Proving Termination of Constrained Term Rewriting Systems

Tsubasa Sakata,
(joint work with Naoki Nishida)

Nagoya University
August 2, 2010

Background

- We have proposed a method for proving equivalence of imperative programs
  - Transforming imperative programs into constrained TRSs
  - Proving inductive theorems of constrained TRSs
    - We have proposed rewriting induction on constrained TRSs to prove inductive theorems
    - Termination of constrained TRSs is necessary to prove inductive theorems (like KB)

Purpose

- We propose a method for proving termination of constrained TRSs

Constrained TRS[1/2]

- A constrained TRS R is a finite set of rewriting rules with constraint of the form

$$l \to r \underline{\Leftarrow \phi}$$

when $l, r \in \mathrm{T}(F \bigcup G, V)$ and $\phi \in QF(G, P, V)$

- $C[l\theta] \to_R C[r\theta]$ if for any $l \to r \Leftarrow \phi \in R, C, \theta,$ $(\phi\theta)^M$ is true w.r.t a (G, P)-structure M
  - For simply, we think M is integers

Constrained TRS[2/2]

$$R = \begin{cases} f(x) & \rightarrow & g(x, 0, p(0)) & \Leftarrow & x > 0 \\ f(x) & \rightarrow & 0 & \Leftarrow & x \leq 0 \\ g(n, i, z) & \rightarrow & g(n, s(i), minus(z, f(i))) & \Leftarrow & i < n \\ g(n, i, z) & \rightarrow & z & \Leftarrow & i \geq n \\ minus(x, y) & \rightarrow & p(minus(x, p(y))) & \Leftarrow & y > 0 \\ minus(x, y) & \rightarrow & s(minus(x, s(y))) & \Leftarrow & y < 0 \\ minus(x, y) & \rightarrow & x & \Leftarrow & y = 0 \end{cases}$$

$$0^M = 0,\ s^M(x_1) = x_1 + 1,\ p^M(x_1) = x_1 - 1,\ minus^M(x_1, x_2) = x_1 - x_2$$

$f(f(0)) \rightarrow_R f(0)$ $\quad (0 \leq 0)^M$ is true

$\not\searrow_R f(g(0,0,s(0)))$ $\quad (0 > 0)^M$ is false

$\not\searrow_R 0$ $\quad f(0) \leq 0$ is not over $QF(G, P)$

Results

- We propose a method for proving termination of constrained TRSs
  - Based on DP framework
    - Dependency pair : natural extension
    - Chain : natural extension
    - Processor : proposed a new processor (using tree homomorphisms)

Dependency pairs

- Definition
  - $l^{\#} \to t^{\#} \Leftarrow \phi \in DP(R)$ iff $l \to r \Leftarrow \phi \in R$ and t is a subterm of r and $root(t)$ is a defined symbol
- Example

$$g(n,i,z) \to g(n,s(i),minus(z,f(i))) \Leftarrow i < n$$

DP

$$\begin{array}{lcll} g^{\#}(n,i,z) & \to & g^{\#}(n,s(i),minus(z,f(i))) & \Leftarrow & i<n \\ g^{\#}(n,i,z) & \to & minus^{\#}(z,f(i)) & \Leftarrow & i<n \\ g^{\#}(n,i,z) & \to & f^{\#}(i) & \Leftarrow & i<n \end{array}$$

Chains

- Definition
  - $s_1 \to t_1 \Leftarrow \phi_1, s_2 \to t_2 \Leftarrow \phi_2, \cdots \in P$ is a (P, R)-chain with θ iff for all $i = 1, 2, \cdots$,
    - $t_i\theta \xrightarrow{*}_R s_{i+1}\theta$
    - $(\phi_i\theta)^M$ is true
- Theorem
  - R is terminating iff there exists no infinite $(DP(R), R)$-chain

Tree homomorphism[1/2]

- Definition
  - A tree homomorphism is a homomorphic extension of a mapping $\mathrm{H}: F \to \mathrm{T}(F \cup G, V)$ such that
    - $\mathrm{H}(f^{\#}) \in \mathrm{T}(G, \{x_1, \cdots, x_{arity(f^{\#})}\})$
    - $\mathrm{H}(f) = f(x_1, \cdots, x_{arity(f)})$
- Example
  - If $\mathrm{H}(g^{\#}) = minus(x_1, x_3)$ then
    - $\mathrm{H}(g^{\#}(n, i, z)) = minus(n, z)$
    - $\mathrm{H}(g^{\#}(n, s(i), minus(z, f(i)))) = minus(n, minus(z, f(i)))$

