, ys)) \\
\mathsf{if}(\mathsf{true}, x, \mathsf{cons}(y, ys)) &\to \mathsf{cons}(y, \mathsf{insert}(x, ys)) \\
\mathsf{if}(\mathsf{false}, x, \mathsf{cons}(y, ys)) &\to \mathsf{cons}(x, \mathsf{cons}(y, ys)) \\
\mathsf{gt}(\mathsf{0}, y) &\xrightarrow{=} \mathsf{false} \\
\mathsf{gt}(\mathsf{s}(x), \mathsf{0}) &\xrightarrow{=} \mathsf{true} \\
\mathsf{gt}(\mathsf{s}(x), \mathsf{s}(y)) &\xrightarrow{=} \mathsf{gt}(x, y)
\end{aligned}
$$

- the recursive isort rule is at most applied linearly often
- the recursive insert rule is at most applied quadratically often

Using Dependency Tuples: Top-Down

Example

$$
\begin{array}{rcl}
\mathsf{isort}(\mathsf{nil}, ys) & \longrightarrow & ys \\
\mathsf{isort}(\mathsf{cons}(x, xs), ys) & \longrightarrow & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) \\
\mathsf{insert}(x, \mathsf{nil}) & \longrightarrow & \mathsf{cons}(x, \mathsf{nil}) \\
\mathsf{insert}(x, \mathsf{cons}(y, ys)) & \longrightarrow & \mathsf{if}(\mathsf{gt}(x, y), x, \mathsf{cons}(y, ys)) \\
\mathsf{if}(\mathsf{true}, x, \mathsf{cons}(y, ys)) & \longrightarrow & \mathsf{cons}(y, \mathsf{insert}(x, ys)) \\
\mathsf{if}(\mathsf{false}, x, \mathsf{cons}(y, ys)) & \longrightarrow & \mathsf{cons}(x, \mathsf{cons}(y, ys)) \\
\mathsf{gt}(\mathsf{0}, y) & \xrightarrow{=} & \mathsf{false} \\
\mathsf{gt}(\mathsf{s}(x), \mathsf{0}) & \xrightarrow{=} & \mathsf{true} \\
\mathsf{gt}(\mathsf{s}(x), \mathsf{s}(y)) & \xrightarrow{=} & \mathsf{gt}(x, y)
\end{array}
$$

- the recursive isort rule is at most applied linearly often
- the recursive insert rule is at most applied quadratically often
  - note: requires reasoning about isort, insert, and if rules!

Using Dependency Tuples: Top-Down

Example

$$
\begin{array}{rcl}
\mathsf{isort}(\mathsf{nil}, ys) & \to & ys \\
\mathsf{isort}(\mathsf{cons}(x, xs), ys) & \to & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) \\
\mathsf{insert}(x, \mathsf{nil}) & \to & \mathsf{cons}(x, \mathsf{nil}) \\
\mathsf{insert}(x, \mathsf{cons}(y, ys)) & \to & \mathsf{if}(\mathsf{gt}(x, y), x, \mathsf{cons}(y, ys)) \\
\mathsf{if}(\mathsf{true}, x, \mathsf{cons}(y, ys)) & \to & \mathsf{cons}(y, \mathsf{insert}(x, ys)) \\
\mathsf{if}(\mathsf{false}, x, \mathsf{cons}(y, ys)) & \to & \mathsf{cons}(x, \mathsf{cons}(y, ys)) \\
\mathsf{gt}(\mathsf{0}, y) & \xrightarrow{=} & \mathsf{false} \\
\mathsf{gt}(\mathsf{s}(x), \mathsf{0}) & \xrightarrow{=} & \mathsf{true} \\
\mathsf{gt}(\mathsf{s}(x), \mathsf{s}(y)) & \xrightarrow{=} & \mathsf{gt}(x, y)
\end{array}
$$

- the recursive isort rule is at most applied linearly often
- the recursive insert rule is at most applied quadratically often
  - note: requires reasoning about isort, insert, and if rules!
  - found via quadratic polynomial interpretation

Using Dependency Tuples: Top-Down

Example

$$
\begin{array}{rcl}
\mathsf{isort}(\mathsf{nil}, ys) & \to & ys \\
\mathsf{isort}(\mathsf{cons}(x, xs), ys) & \to & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) \\
\mathsf{insert}(x, \mathsf{nil}) & \to & \mathsf{cons}(x, \mathsf{nil}) \\
\mathsf{insert}(x, \mathsf{cons}(y, ys)) & \to & \mathsf{if}(\mathsf{gt}(x, y), x, \mathsf{cons}(y, ys)) \\
\mathsf{if}(\mathsf{true}, x, \mathsf{cons}(y, ys)) & \to & \mathsf{cons}(y, \mathsf{insert}(x, ys)) \\
\mathsf{if}(\mathsf{false}, x, \mathsf{cons}(y, ys)) & \to & \mathsf{cons}(x, \mathsf{cons}(y, ys)) \\
\mathsf{gt}(\mathsf{0}, y) & \xrightarrow{=} & \mathsf{false} \\
\mathsf{gt}(\mathsf{s}(x), \mathsf{0}) & \xrightarrow{=} & \mathsf{true} \\
\mathsf{gt}(\mathsf{s}(x), \mathsf{s}(y)) & \xrightarrow{=} & \mathsf{gt}(x, y)
\end{array}
$$

- the recursive isort rule is at most applied linearly often
- the recursive insert rule is at most applied quadratically often
  - note: requires reasoning about isort, insert, and if rules!
  - found via quadratic polynomial interpretation
- the recursive if rule is applied as often as the recursive insert rule

Bird's Eye View of the Transformation

Example

$$
\begin{aligned}
\mathsf{isort}(\mathsf{nil}, ys) &\to ys \\
\mathsf{isort}(\mathsf{cons}(x, xs), ys) &\to \mathsf{isort}(xs, \mathsf{insert}(x, ys)) \\
\mathsf{insert}(x, \mathsf{nil}) &\to \mathsf{cons}(x, \mathsf{nil}) \\
\mathsf{insert}(x, \mathsf{cons}(y, ys)) &\to \mathsf{if}(\mathsf{gt}(x, y), x, \mathsf{cons}(y, ys)) \\
\mathsf{if}(\mathsf{true}, x, \mathsf{cons}(y, ys)) &\to \mathsf{cons}(y, \mathsf{insert}(x, ys)) \\
\mathsf{if}(\mathsf{false}, x, \mathsf{cons}(y, ys)) &\to \mathsf{cons}(x, \mathsf{cons}(y, ys)) \\
\mathsf{gt}(0, y) &\xrightarrow{=} \mathsf{false} \\
\mathsf{gt}(\mathsf{s}(x), 0) &\xrightarrow{=} \mathsf{true} \\
\mathsf{gt}(\mathsf{s}(x), \mathsf{s}(y)) &\xrightarrow{=} \mathsf{gt}(x, y)
\end{aligned}
$$

1. abstract terms to integers

Bird's Eye View of the Transformation

Example

$$
\begin{array}{rcll}
\mathsf{isort}(xs', ys) & \xrightarrow{1} & ys & \mid \quad xs' = 1 \\
\mathsf{isort}(\mathsf{cons}(x, xs), ys) & \to & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) & \\
\mathsf{insert}(x, \mathsf{nil}) & \to & \mathsf{cons}(x, \mathsf{nil}) & \\
\mathsf{insert}(x, \mathsf{cons}(y, ys)) & \to & \mathsf{if}(\mathsf{gt}(x, y), x, \mathsf{cons}(y, ys)) & \\
\mathsf{if}(\mathsf{true}, x, \mathsf{cons}(y, ys)) & \to & \mathsf{cons}(y, \mathsf{insert}(x, ys)) & \\
\mathsf{if}(\mathsf{false}, x, \mathsf{cons}(y, ys)) & \to & \mathsf{cons}(x, \mathsf{cons}(y, ys)) & \\
\mathsf{gt}(0, y) & \xrightarrow{=} & \mathsf{false} & \\
\mathsf{gt}(\mathsf{s}(x), 0) & \xrightarrow{=} & \mathsf{true} & \\
\mathsf{gt}(\mathsf{s}(x), \mathsf{s}(y)) & \xrightarrow{=} & \mathsf{gt}(x, y) &
\end{array}
$$

1. abstract terms to integers

Bird's Eye View of the Transformation

Example

$$
\begin{array}{rcll}
\mathsf{isort}(xs', ys) & \xrightarrow{1} & ys & \mid \quad xs' = 1 \\
\mathsf{isort}(xs', ys) & \xrightarrow{1} & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) & \mid \quad xs' = 1 + x + xs \\
\mathsf{insert}(x, \mathsf{nil}) & \to & \mathsf{cons}(x, \mathsf{nil}) & \\
\mathsf{insert}(x, \mathsf{cons}(y, ys)) & \to & \mathsf{if}(\mathsf{gt}(x, y), x, \mathsf{cons}(y, ys)) & \\
\mathsf{if}(\mathsf{true}, x, \mathsf{cons}(y, ys)) & \to & \mathsf{cons}(y, \mathsf{insert}(x, ys)) & \\
\mathsf{if}(\mathsf{false}, x, \mathsf{cons}(y, ys)) & \to & \mathsf{cons}(x, \mathsf{cons}(y, ys)) & \\
\mathsf{gt}(0, y) & \xrightarrow{=} & \mathsf{false} & \\
\mathsf{gt}(\mathsf{s}(x), 0) & \xrightarrow{=} & \mathsf{true} & \\
\mathsf{gt}(\mathsf{s}(x), \mathsf{s}(y)) & \xrightarrow{=} & \mathsf{gt}(x, y) &
\end{array}
$$

1. abstract terms to integers

Bird's Eye View of the Transformation

Example

$$
\begin{array}{rcll}
\mathsf{isort}(xs', ys) & \xrightarrow{1} & ys & \mid \quad xs' = 1 \\
\mathsf{isort}(xs', ys) & \xrightarrow{1} & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) & \mid \quad xs' = 1 + x + xs \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & 2 + x & \mid \quad ys' = 1 \\
\mathsf{insert}(x, \mathsf{cons}(y, ys)) & \to & \mathsf{if}(\mathsf{gt}(x, y), x, \mathsf{cons}(y, ys)) & \\
\mathsf{if}(\mathsf{true}, x, \mathsf{cons}(y, ys)) & \to & \mathsf{cons}(y, \mathsf{insert}(x, ys)) & \\
\mathsf{if}(\mathsf{false}, x, \mathsf{cons}(y, ys)) & \to & \mathsf{cons}(x, \mathsf{cons}(y, ys)) & \\
\mathsf{gt}(0, y) & \xrightarrow{=} & \mathsf{false} & \\
\mathsf{gt}(\mathsf{s}(x), 0) & \xrightarrow{=} & \mathsf{true} & \\
\mathsf{gt}(\mathsf{s}(x), \mathsf{s}(y)) & \xrightarrow{=} & \mathsf{gt}(x, y) &
\end{array}
$$

1. abstract terms to integers

Bird's Eye View of the Transformation

Example

$$
\begin{array}{rcll}
\mathsf{isort}(xs', ys) & \xrightarrow{1} & ys & \mid \quad xs' = 1 \\
\mathsf{isort}(xs', ys) & \xrightarrow{1} & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) & \mid \quad xs' = 1 + x + xs \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & 2 + x & \mid \quad ys' = 1 \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & \mathsf{if}(\mathsf{gt}(x, y), x, ys') & \mid \quad ys' = 1 + y + ys \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + y + \mathsf{insert}(x, ys) & \mid \quad b = 1 \wedge ys' = 1 + y + ys \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + ys' & \mid \quad b = 1 \wedge ys' = 1 + y + ys \\
\mathsf{gt}(x', y') & \xrightarrow{0} & 1 & \mid \quad x' = 1 \\
\mathsf{gt}(x', y') & \xrightarrow{0} & 1 & \mid \quad x' = 1 + x \wedge y' = 1 \\
\mathsf{gt}(x', y') & \xrightarrow{0} & \mathsf{gt}(x, y) & \mid \quad x' = 1 + x \wedge y' = 1 + y
\end{array}
$$

1. abstract terms to integers

Bird's Eye View of the Transformation

Example

$$
\begin{array}{rcll}
\mathsf{isort}(xs', ys) & \xrightarrow{1} & ys & \mid \quad xs' = 1 \\
\mathsf{isort}(xs', ys) & \xrightarrow{1} & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) & \mid \quad xs' = 1 + x + xs \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & 2 + x & \mid \quad ys' = 1 \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & \mathsf{if}(\mathsf{gt}(x, y), x, ys') & \mid \quad ys' = 1 + y + ys \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + y + \mathsf{insert}(x, ys) & \mid \quad b = 1 \wedge ys' = 1 + y + ys \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + ys' & \mid \quad b = 1 \wedge ys' = 1 + y + ys \\
\mathsf{gt}(x', y') & \xrightarrow{0} & 1 & \mid \quad x' = 1 \\
\mathsf{gt}(x', y') & \xrightarrow{0} & 1 & \mid \quad x' = 1 + x \wedge y' = 1 \\
\mathsf{gt}(x', y') & \xrightarrow{0} & \mathsf{gt}(x, y) & \mid \quad x' = 1 + x \wedge y' = 1 + y
\end{array}
$$

1. abstract terms to integers
   - $[c](x_1, \ldots, x_n) = 1 + x_1 + \cdots + x_n$ for constructors c
   - note: variables range over $\mathbb{N}$
   - just $+$ and $\cdot$

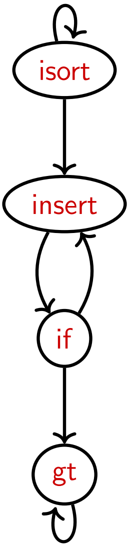
Bird's Eye View of the Transformation

Example

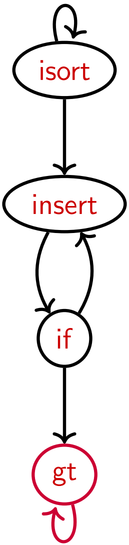
$$
\begin{array}{rcll}
\mathsf{isort}(xs', ys) & \xrightarrow{1} & ys & \mid \quad xs' = 1 \\
\mathsf{isort}(xs', ys) & \xrightarrow{1} & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) & \mid \quad xs' = 1 + x + xs \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & 2 + x & \mid \quad ys' = 1 \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & \mathsf{if}(\mathsf{gt}(x, y), x, ys') & \mid \quad ys' = 1 + y + ys \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + y + \mathsf{insert}(x, ys) & \mid \quad b = 1 \wedge ys' = 1 + y + ys \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + ys' & \mid \quad b = 1 \wedge ys' = 1 + y + ys \\
\mathsf{gt}(x', y') & \xrightarrow{0} & 1 & \mid \quad x' = 1 \\
\mathsf{gt}(x', y') & \xrightarrow{0} & 1 & \mid \quad x' = 1 + x \wedge y' = 1 \\
\mathsf{gt}(x', y') & \xrightarrow{0} & \mathsf{gt}(x, y) & \mid \quad x' = 1 + x \wedge y' = 1 + y
\end{array}
$$

