Computational Logic

Automatic Proofs in Equational Logic

Status Report

Thomas Sternagel, BSc.

Computational Logic
Institute of Computer Science
University of Innsbruck

May 9, 2012

Outline

- Objective
- Preliminaries
- Recording Completion
- Implementation
- Live-Demo
- Current State
- Résumé

Objective

Objective

- Proving $E \vdash s \approx t$ is a fundamental problem in CS.

Objective

- Proving $E \vdash s \approx t$ is a fundamental problem in CS.
- Two possibilities:
  - Equational logic (find proof tree in positive case).
  - Knuth-Bendix completion (yielding decision procedure).

Objective

- Proving $E \vdash s \approx t$ is a fundamental problem in CS.
- Two possibilities:
  - Equational logic (find proof tree in positive case).
  - Knuth-Bendix completion (yielding decision procedure).
- Study the relationships between these two methods.

Objective

- Proving $E \vdash s \approx t$ is a fundamental problem in CS.
- Two possibilities:
  - Equational logic (find proof tree in positive case).
  - Knuth-Bendix completion (yielding decision procedure).
- Study the relationships between these two methods.
- Implement the results into an existing tool.

Objective

- Proving $E \vdash s \approx t$ is a fundamental problem in CS.
- Two possibilities:
  - Equational logic (find proof tree in positive case).
  - Knuth-Bendix completion (yielding decision procedure).
- Study the relationships between these two methods.
- Implement the results into an existing tool.
- Possible extensions:
  - Short proof trees.
  - Proof trees for E where completion fails.
  - Disproofs.

Preliminaries: Completion

Preliminaries: Completion

deduce $\dfrac{(E, R)}{(E \cup \{s \approx t\}, R)}$ if $s \leftarrow u \rightarrow t$

delete $\dfrac{(E \cup \{s \approx s\}, R)}{(E, R)}$

orient $\dfrac{(E \cup \{s \mathrel{\dot{\approx}} t\}, R)}{(E, R \cup \{s \rightarrow t\})}$ if $s > t$

compose $\dfrac{(E, R \cup \{s \rightarrow t\})}{(E, R \cup \{s \rightarrow u\})}$ if $t \rightarrow u$

simplify $\dfrac{(E \cup \{s \mathrel{\dot{\approx}} t\}, R)}{(E \cup \{u \mathrel{\dot{\approx}} t\}, R)}$ if $s \rightarrow u$

collapse $\dfrac{(E, R \cup \{s \rightarrow t\})}{(E \cup \{u \approx t\}, R)}$ if $s \overset{!}{\rightarrow} u$

Preliminaries: Completion

deduce $\dfrac{(E, R)}{(E \cup \{s \approx t\}, R)}$ if $s \leftarrow u \rightarrow t$

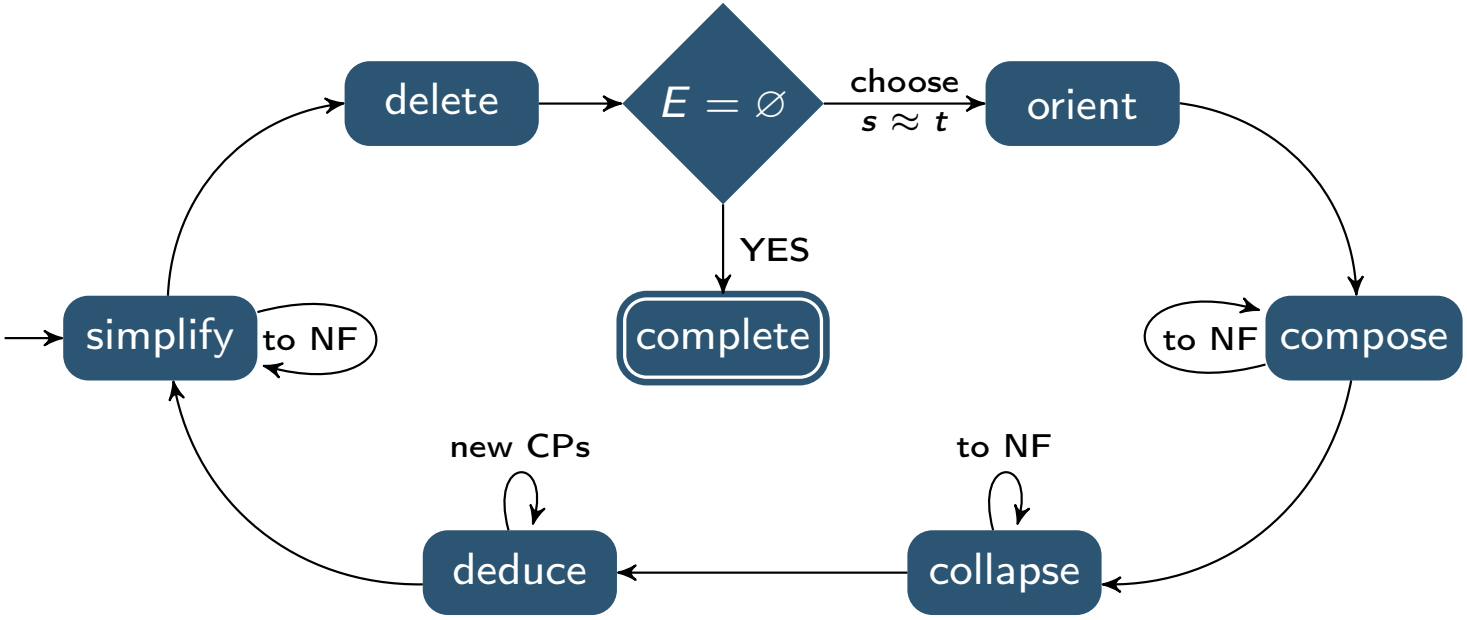
delete $\dfrac{(E \cup \{s \approx s\}, R)}{(E, R)}$