Tree homomorphism[2/2]

- Lemma
  - If $s^{\#} \xrightarrow{*}_R t^{\#}$ then $\mathrm{H}(s^{\#}) \xrightarrow{*}_R \mathrm{H}(t^{\#})$
  - Illustrated by an example

    We think an example such that $\mathrm{H}(g^{\#}) = minus(x_1, x_3)$,
    $s^{\#} \equiv g^{\#}(f(0), 0, minus(s(0), 0))$ and $t^{\#} \equiv g^{\#}(0, 0, s(0))$.
    At this time, $f(0) \xrightarrow{*}_R 0$ and $minus(s(0), 0) \xrightarrow{*}_R s(0)$.
    On the other hand, $\mathrm{H}(s^{\#}) = minus(f(0), minus(s(0), 0))$
    and $\mathrm{H}(t^{\#}) = minus(0, s(0))$.
    So, $\mathrm{H}(s^{\#}) \xrightarrow{*}_R \mathrm{H}(t^{\#})$.

Order used in processor

- Monotonicity of $\geq$ is not necessary
  - Minus operator can be treated
    - R is assumed to be locally sound
- Well-foundedness of $>$ is not necessary
  - $>$ over integer can be treated
    - Lower bound of integer sequences should be specified from processor

Processor

Let $P_X = \{s \to t \Leftarrow \phi \mid X\}$ be a set of dependency pairs such that for each X of the following conditions

- A1 : $Var(\mathrm{H}(t)) \subseteq fv(\phi) \cup Var(\mathrm{H}(s))$ and $\mathrm{H}(s), \mathrm{H}(t) \in \mathrm{T}(G,V)$
- A2 : $Var(\mathrm{H}(t)) \subseteq fv(\phi)$
- B1 : $\neg\phi \vee \mathrm{H}(s) \geq \mathrm{H}(t)$ is M-valid
- B2 : $\neg\phi \vee \mathrm{H}(s) > \mathrm{H}(t)$ is M-valid
- C : $\neg\phi \vee \mathrm{H}(t) > u$ is M-valid for some $u \in \mathrm{T}(G)$

Lower bound

Processor $Proc_{\mathrm{H}}$ defined that

$$Proc_{\mathrm{H}}((P,R)) = \begin{cases} \{(P \setminus P_{A2}, R), (P \setminus P_{B2}, R), (P \setminus P_C, R)\} & \text{if } P \subseteq P_{A1} \cap P_{B1} \\ \{(P,R)\} & \text{otherwise} \end{cases}$$

Property of $P_{A1} \sim P_C$

For each $s \to t \Leftarrow \phi$ in a (P, R)-chain with θ,

$s \to t \Leftarrow \phi \in P_{A1}$: $t\theta \in \mathrm{T}(G)$ if $s\theta \in \mathrm{T}(G)$

$s \to t \Leftarrow \phi \in P_{A2}$: $t\theta \in \mathrm{T}(G)$

$s \to t \Leftarrow \phi \in P_{B1}$: $\mathrm{H}(s\theta)^M \geq \mathrm{H}(t\theta)^M$ if $s\theta, t\theta \in \mathrm{T}(G)$

$s \to t \Leftarrow \phi \in P_{B2}$: $\mathrm{H}(s\theta)^M > \mathrm{H}(t\theta)^M$ if $s\theta, t\theta \in \mathrm{T}(G)$

$s \to t \Leftarrow \phi \in P_C$: $\mathrm{H}(t\theta)^M > u^M$ for some $u \in \mathrm{T}(G)$
if $s\theta, t\theta \in \mathrm{T}(G)$

Lower bound

Local soundness

- Local soundness of R is necessary to use $Proc_{\mathrm{H}}$
- Definition
  - R is locally sound iff for all s and t,
    $s \in T(G)$ and $s \xrightarrow{*}_R t$ imply that
    - $t \in T(G)$, and
    - $s^M = t^M$ is true
- Example