1. abstract terms to integers
   - $[c](x_1, \dots, x_n) = 1 + x_1 + \cdots + x_n$ for constructors c
   - note: variables range over $\mathbb{N}$
   - just $+$ and $\cdot$
2. analyse result size for bottom-SCC (Strongly Connected Component) of call graph using standard ITS tools

Call Graph & Bottom SCCs



Call Graph & Bottom SCCs



Bird's Eye View

Example

$$
\begin{array}{rcl|l}
\mathsf{isort}(xs', ys) & \xrightarrow{1} & ys & xs' = 1 \\
\mathsf{isort}(xs', ys) & \xrightarrow{1} & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) & xs' = 1 + x + xs \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & 2 + x & ys' = 1 \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & \mathsf{if}(\mathsf{gt}(x, y), x, ys') & ys' = 1 + y + ys \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + y + \mathsf{insert}(x, ys) & b = 1 \land ys' = 1 + y + ys \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + ys' & b = 1 \land ys' = 1 + y + ys \\
\mathsf{gt}(x', y') & \xrightarrow{0} & 1 & x' = 1 \\
\mathsf{gt}(x', y') & \xrightarrow{0} & 1 & x' = 1 + x \land y' = 1 \\
\mathsf{gt}(x', y') & \xrightarrow{0} & \mathsf{gt}(x, y) & x' = 1 + x \land y' = 1 + y
\end{array}
$$

1. abstract terms to integers
   - $[c](x_1, \dots, x_n) = 1 + x_1 + \cdots + x_n$ for constructors c
   - note: variables range over $\mathbb{N}$
   - just $+$ and $\cdot$
2. analyse result size for bottom-SCC using standard ITS tools

Bird's Eye View

Example

$$
\begin{array}{rcll}
\mathsf{isort}(xs', ys) & \xrightarrow{1} & ys & \mid \quad xs' = 1 \\
\mathsf{isort}(xs', ys) & \xrightarrow{1} & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) & \mid \quad xs' = 1 + x + xs \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & 2 + x & \mid \quad ys' = 1 \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & \mathsf{if}(\mathsf{gt}(x, y), x, ys') & \mid \quad ys' = 1 + y + ys \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + y + \mathsf{insert}(x, ys) & \mid \quad b = 1 \land ys' = 1 + y + ys \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + ys' & \mid \quad b = 1 \land ys' = 1 + y + ys \\
\mathsf{gt}(x', y') & \xrightarrow{0} & 1 & \mid \quad x' = 1 \\
\mathsf{gt}(x', y') & \xrightarrow{0} & 1 & \mid \quad x' = 1 + x \land y' = 1 \\
\mathsf{gt}(x', y') & \xrightarrow{0} & \mathsf{gt}(x, y) & \mid \quad x' = 1 + x \land y' = 1 + y
\end{array}
$$

1. abstract terms to integers
   - $[c](x_1, \dots, x_n) = 1 + x_1 + \cdots + x_n$ for constructors c
   - note: variables range over $\mathbb{N}$
   - just $+$ and $\cdot$
2. analyse result size for bottom-SCC using standard ITS tools

Bird's Eye View

Example

$$
\begin{array}{rcll}
\mathsf{isort}(xs', ys) & \xrightarrow{1} & ys & \mid \quad xs' = 1 \\
\mathsf{isort}(xs', ys) & \xrightarrow{1} & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) & \mid \quad xs' = 1 + x + xs \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & 2 + x & \mid \quad ys' = 1 \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & \mathsf{if}(\mathsf{gt}(x, y), x, ys') & \mid \quad ys' = 1 + y + ys \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + y + \mathsf{insert}(x, ys) & \mid \quad b = 1 \wedge ys' = 1 + y + ys \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + ys' & \mid \quad b = 1 \wedge ys' = 1 + y + ys \\
\mathsf{gt}(x', y') & \xrightarrow{0} & 1 & \mid \quad x' = 1 \\
\mathsf{gt}(x', y') & \xrightarrow{0} & 1 & \mid \quad x' = 1 + x \wedge y' = 1 \\
\mathsf{gt}(x', y') & \xrightarrow{0} & \mathsf{gt}(x, y) & \mid \quad x' = 1 + x \wedge y' = 1 + y
\end{array}
$$

1. abstract terms to integers
   - $[c](x_1, \dots, x_n) = 1 + x_1 + \cdots + x_n$ for constructors c
   - note: variables range over $\mathbb{N}$
   - just $+$ and $\cdot$
2. analyse result size for bottom-SCC using standard ITS tools
3. analyse runtime of bottom-SCC using standard ITS tools

Bird's Eye View

Example

$$
\begin{array}{rcll}
\mathsf{isort}(xs', ys) & \xrightarrow{1} & ys & \mid \quad xs' = 1 \\
\mathsf{isort}(xs', ys) & \xrightarrow{1} & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) & \mid \quad xs' = 1 + x + xs \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & 2 + x & \mid \quad ys' = 1 \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & \mathsf{if}(b, x, ys') & \mid \quad ys' = 1 + y + ys \wedge b \leq 1 \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + y + \mathsf{insert}(x, ys) & \mid \quad b = 1 \wedge ys' = 1 + y + ys \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + ys' & \mid \quad b = 1 \wedge ys' = 1 + y + ys
\end{array}
$$

1. abstract terms to integers
   - $[c](x_1, \dots, x_n) = 1 + x_1 + \cdots + x_n$ for constructors c
   - note: variables range over $\mathbb{N}$
   - just $+$ and $\cdot$
2. analyse result size for bottom-SCC using standard ITS tools
3. analyse runtime of bottom-SCC using standard ITS tools

Abstracting Terms to Integers: Pitfalls

Terminating Variants

Term Rewriting	Integer Transition Systems
start terms may have variables	ground start terms only

Example

$\mathsf{h}(x) \longrightarrow \mathsf{f}(\mathsf{g}(x)) \qquad \mathsf{f}(x) \longrightarrow \mathsf{f}(x) \qquad \mathsf{g}(\mathsf{a}) \xrightarrow{=} \mathsf{g}(\mathsf{a})$

Terminating Variants

Term Rewriting	Integer Transition Systems
start terms may have variables	ground start terms only

Example

$\mathsf{h}(x) \longrightarrow \mathsf{f}(\mathsf{g}(x)) \qquad \mathsf{f}(x) \longrightarrow \mathsf{f}(x) \qquad \mathsf{g}(\mathsf{a}) \stackrel{=}{\longrightarrow} \mathsf{g}(\mathsf{a})$

innermost rewriting: $\mathsf{h}(x) \longrightarrow \mathsf{f}(\mathsf{g}(x)) \longrightarrow \mathsf{f}(\mathsf{g}(x)) \longrightarrow \ldots$

Terminating Variants

Term Rewriting	**Integer Transition Systems**
start terms may have variables	ground start terms only

Example

$$\mathsf{h}(x) \longrightarrow \mathsf{f}(\mathsf{g}(x)) \qquad \mathsf{f}(x) \longrightarrow \mathsf{f}(x) \qquad \mathsf{g}(\mathsf{a}) \xrightarrow{=} \mathsf{g}(\mathsf{a})$$

innermost rewriting: $\mathsf{h}(x) \longrightarrow \mathsf{f}(\mathsf{g}(x)) \longrightarrow \mathsf{f}(\mathsf{g}(x)) \longrightarrow \ldots$ $\qquad \mathcal{O}(\infty)$

Terminating Variants

Term Rewriting	Integer Transition Systems
start terms may have variables	ground start terms only

Example

$\mathsf{h}(x) \to \mathsf{f}(\mathsf{g}(x)) \qquad \mathsf{f}(x) \to \mathsf{f}(x) \qquad \mathsf{g}(\mathsf{a}) \xrightarrow{=} \mathsf{g}(\mathsf{a})$

innermost rewriting: $\mathsf{h}(x) \to \mathsf{f}(\mathsf{g}(x)) \to \mathsf{f}(\mathsf{g}(x)) \to \dots$ $\mathcal{O}(\infty)$

- Just ground rewriting?

Terminating Variants

Term Rewriting	Integer Transition Systems
start terms may have variables	ground start terms only

Example

$\mathsf{h}(x) \to \mathsf{f}(\mathsf{g}(x)) \qquad \mathsf{f}(x) \to \mathsf{f}(x) \qquad \mathsf{g}(\mathsf{a}) \xrightarrow{=} \mathsf{g}(\mathsf{a})$

innermost rewriting: $\mathsf{h}(x) \to \mathsf{f}(\mathsf{g}(x)) \to \mathsf{f}(\mathsf{g}(x)) \to \dots$ $\qquad \mathcal{O}(\infty)$

ground rewriting: $\mathsf{h}(\mathsf{a}) \to \mathsf{f}(\mathsf{g}(\mathsf{a})) \xrightarrow{=} \mathsf{f}(\mathsf{g}(\mathsf{a})) \xrightarrow{=} \dots$

- Just ground rewriting?

Terminating Variants

Term Rewriting	**Integer Transition Systems**
start terms may have variables	ground start terms only

Example

$\mathsf{h}(x) \longrightarrow \mathsf{f}(\mathsf{g}(x)) \qquad \mathsf{f}(x) \longrightarrow \mathsf{f}(x) \qquad \mathsf{g}(\mathsf{a}) \xrightarrow{=} \mathsf{g}(\mathsf{a})$

innermost rewriting: $\mathsf{h}(x) \longrightarrow \mathsf{f}(\mathsf{g}(x)) \longrightarrow \mathsf{f}(\mathsf{g}(x)) \longrightarrow \ldots$ $\mathcal{O}(\infty)$

ground rewriting: $\mathsf{h}(\mathsf{a}) \longrightarrow \mathsf{f}(\mathsf{g}(\mathsf{a})) \xrightarrow{=} \mathsf{f}(\mathsf{g}(\mathsf{a})) \xrightarrow{=} \ldots$ $\mathcal{O}(1)$

- Just ground rewriting?

Terminating Variants

Term Rewriting	Integer Transition Systems
start terms may have variables	ground start terms only

Example

$$\mathsf{h}(x) \to \mathsf{f}(\mathsf{g}(x)) \qquad \mathsf{f}(x) \to \mathsf{f}(x) \qquad \mathsf{g}(\mathsf{a}) \xrightarrow{=} \mathsf{g}(\mathsf{a})$$

innermost rewriting: $\mathsf{h}(x) \to \mathsf{f}(\mathsf{g}(x)) \to \mathsf{f}(\mathsf{g}(x)) \to \dots$ $\mathcal{O}(\infty)$

ground rewriting: $\mathsf{h}(\mathsf{a}) \to \mathsf{f}(\mathsf{g}(\mathsf{a})) \xrightarrow{=} \mathsf{f}(\mathsf{g}(\mathsf{a})) \xrightarrow{=} \dots$ $\mathcal{O}(1)$

- Just ground rewriting?
- Add terminating variant of relative rules!

Terminating Variants

Term Rewriting	Integer Transition Systems
start terms may have variables	ground start terms only

Example

$$\mathsf{h}(x) \to \mathsf{f}(\mathsf{g}(x)) \qquad \mathsf{f}(x) \to \mathsf{f}(x) \qquad \mathsf{g}(\mathsf{a}) \xrightarrow{=} \mathsf{g}(\mathsf{a})$$

innermost rewriting: $\mathsf{h}(x) \to \mathsf{f}(\mathsf{g}(x)) \to \mathsf{f}(\mathsf{g}(x)) \to \dots$ $\qquad \mathcal{O}(\infty)$

ground rewriting: $\mathsf{h}(\mathsf{a}) \to \mathsf{f}(\mathsf{g}(\mathsf{a})) \xrightarrow{=} \mathsf{f}(\mathsf{g}(\mathsf{a})) \xrightarrow{=} \dots$ $\qquad \mathcal{O}(1)$

- Just ground rewriting?
- Add terminating variant of relative rules!

Definition

$\mathcal{N}$ is a terminating variant of $\mathcal{S}$ iff $\mathcal{N}$ terminates and every $\mathcal{N}$-normal form is an $\mathcal{S}$-normal form.

Terminating Variants

Term Rewriting	Integer Transition Systems
start terms may have variables	ground start terms only

Example

$\mathsf{h}(x) \to \mathsf{f}(\mathsf{g}(x)) \qquad \mathsf{f}(x) \to \mathsf{f}(x) \qquad \mathsf{g}(\mathsf{a}) \xrightarrow{=} \mathsf{g}(\mathsf{a}) \qquad \mathsf{g}(\mathsf{a}) \xrightarrow{=} \mathsf{a}$

innermost rewriting: $\mathsf{h}(x) \to \mathsf{f}(\mathsf{g}(x)) \to \mathsf{f}(\mathsf{g}(x)) \to \dots$ $\quad \mathcal{O}(\infty)$

ground rewriting: $\mathsf{h}(\mathsf{a}) \to \mathsf{f}(\mathsf{g}(\mathsf{a})) \xrightarrow{=} \mathsf{f}(\mathsf{g}(\mathsf{a})) \xrightarrow{=} \dots$ $\quad \mathcal{O}(1)$

- Just ground rewriting?
- Add terminating variant of relative rules!

Definition

$\mathcal{N}$ is a terminating variant of $\mathcal{S}$ iff $\mathcal{N}$ terminates and every $\mathcal{N}$-normal form is an $\mathcal{S}$-normal form.

