# Term Rewriting

Philipp Dablander and **Aart Middeldorp**

# Outline

## Definitions

- $\mathcal{T}(\mathcal{F},\mathcal{V})$ is set of terms built from signature (function symbols with arities) $\mathcal{F}$ and infinitely many variables $\mathcal{V}$ with $\mathcal{F} \cap \mathcal{V} \neq \varnothing$
- context is term with one hole: element of $\mathcal{T}(\mathcal{F} \cup \{\square\},\mathcal{V})$ that contains exactly one occurrence of special constant $\square$
- $C[t]$ denotes result of replacing hole in context $C$ by term $t$
- binary relation $R$ on terms is closed under contexts if for all terms $s$, $t$

$$s\ R\ t \quad\Longrightarrow\quad C[s]\ R\ C[t] \quad \text{for all contexts } C$$

- substitution is mapping $\sigma \colon \mathcal{V} \to \mathcal{T}(\mathcal{F},\mathcal{V})$ such that its domain

$$\mathcal{D}\mathrm{om}(\sigma) = \{x \in \mathcal{V} \mid \sigma(x) \neq x\}$$

is finite

## Definitions

- application of substitution $\sigma$ to term $t$

$$t\sigma = \begin{cases} \sigma(t) & \text{if } t \in \mathcal{V} \\ f(t_1\sigma, \dots, t_n\sigma) & \text{if } t = f(t_1, \dots, t_n) \end{cases}$$

- binary relation $R$ on terms is closed under substitutions if for all terms $s$, $t$

$$s \; R \; t \quad \Longrightarrow \quad s\sigma \; R \; t\sigma \quad \text{for all substitutions } \sigma$$

## Theorem

matching problem

instance: terms $s$, $t$

question: $\exists$ substitution $\sigma$: $s\sigma = t$ ? ($t$ is instance of $s$, $t \geq s$)

is decidable (in linear time)

# Outline

## Motivation

concrete rewrite formalisms

- string rewriting
- term rewriting
- graph rewriting
- $\lambda$–calculus
- interaction nets
- $\cdots$

abstract rewriting

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

# Outline

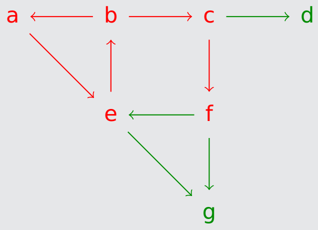
## Definitions (Abstract Rewrite System)

- abstract rewrite system (ARS) is set $A$ equipped with binary relation $\rightarrow$
- elements of $\rightarrow$ are called rewrite steps
- (finite) rewrite sequence is sequence of $(a_0, \ldots, a_n)$ such that $a_i \rightarrow a_{i+1}$ for all $0 \leqslant i < n$

## Example

- ARS $\mathcal{A} = \langle A, \rightarrow \rangle$ with $A = \{\mathsf{a}, \mathsf{b}, \mathsf{c}, \mathsf{d}, \mathsf{e}, \mathsf{f}, \mathsf{g}\}$ and

$$\rightarrow = \left\{ \begin{matrix} (\mathsf{a},\mathsf{e}), (\mathsf{b},\mathsf{a}), (\mathsf{b},\mathsf{c}), (\mathsf{c},\mathsf{d}), (\mathsf{c},\mathsf{f}) \\ (\mathsf{e},\mathsf{b}), (\mathsf{e},\mathsf{g}), (\mathsf{f},\mathsf{e}), (\mathsf{f},\mathsf{g}) \end{matrix} \right\}$$




- rewrite sequences
  - finite $\mathsf{a} \rightarrow \mathsf{e} \rightarrow \mathsf{b} \rightarrow \mathsf{c} \rightarrow \mathsf{f}$
  - empty $\mathsf{a}$
  - infinite $\mathsf{a} \rightarrow \mathsf{e} \rightarrow \mathsf{b} \rightarrow \mathsf{a} \rightarrow \mathsf{e} \rightarrow \mathsf{b} \rightarrow \cdots$

## Definitions (Derived Relations)

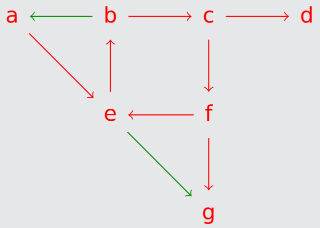
- $\leftarrow$ inverse of $\rightarrow$
- $\rightarrow^*$ transitive and reflexive closure of $\rightarrow$
- ${}^*\!\leftarrow$ inverse of $\rightarrow^*$
- $\downarrow$ joinability $\downarrow \; = \; \rightarrow^* \cdot {}^*\!\leftarrow$
- $\leftrightarrow$ symmetric closure of $\rightarrow$
- $\leftrightarrow^*$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

