Certification of Decreasing Diagrams

Progress Report

Harald Zankl

Institute of Computer Science
University of Innsbruck
Austria

Seminar 3 April 18, 2012

Quiz

Wikimedia

Overview

- Preliminaries
- Decreasing Diagrams
- Conclusion

Preliminaries

Definition (ARS)

$\mathcal{A} = (A, \rightarrow)$

Definition (confluence)

${}^{*}\!\leftarrow \cdot \rightarrow^{*} \subseteq \rightarrow^{*} \cdot {}^{*}\!\leftarrow$

Definition (local confluence)

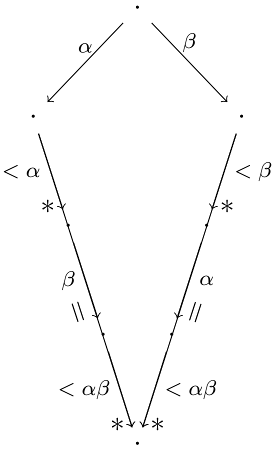
$\leftarrow \cdot \rightarrow \subseteq \rightarrow^{*} \cdot {}^{*}\!\leftarrow$

Theorem (Newman, 1942 & van Oostrom, 1994)

local confluence & termination $\longrightarrow$ *confluence*

local confluence & decreasingness $\longrightarrow$ *confluence*

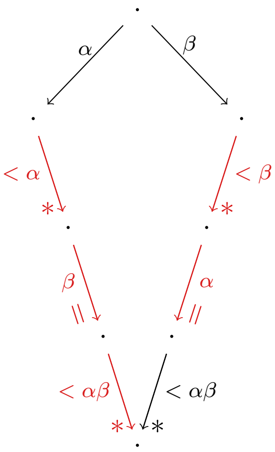
Decreasing Diagrams

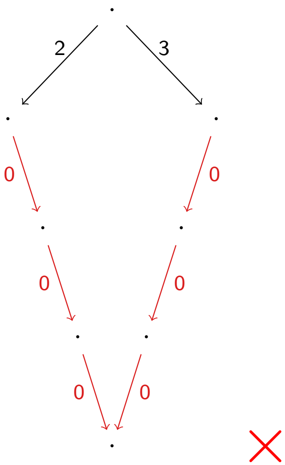


Definition (local decreasing)

$$ {}_{\alpha}\!\leftarrow \cdot \rightarrow_{\beta} \;\subseteq\; \overset{\vee}{\rightarrow}{}^{*}_{\alpha} \cdot \rightarrow^{=}_{\beta} \cdot \overset{\vee}{\rightarrow}{}^{*}_{\alpha\beta} \cdot {}^{*}_{\alpha\beta}\!\overset{\vee}{\leftarrow} \cdot {}^{=}_{\alpha}\!\leftarrow \cdot {}^{*}_{\beta}\!\overset{\vee}{\leftarrow} $$

Decreasing Diagrams – Examples





Formalization & Certification

Demo

Certification

- proof checking by trustable program
- theorem prover – generated program
- Isabelle/HOL

Formalization

- formalize notions in theorem prover (definitions, etc.)
- prove theorems in theorem prover

Bibliography

V. van Oostrom, Confluence by Decreasing Diagrams, TCS 126, 259–280, 1994.

Lemma A.3

1. Intersection and union constitute a distributive lattice ?
2. Sum is commutative and associative. It has $\varnothing$ as neutral element ✓
3. Sum distributes over intersection ✓
4. $S \cap (M \uplus N) = (S \cap M) \uplus (S \cap N)$ ✓
5. $M \cap (N - S) = (M \cap N) - (M \cap S)$ ✓
6. $(M \cap N) - X = (M - X) \cap (N - X)$ ✓
7. $(S \uplus M) - N = (S - N) \uplus (M - N)$ ✓
8. $(M \uplus N) - S = (M - S) \uplus (N - S)$ ✓
9. $(M - N) - X = M - (N \uplus X)$ ✓
10. $M = (M \cap N) \uplus (M - N)$ ✓
11. $(M - N) \cap S = (M \cap S) - N$ ✓

Definition 2.5

1. $\Upsilon\alpha := \{\beta \mid \beta \prec \alpha\}$ ✓
2. $M \prec_{mul} N$ if $\exists X, Y, Z\ M = Z \uplus X, N = Z \uplus Y, X \subseteq \Upsilon Y,\ Y \neq \varnothing$ ✓