Terminating Variants

Term Rewriting	Integer Transition Systems
start terms may have variables	ground start terms only

Example

$\mathsf{h}(x) \to \mathsf{f}(\mathsf{g}(x)) \qquad \mathsf{f}(x) \to \mathsf{f}(x) \qquad \mathsf{g}(\mathsf{a}) \xrightarrow{=} \mathsf{g}(\mathsf{a}) \qquad \mathsf{g}(\mathsf{a}) \xrightarrow{=} \mathsf{a}$

innermost rewriting: $\mathsf{h}(x) \to \mathsf{f}(\mathsf{g}(x)) \to \mathsf{f}(\mathsf{g}(x)) \to \ldots \qquad \mathcal{O}(\infty)$

ground rewriting: $\mathsf{h}(\mathsf{a}) \to \mathsf{f}(\mathsf{g}(\mathsf{a})) \xrightarrow{=} \mathsf{f}(\mathsf{g}(\mathsf{a})) \xrightarrow{=} \ldots \qquad \mathcal{O}(1)$

with terminating variant: $\mathsf{h}(\mathsf{a}) \to \mathsf{f}(\mathsf{g}(\mathsf{a})) \xrightarrow{=} \mathsf{f}(\mathsf{a}) \to \mathsf{f}(\mathsf{a}) \to \ldots$

- Just ground rewriting?
- Add terminating variant of relative rules!

Definition

$\mathcal{N}$ is a terminating variant of $\mathcal{S}$ iff $\mathcal{N}$ terminates and every $\mathcal{N}$-normal form is an $\mathcal{S}$-normal form.

Terminating Variants

Term Rewriting	Integer Transition Systems
start terms may have variables	ground start terms only

Example

$\mathsf{h}(x) \to \mathsf{f}(\mathsf{g}(x)) \qquad \mathsf{f}(x) \to \mathsf{f}(x) \qquad \mathsf{g}(\mathsf{a}) \xrightarrow{=} \mathsf{g}(\mathsf{a}) \qquad \mathsf{g}(\mathsf{a}) \xrightarrow{=} \mathsf{a}$

innermost rewriting: $\mathsf{h}(x) \to \mathsf{f}(\mathsf{g}(x)) \to \mathsf{f}(\mathsf{g}(x)) \to \dots$ $\quad \mathcal{O}(\infty)$

ground rewriting: $\mathsf{h}(\mathsf{a}) \to \mathsf{f}(\mathsf{g}(\mathsf{a})) \xrightarrow{=} \mathsf{f}(\mathsf{g}(\mathsf{a})) \xrightarrow{=} \dots$ $\quad \mathcal{O}(1)$

with terminating variant: $\mathsf{h}(\mathsf{a}) \to \mathsf{f}(\mathsf{g}(\mathsf{a})) \xrightarrow{=} \mathsf{f}(\mathsf{a}) \to \mathsf{f}(\mathsf{a}) \to \dots$ $\quad \mathcal{O}(\infty)$

- Just ground rewriting?
- Add terminating variant of relative rules!

Definition

$\mathcal{N}$ is a terminating variant of $\mathcal{S}$ iff $\mathcal{N}$ terminates and every $\mathcal{N}$-normal form is an $\mathcal{S}$-normal form.

Ensuring Complete Definedness

Term Rewriting	Integer Transition Systems
arbitrary matchers	integer substitutions only

Example

$\mathsf{f}(x) \longrightarrow \mathsf{f}(\mathsf{g}(\mathsf{a}))$ $\qquad$ $\mathsf{g}(\mathsf{b}(\mathsf{a})) \longrightarrow \mathsf{a}$

Ensuring Complete Definedness

Term Rewriting	Integer Transition Systems
arbitrary matchers	integer substitutions only

Example

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

original TRS: $\mathsf{f}(\mathsf{a}) \to \mathsf{f}(\mathsf{g}(\mathsf{a})) \to \mathsf{f}(\mathsf{g}(\mathsf{a})) \to \dots$

Ensuring Complete Definedness

Term Rewriting	**Integer Transition Systems**
arbitrary matchers	integer substitutions only

Example

$\mathsf{f}(x) \longrightarrow \mathsf{f}(\mathsf{g}(\mathsf{a}))$ $\qquad$ $\mathsf{g}(\mathsf{b}(\mathsf{a})) \longrightarrow \mathsf{a}$

original TRS: $\mathsf{f}(\mathsf{a}) \longrightarrow \mathsf{f}(\mathsf{g}(\mathsf{a})) \longrightarrow \mathsf{f}(\mathsf{g}(\mathsf{a})) \longrightarrow \ldots$ $\qquad$ $\mathcal{O}(\infty)$

Ensuring Complete Definedness

Term Rewriting	**Integer Transition Systems**
arbitrary matchers	integer substitutions only

Example

$$\mathsf{f}(x) \longrightarrow \mathsf{f}(\mathsf{g}(\mathsf{a})) \qquad \mathsf{g}(\mathsf{b}(\mathsf{a})) \longrightarrow \mathsf{a}$$

original TRS: $\mathsf{f}(\mathsf{a}) \longrightarrow \mathsf{f}(\mathsf{g}(\mathsf{a})) \longrightarrow \mathsf{f}(\mathsf{g}(\mathsf{a})) \longrightarrow \dots$ $\mathcal{O}(\infty)$

resulting ITS: $\mathsf{f}(1) \xrightarrow{1} \mathsf{f}(\mathsf{g}(1))$

Ensuring Complete Definedness

Term Rewriting	Integer Transition Systems
arbitrary matchers	integer substitutions only

Example

$\mathsf{f}(x) \longrightarrow \mathsf{f}(\mathsf{g}(\mathsf{a}))$ $\qquad \mathsf{g}(\mathsf{b}(\mathsf{a})) \longrightarrow \mathsf{a}$

original TRS: $\mathsf{f}(\mathsf{a}) \longrightarrow \mathsf{f}(\mathsf{g}(\mathsf{a})) \longrightarrow \mathsf{f}(\mathsf{g}(\mathsf{a})) \longrightarrow \dots$ $\qquad \mathcal{O}(\infty)$

resulting ITS: $\mathsf{f}(1) \xrightarrow{1} \mathsf{f}(\mathsf{g}(1))$ $\qquad \mathcal{O}(1)$

Ensuring Complete Definedness

Term Rewriting	**Integer Transition Systems**
arbitrary matchers	integer substitutions only

Example

$$\mathsf{f}(x) \longrightarrow \mathsf{f}(\mathsf{g}(\mathsf{a})) \qquad \mathsf{g}(\mathsf{b}(\mathsf{a})) \longrightarrow \mathsf{a}$$

original TRS: $\mathsf{f}(\mathsf{a}) \longrightarrow \mathsf{f}(\mathsf{g}(\mathsf{a})) \longrightarrow \mathsf{f}(\mathsf{g}(\mathsf{a})) \longrightarrow \dots$ $\mathcal{O}(\infty)$

resulting ITS: $\mathsf{f}(1) \xrightarrow{1} \mathsf{f}(\mathsf{g}(1))$ $\mathcal{O}(1)$

Definition

A TRS is completely defined iff its ground normal forms do not contain defined symbols.

Ensuring Complete Definedness

Term Rewriting	Integer Transition Systems
arbitrary matchers	integer substitutions only

Example

$\mathsf{f}(x) \to \mathsf{f}(\mathsf{g}(\mathsf{a}))$ $\qquad$ $\mathsf{g}(\mathsf{b}(\mathsf{a})) \to \mathsf{a}$ $\qquad$ $\mathsf{g}(x) \xrightarrow{=} \mathsf{a}$

original TRS: $\mathsf{f}(\mathsf{a}) \to \mathsf{f}(\mathsf{g}(\mathsf{a})) \to \mathsf{f}(\mathsf{g}(\mathsf{a})) \to \dots$ $\qquad \mathcal{O}(\infty)$

resulting ITS: $\mathsf{f}(1) \xrightarrow{1} \mathsf{f}(\mathsf{g}(1))$ $\qquad \mathcal{O}(1)$

Definition

A TRS is completely defined iff its ground normal forms do not contain defined symbols.

TRS not completely defined? $\curvearrowright$ Add suitable terminating variant!

Ensuring Complete Definedness

Term Rewriting	Integer Transition Systems
arbitrary matchers	integer substitutions only

Example

$$\mathsf{f}(x) \longrightarrow \mathsf{f}(\mathsf{g}(\mathsf{a})) \qquad \mathsf{g}(\mathsf{b}(\mathsf{a})) \longrightarrow \mathsf{a} \qquad \mathsf{g}(x) \xrightarrow{=} \mathsf{a}$$

original TRS: $\mathsf{f}(\mathsf{a}) \longrightarrow \mathsf{f}(\mathsf{g}(\mathsf{a})) \longrightarrow \mathsf{f}(\mathsf{g}(\mathsf{a})) \longrightarrow \dots$ $\mathcal{O}(\infty)$

resulting ITS: $\mathsf{f}(1) \xrightarrow{1} \mathsf{f}(\mathsf{g}(1))$ $\mathcal{O}(1)$

ITS after completion: $\mathsf{f}(1) \xrightarrow{1} \mathsf{f}(\mathsf{g}(1)) \xrightarrow{0} \mathsf{f}(1) \xrightarrow{1} \mathsf{f}(\mathsf{g}(1)) \xrightarrow{0} \dots$

Definition

A TRS is completely defined iff its ground normal forms do not contain defined symbols.

TRS not completely defined? $\curvearrowright$ Add suitable terminating variant!

Ensuring Complete Definedness

Term Rewriting	Integer Transition Systems
arbitrary matchers	integer substitutions only

Example

$$\mathsf{f}(x) \longrightarrow \mathsf{f}(\mathsf{g}(\mathsf{a})) \qquad \mathsf{g}(\mathsf{b}(\mathsf{a})) \longrightarrow \mathsf{a} \qquad \mathsf{g}(x) \xrightarrow{=} \mathsf{a}$$

original TRS: $\mathsf{f}(\mathsf{a}) \longrightarrow \mathsf{f}(\mathsf{g}(\mathsf{a})) \longrightarrow \mathsf{f}(\mathsf{g}(\mathsf{a})) \longrightarrow \ldots$ $\mathcal{O}(\infty)$

resulting ITS: $\mathsf{f}(1) \xrightarrow{1} \mathsf{f}(\mathsf{g}(1))$ $\mathcal{O}(1)$

ITS after completion: $\mathsf{f}(1) \xrightarrow{1} \mathsf{f}(\mathsf{g}(1)) \xrightarrow{0} \mathsf{f}(1) \xrightarrow{1} \mathsf{f}(\mathsf{g}(1)) \xrightarrow{0} \ldots$ $\mathcal{O}(\infty)$

Definition

A TRS is completely defined iff its ground normal forms do not contain defined symbols.

TRS not completely defined? $\curvearrowright$ Add suitable terminating variant!

Ensuring Complete Definedness

Term Rewriting	Integer Transition Systems
arbitrary matchers	integer substitutions only

Example

$$\mathsf{f}(x) \longrightarrow \mathsf{f}(\mathsf{g}(\mathsf{a})) \qquad \mathsf{g}(\mathsf{b}(\mathsf{a})) \longrightarrow \mathsf{a} \qquad \mathsf{g}(x) \xrightarrow{=} \mathsf{a}$$

original TRS: $\mathsf{f}(\mathsf{a}) \longrightarrow \mathsf{f}(\mathsf{g}(\mathsf{a})) \longrightarrow \mathsf{f}(\mathsf{g}(\mathsf{a})) \longrightarrow \dots$ $\mathcal{O}(\infty)$

resulting ITS: $\mathsf{f}(1) \xrightarrow{1} \mathsf{f}(\mathsf{g}(1))$ $\mathcal{O}(1)$

ITS after completion: $\mathsf{f}(1) \xrightarrow{1} \mathsf{f}(\mathsf{g}(1)) \xrightarrow{0} \mathsf{f}(1) \xrightarrow{1} \mathsf{f}(\mathsf{g}(1)) \xrightarrow{0} \dots$ $\mathcal{O}(\infty)$

Definition

A TRS is completely defined iff its well-typed ground normal forms do not contain defined symbols.

TRS not completely defined? $\curvearrowright$ Add suitable terminating variant!

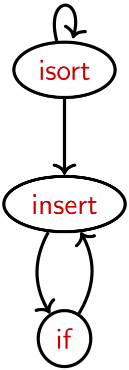
Bird's Eye View

Example

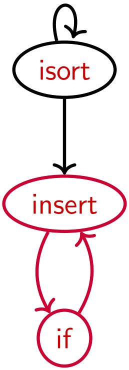
$$
\begin{array}{rcll}
\mathsf{isort}(xs', ys) & \xrightarrow{1} & ys & \mid \quad xs' = 1 \\
\mathsf{isort}(xs', ys) & \xrightarrow{1} & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) & \mid \quad xs' = 1 + x + xs \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & 2 + x & \mid \quad ys' = 1 \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & \mathsf{if}(b, x, ys') & \mid \quad ys' = 1 + y + ys \wedge b \leq 1 \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + y + \mathsf{insert}(x, ys) & \mid \quad b = 1 \wedge ys' = 1 + y + ys \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + ys' & \mid \quad b = 1 \wedge ys' = 1 + y + ys
\end{array}
$$

1. abstract terms to integers
2. analyse result size for bottom-SCC using standard ITS tools
3. analyse runtime of bottom-SCC using standard ITS tools

Call Graph & Bottom SCCs



Call Graph & Bottom SCCs



Bird's Eye View

Example

$$
\begin{array}{rcll}
\mathsf{isort}(xs', ys) & \xrightarrow{1} & ys & \mid \quad xs' = 1 \\
\mathsf{isort}(xs', ys) & \xrightarrow{1} & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) & \mid \quad xs' = 1 + x + xs \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & 2 + x & \mid \quad ys' = 1 \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & \mathsf{if}(b, x, ys') & \mid \quad ys' = 1 + y + ys \wedge b \leq 1 \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + y + \mathsf{insert}(x, ys) & \mid \quad b = 1 \wedge ys' = 1 + y + ys \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + ys' & \mid \quad b = 1 \wedge ys' = 1 + y + ys
\end{array}
$$

1. abstract terms to integers
2. analyse result size for bottom-SCC using standard ITS tools
3. analyse runtime of bottom-SCC using standard ITS tools

Bird's Eye View

Example

$$
\begin{array}{rcll}
\mathsf{isort}(xs', ys) & \xrightarrow{1} & ys & \mid \quad xs' = 1 \\
\mathsf{isort}(xs', ys) & \xrightarrow{1} & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) & \mid \quad xs' = 1 + x + xs \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & 2 + x & \mid \quad ys' = 1 \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & \mathsf{if}(b, x, ys') & \mid \quad ys' = 1 + y + ys \wedge b \leq 1 \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + y + \mathsf{insert}(x, ys) & \mid \quad b = 1 \wedge ys' = 1 + y + ys \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + ys' & \mid \quad b = 1 \wedge ys' = 1 + y + ys
\end{array}
$$

1. abstract terms to integers
2. analyse result size for bottom-SCC using standard ITS tools
3. analyse runtime of bottom-SCC using standard ITS tools