orient $\dfrac{(E \cup \{s \mathrel{\dot{\approx}} t\}, R)}{(E, R \cup \{s \rightarrow t\})}$ if $s > t$

compose $\dfrac{(E, R \cup \{s \rightarrow t\})}{(E, R \cup \{s \rightarrow u\})}$ if $t \rightarrow u$

simplify $\dfrac{(E \cup \{s \mathrel{\dot{\approx}} t\}, R)}{(E \cup \{u \mathrel{\dot{\approx}} t\}, R)}$ if $s \rightarrow u$

collapse $\dfrac{(E, R \cup \{s \rightarrow t\})}{(E \cup \{u \approx t\}, R)}$ if $s \overset{!}{\rightarrow} u$



Preliminaries: Equational Logic

Preliminaries: Equational Logic

[r] reflexivity

$$\frac{}{t \approx t}$$

[s] symmetry

$$\frac{s \approx t}{t \approx s}$$

[t] transitivity

$$\frac{s \approx t, t \approx u}{s \approx u}$$

[a] application

$$\frac{}{l\sigma \approx r\sigma}$$

[c] congruence

$$\frac{s_1 \approx t_1, \ldots, s_n \approx t_n}{f(s_1, \ldots, s_n) \approx f(t_1, \ldots, t_n)}$$

Preliminaries: Equational Logic

[r] reflexivity

$$\frac{}{t \approx t}$$

[s] symmetry

$$\frac{s \approx t}{t \approx s}$$

[t] transitivity

$$\frac{s \approx t, t \approx u}{s \approx u}$$

[a] application

$$\frac{}{l\sigma \approx r\sigma}$$

[c] congruence

$$\frac{s_1 \approx t_1, \ldots, s_n \approx t_n}{f(s_1, \ldots, s_n) \approx f(t_1, \ldots, t_n)}$$

Example

$$E = \{\mathsf{ff} \approx \mathsf{f}, \mathsf{ggf} \approx \mathsf{g}\}$$
$$E \vdash \mathsf{fgf} \approx \mathsf{fgg}$$

$$\dfrac{\dfrac{\dfrac{}{\mathsf{ggff} \approx \mathsf{gf}}\,[\mathsf{a}]}{\mathsf{fggff} \approx \mathsf{fgf}}\,[\mathsf{c}]}{\mathsf{fgf} \approx \mathsf{fggff}}\,[\mathsf{s}] \qquad \dfrac{\dfrac{\dfrac{\mathsf{ff} \approx \mathsf{f}}{\vdots}\,[\mathsf{c}]}{\mathsf{fggff} \approx \mathsf{fggf}}\,[\mathsf{c}] \qquad \dfrac{\vdots \quad \vdots}{\mathsf{fggf} \approx \mathsf{fgg}}\,[\mathsf{t}]}{\mathsf{fggff} \approx \mathsf{fgg}}\,[\mathsf{t}]$$
$$\mathsf{fgf} \approx \mathsf{fgg}\,[\mathsf{t}]$$