$\cdot$ denotes relation composition: $R \cdot S = \{(a, c) \mid a \; R \; b \text{ and } b \; S \; c\}$

## 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



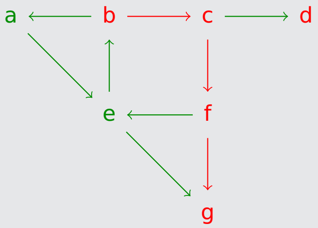

- $\mathsf{a} \to^* \mathsf{f}$
- $\mathsf{e} \downarrow \mathsf{f}$ $\quad$ $\mathsf{f} \downarrow \mathsf{d}$ $\quad$ $\mathsf{g} \not\downarrow \mathsf{d}$
- $\mathsf{g} \leftrightarrow^* \mathsf{d}$

## Definitions (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
- $\mathsf{NF}(\mathcal{A}) = \{\mathsf{d}, \mathsf{g}\}$
- $\mathsf{b} \to^{!} \mathsf{g}$



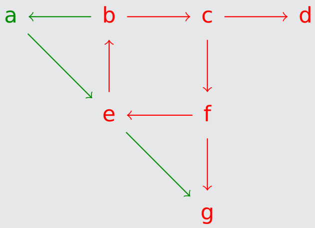
# Outline

## Definitions (Properties)

- SN strong normalization termination
  - no infinite rewrite sequences
- WN (weak) normalization
  - every element has at least one normal form
  - $\forall\, a\, \exists\, b \;\; a \to^! b$
- 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 $b = c$
  - ${}^!\!\leftarrow \cdot \to^! \;\subseteq\; =$

## Example

- ARS $\mathcal{A} = \langle A, \rightarrow \rangle$
- not SN: $\mathsf{b} \rightarrow^{+} \mathsf{b}$
- WN
- not UN: $\mathsf{c} \rightarrow^{!} \mathsf{d}$ and $\mathsf{c} \rightarrow^{!} \mathsf{g}$
- not CR: $\mathsf{d} \uparrow \mathsf{g}$ and $\mathsf{d} \not\downarrow \mathsf{g}$
- WCR



## Definitions (Properties)

- CR confluence
  - $\uparrow \subseteq \downarrow$
  - $\forall\, a, b, c$ $\exists\, d$

$$\begin{array}{ccc} & a & \\ {}^{*}\swarrow & & \searrow{}^{*} \\ b & & c \\ {}^{*}\searrow & & \swarrow{}^{*} \\ & d & \end{array}$$

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

Wikimedia

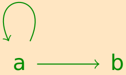
- WCR local confluence weak Church–Rosser property
  - $\leftarrow \cdot \rightarrow \subseteq \downarrow$
  - $\forall\, a, b, c$ $\exists\, d$

$$\begin{array}{ccc} & a & \\ \swarrow & & \searrow \\ b & & c \\ \searrow{}^{*} & & \swarrow{}^{*} \\ & d & \end{array}$$

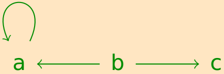
# Outline

## Lemmata

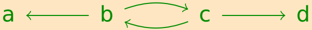
- SN $\Longrightarrow$ WN
- WN $\not\Longrightarrow$ SN




- CR $\Longleftrightarrow$ $\leftrightarrow^* \subseteq \downarrow$ $\Longleftrightarrow$ $\leftrightarrow^* = \downarrow$ Church–Rosser property
- CR $\Longrightarrow$ UN
- UN $\not\Longrightarrow$ CR




- WN & UN $\Longrightarrow$ CR
- CR $\Longrightarrow$ WCR
- WCR $\not\Longrightarrow$ CR



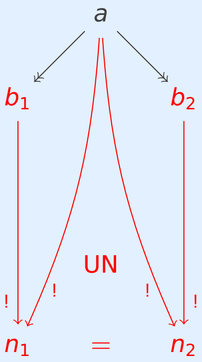

- SN & WCR $\Longrightarrow$ CR Newman's Lemma

## Lemma

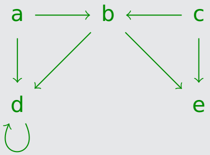
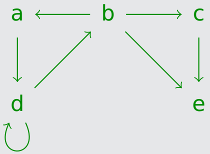
WN & UN $\Longrightarrow$ CR