Analyse Size Using Standard ITS Tools

Using Runtime Analysis to Compute Size Bounds

Idea: time bound for insert in transformed rules gives size bound for insert in original rules

Example

$$
\begin{array}{llll}
\mathsf{insert}(x, ys') & \xrightarrow{1} & 2 + x & \mid \quad ys' = 1 \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & \mathsf{if}(b, x, ys') & \mid \quad ys' = 1 + y + ys \wedge b \leq 1 \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + y + \mathsf{insert}(x, ys) & \mid \quad b = 1 \wedge ys' = 1 + y + ys \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + ys' & \mid \quad b = 1 \wedge ys' = 1 + y + ys
\end{array}
$$

Using Runtime Analysis to Compute Size Bounds

Idea: time bound for insert in transformed rules gives size bound for insert in original rules

Example

$\mathsf{insert}(x, ys')$	$\xrightarrow{1}$	$2 + x$	$\mid$ $ys' = 1$
$\mathsf{insert}(x, ys')$	$\xrightarrow{1}$	$\mathsf{if}(b, x, ys')$	$\mid$ $ys' = 1 + y + ys \land b \leq 1$
$\mathsf{if}(b, x, ys')$	$\xrightarrow{1}$	$1 + y + \mathsf{insert}(x, ys)$	$\mid$ $b = 1 \land ys' = 1 + y + ys$
$\mathsf{if}(b, x, ys')$	$\xrightarrow{1}$	$1 + ys'$	$\mid$ $b = 1 \land ys' = 1 + y + ys$

Idea: move "integer context" to weights

Using Runtime Analysis to Compute Size Bounds

Idea: time bound for insert in transformed rules gives size bound for insert in original rules

Example

$$
\begin{array}{llll}
\mathsf{insert}(x, ys') & \xrightarrow{2+x} & 2 + x & \mid \quad ys' = 1 \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & \mathsf{if}(b, x, ys') & \mid \quad ys' = 1 + y + ys \land b \leq 1 \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + y + \mathsf{insert}(x, ys) & \mid \quad b = 1 \land ys' = 1 + y + ys \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + ys' & \mid \quad b = 1 \land ys' = 1 + y + ys
\end{array}
$$

Idea: move "integer context" to weights

Using Runtime Analysis to Compute Size Bounds

Idea: time bound for insert in transformed rules gives size bound for insert in original rules

Example

$\mathsf{insert}(x, ys')$	$\xrightarrow{2+x}$	$2 + x$	$\mid$	$ys' = 1$
$\mathsf{insert}(x, ys')$	$\xrightarrow{0}$	$\mathsf{if}(b, x, ys')$	$\mid$	$ys' = 1 + y + ys \wedge b \leq 1$
$\mathsf{if}(b, x, ys')$	$\xrightarrow{1}$	$1 + y + \mathsf{insert}(x, ys)$	$\mid$	$b = 1 \wedge ys' = 1 + y + ys$
$\mathsf{if}(b, x, ys')$	$\xrightarrow{1}$	$1 + ys'$	$\mid$	$b = 1 \wedge ys' = 1 + y + ys$

Idea: move "integer context" to weights

Using Runtime Analysis to Compute Size Bounds

Idea: time bound for insert in transformed rules gives size bound for insert in original rules

Example

$$
\begin{array}{llll}
\mathsf{insert}(x, ys') & \xrightarrow{2+x} & 2 + x & \mid \quad ys' = 1 \\
\mathsf{insert}(x, ys') & \xrightarrow{0} & \mathsf{if}(b, x, ys') & \mid \quad ys' = 1 + y + ys \wedge b \leq 1 \\
\mathsf{if}(b, x, ys') & \xrightarrow{1+y} & 1 + y + \mathsf{insert}(x, ys) & \mid \quad b = 1 \wedge ys' = 1 + y + ys \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + ys' & \mid \quad b = 1 \wedge ys' = 1 + y + ys
\end{array}
$$

Idea: move "integer context" to weights

Using Runtime Analysis to Compute Size Bounds

Idea: time bound for insert in transformed rules gives size bound for insert in original rules

Example

$$
\begin{array}{llll}
\mathsf{insert}(x, ys') & \xrightarrow{2+x} & 2 + x & \mid \quad ys' = 1 \\
\mathsf{insert}(x, ys') & \xrightarrow{0} & \mathsf{if}(b, x, ys') & \mid \quad ys' = 1 + y + ys \wedge b \leq 1 \\
\mathsf{if}(b, x, ys') & \xrightarrow{1+y} & 1 + y + \mathsf{insert}(x, ys) & \mid \quad b = 1 \wedge ys' = 1 + y + ys \\
\mathsf{if}(b, x, ys') & \xrightarrow{1+ys'} & 1 + ys' & \mid \quad b = 1 \wedge ys' = 1 + y + ys
\end{array}
$$

Idea: move "integer context" to weights

Using Runtime Analysis to Compute Size Bounds

Idea: time bound for insert in transformed rules gives size bound for insert in original rules

Example

$$
\begin{array}{llll}
\mathsf{insert}(x, ys') & \xrightarrow{2+x} & 2 + x & \mid \quad ys' = 1 \\
\mathsf{insert}(x, ys') & \xrightarrow{0} & \mathsf{if}(b, x, ys') & \mid \quad ys' = 1 + y + ys \land b \leq 1 \\
\mathsf{if}(b, x, ys') & \xrightarrow{1+y} & 1 + y + \mathsf{insert}(x, ys) & \mid \quad b = 1 \land ys' = 1 + y + ys \\
\mathsf{if}(b, x, ys') & \xrightarrow{1+ys'} & 1 + ys' & \mid \quad b = 1 \land ys' = 1 + y + ys
\end{array}
$$

Idea: move "integer context" to weights $\curvearrowright$ $\mathsf{sz}(\mathsf{insert}(x, ys')) \leq 1 + x + ys'$

Using Runtime Analysis to Compute Size Bounds

Idea: time bound for insert in transformed rules gives size bound for insert in original rules

Example

$$
\begin{array}{llll}
\mathsf{insert}(x, ys') & \xrightarrow{2+x} & 2 + x & \mid \quad ys' = 1 \\
\mathsf{insert}(x, ys') & \xrightarrow{0} & \mathsf{if}(b, x, ys') & \mid \quad ys' = 1 + y + ys \wedge b \leq 1 \\
\mathsf{if}(b, x, ys') & \xrightarrow{1+y} & 1 + y + \mathsf{insert}(x, ys) & \mid \quad b = 1 \wedge ys' = 1 + y + ys \\
\mathsf{if}(b, x, ys') & \xrightarrow{1+ys'} & 1 + ys' & \mid \quad b = 1 \wedge ys' = 1 + y + ys
\end{array}
$$

Idea: move "integer context" to weights $\curvearrowright$ $\mathsf{sz}(\mathsf{insert}(x, ys')) \leq 1 + x + ys'$

Example

$$
\mathsf{f}(x) \quad \xrightarrow{1} \quad 2 + x \cdot \mathsf{f}(x - 1) \quad \mid \quad x > 0
$$

Using Runtime Analysis to Compute Size Bounds

Idea: time bound for insert in transformed rules gives size bound for insert in original rules

Example

$$
\begin{array}{llll}
\mathsf{insert}(x, ys') & \xrightarrow{2+x} & 2 + x & \mid \quad ys' = 1 \\
\mathsf{insert}(x, ys') & \xrightarrow{0} & \mathsf{if}(b, x, ys') & \mid \quad ys' = 1 + y + ys \wedge b \leq 1 \\
\mathsf{if}(b, x, ys') & \xrightarrow{1+y} & 1 + y + \mathsf{insert}(x, ys) & \mid \quad b = 1 \wedge ys' = 1 + y + ys \\
\mathsf{if}(b, x, ys') & \xrightarrow{1+ys'} & 1 + ys' & \mid \quad b = 1 \wedge ys' = 1 + y + ys
\end{array}
$$

Idea: move "integer context" to weights $\curvearrowright$ $\mathsf{sz}(\mathsf{insert}(x, ys')) \leq 1 + x + ys'$

Example

$$
\mathsf{f}(x) \quad \xrightarrow{1} \quad 2 + x \cdot \mathsf{f}(x - 1) \quad \mid \quad x > 0
$$

Idea: use accumulator

Using Runtime Analysis to Compute Size Bounds

Idea: time bound for insert in transformed rules gives size bound for insert in original rules

Example

$$\begin{array}{rcll} \mathsf{insert}(x, ys') & \xrightarrow{2+x} & 2 + x & \mid \quad ys' = 1 \\ \mathsf{insert}(x, ys') & \xrightarrow{0} & \mathsf{if}(b, x, ys') & \mid \quad ys' = 1 + y + ys \wedge b \leq 1 \\ \mathsf{if}(b, x, ys') & \xrightarrow{1+y} & 1 + y + \mathsf{insert}(x, ys) & \mid \quad b = 1 \wedge ys' = 1 + y + ys \\ \mathsf{if}(b, x, ys') & \xrightarrow{1+ys'} & 1 + ys' & \mid \quad b = 1 \wedge ys' = 1 + y + ys \end{array}$$

Idea: move "integer context" to weights $\curvearrowright$ $\mathsf{sz}(\mathsf{insert}(x, ys')) \leq 1 + x + ys'$

Example

$$\begin{array}{rcll} \mathsf{f}(x) & \xrightarrow{1} & 2 + x \cdot \mathsf{f}(x - 1) & \mid \quad x > 0 \\ \mathsf{f}(x, acc) & \xrightarrow{acc \cdot 2} & 2 + x \cdot \mathsf{f}(x - 1, acc \cdot x) & \mid \quad x > 0 \end{array}$$

Idea: use accumulator

Bird's Eye View

Example

$$
\begin{array}{rcll}
\mathsf{isort}(xs', ys) & \xrightarrow{1} & ys & \mid \quad xs' = 1 \\
\mathsf{isort}(xs', ys) & \xrightarrow{1} & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) & \mid \quad xs' = 1 + x + xs \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & 2 + x & \mid \quad ys' = 1 \\
\mathsf{insert}(x, ys') & \xrightarrow{1} & \mathsf{if}(b, x, ys') & \mid \quad ys' = 1 + y + ys \wedge b \leq 1 \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + y + \mathsf{insert}(x, ys) & \mid \quad b = 1 \wedge ys' = 1 + y + ys \\
\mathsf{if}(b, x, ys') & \xrightarrow{1} & 1 + ys' & \mid \quad b = 1 \wedge ys' = 1 + y + ys
\end{array}
$$

1. abstract terms to integers
2. analyse result size for bottom-SCC using standard ITS tools
3. analyse runtime of bottom-SCC using standard ITS tools

Bird's Eye View

Example

$$
\begin{array}{llll}
\mathsf{isort}(xs', ys) & \xrightarrow{1} ys & \mid & xs' = 1 \\
\mathsf{isort}(xs', ys) & \xrightarrow{1} \mathsf{isort}(xs, \mathsf{insert}(x, ys)) & \mid & xs' = 1 + x + xs
\end{array}
$$

1. abstract terms to integers
2. analyse result size for bottom-SCC using standard ITS tools
3. analyse runtime of bottom-SCC using standard ITS tools

Analyse Runtime Using Standard Tools

Removing Nested Function Calls

Example

$$\begin{array}{llll} \mathsf{isort}(xs', ys) & \xrightarrow{1} & ys & \mid \quad xs' = 1 \\ \mathsf{isort}(xs', ys) & \xrightarrow{1} & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) & \mid \quad xs' = 1{+}x{+}xs \end{array}$$

- $\mathsf{sz}(\mathsf{insert}(x, ys)) \leq 1 + x + ys$
- $\mathsf{rt}(\mathsf{insert}(x, ys)) \leq 2 \cdot ys$

Removing Nested Function Calls

Example

$$\begin{array}{llll} \mathsf{isort}(xs', ys) & \xrightarrow{1} & ys & \mid \quad xs' = 1 \\ \mathsf{isort}(xs', ys) & \xrightarrow{1} & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) & \mid \quad xs' = 1{+}x{+}xs \end{array}$$

- $\mathsf{sz}(\mathsf{insert}(x, ys)) \leq 1 + x + ys$
- $\mathsf{rt}(\mathsf{insert}(x, ys)) \leq 2 \cdot ys$
- add costs of nested function call

Removing Nested Function Calls

Example

$$\begin{array}{llll} \mathsf{isort}(xs', ys) & \xrightarrow{1} & ys & \mid \quad xs' = 1 \\ \mathsf{isort}(xs', ys) & \xrightarrow{1+2\cdot ys} & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) & \mid \quad xs' = 1{+}x{+}xs \end{array}$$

- $\mathsf{sz}(\mathsf{insert}(x, ys)) \leq 1 + x + ys$
- $\mathsf{rt}(\mathsf{insert}(x, ys)) \leq 2 \cdot ys$
- add costs of nested function call

Removing Nested Function Calls

Example

$$
\begin{array}{llll}
\mathsf{isort}(xs', ys) & \xrightarrow{1} & ys & \mid \quad xs' = 1 \\
\mathsf{isort}(xs', ys) & \xrightarrow{1+2\cdot ys} & \mathsf{isort}(xs, \mathsf{insert}(x, ys)) & \mid \quad xs' = 1{+}x{+}xs
\end{array}
$$

- $\mathsf{sz}(\mathsf{insert}(x, ys)) \leq 1 + x + ys$
- $\mathsf{rt}(\mathsf{insert}(x, ys)) \leq 2 \cdot ys$
- add costs of nested function call
- replace nested function call by fresh variable x_f

Removing Nested Function Calls

Example

$$\mathsf{isort}(xs', ys) \xrightarrow{1} ys \quad | \quad xs' = 1$$
$$\mathsf{isort}(xs', ys) \xrightarrow{1+2\cdot ys} \mathsf{isort}(xs, x_f) \quad | \quad xs' = 1{+}x{+}xs$$

- $\mathsf{sz}(\mathsf{insert}(x, ys)) \leq 1 + x + ys$
- $\mathsf{rt}(\mathsf{insert}(x, ys)) \leq 2 \cdot ys$
- add costs of nested function call
- replace nested function call by fresh variable x_f

Removing Nested Function Calls

Example

$$\mathsf{isort}(xs', ys) \xrightarrow{1} ys \quad | \quad xs' = 1$$

$$\mathsf{isort}(xs', ys) \xrightarrow{1+2\cdot ys} \mathsf{isort}(xs, x_f) \quad | \quad xs' = 1{+}x{+}xs$$

