Certification of Termination Proofs for Term Rewriting

A short story of a long battle...

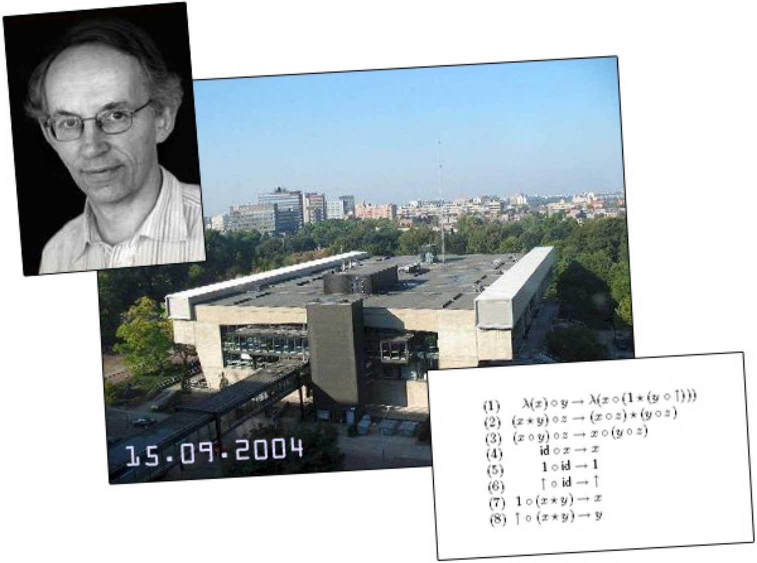
Adam Koprowski

Radboud University Nijmegen
Foundations group, Intelligent Systems, ICIS

16 December 2008

Who am I?

Who am I?



$$
\begin{array}{ll}
(1) & \lambda(x) \circ y \to \lambda(x \circ (1 \star (y \circ \uparrow))) \\
(2) & (x \star y) \circ z \to (x \circ z) \star (y \circ z) \\
(3) & (x \circ y) \circ z \to x \circ (y \circ z) \\
(4) & \mathsf{id} \circ x \to x \\
(5) & 1 \circ \mathsf{id} \to 1 \\
(6) & \uparrow \circ\, \mathsf{id} \to \uparrow \\
(7) & 1 \circ (x \star y) \to x \\
(8) & \uparrow \circ\, (x \star y) \to y
\end{array}
$$

Who am I?

Adam Koprowski
Termination of Rewriting and Its Certification

Who am I?

Who am I?

Heat
$\dot{T} = 2$
$\dot{t} = 1$
$T \leq 10 \land t \leq 3$
$T \geq 9$
$t \geq 2 \to$
$t := 0$
$t \geq 0.5 \to$
$t := 0$
$T \leq 6 \to$
$t := 0$
Cool
$\dot{T} = -T$
$\dot{t} = 1$
$T \geq 5$
Check
$\dot{T} = -T/2$
$\dot{t} = 1$
$t \leq 1$
HUYGENSGEBOUW
01.12.2008

Outline

1. Background: termination of term rewriting

2. CoLoR project: certification of termination proofs
   - Why?... motivation
   - How?... CoLoR's approach to certification
   - When?... history of the project
   - What?... overview of the content
   - Related work
   - Certified competition

3. Conclusions... sort of

Outline

1. Background: termination of term rewriting

2. CoLoR project: certification of termination proofs
   - Why?... motivation
   - How?... CoLoR's approach to certification
   - When?... history of the project
   - What?... overview of the content
   - Related work
   - Certified competition

3. Conclusions... sort of

Introduction to term rewriting

Example (Quick sort)

$$\begin{aligned}
\mathsf{qsort}(\mathsf{nil}) &\rightarrow \mathsf{nil}\\
\mathsf{qsort}(x :: xs) &\rightarrow \mathsf{append}(\mathsf{qsort}(\mathsf{filterLe}(x, xs)), x :: \mathsf{qsort}(\mathsf{filterGe}(x, xs)))
\end{aligned}$$

$$\begin{aligned}
\mathsf{append}(\mathsf{nil}, l) &\rightarrow l\\
\mathsf{append}(x :: xs, l) &\rightarrow x :: \mathsf{append}(xs, l)
\end{aligned}$$

$$\begin{aligned}
\mathsf{filterLe}(n, \mathsf{nil}) &\rightarrow \mathsf{nil}\\
\mathsf{filterLe}(n, x :: xs) &\rightarrow \mathsf{filter}(\mathsf{le}(x, n), x, \mathsf{filterLe}(n, xs))
\end{aligned}$$

$$\begin{aligned}
\mathsf{filterGe}(n, \mathsf{nil}) &\rightarrow \mathsf{nil}\\
\mathsf{filterGe}(n, x :: xs) &\rightarrow \mathsf{filter}(\mathsf{ge}(x, n), x, \mathsf{filterGe}(n, xs))
\end{aligned}$$

$$\begin{aligned}
\mathsf{filter}(\mathsf{false}, x, xs) &\rightarrow xs\\
\mathsf{filter}(\mathsf{true}, x, xs) &\rightarrow x :: xs
\end{aligned}$$

$$\begin{aligned}
\mathsf{ge}(x, y) &\rightarrow \mathsf{le}(y, x)\\
\mathsf{le}(0, y) &\rightarrow \mathsf{true}\\
\mathsf{le}(\mathsf{s}(x), 0) &\rightarrow \mathsf{false}\\
\mathsf{le}(\mathsf{s}(x), \mathsf{s}(y)) &\rightarrow \mathsf{le}(x, y)
\end{aligned}$$

