Introduction to Term Rewriting

lecture 2

Aart Middeldorp and Femke van Raamsdonk

Institute of Computer Science
University of Innsbruck

Department of Computer Science
VU Amsterdam

Sunday

introduction, examples, abstract rewriting, equational reasoning, term rewriting

Monday

termination, completion

Tuesday

completion, termination

Wednesday

confluence, modularity, strategies

Thursday

exam, advanced topics

Outline

Motivation

concrete rewrite formalisms

- string rewriting
- term rewriting
- graph rewriting
- λ-calculus
- interaction nets
- . . .

abstract rewriting

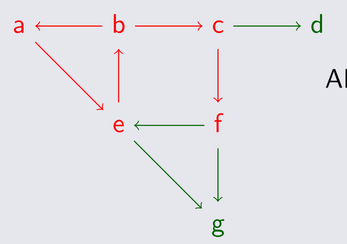
- no structure on objects that are rewritten
- uniform presentation of properties and proofs

Outline

- Abstract Rewrite Systems
  - Definitions
  - Properties
  - Relationships
- Newman's Lemma
- Multiset Orders
- Further Reading

Definitions

- abstract rewrite system (ARS) is set A equipped with binary relation $\rightarrow$



ARS $\mathcal{A} = \langle A, \rightarrow \rangle$

- $A = \{a, b, c, d, e, f, g\}$
- $\rightarrow = \begin{Bmatrix} (a,e),(b,a),(b,c),(c,d),(c,f) \\ (e,b),(e,g),(f,e),(f,g) \end{Bmatrix}$

- rewrite sequence
  - finite $\quad a \rightarrow e \rightarrow b \rightarrow c \rightarrow f$
  - empty $\quad a$
  - infinite $\quad a \rightarrow e \rightarrow b \rightarrow a \rightarrow e \rightarrow b \rightarrow \cdots$

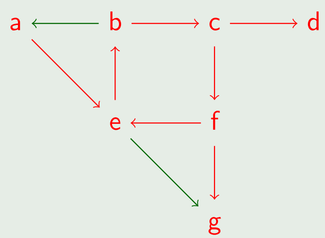
Definition (Derived Relations of $\to$)

- $\leftarrow$ inverse of $\to$
- $\to^*$ transitive and reflexive closure of $\to$
- ${}^*\!\leftarrow$ inverse of $\to^*$ (transitive and reflexive closure of $\leftarrow$)
- $\downarrow$ joinability $\downarrow\; = \;\to^* \cdot {}^*\!\leftarrow$
- $\leftrightarrow$ symmetric closure of $\to$
- $\leftrightarrow^*$ conversion (equivalence relation generated by $\to$)
- $\to^+$ transitive closure of $\to$
- $\to^=$ reflexive closure of $\to$
- $\uparrow$ meetability $\uparrow\; = \;{}^*\!\leftarrow \cdot \to^*$

Terminology

- if $x \to^* y$ then x rewrites to y and y is reduct of x
- if $x \to^* z \;{}^*\!\leftarrow y$ then z is common reduct of x and y
- if $x \leftrightarrow^* y$ then x and y are convertible

Example

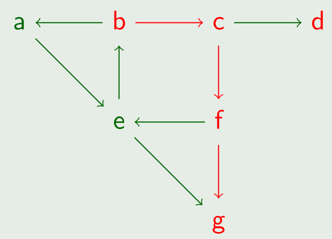


- a $\to^*$ f
- e $\downarrow$ f f $\downarrow$ d not g $\downarrow$ d
- g $\leftrightarrow^*$ d

Definition (Normal Forms)

- normal form is element x such that $x \not\to y$ for all y
- $\mathsf{NF}(\mathcal{A})$ denotes set of normal forms of ARS $\mathcal{A}$
- $x \to^! y$ if $x \to^* y$ for normal form y (x has normal form y)

Example



ARS $\mathcal{A} = \langle A, \to \rangle$

- d is normal form
- $\mathsf{NF}(\mathcal{A}) = \{\mathsf{d}, \mathsf{g}\}$
- $\mathsf{b} \to^! \mathsf{g}$

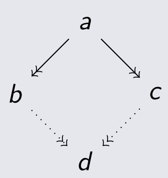
Outline

Definitions

- SN strong normalization termination
  - no infinite rewrite sequences
- WN weak normalization
  - every element has at least one normal form
  - $\forall a \, \exists b \quad a \to^! b$
- UN unique normal forms
  - no element has more than one normal form
  - $\forall a, b, c$ if $a \to^! b$ and $a \to^! c$ then $b = c$
  - ${}^!\!\leftarrow \cdot \to^! \ \subseteq \ =$