If R is locally sound then

$$\begin{aligned} minus(0, s(0)) &\xrightarrow{*}_R p(0) \\ &\not\xrightarrow{*}_R 0 \\ &\not\xrightarrow{*}_R f(s(0)) \end{aligned}$$

Theorem : Soundness of $Proc_{\mathrm{H}}$

- Let R be a locally sound constrained TRS and H be a tree homomorphism. Then $Proc_{\mathrm{H}}$ is sound.
  - A DP processor $Proc$ is sound iff there exists no infinite (P,R)-chain if there exist no infinite (P',R')-chain for all $(P',R') \in Proc((P,R))$

$$Proc_{\mathrm{H}}((P,R)) = \begin{cases} \{(P \setminus P_{A2}, R), (P \setminus P_{B2}, R), (P \setminus P_C, R)\} & \\ & \text{if } P \subseteq P_{A1} \cap P_{B1} \\ \{(P,R)\} & \text{otherwise} \end{cases}$$

Proof

- If $(P,R) \in Proc_{\mathrm{H}}((P,R))$ then
  - $Proc_{\mathrm{H}}$ is clearly sound
- If $(P,R) \notin Proc_{\mathrm{H}}((P,R))$ then
  - $P_{A2} \cap P, P_{B2} \cap P, P_C \cap P$ are not emptyset
  - We show there exists no infinite (P,R)-chain by contradiction when we assume there exist no infinite $(P \setminus P_{A2}, R)$-chain, $(P \setminus P_{B2}, R)$-chain and $(P \setminus P_C, R)$-chain

Proof

$$s_i^{\#}\theta \rightarrow_P t_i^{\#}\theta \xrightarrow{*}_R s_{i+2}^{\#}\theta \rightarrow_P t_{i+2}^{\#}\theta \xrightarrow{*}_R s_{i+2}^{\#}\theta \rightarrow_P t_{i+2}^{\#}\theta \xrightarrow{*}_R$$

$$\mathrm{H}(s_i^{\#}\theta) \quad \mathrm{H}(t_i^{\#}\theta) \quad \mathrm{H}(s_{i+1}^{\#}\theta) \quad \mathrm{H}(t_{i+1}^{\#}\theta) \quad \mathrm{H}(s_{i+2}^{\#}\theta) \quad \mathrm{H}(t_{i+2}^{\#}\theta)$$

First, we assume infinite (P,R)-chain such that

- all DPs in (P,R)-chain are also in $P_{A1} \cap P_{B1}$
- there exists infinite number of DPs are in P_{A2} ,P_{B2} and P_C

Next, all terms in the (P,R)-chain apply H

Proof

$$s_i^{\#}\theta \to_P t_i^{\#}\theta \xrightarrow{*}_R s_{i+2}^{\#}\theta \to_P t_{i+2}^{\#}\theta \xrightarrow{*}_R s_{i+2}^{\#}\theta \to_P t_{i+2}^{\#}\theta \xrightarrow{*}_R$$

$$\mathrm{H}(s_i^{\#}\theta) \quad \mathrm{H}(t_i^{\#}\theta) \boxed{\xrightarrow{*}_R} \mathrm{H}(s_{i+1}^{\#}\theta) \quad \mathrm{H}(t_{i+1}^{\#}\theta) \boxed{\xrightarrow{*}_R} \mathrm{H}(s_{i+2}^{\#}\theta) \quad \mathrm{H}(t_{i+2}^{\#}\theta) \boxed{\xrightarrow{*}_R}$$

From lemma of tree homomorphism, $\mathrm{H}(t_j^{\#}\theta) \xrightarrow{*}_R \mathrm{H}(s_{j+1}^{\#}\theta)$

- Lemma of tree homomorphism
  - If $s^{\#} \xrightarrow{*}_R t^{\#}$ then $\mathrm{H}(s^{\#}) \xrightarrow{*}_R \mathrm{H}(t^{\#})$