- $\mathsf{sz}(\mathsf{insert}(x, ys)) \leq 1 + x + ys$
- $\mathsf{rt}(\mathsf{insert}(x, ys)) \leq 2 \cdot ys$
- add costs of nested function call
- replace nested function call by fresh variable x_f
- add constraint "$x_f \leq$ size bound"

Removing Nested Function Calls

Example

$$\begin{array}{llll} \mathsf{isort}(xs', ys) & \xrightarrow{1} & ys & \mid \quad xs' = 1 \\ \mathsf{isort}(xs', ys) & \xrightarrow{1+2\cdot ys} & \mathsf{isort}(xs, x_f) & \mid \quad xs' = 1{+}x{+}xs \wedge x_f \leq 1{+}x{+}ys \end{array}$$

- $\mathsf{sz}(\mathsf{insert}(x, ys)) \leq 1 + x + ys$
- $\mathsf{rt}(\mathsf{insert}(x, ys)) \leq 2 \cdot ys$
- add costs of nested function call
- replace nested function call by fresh variable x_f
- add constraint "$x_f \leq$ size bound"

Removing Nested Function Calls

Example

$$\begin{array}{llll} \text{isort}(xs', ys) & \xrightarrow{1} & ys & \mid \quad xs' = 1 \\ \text{isort}(xs', ys) & \xrightarrow{1+2\cdot ys} & \text{isort}(xs, x_f) & \mid \quad xs' = 1+x+xs \land x_f \leq 1+x+ys \end{array}$$

- $\text{sz}(\text{insert}(x, ys)) \leq 1 + x + ys$
- $\text{rt}(\text{insert}(x, ys)) \leq 2 \cdot ys$
- add costs of nested function call
- replace nested function call by fresh variable x_f
- add constraint "$x_f \leq$ size bound"

$\curvearrowright$ $\text{rt}(\text{isort}(xs', ys)) \leq \mathcal{O}(xs'^2 + xs' \cdot ys)$

Removing Nested Function Calls

Example

$$\begin{array}{lcl|l} \mathsf{isort}(xs', ys) & \xrightarrow{1} & ys & xs' = 1 \\ \mathsf{isort}(xs', ys) & \xrightarrow{1+2\cdot ys} & \mathsf{isort}(xs, x_f) & xs' = 1{+}x{+}xs \wedge x_f \leq 1{+}x{+}ys \end{array}$$

- $\mathsf{sz}(\mathsf{insert}(x, ys)) \leq 1 + x + ys$
- $\mathsf{rt}(\mathsf{insert}(x, ys)) \leq 2 \cdot ys$
- add costs of nested function call
- replace nested function call by fresh variable x_f
- add constraint "$x_f \leq$ size bound"

↷ $\mathsf{rt}(\mathsf{isort}(xs', ys)) \leq \mathcal{O}(xs'^2 + xs' \cdot ys)$

- similar techniques to eliminate *outer* function calls

Removing Nested Function Calls

Example

$$\begin{array}{lcll} \mathsf{isort}(xs', ys) & \xrightarrow{1} & ys & \mid\ xs' = 1 \\ \mathsf{isort}(xs', ys) & \xrightarrow{1+2\cdot ys} & \mathsf{isort}(xs, x_f) & \mid\ xs' = 1+x+xs \wedge x_f \leq 1+x+ys \end{array}$$

- $\mathsf{sz}(\mathsf{insert}(x, ys)) \leq 1 + x + ys$
- $\mathsf{rt}(\mathsf{insert}(x, ys)) \leq 2 \cdot ys$
- add costs of nested function call
- replace nested function call by fresh variable x_f
- add constraint "$x_f \leq$ size bound"

$\curvearrowright$ $\mathsf{rt}(\mathsf{isort}(xs', ys)) \leq \mathcal{O}(xs'^2 + xs' \cdot ys)$

- similar techniques to eliminate *outer* function calls

$$\mathsf{times}(\mathsf{s}(x), y) \longrightarrow \mathsf{plus}(\mathsf{times}(x, y), y)$$

Removing Nested Function Calls

Example

$$\begin{array}{llll} \mathsf{isort}(xs', ys) & \xrightarrow{1} & ys & \mid \quad xs' = 1 \\ \mathsf{isort}(xs', ys) & \xrightarrow{1+2\cdot ys} & \mathsf{isort}(xs, x_f) & \mid \quad xs' = 1+x+xs \wedge x_f \leq 1+x+ys \end{array}$$

- $\mathsf{sz}(\mathsf{insert}(x, ys)) \leq 1 + x + ys$
- $\mathsf{rt}(\mathsf{insert}(x, ys)) \leq 2 \cdot ys$
- add costs of nested function call
- replace nested function call by fresh variable x_f
- add constraint "$x_f \leq$ size bound"

↷ $\mathsf{rt}(\mathsf{isort}(xs', ys)) \leq \mathcal{O}(xs'^2 + xs' \cdot ys)$

- similar techniques to eliminate *outer* function calls $\Longrightarrow$ see paper!

$$\mathsf{times}(\mathsf{s}(x), y) \longrightarrow \mathsf{plus}(\mathsf{times}(x, y), y)$$

Experiments

ITS tools CoFloCo, KoAT, and PUBS used as back-ends.

ITS tools CoFloCo, KoAT, and PUBS used as back-ends.

Results on the TPDB (922 examples):

Experiments

ITS tools CoFloCo, KoAT, and PUBS used as back-ends.

Results on the TPDB (922 examples):

- AProVE + ITS back-end finds better bounds than AProVE & TcT for 127 TRSs
- transformation a useful additional inference technique for upper bounds

From irc of TRSs to Integer Transition Systems: Summary

- Abstraction from terms to integers
- Modular bottom-up approach using standard ITS tools
- Approach complements and improves state of the art
- Note: abstraction **hard-coded** to term size

⇒ Future work: more flexible approach?

Derivational_Complexity_Full_Rewriting/AG01/#3.12, TPDB

$$\begin{aligned}
\mathsf{app}(\mathsf{nil}, y) &\to y & \mathsf{app}(\mathsf{add}(n, x), y) &\to \mathsf{add}(n, \mathsf{app}(x, y)) \\
\mathsf{reverse}(\mathsf{nil}) &\to \mathsf{nil} & \mathsf{reverse}(\mathsf{add}(n, x)) &\to \mathsf{app}(\mathsf{reverse}(x), \mathsf{add}(n, \mathsf{nil})) \\
\mathsf{shuffle}(\mathsf{nil}) &\to \mathsf{nil} & \mathsf{shuffle}(\mathsf{add}(n, x)) &\to \mathsf{add}(n, \mathsf{shuffle}(\mathsf{reverse}(x)))
\end{aligned}$$

$$\begin{array}{rcl|rcl} \mathsf{app}(\mathsf{nil}, y) & \to & y & \mathsf{app}(\mathsf{add}(n, x), y) & \to & \mathsf{add}(n, \mathsf{app}(x, y)) \\ \mathsf{reverse}(\mathsf{nil}) & \to & \mathsf{nil} & \mathsf{reverse}(\mathsf{add}(n, x)) & \to & \mathsf{app}(\mathsf{reverse}(x), \mathsf{add}(n, \mathsf{nil})) \\ \mathsf{shuffle}(\mathsf{nil}) & \to & \mathsf{nil} & \mathsf{shuffle}(\mathsf{add}(n, x)) & \to & \mathsf{add}(n, \mathsf{shuffle}(\mathsf{reverse}(x))) \end{array}$$

AProVE finds (tight) upper bound $\mathcal{O}(n^4)$ for $\mathrm{dc}_{\mathcal{R}}$:

Derivational_Complexity_Full_Rewriting/AG01/#3.12, TPDB

$$\begin{array}{rcl|rcl} \mathsf{app}(\mathsf{nil}, y) & \to & y & \mathsf{app}(\mathsf{add}(n, x), y) & \to & \mathsf{add}(n, \mathsf{app}(x, y)) \\ \mathsf{reverse}(\mathsf{nil}) & \to & \mathsf{nil} & \mathsf{reverse}(\mathsf{add}(n, x)) & \to & \mathsf{app}(\mathsf{reverse}(x), \mathsf{add}(n, \mathsf{nil})) \\ \mathsf{shuffle}(\mathsf{nil}) & \to & \mathsf{nil} & \mathsf{shuffle}(\mathsf{add}(n, x)) & \to & \mathsf{add}(n, \mathsf{shuffle}(\mathsf{reverse}(x))) \end{array}$$

AProVE finds (tight) upper bound $\mathcal{O}(n^4)$ for $\mathrm{dc}_{\mathcal{R}}$:

1. Add generator rules $\mathcal{G}$, so analyse $\mathrm{rc}_{\mathcal{R}/\mathcal{G}}$ instead (FroCoS'19)

Derivational_Complexity_Full_Rewriting/AG01/#3.12, TPDB

$$\begin{array}{rcl|rcl} \mathsf{app}(\mathsf{nil}, y) & \to & y & \mathsf{app}(\mathsf{add}(n, x), y) & \to & \mathsf{add}(n, \mathsf{app}(x, y)) \\ \mathsf{reverse}(\mathsf{nil}) & \to & \mathsf{nil} & \mathsf{reverse}(\mathsf{add}(n, x)) & \to & \mathsf{app}(\mathsf{reverse}(x), \mathsf{add}(n, \mathsf{nil})) \\ \mathsf{shuffle}(\mathsf{nil}) & \to & \mathsf{nil} & \mathsf{shuffle}(\mathsf{add}(n, x)) & \to & \mathsf{add}(n, \mathsf{shuffle}(\mathsf{reverse}(x))) \end{array}$$

AProVE finds (tight) upper bound $\mathcal{O}(n^4)$ for $\mathrm{dc}_{\mathcal{R}}$:

1. Add generator rules $\mathcal{G}$, so analyse $\mathrm{rc}_{\mathcal{R}/\mathcal{G}}$ instead (FroCoS'19)
2. Detect: innermost is worst case here, analyse $\mathrm{irc}_{\mathcal{R}/\mathcal{G}}$ instead (LPAR'17)

Derivational_Complexity_Full_Rewriting/AG01/#3.12, TPDB

$$\begin{array}{rcl|rcl} \mathsf{app}(\mathsf{nil}, y) & \to & y & \mathsf{app}(\mathsf{add}(n, x), y) & \to & \mathsf{add}(n, \mathsf{app}(x, y)) \\ \mathsf{reverse}(\mathsf{nil}) & \to & \mathsf{nil} & \mathsf{reverse}(\mathsf{add}(n, x)) & \to & \mathsf{app}(\mathsf{reverse}(x), \mathsf{add}(n, \mathsf{nil})) \\ \mathsf{shuffle}(\mathsf{nil}) & \to & \mathsf{nil} & \mathsf{shuffle}(\mathsf{add}(n, x)) & \to & \mathsf{add}(n, \mathsf{shuffle}(\mathsf{reverse}(x))) \end{array}$$

AProVE finds (tight) upper bound $\mathcal{O}(n^4)$ for $\mathrm{dc}_{\mathcal{R}}$:

1. Add generator rules $\mathcal{G}$, so analyse $\mathrm{rc}_{\mathcal{R}/\mathcal{G}}$ instead (FroCoS'19)
2. Detect: innermost is worst case here, analyse $\mathrm{irc}_{\mathcal{R}/\mathcal{G}}$ instead (LPAR'17)
3. Transform TRS to Recursive Integer Transition System (RITS), analyse complexity of RITS instead (FroCoS'17)

$\mathsf{app}(\mathsf{nil}, y)$	$\to$	y	$\mathsf{app}(\mathsf{add}(n, x), y)$	$\to$	$\mathsf{add}(n, \mathsf{app}(x, y))$
$\mathsf{reverse}(\mathsf{nil})$	$\to$	nil	$\mathsf{reverse}(\mathsf{add}(n, x))$	$\to$	$\mathsf{app}(\mathsf{reverse}(x), \mathsf{add}(n, \mathsf{nil}))$
$\mathsf{shuffle}(\mathsf{nil})$	$\to$	nil	$\mathsf{shuffle}(\mathsf{add}(n, x))$	$\to$	$\mathsf{add}(n, \mathsf{shuffle}(\mathsf{reverse}(x)))$

AProVE finds (tight) upper bound $\mathcal{O}(n^4)$ for $\mathrm{dc}_{\mathcal{R}}$:

1. Add generator rules $\mathcal{G}$, so analyse $\mathrm{rc}_{\mathcal{R}/\mathcal{G}}$ instead (FroCoS'19)
2. Detect: innermost is worst case here, analyse $\mathrm{irc}_{\mathcal{R}/\mathcal{G}}$ instead (LPAR'17)
3. Transform TRS to Recursive Integer Transition System (RITS), analyse complexity of RITS instead (FroCoS'17)
4. ITS tools CoFloCo and KoAT find upper bounds for runtime and size of individual RITS functions, combine to complexity of RITS

Derivational_Complexity_Full_Rewriting/AG01/#3.12, TPDB

$\mathsf{app}(\mathsf{nil}, y)$	$\to$	y	$\mathsf{app}(\mathsf{add}(n, x), y)$	$\to$	$\mathsf{add}(n, \mathsf{app}(x, y))$
$\mathsf{reverse}(\mathsf{nil})$	$\to$	nil	$\mathsf{reverse}(\mathsf{add}(n, x))$	$\to$	$\mathsf{app}(\mathsf{reverse}(x), \mathsf{add}(n, \mathsf{nil}))$
$\mathsf{shuffle}(\mathsf{nil})$	$\to$	nil	$\mathsf{shuffle}(\mathsf{add}(n, x))$	$\to$	$\mathsf{add}(n, \mathsf{shuffle}(\mathsf{reverse}(x)))$

AProVE finds (tight) upper bound $\mathcal{O}(n^4)$ for $\mathrm{dc}_{\mathcal{R}}$:

1. Add generator rules $\mathcal{G}$, so analyse $\mathrm{rc}_{\mathcal{R}/\mathcal{G}}$ instead (FroCoS'19)
2. Detect: innermost is worst case here, analyse $\mathrm{irc}_{\mathcal{R}/\mathcal{G}}$ instead (LPAR'17)
3. Transform TRS to Recursive Integer Transition System (RITS), analyse complexity of RITS instead (FroCoS'17)
4. ITS tools CoFloCo and KoAT find upper bounds for runtime and size of individual RITS functions, combine to complexity of RITS
5. Upper bound $\mathcal{O}(n^4)$ for RITS complexity carries over to $\mathrm{dc}_{\mathcal{R}}$ of input!

AProVE finds lower bound $\Omega(n^3)$ for $\mathrm{dc}_{\mathcal{R}}$ using induction technique.