Definitions

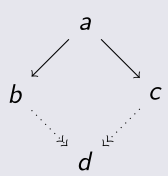
- CR confluence Church-Rosser property
  - $\uparrow \ \subseteq \ \downarrow$
  - $\forall a, b, c$



$\exists d$

Wikimedia

- WCR local confluence weak Church-Rosser property
  - $\leftarrow \cdot \to \ \subseteq \ \downarrow$
  - $\forall a, b, c$



in diagrams: $\twoheadrightarrow$ for $\to^*$

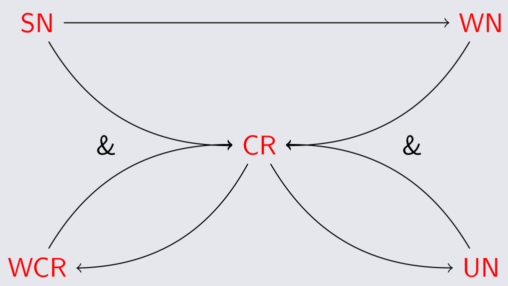
$\exists d$

Outline

Lemmata

1. SN $\Longrightarrow$ WN
2. SN $\not\Longleftarrow$ WN $\circlearrowleft a \longrightarrow b$
3. CR $\iff$ $\leftrightarrow^* \subseteq \downarrow$ $\iff$ $\leftrightarrow^* = \downarrow$
4. CR $\Longrightarrow$ UN
5. CR $\not\Longleftarrow$ UN $\circlearrowleft a \longleftarrow b \longrightarrow c$
6. WN & UN $\Longrightarrow$ CR
7. CR $\Longrightarrow$ WCR
8. CR $\not\Longleftarrow$ WCR $a \longleftarrow b \rightleftarrows c \longrightarrow d$
9. SN & WCR $\Longrightarrow$ CR Newman's Lemma

Summary

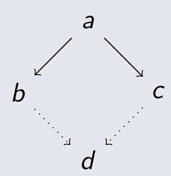


Definitions

- semi-completeness
  - CR & WN
  - every element has unique normal form
- completeness
  - CR & SN

Definition

- diamond property $\diamond$
  - $\leftarrow \cdot \rightarrow \ \subseteq \ \rightarrow \cdot \leftarrow$
  - $\forall a, b, c$



$\exists d$

Lemma

ARS $\mathcal{A} = \langle A, \rightarrow \rangle$ *is confluent if* $\rightarrow \ \subseteq \rightarrow_{\diamond} \subseteq \ \rightarrow^{*}$ *for some relation* $\rightarrow_{\diamond}$ *on* A *with diamond property*

Outline

- Abstract Rewrite Systems
- Newman's Lemma
- Multiset Orders
- Further Reading

Well-Founded Induction

given

- property P of ARSs that satisfies $\mathsf{P}(\mathcal{A}) \iff \forall a\colon \mathsf{P}(a)$
- strongly normalizing ARS $\mathcal{A} = \langle A, \to \rangle$

to conclude

- $\mathsf{P}(\mathcal{A})$

it is sufficient to prove

- if $\underbrace{\mathsf{P}(b) \text{ for every } b \text{ with } a \to b}_{\text{induction hypothesis}}$ then $\mathsf{P}(a)$

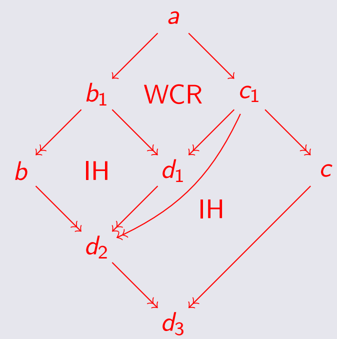
for arbitrary element a

$$\Big(\forall a\colon \big(\forall b\colon a \to b \implies \mathsf{P}(b)\big) \implies \mathsf{P}(a)\Big) \implies \forall a\colon \mathsf{P}(a)$$

Newman's Lemma

SN($\mathcal{A}$) & WCR($\mathcal{A}$) $\implies$ CR($\mathcal{A}$)

First Proof



induction hypothesis CR(b_1) & CR(c_1)

$\forall a'$: if $a \to a'$ then CR(a')

Outline

Definitions (Multiset)