Introduction to term rewriting

Example (Quick sort)

$$\begin{aligned}
\mathrm{qsort}(\mathrm{nil}) &\to \mathrm{nil} \\
\mathrm{qsort}(x :: xs) &\to \mathrm{append}(\mathrm{qsort}(\mathrm{filterLe}(x, xs)), x :: \mathrm{qsort}(\mathrm{filterGe}(x, xs)))
\end{aligned}$$

$$\mathrm{append}(\mathrm{nil}, l) \to l$$

$$\mathrm{ge}(x, y) \to \mathrm{le}(y, x)$$

$$\begin{aligned}
\mathrm{filter}(\mathrm{false}, x, xs) &\to xs & \mathrm{le}(0, y) &\to \mathrm{true} \\
\mathrm{filter}(\mathrm{true}, x, xs) &\to x :: xs & \mathrm{le}(\mathrm{s}(x), 0) &\to \mathrm{false} \\
& & \mathrm{le}(\mathrm{s}(x), \mathrm{s}(y)) &\to \mathrm{le}(x, y)
\end{aligned}$$

Example (Collatz conjecture)

$$\begin{aligned}
\mathrm{collatz}(\mathrm{s}(\mathrm{s}(x))) &\to \mathrm{f}(\mathrm{even}(x), \mathrm{s}(\mathrm{s}(x))) & \mathrm{even}(0) &\to \mathrm{true} \\
\mathrm{f}(\mathit{true}, x) &\to \mathrm{collatz}(\mathrm{half}(x)) & \mathrm{even}(\mathrm{s}(0)) &\to \mathrm{false} \\
\mathrm{f}(\mathit{false}, x) &\to \mathrm{collatz}(\mathrm{s}(\mathrm{triple}(x))) & \mathrm{even}(\mathrm{s}(\mathrm{s}(x))) &\to \mathrm{even}(x)
\end{aligned}$$

$$\begin{aligned}
\mathrm{half}(0) &\to 0 & \mathrm{triple}(0) &\to 0 \\
\mathrm{half}(\mathrm{s}(\mathrm{s}(x))) &\to \mathrm{s}(\mathrm{half}(x)) & \mathrm{triple}(\mathrm{s}(x)) &\to \mathrm{s}(\mathrm{s}(\mathrm{s}(\mathrm{triple}(x))))
\end{aligned}$$

Introduction to term rewriting

Example (Quick sort)

$$\mathsf{qsort}(\mathsf{nil}) \to \mathsf{nil}$$

$$\mathsf{qsort}(x :: xs) \to \mathsf{append}(\mathsf{qsort}(\mathsf{filterLe}(x, xs)), x :: \mathsf{qsort}(\mathsf{filterGe}(x, xs)))$$

$$\mathsf{append}(\mathsf{nil}, l) \to l$$

Example (Collatz conjecture)

$\mathsf{collatz}(\mathsf{s}(\mathsf{s}(x))) \to \mathsf{f}(\mathsf{even}(x), \mathsf{s}(\mathsf{s}(x)))$ $\qquad$ $\mathsf{even}(0) \to \mathsf{true}$

$\mathsf{f}(\mathit{tru}$

$\mathsf{f}(\mathit{fals}$

Definition

A TRS is terminating iff it does not admit infinite reductions.

$\mathsf{half}(0) \to 0$ $\qquad$ $\mathsf{triple}(0) \to 0$

$\mathsf{half}(\mathsf{s}(\mathsf{s}(x))) \to \mathsf{s}(\mathsf{half}(x))$ $\qquad$ $\mathsf{triple}(\mathsf{s}(x)) \to \mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{triple}(x))))$

$\mathsf{ge}(x, y) \to \mathsf{le}(y, x)$

$\mathsf{filter}(\mathsf{false}, x, xs) \to xs$ $\qquad$ $\mathsf{le}(0, y) \to \mathsf{true}$

$\mathsf{filter}(\mathsf{true}, x, xs) \to x :: xs$ $\qquad$ $\mathsf{le}(\mathsf{s}(x), 0) \to \mathsf{false}$

$\mathsf{le}(\mathsf{s}(x), \mathsf{s}(y)) \to \mathsf{le}(x, y)$

Termination of rewriting

Termination of rewriting:

- Is undecidable.
- Is an important topic in term rewriting.
- Many methods exist and new ones are constantly being developed.
- Recently the emphasis is on automation.
- There exists a number of tools for proving termination.
- Stimulated by the termination competition.
- Tools (and proofs that they produce) are getting more and more complex, so reliability is an issue (tools disqualifications in the competition).
- In 2007 a new category of certified termination introduced in the competition.

Termination of rewriting

Termination of rewriting:

- Is undecidable.
- Is an important topic in term rewriting.
- Many methods exist and new ones are constantly being developed.
- Recently the emphasis is on automation.
- There exists a number of tools for proving termination.
- Stimulated by the termination competition.
- Tools (and proofs that they produce) are getting more and more complex, so reliability is an issue (tools disqualifications in the competition).
- In 2007 a new category of certified termination introduced in the competition.

Termination of rewriting

Termination of rewriting:

- Is undecidable.
- Is an important topic in term rewriting.
- Many methods exist and new ones are constantly being developed.
- Recently the emphasis is on automation.
- There exists a number of tools for proving termination.
- Stimulated by the termination competition.
- Tools (and proofs that they produce) are getting more and more complex, so reliability is an issue (tools disqualifications in the competition).
- In 2007 a new category of certified termination introduced in the competition.

Termination of rewriting

Termination of rewriting:

- Is undecidable.
- Is an important topic in term rewriting.
- Many methods exist and new ones are constantly being developed.
- Recently the emphasis is on automation.
- There exists a number of tools for proving termination.
- Stimulated by the termination competition.
- Tools (and proofs that they produce) are getting more and more complex, so reliability is an issue (tools disqualifications in the competition).
- In 2007 a new category of certified termination introduced in the competition.