Proof

$$\mathrm{H}(s_i^\# \theta) \quad \mathrm{H}(t_i^\# \theta) \xrightarrow{*}_R \mathrm{H}(s_{i+1}^\# \theta) \quad \mathrm{H}(t_{i+1}^\# \theta) \xrightarrow{*}_R \mathrm{H}(s_{i+2}^\# \theta) \quad \mathrm{H}(t_{i+2}^\# \theta) \xrightarrow{*}_R$$

$$\Cap$$

$$\mathrm{T}(G)$$

From property of P_{A2} , $\mathrm{H}(t_i^\# \theta) \in \mathrm{T}(G)$ for some i because there exists infinite number of DPs are in P_{A2}

- Property of P_{A2}
  - For each $s \to t \Leftarrow \phi$ in a (P, R)-chain with θ ,
    $s \to t \Leftarrow \phi \in P_{A2}$: $\mathrm{H}(t\theta) \in \mathrm{T}(G)$

Proof

$$\mathrm{H}(s_i^{\#}\theta) \quad \mathrm{H}(t_i^{\#}\theta) \xrightarrow{*}_R \mathrm{H}(s_{i+1}^{\#}\theta) \quad \mathrm{H}(t_{i+1}^{\#}\theta) \xrightarrow{*}_R \mathrm{H}(s_{i+2}^{\#}\theta) \quad \mathrm{H}(t_{i+2}^{\#}\theta) \xrightarrow{*}_R$$

$$\Cap \qquad\qquad \Cap$$

$$\mathrm{T}(G) \qquad\qquad \mathrm{T}(G)$$

From local soundness of R , $\mathrm{H}(s_{i+1}^{\#}\theta) \in \mathrm{T}(G)$

- Local soundness of R
  - for all s and t , $s \in T(G)$ and $s \xrightarrow{*}_R t$ imply that
    - $t \in T(G)$
    - $s^M = t^M$ is true

Proof

$$\mathrm{H}(s_i^{\#}\theta) \quad \mathrm{H}(t_i^{\#}\theta) \xrightarrow{*}_R \mathrm{H}(s_{i+1}^{\#}\theta) \quad \mathrm{H}(t_{i+1}^{\#}\theta) \xrightarrow{*}_R \mathrm{H}(s_{i+2}^{\#}\theta) \quad \mathrm{H}(t_{i+2}^{\#}\theta) \xrightarrow{*}_R$$

$$\Cap \qquad\qquad \Cap \qquad\qquad \Cap$$

$$\mathrm{T}(G) \qquad \mathrm{T}(G) \qquad \mathrm{T}(G)$$

From property of P_{A1} , $\mathrm{H}(t_{i+1}^{\#}\theta) \in \mathrm{T}(G)$
because all DPs in (P, R)-chain are also in $P_{A1} \cap P_{B1}$

- Property of P_{A1}
  - For each $s \to t \Leftarrow \phi$ in a (P, R)-chain with θ ,
    $s \to t \Leftarrow \phi \in P_{A1}$: $\mathrm{H}(t\theta) \in \mathrm{T}(G)$ if $\mathrm{H}(s\theta) \in \mathrm{T}(G)$

Proof

$$\mathrm{H}(s_i^{\#}\theta) \quad \mathrm{H}(t_i^{\#}\theta) \xrightarrow{*}{}_R \mathrm{H}(s_{i+1}^{\#}\theta) \quad \mathrm{H}(t_{i+1}^{\#}\theta) \xrightarrow{*}{}_R \mathrm{H}(s_{i+2}^{\#}\theta) \quad \mathrm{H}(t_{i+2}^{\#}\theta) \xrightarrow{*}{}_R$$

$$\begin{array}{ccccccc} \Cap & & \Cap & & \Cap & \Cap & \Cap \\ \mathrm{T}(G) & & \mathrm{T}(G) & & \mathrm{T}(G) & \mathrm{T}(G) & \mathrm{T}(G) \quad \cdots \end{array}$$

From property of P_{A1} and local soundness of R ,
$\mathrm{H}(s_j^{\#}), \mathrm{H}(t_j^{\#}) \in \mathrm{T}(G)$ for all $j > i$