Recording Completion

Recording Completion

deduce

$$\frac{(E, R, H)}{(E \cup \{m : s \approx t\}, R, H \cup \{m : s \overset{j}{\leftarrow} u \overset{k}{\rightarrow} t\})} \quad \text{if } s \overset{j}{\leftarrow} u \overset{k}{\rightarrow} t$$

orient$_l$

$$\frac{(E \cup \{i : s \mathrel{\dot{\approx}} t\}, R, H)}{(E, R \cup \{i : s \rightarrow t\}, H)} \quad \text{if } s > t$$

orient$_r$

$$\frac{(E \cup \{i : s \approx t\}, R, H \cup \{i : s \overset{j}{\circ_1} u \overset{k}{\circ_2} t\})}{(E, R \cup \{i : t \rightarrow s\}, H \cup \{i : t \overset{k}{(\circ_2)}^{-1} u \overset{j}{(\circ_1)}^{-1} s\})} \quad \text{if } t > s$$

simplify

$$\frac{(E \cup \{i : s \mathrel{\dot{\approx}} t\}, R, H)}{(E \cup \{m : u \mathrel{\dot{\approx}} t\}, R, H \cup \{m : u \overset{l}{\leftarrow} s \overset{i}{\rightarrow} t\})} \quad \text{if } s \overset{l}{\rightarrow} u$$

delete

$$\frac{(E \cup \{i : s \approx s\}, R, H \cup \{i : s \circ_1 v \circ_2 s\})}{(E, R, H)}$$

compose

$$\frac{(E, R \cup \{i : s \rightarrow t\}, H)}{(E, R \cup \{m : s \rightarrow u\}, H \cup \{m : s \overset{i}{\rightarrow} t \overset{j}{\rightarrow} u\})} \quad \text{if } t \overset{j}{\rightarrow} u$$

collapse

$$\frac{(E, R \cup \{i : s \rightarrow t\}, H)}{(E \cup \{m : u \approx t\}, R, H \cup \{m : u \overset{j}{\leftarrow} s \overset{i}{\rightarrow} t\})} \quad \text{if } s \overset{\sqsupset j}{\rightarrow} u$$

Recording Completion

deduce

$$\frac{(E, R, H)}{(E \cup \{m : s \approx t\}, R, H \cup \{m : s \overset{j}{\leftarrow} u \overset{k}{\rightarrow} t\})} \quad \text{if } s \overset{j}{\leftarrow} u \overset{k}{\rightarrow} t$$

orient$_l$

$$\frac{(E \cup \{i : s \mathrel{\dot{\approx}} t\}, R, H)}{(E, R \cup \{i : s \rightarrow t\}, H)} \quad \text{if } s > t$$

orient$_r$

$$\frac{(E \cup \{i : s \approx t\}, R, H \cup \{i : s \overset{j}{\circ_1} u \overset{k}{\circ_2} t\})}{(E, R \cup \{i : t \rightarrow s\}, H \cup \{i : t \overset{k}{(\circ_2)}^{-1} u \overset{j}{(\circ_1)}^{-1} s\})} \quad \text{if } t > s$$

simplify

$$\frac{(E \cup \{i : s \mathrel{\dot{\approx}} t\}, R, H)}{(E \cup \{m : u \mathrel{\dot{\approx}} t\}, R, H \cup \{m : u \overset{l}{\leftarrow} s \overset{i}{\rightarrow} t\})} \quad \text{if } s \overset{l}{\rightarrow} u$$

delete

$$\frac{(E \cup \{i : s \approx s\}, R, H \cup \{i : s \circ_1 v \circ_2 s\})}{(E, R, H)}$$

compose

$$\frac{(E, R \cup \{i : s \rightarrow t\}, H)}{(E, R \cup \{m : s \rightarrow u\}, H \cup \{m : s \overset{i}{\rightarrow} t \overset{j}{\rightarrow} u\})} \quad \text{if } t \overset{j}{\rightarrow} u$$

collapse

$$\frac{(E, R \cup \{i : s \rightarrow t\}, H)}{(E \cup \{m : u \approx t\}, R, H \cup \{m : u \overset{j}{\leftarrow} s \overset{i}{\rightarrow} t\})} \quad \text{if } s \overset{\sqsupset j}{\rightarrow} u$$

Record → Compare → Recall → Plant & Grow

Implementation

Implementation

KBCV 1.0

$\sim$4100 LOC

Implementation

KBCV 1.0

~4100 LOC

termlib 1.2

~1700 LOC

- Indices
- Recording completion
- Performance optimization

Implementation

KBCV 1.0

∼4100 LOC

termlib 1.2

∼1700 LOC

- Indices
- Recording completion
- Performance optimization

KBCV 1.7

∼4600 LOC

- Enhanced automatic completion
- Equational logic proofs
- Certifiable output

Implementation

KBCV 1.0

~4100 LOC

termlib 1.2

~1700 LOC

- Indices
- Recording completion
- Performance optimization

KBCV 1.7

~4600 LOC

- Enhanced automatic completion
- Equational logic proofs
- Certifiable output

	KBCV	MAXCOMP	MKBTT	Slothrop
completed	86	86	81	71
`LS94_P1`	✓			
`SK90_3.26`	✓			

Table: Experimental results on 115 systems.