Termination of rewriting

Termination of rewriting:

- Is undecidable.
- Is an important topic in term rewriting.
- Many methods exist and new ones are constantly being developed.
- Recently the emphasis is on automation.
- There exists a number of tools for proving termination.
- Stimulated by the termination competition.
- Tools (and proofs that they produce) are getting more and more complex, so reliability is an issue (tools disqualifications in the competition).
- In 2007 a new category of certified termination introduced in the competition.

Termination of rewriting

Termination of rewriting:

- Is undecidable.
- Is an important topic in term rewriting.
- Many methods exist and new ones are constantly being developed.
- Recently the emphasis is on automation.
- There exists a number of tools for proving termination.
- Stimulated by the termination competition.
- Tools (and proofs that they produce) are getting more and more complex, so reliability is an issue (tools disqualifications in the competition).
- In 2007 a new category of certified termination introduced in the competition.

Termination of rewriting

Termination of rewriting:

- Is undecidable.
- Is an important topic in term rewriting.
- Many methods exist and new ones are constantly being developed.
- Recently the emphasis is on automation.
- There exists a number of tools for proving termination.
- Stimulated by the termination competition.
- Tools (and proofs that they produce) are getting more and more complex, so reliability is an issue (tools disqualifications in the competition).
- In 2007 a new category of certified termination introduced in the competition.

Termination of rewriting

Termination of rewriting:

- Is undecidable.
- Is an important topic in term rewriting.
- Many methods exist and new ones are constantly being developed.
- Recently the emphasis is on automation.
- There exists a number of tools for proving termination.
- Stimulated by the termination competition.
- Tools (and proofs that they produce) are getting more and more complex, so reliability is an issue (tools disqualifications in the competition).
- In 2007 a new category of certified termination introduced in the competition.

Outline

1. Background: termination of term rewriting

2. CoLoR project: certification of termination proofs
   - Why?... motivation
   - How?... CoLoR's approach to certification
   - When?... history of the project
   - What?... overview of the content
   - Related work
   - Certified competition

3. Conclusions... sort of

Motivation

CoLoR

http://color.loria.fr

CoLoR: Coq Library on Rewriting and Termination.
Goal: certification of termination proofs produced by various termination provers.

- Increasing reliability of termination provers.
- Common proof format for termination provers:
  - common tools (proof presentation, manipulation, . . .),
  - control language for provers (integration of tools)
- Extension of proof assistance kernels.

Motivation

CoLoR

`http://color.loria.fr`

CoLoR: Coq Library on Rewriting and Termination.
Goal: certification of termination proofs produced by various termination provers.

- Increasing reliability of termination provers.
- Common proof format for termination provers:
  - common tools (proof presentation, manipulation, . . .),
  - control language for provers (integration of tools).
- Extension of proof assistance kernels.

Motivation

CoLoR

http://color.loria.fr

CoLoR: Coq Library on Rewriting and Termination.
Goal: certification of termination proofs produced by various termination provers.

- Increasing reliability of termination provers.
- Common proof format for termination provers:
  - common tools (proof presentation, manipulation, . . .),
  - control language for provers (integration of tools)
- Extension of proof assistance kernels.

Motivation

CoLoR

http://color.loria.fr

CoLoR: Coq Library on Rewriting and Termination.
Goal: certification of termination proofs produced by various termination provers.

- Increasing reliability of termination provers.
- Common proof format for termination provers:
  - common tools (proof presentation, manipulation, . . .),
  - control language for provers (integration of tools)
- Extension of proof assistance kernels.

Motivation

CoLoR

http://color.loria.fr

CoLoR: Coq Library on Rewriting and Termination.
Goal: certification of termination proofs produced by various termination provers.

- Increasing reliability of termination provers.
- Common proof format for termination provers:
  - common tools (proof presentation, manipulation, . . .),
  - control language for provers (integration of tools)
- Extension of proof assistance kernels.

Motivation

CoLoR

http://color.loria.fr

CoLoR: Coq Library on Rewriting and Termination.
Goal: certification of termination proofs produced by various termination provers.

- Increasing reliability of termination provers.
- Common proof format for termination provers:
  - common tools (proof presentation, manipulation, ...),
  - control language for provers (integration of tools)
- Extension of proof assistance kernels.

CoLoR's approach to certification

How to certify termination results?

- Possibility: certification of tools source code.
  ⇒ difficult, tool dependent, extra work with every change, . . .
- CoLoR's approach:
  - TPG: common format for termination proofs.
  - Tools output proofs in TPG format.
  - CoLoR: a Coq library of results on termination.
  - Rainbow: a tool for translation from proofs in TPG format to Coq proofs, using results from CoLoR.

CoLoR's approach to certification

How to certify termination results?

- Possibility: certification of tools source code.
  ⇒ difficult, tool dependent, extra work with every change, . . .
- CoLoR's approach:
  - TPG: common format for termination proofs.
  - Tools output proofs in TPG format.
  - CoLoR: a Coq library of results on termination.
  - Rainbow: a tool for translation from proofs in TPG format to Coq proofs, using results from CoLoR.

CoLoR's approach to certification

How to certify termination results?

- Possibility: certification of tools source code.
  ⇒ difficult, tool dependent, extra work with every change, ...
- CoLoR's approach:
  - TPG: common format for termination proofs.
  - Tools output proofs in TPG format.
  - CoLoR: a Coq library of results on termination.
  - Rainbow: a tool for translation from proofs in TPG format to Coq proofs, using results from CoLoR.

CoLoR's approach to certification

How to certify termination results?

- Possibility: certification of tools source code.
  ⇒ difficult, tool dependent, extra work with every change, . . .
- CoLoR's approach:
  - TPG: common format for termination proofs.
  - Tools output proofs in TPG format.
  - CoLoR: a Coq library of results on termination.
  - Rainbow: a tool for translation from proofs in TPG format to Coq proofs, using results from CoLoR.

CoLoR's approach to certification

How to certify termination results?