Proof

$$\mathrm{H}(s_i^{\#}\theta) \quad \mathrm{H}(t_i^{\#}\theta) \xrightarrow{*}_R \mathrm{H}(s_{i+1}^{\#}\theta) \quad \mathrm{H}(t_{i+1}^{\#}\theta) \xrightarrow{*}_R \mathrm{H}(s_{i+2}^{\#}\theta) \quad \mathrm{H}(t_{i+2}^{\#}\theta) \xrightarrow{*}_R$$

$$\Cap \qquad \Cap \qquad \Cap \qquad \Cap \qquad \Cap$$

$$\mathrm{T}(G) \qquad \mathrm{T}(G) \qquad \mathrm{T}(G) \qquad \mathrm{T}(G) \qquad \mathrm{T}(G)$$

$$H(s_i\theta) \quad H(t_i\theta)^M = H(s_{i+1}\theta)^M \quad H(t_{i+1}\theta)^M = H(s_{i+2}\theta)^M \quad H(t_{i+2}\theta)^M =$$

From local soundness of R, $\mathrm{H}(t_j^{\#}\theta)^M = \mathrm{H}(s_{j+1}^{\#}\theta)^M$ for all $j \geq i$

- Local soundness of R
  - for all s and t, $s \in T(G)$ and $s \xrightarrow{*}_R t$ imply that
    - $t \in T(G)$
    - $s^M = t^M$ is true

Proof

$$\mathrm{H}(s_i^{\#}\theta) \quad \mathrm{H}(t_i^{\#}\theta) \xrightarrow{*}{}_R \mathrm{H}(s_{i+1}^{\#}\theta) \quad \mathrm{H}(t_{i+1}^{\#}\theta) \xrightarrow{*}{}_R \mathrm{H}(s_{i+2}^{\#}\theta) \quad \mathrm{H}(t_{i+2}^{\#}\theta) \xrightarrow{*}{}_R$$

$$\Cap \qquad \Cap \qquad \Cap \qquad \Cap \qquad \Cap$$

$$\mathrm{T}(G) \qquad \mathrm{T}(G) \qquad \mathrm{T}(G) \qquad \mathrm{T}(G) \qquad \mathrm{T}(G)$$

$$H(s_i\theta) \quad H(t_i\theta)^M = H(s_{i+1}\theta)^M \quad H(t_{i+1}\theta)^M = H(s_{i+2}\theta)^M \quad H(t_{i+2}\theta)^M =$$

If $\xrightarrow{*}_R$ is transformed into $\geq$, monotonicity of $\geq$ is necessary because rewriting position is not root.
However, $\xrightarrow{*}_R$ is transformed into $=$ now, so monotonicity of $\geq$ is not necessary.
Instead, monotonicity of $=$ is necessary, but it is clear.

Proof

$$\begin{array}{ccccccccc} \mathrm{H}(s_i^{\#}\theta) & \mathrm{H}(t_i^{\#}\theta) \xrightarrow{*}_R & \mathrm{H}(s_{i+1}^{\#}\theta) & \mathrm{H}(t_{i+1}^{\#}\theta) \xrightarrow{*}_R & \mathrm{H}(s_{i+2}^{\#}\theta) & \mathrm{H}(t_{i+2}^{\#}\theta) \xrightarrow{*}_R \\ & \Cap & \Cap & \Cap & \Cap & \Cap \\ & \mathrm{T}(G) & \mathrm{T}(G) & \mathrm{T}(G) & \mathrm{T}(G) & \mathrm{T}(G) \end{array}$$

$$H(s_i\theta) \quad H(t_i\theta)^M = H(s_{i+1}\theta)^M \boxed{\geq} H(t_{i+1}\theta)^M = H(s_{i+2}\theta)^M \boxed{\geq} H(t_{i+2}\theta)^M =$$

From property of P_{B1}, $\mathrm{H}(s_j^{\#}\theta)^M \geq \mathrm{H}(t_j^{\#}\theta)^M$ for all $j > i$ because all DPs in (P,R)-chain are also in $P_{A1} \cap P_{B1}$

- Property of P_{B1}
  - For each $s \to t \Leftarrow \phi$ in a (P,R)-chain with θ,
    $s \to t \Leftarrow \phi \in P_{B1}$: $\mathrm{H}(s\theta)^M \geq \mathrm{H}(t\theta)^M$
    if $\mathrm{H}(s\theta), \mathrm{H}(t\theta) \in \mathrm{T}(G)$