- $\prec$ well-founded $\Rightarrow$ $\prec_{mul}$ well-founded ✓

Lemma 2.6

1. Taking the down-set distributes over union and sum.
   $\Upsilon(M - N) \supseteq \Upsilon M - \Upsilon N$ ✓
2. $M \subseteq N \Rightarrow M \preceq_{mul} N \Rightarrow \Upsilon M \subseteq \Upsilon N$ ✓
3. X, Y in Def 2.5 disjoint (finite multisets) ✓(more or less)
4. If $G \neq \varnothing$, then $F \subseteq \Upsilon G \Rightarrow F \prec_{mul} G$ ✓
5. If $\Upsilon S \subseteq S$, then $F \preceq_{mul} G \Leftrightarrow F - S \preceq_{mul} G - S$ ✓
6. If $H \subseteq F, G$, then $F \preceq_{mul} G \Leftrightarrow F - H \preceq_{mul} G - H$?
7. If $H \subseteq \Upsilon G - \Upsilon F$, then $F \preceq_{mul} G \Leftrightarrow F \uplus H \preceq_{mul} G$ ✓($\Rightarrow$), ?($\Leftarrow$)

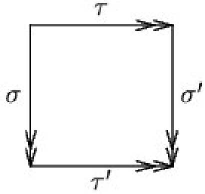
Definition 3.1

- $|\varepsilon| := []$ ✓
- $|\alpha\sigma| := [\alpha] \uplus (|\sigma| - \Upsilon\alpha)$ ✓

Lemma 3.2

1. $\Upsilon|\sigma| = \Upsilon\sigma$ ✓
2. $|\sigma\tau| = |\sigma| \uplus (|\tau| - \Upsilon\sigma)$ ✓

Definition 3.3 (decreasing)



D decreasing $:\Leftrightarrow |\sigma\tau'| \preceq_{mul} |\tau| \uplus |\sigma| \succeq_{mul} |\tau\sigma'|$ ✓

Lemma hidden in Definition 3.3

D decreasing $\Leftrightarrow |\tau'| - \Upsilon\sigma \preceq_{mul} |\tau|$ & $|\sigma| \succeq_{mul} |\sigma'| - \Upsilon\tau$ ✓

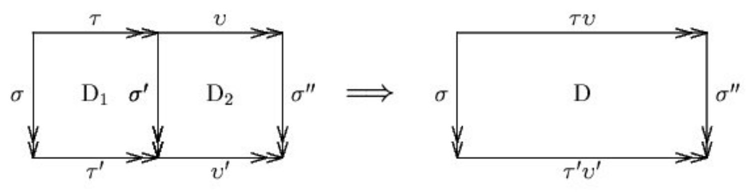
Proposition 3.4

locally decreasing diagram is

$$ {}_{\alpha}\!\leftarrow \cdot \rightarrow_{\beta} \;\subseteq\; \overset{\vee}{\rightarrow}{}^{*}_{\alpha} \cdot \rightarrow^{=}_{\beta} \cdot \overset{\vee}{\rightarrow}{}^{*}_{\alpha\beta} \cdot {}^{*}_{\alpha\beta}\overset{\vee}{\leftarrow} \cdot {}^{=}_{\alpha}\!\leftarrow \cdot {}^{*}_{\beta}\overset{\vee}{\leftarrow} $$

?

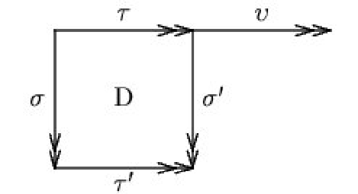
Lemma 3.5 (pasting preserves decreasingness)



✓(one page paper proof)

Lemma 3.6 (pasting is hypothesis decreasing)

If τ is non-empty and



then $|\sigma'| \uplus |\nu| \prec_{mul} |\sigma| \uplus |\tau\nu|$ ✓

Theorem 3.7 (main theorem)

ARS $\mathcal{A} = (A, \langle \rightarrow_\alpha \rangle_{\alpha \in I})$ and well-founded partial order $\prec$ on I. Let I_v and I_h be (not necessarily disjoint) subsets of I, with $\rightarrow_v := \bigcup_{\alpha \in I_v} \rightarrow_\alpha$ and $\rightarrow_h := \bigcup_{\beta \in I_v} \rightarrow_\beta$. If, for all $\alpha \in I_v$ and $\beta \in I_h$ we have local decreasingness, then $\rightarrow_v$ commutes with $\rightarrow_h$ (i.e., $\rightarrow$ is confluent). ✗

Future Work

Open Issues

- prove Theorem 3.7 (for labels)
- lift from labels to rewrite steps (ARSs)
- lift from ARSs to TRSs
- formalize
    - modularity (Toyama 1987)
    - Newman's lemma (Newman 1943)
    - rule labeling (van Oostrom 2008)
    - relative termination labeling (Hirokawa & Middeldorp 2010/2012)
    - incremental labeling (Zankl et al. 2011)
    - ...
- certify CSI output

Quiz

Google Maps

C S I