- Possibility: certification of tools source code.
  $\Rightarrow$ difficult, tool dependent, extra work with every change, ...
- CoLoR's approach:
  - TPG: common format for termination proofs.
  - Tools output proofs in TPG format.
  - CoLoR: a Coq library of results on termination.
  - Rainbow: a tool for translation from proofs in TPG format to Coq proofs, using results from CoLoR.

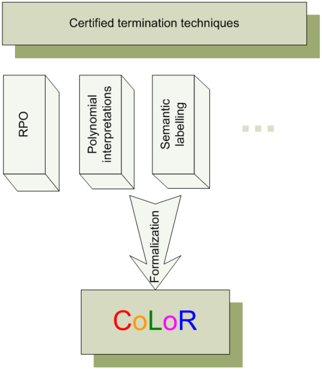
CoLoR's approach to certification

How to certify termination results?

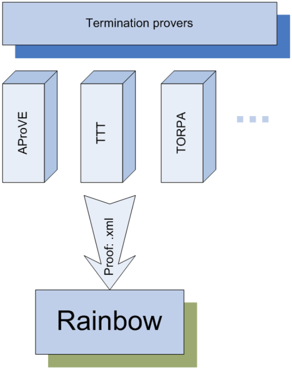
- Possibility: certification of tools source code.

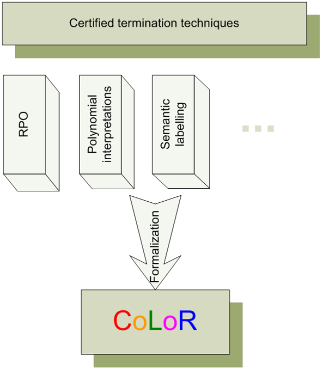
  ⇒ difficult, tool dependent, extra work with every change, . . .
- CoLoR's approach:
  - TPG: common format for termination proofs.
  - Tools output proofs in TPG format.
  - CoLoR: a Coq library of results on termination.
  - Rainbow: a tool for translation from proofs in TPG format to Coq proofs, using results from CoLoR.

CoLoR's architecture overview

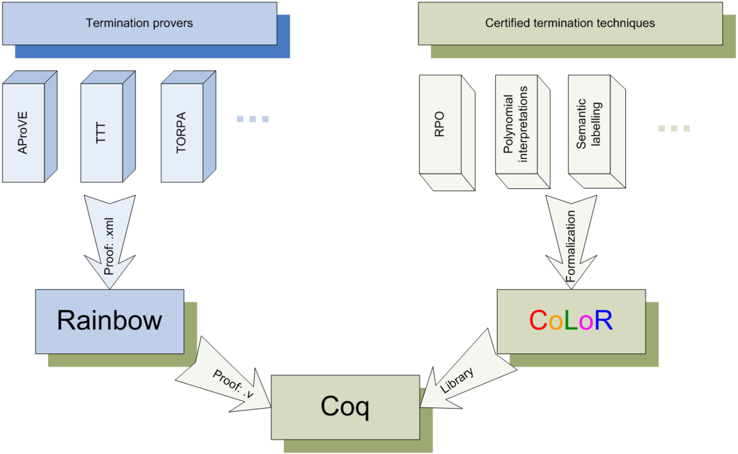


CoLoR's architecture overview





CoLoR's architecture overview



History

Project started (Blanqui)	March 2004
First release	March 2005
First certified proofs	July 2006
First certification workshop	May 2007
First certified competition	June 2007

History

Project started (Blanqui)	March 2004
First release	March 2005
First certified proofs	July 2006
First certification workshop	May 2007
First certified competition	June 2007

History

Project started (Blanqui)	March 2004
First release	March 2005
First certified proofs	July 2006
First certification workshop	May 2007
First certified competition	June 2007

History

Project started (Blanqui)	March 2004
First release	March 2005
First certified proofs	July 2006
First certification workshop	May 2007
First certified competition	June 2007

History

Project started (Blanqui)	March 2004
First release	March 2005
First certified proofs	July 2006
First certification workshop	May 2007
First certified competition	June 2007

Content of CoLoR.

- Termination criteria:
  - **polynomial interpretations** [Hinderer]
  - multiset ordering [Koprowski]
  - recursive path ordering [Coupet-Grimal, Delobel]
  - higher-order recursive path ordering [Koprowski]
  - dependency graph cycles [Blanqui]
  - **matrix interpretations** [Koprowski, Zantema]
  - **arctic interpretations** [Koprowski, Waldmann]
- Transformation techniques:
  - **dependency pairs** [Blanqui]
  - **dependency graph decomposition** [Lucas, Blanqui]
  - arguments filtering [Blanqui]
  - term conversions [Blanqui]

Content of CoLoR.

- Termination criteria:
  - **polynomial interpretations** [Hinderer]
  - multiset ordering [Koprowski]
  - recursive path ordering [Coupet-Grimal, Delobel]
  - higher-order recursive path ordering [Koprowski]
  - dependency graph cycles [Blanqui]
  - **matrix interpretations** [Koprowski, Zantema]
  - **arctic interpretations** [Koprowski, Waldmann]
- Transformation techniques:
  - **dependency pairs** [Blanqui]
  - **dependency graph decomposition** [Lucas, Blanqui]
  - arguments filtering [Blanqui]
  - term conversions [Blanqui]

Content of CoLoR.

- Termination criteria:
  - **polynomial interpretations** [Hinderer]
  - multiset ordering [Koprowski]
  - recursive path ordering [Coupet-Grimal, Delobel]
  - higher-order recursive path ordering [Koprowski]
  - dependency graph cycles [Blanqui]
  - **matrix interpretations** [Koprowski, Zantema]
  - **arctic interpretations** [Koprowski, Waldmann]
- Transformation techniques:
  - **dependency pairs** [Blanqui]
  - **dependency graph decomposition** [Lucas, Blanqui]
  - arguments filtering [Blanqui]
  - term conversions [Blanqui]

Content of CoLoR.