Input for Automated Tools (1/4)

Automated tools for TRS Complexity at the Termination Competition 2022:

- AProVE: https://aprove.informatik.rwth-aachen.de/
- TcT: https://tcs-informatik.uibk.ac.at/tools/tct/

[57] For TcT Web, use only VAR and RULES entries in the text format and configure other aspects (e.g., start terms) in the web interface.

Input for Automated Tools (1/4)

Automated tools for TRS Complexity at the Termination Competition 2022:

- AProVE: https://aprove.informatik.rwth-aachen.de/
- TcT: https://tcs-informatik.uibk.ac.at/tools/tct/

Web interfaces available:

- AProVE: https://aprove.informatik.rwth-aachen.de/interface
- TcT: http://colo6-c703.uibk.ac.at/tct/tct-trs/

[57] For TcT Web, use only VAR and RULES entries in the text format and configure other aspects (e.g., start terms) in the web interface.

Input for Automated Tools (1/4)

Automated tools for TRS Complexity at the Termination Competition 2022:

- AProVE: https://aprove.informatik.rwth-aachen.de/
- TcT: https://tcs-informatik.uibk.ac.at/tools/tct/

Web interfaces available:

- AProVE: https://aprove.informatik.rwth-aachen.de/interface
- TcT: http://colo6-c703.uibk.ac.at/tct/tct-trs/

Input format for runtime complexity:[57]

```
(VAR x y)
(GOAL COMPLEXITY)
(STARTTERM CONSTRUCTOR-BASED)
(RULES
  plus(0, y) -> y
  plus(s(x), y) -> s(plus(x, y))
)
```

[57] For TcT Web, use only VAR and RULES entries in the text format and configure other aspects (e.g., start terms) in the web interface.

Input for Automated Tools (2/4)

Innermost runtime complexity:

```
(VAR x y)
(GOAL COMPLEXITY)
(STARTTERM CONSTRUCTOR-BASED)
(STRATEGY INNERMOST)
(RULES
  plus(0, y) -> y
  plus(s(x), y) -> s(plus(x, y))
)
```

Input for Automated Tools (3/4)

Derivational complexity:

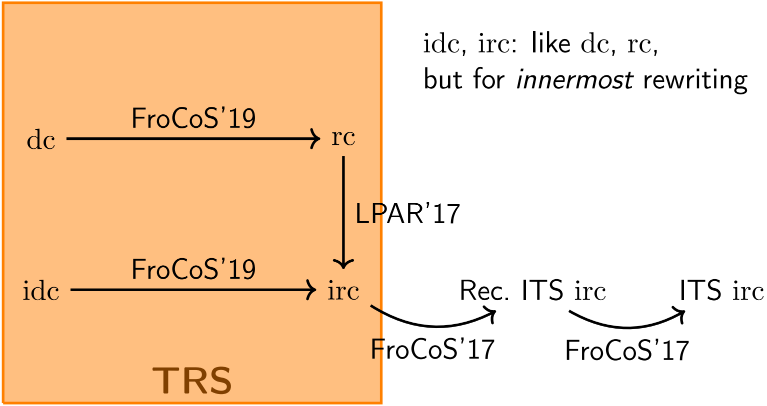
```
(VAR x y)
(GOAL COMPLEXITY)
(STARTTERM UNRESTRICTED)
(RULES
  plus(0, y) -> y
  plus(s(x), y) -> s(plus(x, y))
)
```

Input for Automated Tools (4/4)

Innermost derivational complexity:

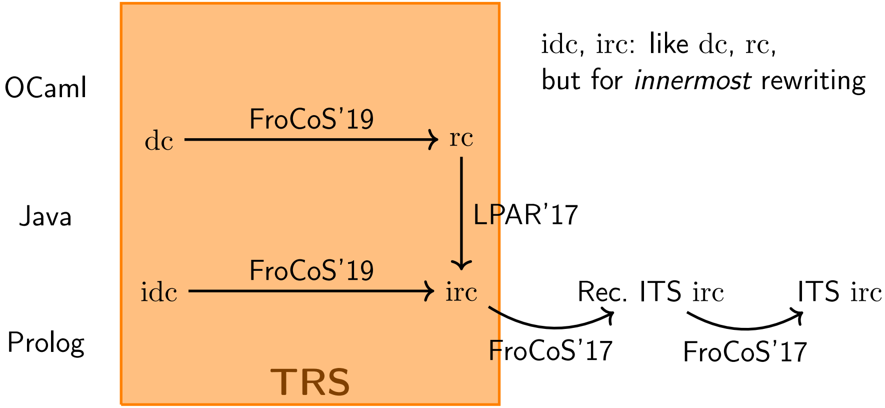
```
(VAR x y)
(GOAL COMPLEXITY)
(STARTTERM UNRESTRICTED)
(STRATEGY INNERMOST)
(RULES
  plus(0, y) -> y
  plus(s(x), y) -> s(plus(x, y))
)
```

A Landscape of Complexity Properties and Transformations



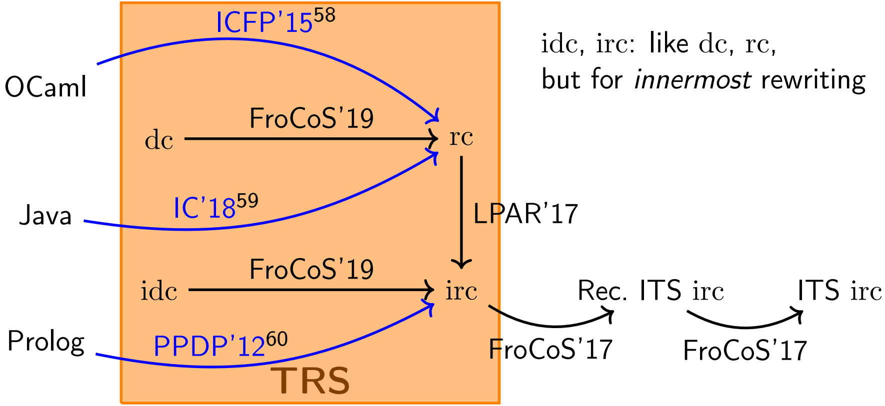
idc, irc: like dc, rc,
but for *innermost* rewriting

A Landscape of Complexity Properties and Transformations



idc, irc: like dc, rc,
but for *innermost* rewriting

A Landscape of Complexity Properties and Transformations



idc, irc: like dc, rc,
but for *innermost* rewriting

[58] M. Avanzini, U. Dal Lago, G. Moser: *Analysing the Complexity of Functional Programs: Higher-Order Meets First-Order*, ICFP '15

[59] G. Moser, M. Schaper: *From Jinja bytecode to term rewriting: A complexity reflecting transformation*, IC '18

[60] J. Giesl, T. Ströder, P. Schneider-Kamp, F. Emmes, C. Fuhs: *Symbolic evaluation graphs and term rewriting: A general methodology for analyzing logic programs*, PPDP '12

Program Complexity Analysis via Term Rewriting: OCaml

Complexity analysis for functional programs (OCaml) by translation to term rewriting

Program Complexity Analysis via Term Rewriting: OCaml

Complexity analysis for functional programs (OCaml) by translation to term rewriting

Challenge for translation to TRS: OCaml is higher-order – functions can take functions as arguments: map(F, xs)

Program Complexity Analysis via Term Rewriting: OCaml

Complexity analysis for functional programs (OCaml) by translation to term rewriting

Challenge for translation to TRS: OCaml is higher-order – functions can take functions as arguments: $\mathsf{map}(F, xs)$

Solution:

- Defunctionalisation to: $\mathsf{a}(\mathsf{a}(\mathsf{map}, F), xs)$
- Analyse start term with non-functional parameter types, then partially evaluate functions to instantiate higher-order variables
- Further program transformations

⇒ First-order TRS $\mathcal{R}$ with $\mathrm{rc}_{\mathcal{R}}(n)$ an upper bound for the complexity of the OCaml program

Program Complexity Analysis via Term Rewriting: Prolog and Java

Complexity analysis for Prolog programs and for Java programs by translation to term rewriting

Program Complexity Analysis via Term Rewriting: Prolog and Java

Complexity analysis for Prolog programs and for Java programs by translation to term rewriting

Common ideas:

- Analyse program via symbolic execution and generalisation (a form of abstract interpretation[61])
- Deal with language specifics in program analysis
- Extract TRS $\mathcal{R}$ such that $\mathrm{rc}_{\mathcal{R}}(n)$ is provably at least as high as runtime of program on input of size n
- Can represent tree structures of program as terms in TRS!

[61] P. Cousot, R. Cousot: *Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints*, POPL '77

Current Developments

- **amortised** complexity analysis for term rewriting[62]

[62] G. Moser, M. Schneckenreither: *Automated amortised resource analysis for term rewrite systems*, SCP '20

Current Developments

- **amortised** complexity analysis for term rewriting[62]
- **probabilistic** term rewriting $\longrightarrow$ upper bounds on **expected runtime**[63]

[62] G. Moser, M. Schneckenreither: *Automated amortised resource analysis for term rewrite systems*, SCP '20
[63] M. Avanzini, U. Dal Lago, A. Yamada: *On probabilistic term rewriting*, SCP '20

Current Developments

- **amortised** complexity analysis for term rewriting[62]
- **probabilistic** term rewriting $\longrightarrow$ upper bounds on **expected runtime**[63]
- complexity analysis for **logically constrained rewriting** with built-in data types from SMT theories (integers, booleans, arrays, ...)[64]

[62] G. Moser, M. Schneckenreither: *Automated amortised resource analysis for term rewrite systems*, SCP '20
[63] M. Avanzini, U. Dal Lago, A. Yamada: *On probabilistic term rewriting*, SCP '20
[64] S. Winkler, G. Moser: *Runtime complexity analysis of logically constrained rewriting*, LOPSTR '20

Current Developments

- **amortised** complexity analysis for term rewriting[62]
- **probabilistic** term rewriting $\longrightarrow$ upper bounds on **expected runtime**[63]
- complexity analysis for **logically constrained rewriting** with built-in data types from SMT theories (integers, booleans, arrays, . . .)[64]
- direct analysis of complexity for **higher-order term rewriting**[65]

[62] G. Moser, M. Schneckenreither: *Automated amortised resource analysis for term rewrite systems*, SCP '20
[63] M. Avanzini, U. Dal Lago, A. Yamada: *On probabilistic term rewriting*, SCP '20
[64] S. Winkler, G. Moser: *Runtime complexity analysis of logically constrained rewriting*, LOPSTR '20
[65] C. Kop, D. Vale: *Tuple interpretations for higher-order rewriting*, FSCD '21

Current Developments

- **amortised** complexity analysis for term rewriting[62]
- **probabilistic** term rewriting $\longrightarrow$ upper bounds on **expected runtime**[63]
- complexity analysis for **logically constrained rewriting** with built-in data types from SMT theories (integers, booleans, arrays, ...)[64]
- direct analysis of complexity for **higher-order term rewriting**[65]
- analysis of **parallel**-innermost runtime complexity[66]

---

[62] G. Moser, M. Schneckenreither: *Automated amortised resource analysis for term rewrite systems*, SCP '20
[63] M. Avanzini, U. Dal Lago, A. Yamada: *On probabilistic term rewriting*, SCP '20
[64] S. Winkler, G. Moser: *Runtime complexity analysis of logically constrained rewriting*, LOPSTR '20
[65] C. Kop, D. Vale: *Tuple interpretations for higher-order rewriting*, FSCD '21
[66] T. Baudon, C. Fuhs, L. Gonnord: *Analysing parallel complexity of term rewriting*, LOPSTR '22

III. Termination and Complexity Proof Certification

Certification: Who Watches the Watchers?

- Termination and complexity analysis tools are large, e.g., AProVE has several 100,000s LOC – most likely with bugs!

Certification: Who Watches the Watchers?

- Termination and complexity analysis tools are large, e.g., AProVE has several 100,000s LOC – most likely with bugs!
- Observation in early Termination Competitions: some tools **disagreed** on YES / NO for termination

Certification: Who Watches the Watchers?

- Termination and complexity analysis tools are large, e.g., AProVE has several 100,000s LOC – most likely with bugs!
- Observation in early Termination Competitions: some tools **disagreed** on YES / NO for termination
- **Step 1**: Require human-readable proof output. But: can be large!

Certification: Who Watches the Watchers?

- Termination and complexity analysis tools are large, e.g., AProVE has several 100,000s LOC – most likely with bugs!
- Observation in early Termination Competitions: some tools **disagreed** on YES / NO for termination
- **Step 1**: Require human-readable proof output. But: can be large!
- **Step 2**: Machine-readable XML proof output, can be certified independently by **trustworthy** tools based on Coq and Isabelle

Certification: Who Watches the Watchers?

- Termination and complexity analysis tools are large, e.g., AProVE has several 100,000s LOC – most likely with bugs!
- Observation in early Termination Competitions: some tools **disagreed** on YES / NO for termination
- **Step 1**: Require human-readable proof output. But: can be large!
- **Step 2**: Machine-readable XML proof output, can be certified independently by **trustworthy** tools based on Coq and Isabelle
- $\sim$ 2007/8: projects A3PAT[67], CoLoR[68], IsaFoR[69] formalise term rewriting, termination, proof techniques $\longrightarrow$ automatic proof checkers

---

[67] E. Contejean,P. Courtieu, J. Forest, O. Pons, X. Urbain: *Automated Certified Proofs with CiME3*, RTA '11

[68] F. Blanqui, A. Koprowski: *CoLoR: a Coq library on well-founded rewrite relations and its application to the automated verification of termination certificates*, MSCS '11

[69] R. Thiemann, C. Sternagel: *Certification of Termination Proofs using CeTA*, TPHOLs '09

Certification: Who Watches the Watchers?

- Termination and complexity analysis tools are large, e.g., AProVE has several 100,000s LOC – most likely with bugs!
- Observation in early Termination Competitions: some tools **disagreed** on YES / NO for termination
- **Step 1**: Require human-readable proof output. But: can be large!
- **Step 2**: Machine-readable XML proof output, can be certified independently by **trustworthy** tools based on Coq and Isabelle
- $\sim$ 2007/8: projects A3PAT[67], CoLoR[68], IsaFoR[69] formalise term rewriting, termination, proof techniques $\longrightarrow$ automatic proof checkers
- performance bottleneck: computations in theorem prover

---

[67] E. Contejean,P. Courtieu, J. Forest, O. Pons, X. Urbain: *Automated Certified Proofs with CiME3*, RTA '11

[68] F. Blanqui, A. Koprowski: *CoLoR: a Coq library on well-founded rewrite relations and its application to the automated verification of termination certificates*, MSCS '11

[69] R. Thiemann, C. Sternagel: *Certification of Termination Proofs using CeTA*, TPHOLs '09

Certification: Who Watches the Watchers?