Live-Demo

Current State

- Study the relationships between the two methods.

Current State

- ~~Study the relationships between the two methods.~~ ✓
- Implement the results into an existing tool.

Current State

- ~~Study the relationships between the two methods.~~ ✓
- ~~Implement the results into an existing tool.~~ ✓

Current State

- ~~Study the relationships between the two methods.~~ ✓
- ~~Implement the results into an existing tool.~~ ✓
- Possible extensions:
  - Short proof trees.
  - Proof trees for E where completion fails.
  - Disproofs.

Current State

- ~~Study the relationships between the two methods.~~ ✓
- ~~Implement the results into an existing tool.~~ ✓
- Possible extensions:
  - Short proof trees. ∼
  - Proof trees for E where completion fails.
  - Disproofs.

Current State

- ~~Study the relationships between the two methods.~~ ✓
- ~~Implement the results into an existing tool.~~ ✓
- Possible extensions:
  - Short proof trees. ∼
  - Proof trees for E where completion fails. ∼
  - Disproofs.

Current State

- ~~Study the relationships between the two methods.~~ ✓
- ~~Implement the results into an existing tool.~~ ✓
- Possible extensions:
  - Short proof trees. $\sim$
  - Proof trees for E where completion fails. $\sim$
  - Disproofs. $\sim$

Current State

- ~~Study the relationships between the two methods.~~ ✓
- ~~Implement the results into an existing tool.~~ ✓
- Possible extensions:
  - Short proof trees. $\sim$
  - Proof trees for E where completion fails. $\sim$
  - Disproofs. $\sim$

Completion	$E \vdash s \approx t$	
successful	yes	✓

Current State

- ~~Study the relationships between the two methods.~~ ✓
- ~~Implement the results into an existing tool.~~ ✓
- Possible extensions:
  - Short proof trees. $\sim$
  - Proof trees for E where completion fails. $\sim$
  - Disproofs. $\sim$

Completion	$E \vdash s \approx t$	
successful	yes	✓
successful	no	✓

Current State

- ~~Study the relationships between the two methods.~~ ✓
- ~~Implement the results into an existing tool.~~ ✓
- Possible extensions:
  - Short proof trees. $\sim$
  - Proof trees for E where completion fails. $\sim$
  - Disproofs. $\sim$

Completion	$E \vdash s \approx t$	
successful	yes	✓
successful	no	✓
not successful	yes	$\sim$

Current State

- ~~Study the relationships between the two methods.~~ ✓
- ~~Implement the results into an existing tool.~~ ✓
- Possible extensions:
  - Short proof trees. $\sim$
  - Proof trees for E where completion fails. $\sim$
  - Disproofs. $\sim$

Completion	$E \vdash s \approx t$	
successful	yes	✓
successful	no	✓
not successful	yes	$\sim$
not successful	no	×

Résumé

- Assignment: Automatic proofs in equational logic.
- Basics: Completion and equational logic.
- Recording completion.
- Implementation in KBCV.
- Demo.
- Current state.

More Information

Visualizing Knuth-Bendix Completion

Thomas Sternagel

Bachelor Thesis, University of Innsbruck, 2010.

Automatic Proofs in Equational Logic

Thomas Sternagel

Master Seminar Report, University of Innsbruck, 2010.

Automatic Proofs in Equational Logic (2) - Model Finding

Thomas Sternagel

Master Seminar Report, University of Innsbruck, 2011.

KBCV- Knuth-Bendix completion visualizer

Thomas Sternagel and Harald Zankl

System Description, IJCAR 2012, LNAI, 2012. To appear.

Recording completion for finding and certifying proofs in equational logic

Thomas Sternagel, René Thiemann, Harald Zankl, Christian Sternagel

IWC 2012, 2012. To appear.

Feedback

»This tool will be of interest to all students and users of completion.«

Reviewer X

»I downloaded and installed KBCV and found it a pleasure to use. The nice graphical user interface is intuitive and useful for experimentation.«

Reviewer Y

»This tool will be of interest to all students and users of completion.«

Reviewer X

»I downloaded and installed KBCV and found it a pleasure to use. The nice graphical user interface is intuitive and useful for experimentation.«

Reviewer Y

The talk is complete now!!!

Thank you for your attention!

Any questions?