- Termination criteria:
  - **polynomial interpretations** [Hinderer]
  - multiset ordering [Koprowski]
  - recursive path ordering [Coupet-Grimal, Delobel]
  - higher-order recursive path ordering [Koprowski]
  - dependency graph cycles [Blanqui]
  - **matrix interpretations** [Koprowski, Zantema]
  - **arctic interpretations** [Koprowski, Waldmann]
- Transformation techniques:
  - **dependency pairs** [Blanqui]
  - **dependency graph decomposition** [Lucas, Blanqui]
  - arguments filtering [Blanqui]
  - term conversions [Blanqui]

Content of CoLoR.

- Termination criteria:
  - **polynomial interpretations** [Hinderer]
  - multiset ordering [Koprowski]
  - recursive path ordering [Coupet-Grimal, Delobel]
  - higher-order recursive path ordering [Koprowski]
  - dependency graph cycles [Blanqui]
  - **matrix interpretations** [Koprowski, Zantema]
  - **arctic interpretations** [Koprowski, Waldmann]
- Transformation techniques:
  - **dependency pairs** [Blanqui]
  - **dependency graph decomposition** [Lucas, Blanqui]
  - arguments filtering [Blanqui]
  - term conversions [Blanqui]

Content of CoLoR.

- Termination criteria:
  - **polynomial interpretations** [Hinderer]
  - multiset ordering [Koprowski]
  - recursive path ordering [Coupet-Grimal, Delobel]
  - higher-order recursive path ordering [Koprowski]
  - dependency graph cycles [Blanqui]
  - **matrix interpretations** [Koprowski, Zantema]
  - **arctic interpretations** [Koprowski, Waldmann]
- Transformation techniques:
  - **dependency pairs** [Blanqui]
  - **dependency graph decomposition** [Lucas, Blanqui]
  - arguments filtering [Blanqui]
  - term conversions [Blanqui]

Content of CoLoR.

- Termination criteria:
  - **polynomial interpretations** [Hinderer]
  - multiset ordering [Koprowski]
  - recursive path ordering [Coupet-Grimal, Delobel]
  - higher-order recursive path ordering [Koprowski]
  - dependency graph cycles [Blanqui]
  - **matrix interpretations** [Koprowski, Zantema]
  - **arctic interpretations** [Koprowski, Waldmann]
- Transformation techniques:
  - **dependency pairs** [Blanqui]
  - **dependency graph decomposition** [Lucas, Blanqui]
  - arguments filtering [Blanqui]
  - term conversions [Blanqui]

Content of CoLoR.

- Termination criteria:
  - **polynomial interpretations** [Hinderer]
  - multiset ordering [Koprowski]
  - recursive path ordering [Coupet-Grimal, Delobel]
  - higher-order recursive path ordering [Koprowski]
  - dependency graph cycles [Blanqui]
  - **matrix interpretations** [Koprowski, Zantema]
  - **arctic interpretations** [Koprowski, Waldmann]
- Transformation techniques:
  - **dependency pairs** [Blanqui]
  - **dependency graph decomposition** [Lucas, Blanqui]
  - arguments filtering [Blanqui]
  - term conversions [Blanqui]

Content of CoLoR.

- Termination criteria:
  - **polynomial interpretations** [Hinderer]
  - multiset ordering [Koprowski]
  - recursive path ordering [Coupet-Grimal, Delobel]
  - higher-order recursive path ordering [Koprowski]
  - dependency graph cycles [Blanqui]
  - **matrix interpretations** [Koprowski, Zantema]
  - **arctic interpretations** [Koprowski, Waldmann]
- Transformation techniques:
  - **dependency pairs** [Blanqui]
  - **dependency graph decomposition** [Lucas, Blanqui]
  - arguments filtering [Blanqui]
  - term conversions [Blanqui]

Content of CoLoR.

- Termination criteria:
  - **polynomial interpretations** [Hinderer]
  - multiset ordering [Koprowski]
  - recursive path ordering [Coupet-Grimal, Delobel]
  - higher-order recursive path ordering [Koprowski]
  - dependency graph cycles [Blanqui]
  - **matrix interpretations** [Koprowski, Zantema]
  - **arctic interpretations** [Koprowski, Waldmann]
- Transformation techniques:
  - **dependency pairs** [Blanqui]
  - **dependency graph decomposition** [Lucas, Blanqui]
  - arguments filtering [Blanqui]
  - term conversions [Blanqui]

Content of CoLoR.

- Termination criteria:
  - **polynomial interpretations** [Hinderer]
  - multiset ordering [Koprowski]
  - recursive path ordering [Coupet-Grimal, Delobel]
  - higher-order recursive path ordering [Koprowski]
  - dependency graph cycles [Blanqui]
  - **matrix interpretations** [Koprowski, Zantema]
  - **arctic interpretations** [Koprowski, Waldmann]
- Transformation techniques:
  - **dependency pairs** [Blanqui]
  - **dependency graph decomposition** [Lucas, Blanqui]
  - arguments filtering [Blanqui]
  - term conversions [Blanqui]

Content of CoLoR.

- Termination criteria:
  - **polynomial interpretations** [Hinderer]
  - multiset ordering [Koprowski]
  - recursive path ordering [Coupet-Grimal, Delobel]
  - higher-order recursive path ordering [Koprowski]
  - dependency graph cycles [Blanqui]
  - **matrix interpretations** [Koprowski, Zantema]
  - **arctic interpretations** [Koprowski, Waldmann]
- Transformation techniques:
  - **dependency pairs** [Blanqui]
  - **dependency graph decomposition** [Lucas, Blanqui]
  - arguments filtering [Blanqui]
  - term conversions [Blanqui]

Content of CoLoR.