- Termination and complexity analysis tools are large, e.g., AProVE has several 100,000s LOC – most likely with bugs!
- Observation in early Termination Competitions: some tools **disagreed** on YES / NO for termination
- **Step 1**: Require human-readable proof output. But: can be large!
- **Step 2**: Machine-readable XML proof output, can be certified independently by **trustworthy** tools based on Coq and Isabelle
- $\sim$ 2007/8: projects A3PAT[67], CoLoR[68], IsaFoR[69] formalise term rewriting, termination, proof techniques $\longrightarrow$ automatic proof checkers
- performance bottleneck: computations in theorem prover
- solution: extract source code (Haskell, OCaml, ...) for proof checker $\longrightarrow$ CeTA tool from IsaFoR

[67] E. Contejean, P. Courtieu, J. Forest, O. Pons, X. Urbain: *Automated Certified Proofs with CiME3*, RTA '11

[68] F. Blanqui, A. Koprowski: *CoLoR: a Coq library on well-founded rewrite relations and its application to the automated verification of termination certificates*, MSCS '11

[69] R. Thiemann, C. Sternagel: *Certification of Termination Proofs using CeTA*, TPHOLs '09

Proof Certification with CeTA

http://cl-informatik.uibk.ac.at/isafor/

CeTA can certify proofs for...

Proof Certification with CeTA

http://cl-informatik.uibk.ac.at/isafor/

CeTA can certify proofs for...

- termination of TRSs (several flavours), ITSs, and LLVM programs[70]

[70] M. Haslbeck, R. Thiemann: *An Isabelle/HOL formalization of AProVE's termination method for LLVM IR*, CPP '21

Proof Certification with CeTA

http://cl-informatik.uibk.ac.at/isafor/

CeTA can certify proofs for...

- termination of TRSs (several flavours), ITSs, and LLVM programs[70]
- non-termination for TRSs

[70] M. Haslbeck, R. Thiemann: *An Isabelle/HOL formalization of AProVE's termination method for LLVM IR*, CPP '21

Proof Certification with CeTA

http://cl-informatik.uibk.ac.at/isafor/

CeTA can certify proofs for...

- termination of TRSs (several flavours), ITSs, and LLVM programs[70]
- non-termination for TRSs
- upper bounds for complexity

[70] M. Haslbeck, R. Thiemann: *An Isabelle/HOL formalization of AProVE's termination method for LLVM IR*, CPP '21

Proof Certification with CeTA

http://cl-informatik.uibk.ac.at/isafor/

CeTA can certify proofs for...

- termination of TRSs (several flavours), ITSs, and LLVM programs[70]
- non-termination for TRSs
- upper bounds for complexity
- confluence and non-confluence proofs for TRSs

[70] M. Haslbeck, R. Thiemann: *An Isabelle/HOL formalization of AProVE's termination method for LLVM IR*, CPP '21

Proof Certification with CeTA

http://cl-informatik.uibk.ac.at/isafor/

CeTA can certify proofs for...

- termination of TRSs (several flavours), ITSs, and LLVM programs[70]
- non-termination for TRSs
- upper bounds for complexity
- confluence and non-confluence proofs for TRSs
- safety: invariants for ITSs[71]

[70] M. Haslbeck, R. Thiemann: *An Isabelle/HOL formalization of AProVE's termination method for LLVM IR*, CPP '21

[71] M. Brockschmidt, S. Joosten, R. Thiemann, A. Yamada: *Certifying Safety and Termination Proofs for Integer Transition Systems*, CADE '17

Proof Certification with CeTA

http://cl-informatik.uibk.ac.at/isafor/

CeTA can certify proofs for...

- termination of TRSs (several flavours), ITSs, and LLVM programs[70]
- non-termination for TRSs
- upper bounds for complexity
- confluence and non-confluence proofs for TRSs
- safety: invariants for ITSs[71]

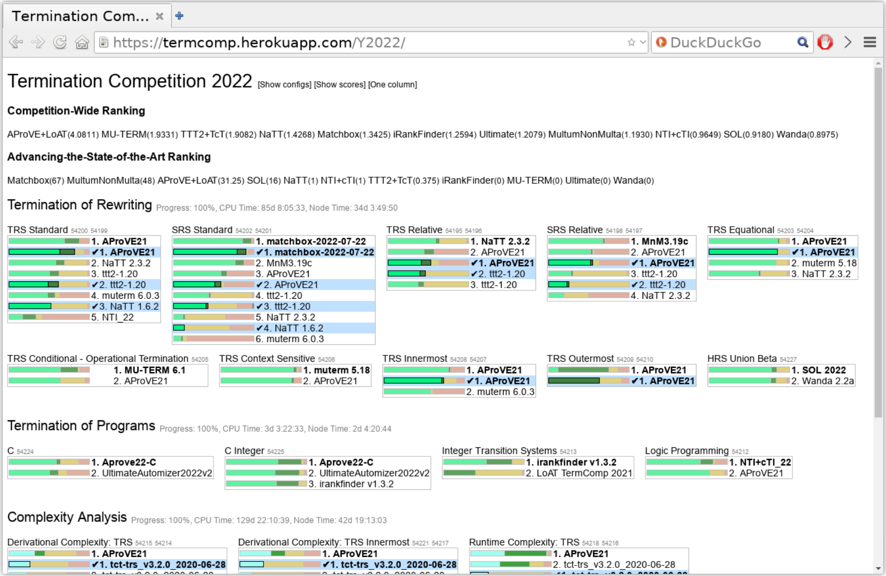
If certification unsuccessful:
CeTA indicates **which part** of the proof it could not follow

---

[70] M. Haslbeck, R. Thiemann: *An Isabelle/HOL formalization of AProVE's termination method for LLVM IR*, CPP '21

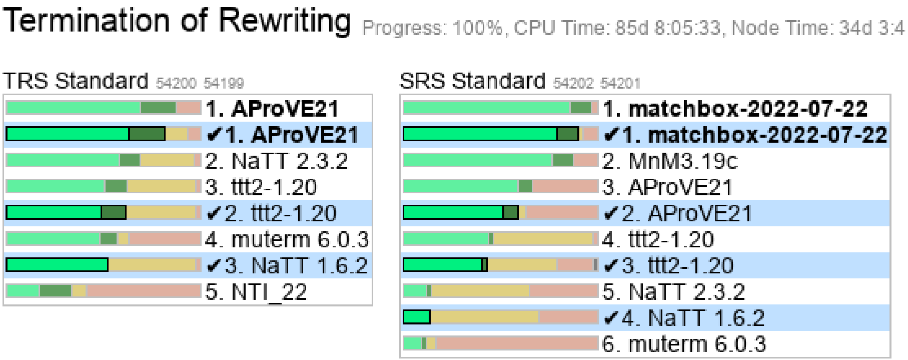
[71] M. Brockschmidt, S. Joosten, R. Thiemann, A. Yamada: *Certifying Safety and Termination Proofs for Integer Transition Systems*, CADE '17

termCOMP with Certification (✓) (1/2)



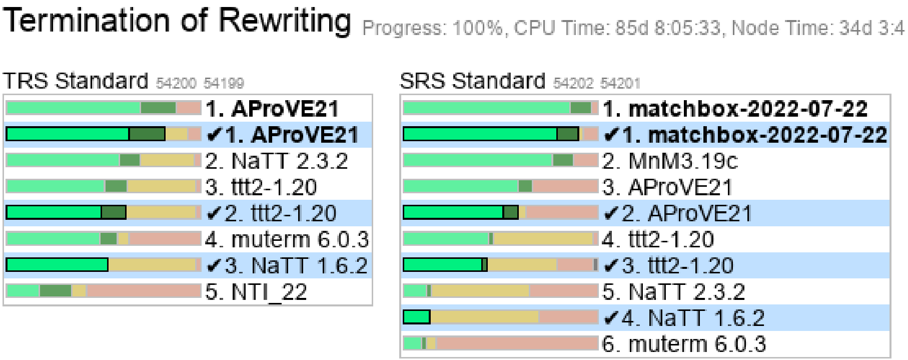
termCOMP with Certification (✓) (2/2)

Let's zoom in ...



termCOMP with Certification (✓) (2/2)

Let's zoom in ...



⇒ proof certification is competitive!

Termination and Complexity: Conclusion

- Termination and complexity analysis: active fields of research

Termination and Complexity: Conclusion

- Termination and complexity analysis: active fields of research
- Push-button tools to prove (non-)termination and to infer upper and lower complexity bounds available

Termination and Complexity: Conclusion

- Termination and complexity analysis: active fields of research
- Push-button tools to prove (non-)termination and to infer upper and lower complexity bounds available
- Cross-fertilisation between techniques for different formalisms (integer transition systems, functional programs, ...)

Termination and Complexity: Conclusion

- Termination and complexity analysis: active fields of research
- Push-button tools to prove (non-)termination and to infer upper and lower complexity bounds available
- Cross-fertilisation between techniques for different formalisms (integer transition systems, functional programs, . . .)
- Certification helps raise trust in automatically found proofs of (non-)termination and complexity bounds

Termination and Complexity: Conclusion

- Termination and complexity analysis: active fields of research
- Push-button tools to prove (non-)termination and to infer upper and lower complexity bounds available
- Cross-fertilisation between techniques for different formalisms (integer transition systems, functional programs, . . .)
- Certification helps raise trust in automatically found proofs of (non-)termination and complexity bounds

Thanks a lot for your attention!

References I

E. Albert, P. Arenas, S. Genaim, G. Puebla, and D. Zanardini. Cost analysis of object-oriented bytecode programs. *Theoretical Computer Science*, 413(1):142–159, 2012.

C. Alias, A. Darte, P. Feautrier, and L. Gonnord. Multi-dimensional rankings, program termination, and complexity bounds of flowchart programs. In *SAS '10*, pages 117–133, 2010.

T. Arts and J. Giesl. Termination of term rewriting using dependency pairs. *Theoretical Computer Science*, 236(1-2):133–178, 2000.

M. Avanzini and G. Moser. Dependency pairs and polynomial path orders. In *RTA '09*, pages 48–62, 2009.

M. Avanzini and G. Moser. A combination framework for complexity. *Information and Computation*, 248:22–55, 2016.

References II

- M. Avanzini, G. Moser, and M. Schaper. TcT: Tyrolean Complexity Tool. In *TACAS '16*, pages 407–423, 2016.
- M. Avanzini, U. Dal Lago, and A. Yamada. On probabilistic term rewriting. *Science of Computer Programming*, 185, 2020.
- T. Baudon, C. Fuhs, and L. Gonnord. Analysing parallel complexity of term rewriting. In *LOPSTR '22*, 2022. To appear.
- J. Berdine, B. Cook, D. Distefano, and P. W. O'Hearn. Automatic termination proofs for programs with shape-shifting heaps. In *CAV '06*, pages 386–400, 2006.
- R. Blanc, T. A. Henzinger, T. Hottelier, and L. Kovács. ABC: algebraic bound computation for loops. In *LPAR (Dakar) '10*, pages 103–118, 2010.

References III

- F. Blanqui and A. Koprowski. CoLoR: a Coq library on well-founded rewrite relations and its application to the automated verification of termination certificates. *Mathematical Structures in Computer Science*, 21(4):827–859, 2011.
- G. Bonfante, A. Cichon, J. Marion, and H. Touzet. Algorithms with polynomial interpretation termination proof. *Journal of Functional Programming*, 11(1):33–53, 2001.
- C. Borralleras, S. Lucas, A. Oliveras, E. Rodríguez-Carbonell, and A. Rubio. SAT modulo linear arithmetic for solving polynomial constraints. *Journal of Automated Reasoning*, 48(1):107–131, 2012.
- M. Brockschmidt, C. Otto, and J. Giesl. Modular termination proofs of recursive Java Bytecode programs by term rewriting. In *RTA '11*, pages 155–170, 2011.

References IV

- M. Brockschmidt, R. Musiol, C. Otto, and J. Giesl. Automated termination proofs for Java programs with cyclic data. In *CAV '12*, pages 105–122, 2012a.
- M. Brockschmidt, T. Ströder, C. Otto, and J. Giesl. Automated detection of non-termination and `NullPointerExceptions` for Java Bytecode. In *FoVeOOS '11*, pages 123–141, 2012b.
- M. Brockschmidt, B. Cook, and C. Fuhs. Better termination proving through cooperation. In *CAV '13*, pages 413–429, 2013.
- M. Brockschmidt, B. Cook, S. Ishtiaq, H. Khlaaf, and N. Piterman. T2: temporal property verification. In *TACAS '16*, pages 387–393, 2016a.
- M. Brockschmidt, F. Emmes, S. Falke, C. Fuhs, and J. Giesl. Analyzing runtime and size complexity of integer programs. *ACM Transactions on Programming Languages and Systems*, 38(4), 2016b.

- M. Brockschmidt, S. J. C. Joosten, R. Thiemann, and A. Yamada. Certifying safety and termination proofs for integer transition systems. In *CADE '17*, pages 454–471, 2017.
- H.-Y. Chen, B. Cook, C. Fuhs, K. Nimkar, and P. W. O'Hearn. Proving nontermination via safety. In *TACAS '14*, pages 156–171, 2014.
- M. Codish, J. Giesl, P. Schneider-Kamp, and R. Thiemann. SAT solving for termination proofs with recursive path orders and dependency pairs. *Journal of Automated Reasoning*, 49(1):53–93, 2012.
- E. Contejean, P. Courtieu, J. Forest, O. Pons, and X. Urbain. Automated certified proofs with CiME3. In *RTA '11*, pages 21–30, 2011.
- B. Cook, A. Podelski, and A. Rybalchenko. Terminator: Beyond safety. In *CAV '06*, pages 415–418, 2006a.

- B. Cook, A. Podelski, and A. Rybalchenko. Termination proofs for systems code. In *PLDI '06*, pages 415–426, 2006b.
- B. Cook, A. Podelski, and A. Rybalchenko. Proving thread termination. In *PLDI '07*, pages 320–330, 2007.
- B. Cook, C. Fuhs, K. Nimkar, and P. W. O'Hearn. Disproving termination with overapproximation. In *FMCAD '14*, pages 67–74, 2014.
- B. Cook, H. Khlaaf, and N. Piterman. Verifying increasingly expressive temporal logics for infinite-state systems. *Journal of the ACM*, 64(2): 15:1–15:39, 2017.
- P. Cousot and R. Cousot. Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *POPL '77*, pages 238–252, 1977.