- finite multiset M over A is function from A to $\mathbb{N}$ such that $M(a) = 0$ for all but finitely many $a \in A$
- $M(a)$ is multiplicity of a
- set of all finite multisets over A is denoted by $\mathcal{M}(A)$

Example

$\{a, a, a, b, d, d, d\} \in \mathcal{M}(\{a, b, c, d\})$:

$$a \mapsto 3 \qquad b \mapsto 1 \qquad c \mapsto 0 \qquad d \mapsto 3$$

Definitions (Operations on Multisets)

- sum $\forall a\colon (M_1 \uplus M_2)(a) = M_1(a) + M_2(a)$
- difference $\forall a\colon (M_1 - M_2)(a) = \max\{M_1(a) - M_2(a), 0\}$
- ...

Example

- $\{a, a, a, b, d, d, d\} \uplus \{a, c, c\} = \{a, a, a, a, b, c, c, d, d, d\}$
- $\{a, a, a, b, d, d, d\} - \{a, c, c\} = \{a, a, b, d, d, d\}$

Definition

multiset extension of proper order $>$ on A is relation $>_{\text{mul}}$ defined on $\mathcal{M}(A)$ as follows: $M_1 >_{\text{mul}} M_2$ if $\exists X, Y \in \mathcal{M}(A)$ such that

- $M_2 = (M_1 - X) \uplus Y$
- $\varnothing \neq X \subseteq M_1$
- $\forall y \in Y\ \exists x \in X : x > y$

Example

$$\{2,3\} >_{\text{mul}} \{0,1,3\} >_{\text{mul}} \{0,1,1,2,2,2\} >_{\text{mul}} \{0,1,1,0,1,1,2,2\}$$
$$>_{\text{mul}} \{0,1,0,1,1,2,2\} >_{\text{mul}} \{0,1,0,1,0,0,2\} >_{\text{mul}} \{1,1,1,1,1,1\}$$
$$>_{\text{mul}} \{1,1,1,1\} >_{\text{mul}} \{0,0,0,0,1,1,1\} >_{\text{mul}} \cdots$$

Theorem

- *multiset extension of proper order is proper order*
- *multiset extension of well-founded order is well-founded*

Newman's Lemma

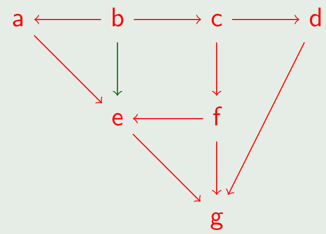
$\mathrm{SN}(\mathcal{A})$ & $\mathrm{WCR}(\mathcal{A}) \implies \mathrm{CR}(\mathcal{A})$

Second Proof

- given $b\ {}^*\!\leftarrow a \rightarrow^* c$
- construct sequence of conversions $(C_i)_{i \geqslant 0}$ between b and c
  - C_0 is initial conversion $b\ {}^*\!\leftarrow a \rightarrow^* c$
  - C_{i+1} is obtained from C_i by replacing peak $e \leftarrow d \rightarrow f$ in C_i by valley $e \rightarrow^* \cdot\ {}^*\!\leftarrow f$
- $|C_i|$ is multiset of elements appearing in C_i
- $|C_i|\ (\rightarrow^+)_{\text{mul}}\ |C_{i+1}|$
- $(\rightarrow^+)_{\text{mul}}$ is well-founded
- hence $\exists n$ such that C_n has no peaks $\implies C_n : b \rightarrow^* \cdot\ {}^*\!\leftarrow c$

Example

- ARS



- conversion

conversion	multiset	
$a \leftarrow b \rightarrow c \rightarrow d$	$\{a, b, c, d\}$	
$a \rightarrow e \leftarrow f \leftarrow c \rightarrow d$	$\{a, e, f, c, d\}$	
$a \rightarrow e \leftarrow f \rightarrow g \leftarrow d$	$\{a, e, f, g, d\}$	
$a \rightarrow e \rightarrow g \leftarrow d$	$\{a, e, g, d\}$	rewrite proof

Outline

- Abstract Rewrite Systems
- Newman's Lemma
- Multiset Orders
- Further Reading

Confluent Reductions: Abstract Properties and Applications to Term Rewriting Systems
Gérard Huet
JACM 27(4), pp. 797 – 821, 1980

Proving Termination with Multiset Orderings
Nachum Dershowitz and Zohar Manna
CACM 22(8), pp. 465 – 476, 1979

Confluence by Decreasing Diagrams
Vincent van Oostrom
TCS 126(2), pp. 259 – 280, 1994