- Termination criteria:
  - **polynomial interpretations** [Hinderer]
  - multiset ordering [Koprowski]
  - recursive path ordering [Coupet-Grimal, Delobel]
  - higher-order recursive path ordering [Koprowski]
  - dependency graph cycles [Blanqui]
  - **matrix interpretations** [Koprowski, Zantema]
  - **arctic interpretations** [Koprowski, Waldmann]
- Transformation techniques:
  - **dependency pairs** [Blanqui]
  - **dependency graph decomposition** [Lucas, Blanqui]
  - arguments filtering [Blanqui]
  - term conversions [Blanqui]

Content of CoLoR.

- Term structures:
  - simply typed lambda-terms [Koprowski]
  - varyadic terms [Blanqui]
  - algebraic terms with symbols of fixed arity [Hinderer, Blanqui]
- General libraries and algorithms:
  - matrices [Koprowski]
  - semi-rings [Koprowski,Zantema]
  - finite multisets [Koprowski]
  - integer polynomials with multiple variables [Hinderer]
  - computation of strongly connected components (SCCs) [Ducas]
  - lists, vectors, relations, etc.

Content of CoLoR.

- Term structures:
  - simply typed lambda-terms [Koprowski]
  - varyadic terms [Blanqui]
  - algebraic terms with symbols of fixed arity [Hinderer, Blanqui]
- General libraries and algorithms:
  - matrices [Koprowski]
  - semi-rings [Koprowski,Zantema]
  - finite multisets [Koprowski]
  - integer polynomials with multiple variables [Hinderer]
  - computation of strongly connected components (SCCs) [Ducas]
  - lists, vectors, relations, etc.

Content of CoLoR.

- Term structures:
  - simply typed lambda-terms [Koprowski]
  - varyadic terms [Blanqui]
  - algebraic terms with symbols of fixed arity [Hinderer, Blanqui]
- General libraries and algorithms:
  - matrices [Koprowski]
  - semi-rings [Koprowski,Zantema]
  - finite multisets [Koprowski]
  - integer polynomials with multiple variables [Hinderer]
  - computation of strongly connected components (SCCs) [Ducas]
  - lists, vectors, relations, etc.

Content of CoLoR.

- Term structures:
  - simply typed lambda-terms [Koprowski]
  - varyadic terms [Blanqui]
  - algebraic terms with symbols of fixed arity [Hinderer, Blanqui]
- General libraries and algorithms:
  - matrices [Koprowski]
  - semi-rings [Koprowski,Zantema]
  - finite multisets [Koprowski]
  - integer polynomials with multiple variables [Hinderer]
  - computation of strongly connected components (SCCs) [Ducas]
  - lists, vectors, relations, etc.

Content of CoLoR.

- Term structures:
  - simply typed lambda-terms [Koprowski]
  - varyadic terms [Blanqui]
  - algebraic terms with symbols of fixed arity [Hinderer, Blanqui]
- General libraries and algorithms:
  - matrices [Koprowski]
  - semi-rings [Koprowski,Zantema]
  - finite multisets [Koprowski]
  - integer polynomials with multiple variables [Hinderer]
  - computation of strongly connected components (SCCs) [Ducas]
  - lists, vectors, relations, etc.

Content of CoLoR.

- Term structures:
  - simply typed lambda-terms [Koprowski]
  - varyadic terms [Blanqui]
  - algebraic terms with symbols of fixed arity [Hinderer, Blanqui]
- General libraries and algorithms:
  - matrices [Koprowski]
  - semi-rings [Koprowski,Zantema]
  - finite multisets [Koprowski]
  - integer polynomials with multiple variables [Hinderer]
  - computation of strongly connected components (SCCs) [Ducas]
  - lists, vectors, relations, etc.

Content of CoLoR.

- Term structures:
  - simply typed lambda-terms [Koprowski]
  - varyadic terms [Blanqui]
  - algebraic terms with symbols of fixed arity [Hinderer, Blanqui]
- General libraries and algorithms:
  - matrices [Koprowski]
  - semi-rings [Koprowski,Zantema]
  - finite multisets [Koprowski]
  - integer polynomials with multiple variables [Hinderer]
  - computation of strongly connected components (SCCs) [Ducas]
  - lists, vectors, relations, etc.

Content of CoLoR.

- Term structures:
  - simply typed lambda-terms [Koprowski]
  - varyadic terms [Blanqui]
  - algebraic terms with symbols of fixed arity [Hinderer, Blanqui]
- General libraries and algorithms:
  - matrices [Koprowski]
  - semi-rings [Koprowski,Zantema]
  - finite multisets [Koprowski]
  - integer polynomials with multiple variables [Hinderer]
  - computation of strongly connected components (SCCs) [Ducas]
  - lists, vectors, relations, etc.

Content of CoLoR.

- Term structures:
  - simply typed lambda-terms [Koprowski]
  - varyadic terms [Blanqui]
  - algebraic terms with symbols of fixed arity [Hinderer, Blanqui]
- General libraries and algorithms:
  - matrices [Koprowski]
  - semi-rings [Koprowski,Zantema]
  - finite multisets [Koprowski]
  - integer polynomials with multiple variables [Hinderer]
  - computation of strongly connected components (SCCs) [Ducas]
  - lists, vectors, relations, etc.

Content of CoLoR.

- Term structures:
  - simply typed lambda-terms [Koprowski]
  - varyadic terms [Blanqui]
  - algebraic terms with symbols of fixed arity [Hinderer, Blanqui]
- General libraries and algorithms:
  - matrices [Koprowski]
  - semi-rings [Koprowski,Zantema]
  - finite multisets [Koprowski]
  - integer polynomials with multiple variables [Hinderer]
  - computation of strongly connected components (SCCs) [Ducas]
  - lists, vectors, relations, etc.

Content of CoLoR.