References VII

N. Dershowitz. Orderings for term-rewriting systems. *Theoretical Computer Science*, 17(3):279–301, 1982.

N. Dershowitz and Z. Manna. Proving termination with multiset orderings. *Communications of the ACM*, 22(8):465–476, 1979.

F. Emmes, T. Enger, and J. Giesl. Proving non-looping non-termination automatically. In *IJCAR '12*, pages 225–240, 2012.

J. Endrullis, J. Waldmann, and H. Zantema. Matrix interpretations for proving termination of term rewriting. *Journal of Automated Reasoning*, 40(2–3):195–220, 2008.

S. Falke and D. Kapur. A term rewriting approach to the automated termination analysis of imperative programs. In *CADE '09*, pages 277–293, 2009.

- A. Flores-Montoya and R. Hähnle. Resource analysis of complex programs with cost equations. In *APLAS '14*, pages 275–295, 2014.
- F. Frohn and J. Giesl. Analyzing runtime complexity via innermost runtime complexity. In *Proc. LPAR '17*, pages 249–268, 2017a.
- F. Frohn and J. Giesl. Complexity analysis for Java with AProVE. In *iFM '17*, pages 85–101, 2017b.
- F. Frohn and J. Giesl. Proving non-termination and lower runtime bounds with loat (system description). In *IJCAR '22*, pages 712–722, 2022.
- F. Frohn, J. Giesl, J. Hensel, C. Aschermann, and T. Ströder. Lower bounds for runtime complexity of term rewriting. *Journal of Automated Reasoning*, 59(1):121–163, 2017.

- F. Frohn, M. Naaf, M. Brockschmidt, and J. Giesl. Inferring lower runtime bounds for integer programs. *ACM Transactions on Programming Languages and Systems*, 42(3):13:1–13:50, 2020.
- C. Fuhs. Transforming derivational complexity of term rewriting to runtime complexity. In *FroCoS '19*, pages 348–364, 2019.
- C. Fuhs, J. Giesl, A. Middeldorp, P. Schneider-Kamp, R. Thiemann, and H. Zankl. SAT solving for termination analysis with polynomial interpretations. In *SAT '07*, pages 340–354, 2007.
- C. Fuhs, J. Giesl, A. Middeldorp, P. Schneider-Kamp, R. Thiemann, and H. Zankl. Maximal termination. In *RTA '08*, pages 110–125, 2008a.
- C. Fuhs, R. Navarro-Marset, C. Otto, J. Giesl, S. Lucas, and P. Schneider-Kamp. Search techniques for rational polynomial orders. In *AISC '08*, pages 109–124, 2008b.

- C. Fuhs, J. Giesl, M. Plücker, P. Schneider-Kamp, and S. Falke. Proving termination of integer term rewriting. In *RTA '09*, pages 32–47, 2009.
- A. Geser, D. Hofbauer, and J. Waldmann. Match-bounded string rewriting systems. *Applicable Algebra in Engineering, Communication and Computing*, 15(3–4):149–171, 2004.
- J. Giesl, R. Thiemann, and P. Schneider-Kamp. Proving and disproving termination of higher-order functions. In *FroCoS '05*, pages 216–231, 2005.
- J. Giesl, R. Thiemann, P. Schneider-Kamp, and S. Falke. Mechanizing and improving dependency pairs. *Journal of Automated Reasoning*, 37 (3):155–203, 2006.

- J. Giesl, M. Raffelsieper, P. Schneider-Kamp, S. Swiderski, and R. Thiemann. Automated termination proofs for Haskell by term rewriting. *ACM Transactions on Programming Languages and Systems*, 33(2):1–39, 2011. See also http://aprove.informatik.rwth-aachen.de/eval/Haskell/.
- J. Giesl, T. Ströder, P. Schneider-Kamp, F. Emmes, and C. Fuhs. Symbolic evaluation graphs and term rewriting: A general methodology for analyzing logic programs. In *PPDP '12*, pages 1–12, 2012.
- J. Giesl, C. Aschermann, M. Brockschmidt, F. Emmes, F. Frohn, C. Fuhs, J. Hensel, C. Otto, M. Plücker, P. Schneider-Kamp, T. Ströder, S. Swiderski, and R. Thiemann. Analyzing program termination and complexity automatically with AProVE. *Journal of Automated Reasoning*, 58(1):3–31, 2017.

References XII

- S. Gulwani, K. K. Mehra, and T. M. Chilimbi. SPEED: precise and efficient static estimation of program computational complexity. In *POPL '09*, pages 127–139, 2009.
- A. Gupta, T. A. Henzinger, R. Majumdar, A. Rybalchenko, and R.-G. Xu. Proving non-termination. In *POPL '08*, pages 147–158, 2008.
- M. W. Haslbeck and R. Thiemann. An isabelle/hol formalization of aprove's termination method for LLVM IR. In *CPP '21*, pages 238–249, 2021.
- J. Hensel, J. Giesl, F. Frohn, and T. Ströder. Termination and complexity analysis for programs with bitvector arithmetic by symbolic execution. *Journal of Logical and Algebraic Methods in Programming*, 97:105–130, 2018.

- J. Hensel, C. Mensendiek, and J. Giesl. AProVE: Non-termination witnesses for C programs - (competition contribution). In *TACAS '22, Part II*, pages 403–407, 2022.
- N. Hirokawa and A. Middeldorp. Tyrolean Termination Tool: Techniques and features. *Information and Computation*, 205(4): 474–511, 2007.
- N. Hirokawa and G. Moser. Automated complexity analysis based on the dependency pair method. In *IJCAR '08*, pages 364–379, 2008.
- N. Hirokawa and G. Moser. Automated complexity analysis based on context-sensitive rewriting. In *RTA-TLCA '14*, pages 257–271, 2014.
- D. Hofbauer and C. Lautemann. Termination proofs and the length of derivations. In *RTA '89*, pages 167–177, 1989.

- J. Hoffmann and S. Jost. Two decades of automatic amortized resource analysis. *Mathematical Structures in Computer Science*, pages 1–31, 2022.
- J. Hoffmann and Z. Shao. Type-based amortized resource analysis with integers and arrays. *Journal of Functional Programming*, 25, 2015.
- J. Hoffmann, K. Aehlig, and M. Hofmann. Resource aware ML. In *CAV '12*, pages 781–786, 2012.
- H. Hong and D. Jakuš. Testing positiveness of polynomials. *Journal of Automated Reasoning*, 21(1):23–38, 1998.
- I. S. Hristakiev. *Confluence Analysis for a Graph Programming Language*. PhD thesis, University of York, 2009.

References XV

S. Kamin and J.-J. Lévy. Two generalizations of the recursive path ordering. Unpublished Manuscript, University of Illinois, Urbana, IL, USA, 1980.

D. E. Knuth and P. B. Bendix. Simple word problems in universal algebras. *Computational Problems in Abstract Algebra*, pages 263–297, 1970.

C. Kop. *Higher Order Termination*. PhD thesis, VU Amsterdam, 2012.

C. Kop and N. Nishida. Term rewriting with logical constraints. In *FroCoS '13*, pages 343–358, 2013.

C. Kop and D. Vale. Tuple interpretations for higher-order complexity. In *FSCD '21*, pages 31:1–31:22, 2021.

A. Koprowski and J. Waldmann. Max/plus tree automata for termination of term rewriting. *Acta Cybernetica*, 19(2):357–392, 2009.

- K. Korovin and A. Voronkov. Orienting rewrite rules with the Knuth-Bendix order. *Information and Computation*, 183(2):165–186, 2003.
- M. Korp, C. Sternagel, H. Zankl, and A. Middeldorp. Tyrolean Termination Tool 2. In *RTA '09*, pages 295–304, 2009.
- D. S. Lankford. Canonical algebraic simplification in computational logic. Technical Report ATP-25, University of Texas, 1975.
- D. Larraz, A. Oliveras, E. Rodríguez-Carbonell, and A. Rubio. Proving termination of imperative programs using Max-SMT. In *FMCAD '13*, pages 218–225, 2013.
- L. Leutgeb, G. Moser, and F. Zuleger. Automated expected amortised cost analysis of probabilistic data structures. In *CAV '22, Part II*, pages 70–91, 2022.

- N. Lommen, F. Meyer, and J. Giesl. Automatic complexity analysis of integer programs via triangular weakly non-linear loops. In *IJCAR '22*, pages 734–754, 2022.
- S. Lucas. Polynomials over the reals in proofs of termination: from theory to practice. *RAIRO - Theoretical Informatics and Applications*, 39(3):547–586, 2005.
- S. Lucas. Context-sensitive rewriting. *ACM Computing Surveys*, 53(4): 78:1–78:36, 2020.
- J. McCarthy. Recursive functions of symbolic expressions and their computation by machine, part I. *Communications of the ACM*, 3(4): 184–195, 1960.
- A. Merayo Corcoba. *Resource analysis of integer and abstract programs*. PhD thesis, Universidad Complutense de Madrid, 2022.

- F. Meyer, M. Hark, and J. Giesl. Inferring expected runtimes of probabilistic integer programs using expected sizes. In *TACAS '21, Part I*, pages 250–269, 2021.
- G. Moser and M. Schaper. From Jinja bytecode to term rewriting: A complexity reflecting transformation. *Information and Computation*, 261:116–143, 2018.
- G. Moser and A. Schnabl. The derivational complexity induced by the dependency pair method. *Logical Methods in Computer Science*, 7(3), 2011a.
- G. Moser and A. Schnabl. Termination proofs in the dependency pair framework may induce multiple recursive derivational complexity. In *RTA '11*, pages 235–250, 2011b.

References XIX

- G. Moser and M. Schneckenreither. Automated amortised resource analysis for term rewrite systems. *Science of Computer Programming*, 185, 2020.
- G. Moser, A. Schnabl, and J. Waldmann. Complexity analysis of term rewriting based on matrix and context dependent interpretations. In *FSTTCS '08*, pages 304–315, 2008.
- M. Naaf, F. Frohn, M. Brockschmidt, C. Fuhs, and J. Giesl. Complexity analysis for term rewriting by integer transition systems. In *FroCoS '17*, pages 132–150, 2017.
- F. Neurauter, H. Zankl, and A. Middeldorp. Revisiting matrix interpretations for polynomial derivational complexity of term rewriting. In *LPAR (Yogyakarta) '10*, pages 550–564, 2010.

References XX

- L. Noschinski, F. Emmes, and J. Giesl. Analyzing innermost runtime complexity of term rewriting by dependency pairs. *Journal of Automated Reasoning*, 51(1):27–56, 2013.
- P. W. O'Hearn, J. C. Reynolds, and H. Yang. Local reasoning about programs that alter data structures. In *CSL '01*, pages 1–19, 2001.
- C. Otto, M. Brockschmidt, C. v. Essen, and J. Giesl. Automated termination analysis of Java Bytecode by term rewriting. In *RTA '10*, pages 259–276, 2010.
- É. Payet. Loop detection in term rewriting using the eliminating unfoldings. *Theoretical Computer Science*, 403(2-3), 2008.
- A. Podelski and A. Rybalchenko. A complete method for the synthesis of linear ranking functions. In *VMCAI '04*, pages 239–251, 2004.

- A. Schnabl and J. G. Simonsen. The exact hardness of deciding derivational and runtime complexity. In *CSL '11*, pages 481–495, 2011.
- P. Schneider-Kamp, J. Giesl, A. Serebrenik, and R. Thiemann. Automated termination proofs for logic programs by term rewriting. *ACM Transactions on Computational Logic*, 11(1):1–52, 2009.
- M. Sinn, F. Zuleger, and H. Veith. A simple and scalable static analysis for bound analysis and amortized complexity analysis. In *CAV '14*, pages 745–761, 2014.
- T. Ströder, F. Emmes, P. Schneider-Kamp, J. Giesl, and C. Fuhs. A linear operational semantics for termination and complexity analysis of ISO Prolog. In *LOPSTR '11*, pages 237–252, 2012.

- T. Ströder, J. Giesl, M. Brockschmidt, F. Frohn, C. Fuhs, J. Hensel, P. Schneider-Kamp, and C. Aschermann. Automatically proving termination and memory safety for programs with pointer arithmetic. *Journal of Automated Reasoning*, 58(1):33–65, 2017.
- A. Stump, G. Sutcliffe, and C. Tinelli. Starexec: A cross-community infrastructure for logic solving. In *IJCAR '14*, pages 367–373, 2014. https://www.starexec.org/.
- R. Thiemann and C. Sternagel. Certification of termination proofs using CeTA. In *TPHOLs '09*, pages 452–468, 2009.
- A. M. Turing. On computable numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, 42(2):230–265, 1936.
- A. M. Turing. Checking a large routine. In *Report of a Conference on High Speed Automatic Calculating Machines*, pages 67–69, 1949.

- F. van Raamsdonk. Translating logic programs into conditional rewriting systems. In *ICLP '97*, pages 168–182, 1997.
- P. Wang, H. Fu, A. K. Goharshady, K. Chatterjee, X. Qin, and W. Shi. Cost analysis of nondeterministic probabilistic programs. In *PLDI '19*, pages 204–220, 2019.
- A. Weiermann. Termination proofs for term rewriting systems by lexicographic path orderings imply multiply recursive derivation lengths. *Theoretical Computer Science*, 139(1&2):355–362, 1995.
- S. Winkler and G. Moser. Runtime complexity analysis of logically constrained rewriting. In *LOPSTR '20*, pages 37–55, 2020.
- A. Yamada. Tuple interpretations for termination of term rewriting. *Journal of Automated Reasoning*, 2022. To appear. Online at `https://doi.org/10.1007/s10817-022-09640-4`.

References XXIV

- A. Yamada, K. Kusakari, and T. Sakabe. A unified ordering for termination proving. *Science of Computer Programming*, 111:110–134, 2015.
- H. Zankl and A. Middeldorp. Satisfiability of non-linear (ir)rational arithmetic. In *LPAR (Dakar) '10*, pages 481–500, 2010.
- H. Zankl, N. Hirokawa, and A. Middeldorp. KBO orientability. *Journal of Automated Reasoning*, 43(2):173–201, 2009.
- H. Zankl, C. Sternagel, D. Hofbauer, and A. Middeldorp. Finding and certifying loops. In *SOFSEM '10*, pages 755–766, 2010.
- J. Zhao, S. Nagarakatte, M. M. K. Martin, and S. Zdancewic. Formalizing the LLVM intermediate representation for verified program transformations. In *POPL '12*, pages 427–440, 2012.