Certification of Confluence Proofs using CeTA

René Thiemann

Computational Logic, University of Innsbruck

29 May 2012

From termination to confluence

- CeTA: tool for **Ce***rtified* **T***ermination* **A***nalysis*

From termination to confluence

- CeTA: tool for **Ce***rtified* **T***ermination* **A***nalysis*
- . . . so why participate in confluence competition?

From termination to confluence

- CeTA: tool for **Ce***rtified* **T***ermination* **A***nalysis*
- . . . so why participate in confluence competition?
- starting point was important result of Gramlich:

  a locally confluent overlay system is termination
  iff it is innermost terminating

From termination to confluence

- CeTA: tool for **Ce***rtified* **T***ermination* **A***nalysis*
- . . . so why participate in confluence competition?
- starting point was important result of Gramlich:

  a locally confluent overlay system is termination
  iff it is innermost terminating

$\Rightarrow$ to benefit from innermost termination techniques we had to certify the local confluence criterion: critical pair lemma

From termination to confluence

- CeTA: tool for **Ce***rtified* **T***ermination* **A***nalysis*
- . . . so why participate in confluence competition?
- starting point was important result of Gramlich:

  a locally confluent overlay system is termination
  iff it is innermost terminating

$\Rightarrow$ to benefit from innermost termination techniques we had to certify the local confluence criterion: critical pair lemma

$\Rightarrow$ first step towards pure confluence certification was done

Techniques formalized so far

- critical pair lemma (tedious)
- Newman's lemma (trivial)
- (several termination techniques, with Christian Sternagel)

$\Rightarrow$ decision procedure of confluence for large class of systems (over 1500 TRSs from TPDB)

Techniques formalized so far

- critical pair lemma (tedious)
- Newman's lemma (trivial)
- (several termination techniques, with Christian Sternagel)

$\Rightarrow$ decision procedure of confluence for large class of systems
(over 1500 TRSs from TPDB)

- weak orthogonality (similar effort as critical pair lemma)
- not (yet): parallel closed
(expect tedious reasoning on measure of parallel forks)

Techniques formalized so far

- critical pair lemma (tedious)
- Newman's lemma (trivial)
- (several termination techniques, with Christian Sternagel)

$\Rightarrow$ decision procedure of confluence for large class of systems
(over 1500 TRSs from TPDB)

- weak orthogonality (similar effort as critical pair lemma)
- not (yet): parallel closed
(expect tedious reasoning on measure of parallel forks)

- non-joinable forks
- use idea from CSI: tcap as detection criterion for non-joinability
(formalization trivial, if tcap is available)

CeTA as certifier?

- CeTA is a Haskell program (20,000 lines)

CeTA as certifier?

- CeTA is a Haskell program (20,000 lines)
- it is completely generated from Isabelle's code generator

CeTA as certifier?

- CeTA is a Haskell program (20,000 lines)
- it is completely generated from Isabelle's code generator
- soundness is proven within IsaFoR:
  Isa*belle* **F***ormalization* **o***f* **R***ewriting*

CeTA as certifier?

- CeTA is a Haskell program (20,000 lines)
- it is completely generated from Isabelle's code generator
- soundness is proven within IsaFoR:
  Isa*belle* **F***ormalization* **o***f* **R***ewriting*
- IsaFoR contains required theorems
  (critical pair lemma, . . .)

CeTA as certifier?

- CeTA is a Haskell program (20,000 lines)
- it is completely generated from Isabelle's code generator
- soundness is proven within IsaFoR:
  Isa*belle* **F***ormalization* **o***f* **R***ewriting*
- IsaFoR contains required theorems
  (critical pair lemma, . . .)
- IsaFoR contains executable functions which guarantee correct application of theorems
  (check joinability, . . .)

Workflow

- confluence tool produces proof in XML (certification problem format, CPF)

Workflow

- confluence tool produces proof in XML
  (certification problem format, CPF)
- CeTA accepts proof or delivers readable error message

Workflow

- confluence tool produces proof in XML
  (certification problem format, CPF)
- CeTA accepts proof or delivers readable error message
- overhead for confluence tool:
  - produce XML output
  - minimal runtime increase when invoking CeTA

Workflow

- confluence tool produces proof in XML
  (certification problem format, CPF)
- CeTA accepts proof or delivers readable error message
- overhead for confluence tool:
  - produce XML output
  - minimal runtime increase when invoking CeTA
- gain for confluence tool:
  - direct detection of errors
  - pretty printer for XML available

Workflow

- confluence tool produces proof in XML
  (certification problem format, CPF)
- CeTA accepts proof or delivers readable error message
- overhead for confluence tool:
  - produce XML output
  - minimal runtime increase when invoking CeTA
- gain for confluence tool:
  - direct detection of errors
  - pretty printer for XML available
- just try it

  `http://cl-informatik.uibk.ac.at/software/ceta/`