- Term structures:
  - simply typed lambda-terms [Koprowski]
  - varyadic terms [Blanqui]
  - algebraic terms with symbols of fixed arity [Hinderer, Blanqui]
- General libraries and algorithms:
  - matrices [Koprowski]
  - semi-rings [Koprowski,Zantema]
  - finite multisets [Koprowski]
  - integer polynomials with multiple variables [Hinderer]
  - computation of strongly connected components (SCCs) [Ducas]
  - lists, vectors, relations, etc.

Content of CoLoR.

In total:

- ≈ 50.000 lines of code.
- ≈ 1.000 definitions and ≈ 3.000 lemmas.
- Only 20% of that is the code for actual termination methods!

Size comparison with other libraries:

- Coq standard library
- C-CoRN
- COMPCERT
- CoLoR

Content of CoLoR.

In total:

- ≈ 50.000 lines of code.
- ≈ 1.000 definitions and ≈ 3.000 lemmas.
- Only 20% of that is the code for actual termination methods!

Size comparison with other libraries:

- Coq standard library
- C-CoRN
- COMPCERT
- CoLoR

Content of CoLoR.

In total:

- ≈ 50.000 lines of code.
- ≈ 1.000 definitions and ≈ 3.000 lemmas.
- Only 20% of that is the code for actual termination methods!

Size comparison with other libraries:

- Coq standard library
- C-CoRN
- COMPCERT
- CoLoR

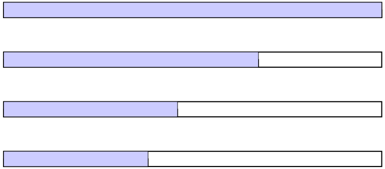
Content of CoLoR.

In total:

- ≈ 50.000 lines of code.
- ≈ 1.000 definitions and ≈ 3.000 lemmas.
- Only 20% of that is the code for actual termination methods!

Size comparison with other libraries:

- Coq standard library
- C-CoRN
- COMPCERT
- CoLoR



Related work

- CoLoR project
  Authors: Blanqui, . . .
  Proof assistant: Coq
- A3PAT project
  Authors: Contejean, . . .
  Proof assistant: Coq
- Isabelle/HOL termination checker
  Authors: Bulwahn, Krauss, Nipkow, . . .
  Proof assistant: Isabelle/HOL

Related work

- CoLoR project
  Authors: Blanqui, ...
  Proof assistant: Coq
- A3PAT project
  Authors: Contejean, ...
  Proof assistant: Coq
- Isabelle/HOL termination checker
  Authors: Bulwahn, Krauss, Nipkow, ...
  Proof assistant: Isabelle/HOL

Related work

- CoLoR project
  Authors: Blanqui, . . .
  Proof assistant: Coq
- A3PAT project
  Authors: Contejean, . . .
  Proof assistant: Coq
- Isabelle/HOL termination checker
  Authors: Bulwahn, Krauss, Nipkow, . . .
  Proof assistant: Isabelle/HOL

Certified competition

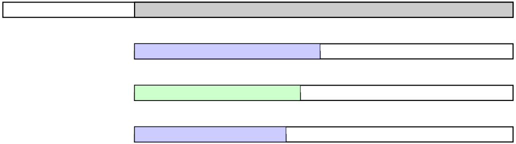
- In the 2007 termination competition a new “certified” category was introduced.
- Participants 2007 (975 problems):
  - TPA + CoLoR
  - CiME + A3PAT
  - $\mathrm{T_TT_2}$ + CoLoR
- Participants 2008 (1391 problems):
  - AProVE + CoLoR + A3PAT
  - AProVE + CoLoR
  - AProVE + A3PAT
  - CiME3 + A3PAT
  - Matchbox + CoLoR

Certified competition

- In the 2007 termination competition a new “certified” category was introduced.
- Participants 2007 (975 problems):
  - TPA + CoLoR
  - C*i*ME + A3PAT
  - $\text{T}_\text{T}\text{T}_2$ + CoLoR
- Participants 2008 (1391 problems):
  - AProVE + CoLoR+ A3PAT
  - AProVE + CoLoR
  - AProVE + A3PAT
  - CiME3 + A3PAT
  - Matchbox + CoLoR

Certified competition

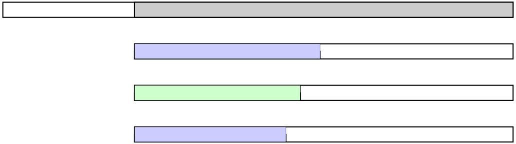
- In the 2007 termination competition a new “certified” category was introduced.
- Participants 2007 (975 problems):
  - *AProVE (non-certified)* *723*
  - TPA + CoLoR 354
  - C*i*ME + A3PAT 317
  - T$_{\text{T}}$T$_2$ + CoLoR 289



- Participants 2008 (1391 problems):
  - AProVE + CoLoR + A3PAT
  - AProVE + CoLoR
  - AProVE + A3PAT
  - CiME3 + A3PAT
  - Matchbox + CoLoR

Certified competition

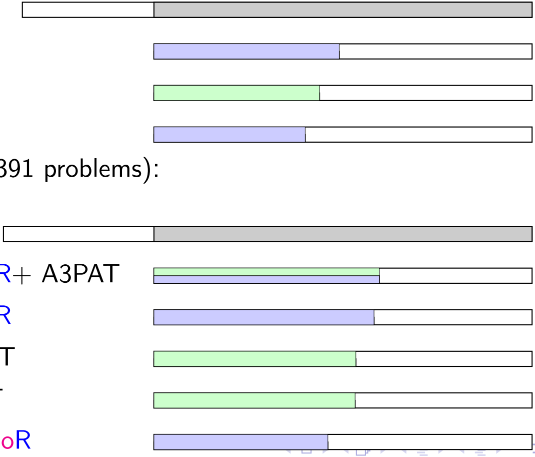
- In the 2007 termination competition a new “certified” category was introduced.
- Participants 2007 (975 problems):
  - *AProVE (non-certified)* *723*
  - TPA + CoLoR 354
  - C*i*ME + A3PAT 317
  - $\mathrm{T_TT_2}$ + CoLoR 289