Proof

$$\mathrm{H}(s_i^{\#}\theta) \quad \mathrm{H}(t_i^{\#}\theta) \xrightarrow{*}{}_R \mathrm{H}(s_{i+1}^{\#}\theta) \quad \mathrm{H}(t_{i+1}^{\#}\theta) \xrightarrow{*}{}_R \mathrm{H}(s_{i+2}^{\#}\theta) \quad \mathrm{H}(t_{i+2}^{\#}\theta) \xrightarrow{*}{}_R$$

$$\Cap \qquad \Cap \qquad \Cap \qquad \Cap \qquad \Cap$$

$$\mathrm{T}(G) \qquad \mathrm{T}(G) \qquad \mathrm{T}(G) \qquad \mathrm{T}(G) \qquad \mathrm{T}(G)$$

$$H(s_i\theta) \quad H(t_i\theta)^M = H(s_{i+1}\theta)^M > H(t_{i+1}\theta)^M = H(s_{i+2}\theta)^M \geq H(t_{i+2}\theta)^M =$$

From property of P_{B2}, there exist infinite number of $j > i$ such that $\mathrm{H}(s_j^{\#}\theta)^M > \mathrm{H}(t_j^{\#}\theta)^M$ because there exists infinite number of DPs are in P_{B2}

- Property of P_{B2}
  - For each $s \to t \Leftarrow \phi$ in a (P, R)-chain with θ ,
    $s \to t \Leftarrow \phi \in P_{B2}$: $\mathrm{H}(s\theta)^M > \mathrm{H}(t\theta)^M$
    if $\mathrm{H}(s\theta), \mathrm{H}(t\theta) \in \mathrm{T}(G)$

Proof

$$\begin{array}{ccccccccccc} \mathrm{H}(s_i^{\#}\theta) & \mathrm{H}(t_i^{\#}\theta) & \xrightarrow{*}_R & \mathrm{H}(s_{i+1}^{\#}\theta) & \mathrm{H}(t_{i+1}^{\#}\theta) & \xrightarrow{*}_R & \mathrm{H}(s_{i+2}^{\#}\theta) & \mathrm{H}(t_{i+2}^{\#}\theta) & \xrightarrow{*}_R \\ & \Cap & & \Cap & \Cap & & \Cap & \Cap & \\ & \mathrm{T}(G) & & \mathrm{T}(G) & \mathrm{T}(G) & & \mathrm{T}(G) & \mathrm{T}(G) & \end{array}$$

$$H(s_i\theta) \quad H(t_i\theta)^M = H(s_{i+1}\theta)^M > H(t_{i+1}\theta)^M = H(s_{i+2}\theta)^M \geq H(t_{i+2}\theta)^M =$$

$$\underset{u^M}{\vee}$$

From property of P_C , there exist infinite number of $j > i$ such that $\mathrm{H}(t_j^{\#}\theta)^M > u^M$

because there exists infinite number of DPs are in P_C

- Property of P_C
  - For each $s \to t \Leftarrow \phi$ in a (P, R)-chain with θ ,

    $s \to t \Leftarrow \phi \in P_C$: $\mathrm{H}(t\theta)^M > u^M$ for some $u \in \mathrm{T}(G)$

    if $\mathrm{H}(s\theta), \mathrm{H}(t\theta) \in \mathrm{T}(G)$

Proof

$$H(s_i\theta) \quad H(t_i\theta)^M = H(s_{i+1}\theta)^M > H(t_{i+1}\theta)^M = H(s_{i+2}\theta)^M \geq \underset{\substack{\vee \\ u^M}}{H(t_{i+2}\theta)^M} =$$

Infinite (P,R)-chain is transformed into a integer decreasing sequence such that all integers in the sequence are greater than u^M. However, there exists no such sequence.

So there exists no infinite (P,R)-chain.

Note

- M is not restricted to integers if
  - $\succ$ over M is transitive
  - $\succ$ and $\succeq$ over M are compatible
  - $\succ$ over M is Non-Infinitesimal

  - Non-Infinitesimal [Giesl et.al. 07]
    - There don't exist any $t, s_0, s_1, \ldots$ with $s_i \succ s_{i+1}$ and $s_i \succ t$ for all i

Conclusion

- We have proposed proving method of termination on constrained TRSs
  - Based on DP framework
  - Proposed new processor
- We have proved soundness of processor