- Participants 2008 (1391 problems):
  - AProVE + CoLoR+ A3PAT
  - AProVE + CoLoR
  - AProVE + A3PAT
  - C*i*ME3 + A3PAT
  - Matchbox + CoLoR

Certified competition

- In the 2007 termination competition a new “certified” category was introduced.
- Participants 2007 (975 problems):
  - *AProVE (non-certified)* *723*
  - TPA + CoLoR 354
  - C*i*ME + A3PAT 317
  - $\mathrm{T_TT_2}$ + CoLoR 289
- Participants 2008 (1391 problems):
  - *AProVE (non-certified)* *995*
  - AProVE + CoLoR+ A3PAT 594
  - AProVE + CoLoR 580
  - AProVE + A3PAT 532
  - C*i*ME3 + A3PAT 531
  - Matchbox + CoLoR 458



Outline

1. Background: termination of term rewriting

2. CoLoR project: certification of termination proofs
   - Why?... motivation
   - How?... CoLoR's approach to certification
   - When?... history of the project
   - What?... overview of the content
   - Related work
   - Certified competition

3. Conclusions... sort of

Lessons learned

- Lesson 1

  If it is possible do (involved) computations/reasoning in an unsafe setting and verify the results in Coq a posteriori.

  That requires some notion of a certificate.

  Proof search is usually much more complex than proof verification.

  We see that even in theorem provers — proof checking VS proof searching.

Lessons learned

- Lesson 1

  If it is possible do (involved) computations/reasoning in an unsafe setting and verify the results in Coq a posteriori.

  That requires some notion of a certificate.

  Proof search is usually much more complex than proof verification.

  We see that even in theorem provers — proof checking VS proof searching.

Lessons learned

- Lesson 1

  If it is possible do (involved) computations/reasoning in an unsafe setting and verify the results in Coq a posteriori.

  That requires some notion of a certificate.

  Proof search is usually much more complex than proof verification.

  We see that even in theorem provers — proof checking VS proof searching.

Lessons learned

- Lesson 1

  If it is possible do (involved) computations/reasoning in an unsafe setting and verify the results in Coq a posteriori.

  That requires some notion of a certificate.

  Proof search is usually much more complex than proof verification.

  We see that even in theorem provers — proof checking VS proof searching.

Lessons learned ctd.

- Lesson 2

  It is not unusual for software projects to be behind schedule / run out of budget.

  It is even more so for Coq projects.

  Why?

  - $$\begin{array}{rcl} \text{algorithm} & \mapsto & \text{program} \\ \text{paper proof} & \mapsto & \text{formal proof in Coq} \end{array}$$
  - Lack of libraries.
  - Proof engineering is not yet as mature as software engineering (re-usability, re-factoring etc.)

Lessons learned ctd.

- Lesson 2

  It is not unusual for software projects to be behind schedule / run out of budget.

  It is even more so for Coq projects.

  Why?

  - algorithm ↦ program
    paper proof ↦ formal proof in Coq
  - Lack of libraries.
  - Proof engineering is not yet as mature as software engineering (re-usability, re-factoring etc.)

Lessons learned ctd.

- Lesson 2

  It is not unusual for software projects to be behind schedule / run out of budget.

  It is even more so for Coq projects.

  Why?

  - $$\begin{array}{rcl} \text{algorithm} & \mapsto & \text{program} \\ \text{paper proof} & \mapsto & \text{formal proof in Coq} \end{array}$$
  - Lack of libraries.
  - Proof engineering is not yet as mature as software engineering (re-usability, re-factoring etc.)

Lessons learned ctd.

- Lesson 2

  It is not unusual for software projects to be behind schedule / run out of budget.

  It is even more so for Coq projects.

  Why?

  - $$\begin{array}{rcl} \text{algorithm} & \mapsto & \text{program} \\ \text{paper proof} & \mapsto & \text{formal proof in Coq} \end{array}$$
  - Lack of libraries.
  - Proof engineering is not yet as mature as software engineering (re-usability, re-factoring etc.)

Lessons learned ctd.

- Lesson 2

  It is not unusual for software projects to be behind schedule / run out of budget.

  It is even more so for Coq projects.

  Why?

  - $$\begin{array}{rcl} \text{algorithm} & \mapsto & \text{program} \\ \text{paper proof} & \mapsto & \text{formal proof in Coq} \end{array}$$
  - Lack of libraries.
  - Proof engineering is not yet as mature as software engineering (re-usability, re-factoring etc.)

Lessons learned ctd.

- Lesson 3

  When writing your definitions there is usually plenty of choice.

  You want to make the right choices. You really do.

  Because that will have a tremendous impact on the reasoning about those definitions that you are going to do for long hours afterwards.

Lessons learned ctd.

- Lesson 3

  When writing your definitions there is usually plenty of choice.

  You want to make the right choices. You really do.

  Because that will have a tremendous impact on the reasoning about those definitions that you are going to do for long hours afterwards.

Lessons learned ctd.

- Lesson 3

  When writing your definitions there is usually plenty of choice.

  You want to make the right choices. You really do.

  Because that will have a tremendous impact on the reasoning about those definitions that you are going to do for long hours afterwards.

Lessons learned ctd.

- Lesson 3

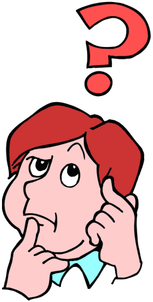
  When writing your definitions there is usually plenty of choice.

  You want to make the right choices. You really do.

  Because that will have a tremendous impact on the reasoning about those definitions that you are going to do for long hours afterwards.

The end

http://color.loria.fr



Thank you for your attention.