## Proof

- WN $\Longrightarrow$ $\exists\, n_1, n_2$ such that $b_1 \to^! n_1$ and $b_2 \to^! n_2$
- $\to^* \cdot \to^! \subseteq \to^!$
- UN $\Longrightarrow$ $n_1 = n_2$ $\Longrightarrow$ $b_1 \downarrow b_2$

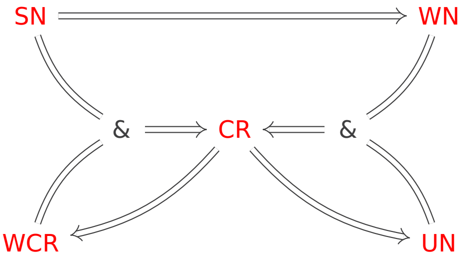


# Examples

| ARS | SN | WN | CR | WCR | UN |
|---|---|---|---|---|---|
|  | 🙁 | 🙁 | 🙁 | 🙁 | 🙂 |
|  | 🙁 | 🙂 | 🙂 | 🙂 | 🙂 |

$\langle \mathbb{N}, \to \rangle$ with $\to \; = \{(0,2),\ (1,3)\} \cup \{(x^2, x),\ (x+3, x) \mid x \in \mathbb{N}\}$

| | SN | WN | CR | WCR | UN |
|---|---|---|---|---|---|
| | ? | ? | ? | ? | ? |

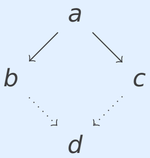



## Definitions (Properties)

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

## Definition (Diamond Property)

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




$\exists\, d$

## Lemmata

- every ARS with diamond property is confluent
- ARS $\langle A, \rightarrow \rangle$ is confluent $\iff$ ARS $\langle A, \rightarrowtail \rangle$ with $\rightarrowtail^* = \rightarrow^*$ is confluent

## Corollary

ARS $\langle A, \rightarrow \rangle$ is confluent if $\rightarrow \;\subseteq\; \rightarrowtail \;\subseteq\; \rightarrow^*$ for some relation $\rightarrowtail$ with diamond property

# Outline

# Well–Founded Induction

given

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

to conclude

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

it is sufficient to prove

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

for arbitrary element $a \in A$

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

## Definitions (Properties of Elements)

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

- $\mathrm{CR}(a) \iff b \downarrow c$ whenever $b \;{}^{*}\!\leftarrow a \to^{*} c$
- $\mathrm{WCR}(a) \iff b \downarrow c$ whenever $b \leftarrow a \to c$
- $\mathrm{SN}(a) \iff$ there are no infinite rewrite sequences starting from $a$
- $\mathrm{WN}(a) \iff a \to^{!} b$ for some $b$
- $\mathrm{UN}(a) \iff b = c$ whenever $b \;{}^{!}\!\leftarrow a \to^{!} c$

## Lemma

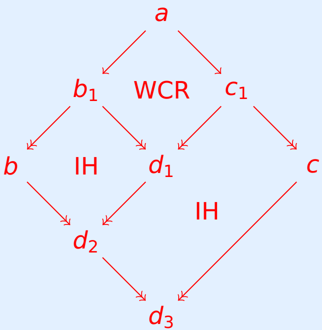
ARS $\mathcal{A} = \langle A, \to \rangle$

- $\mathrm{CR}(\mathcal{A}) \iff \forall\, a \in A \;\; \mathrm{CR}(a)$
- $\cdots$

## Newman's Lemma

SN & WCR $\Longrightarrow$ CR

## First Proof




induction hypothesis CR($b_1$) & CR($c_1$)

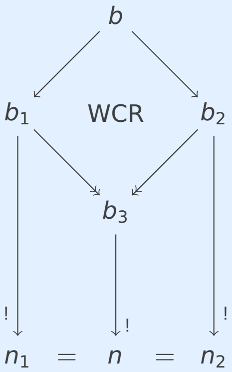
$\forall\, a'$ if $a \to a'$ then CR($a'$)

## Newman's Lemma

$\text{SN} \ \& \ \text{WCR} \implies \text{CR}$

## Second Proof

- it suffices to show UN because $\text{SN} \implies \text{WN}$ and $\text{WN} \ \& \ \text{UN} \implies \text{CR}$
- suppose $B = \{a \in A \mid \neg\text{UN}(a)\} \neq \varnothing$
- let $b \in B$ be minimal element (with respect to $\rightarrow$)
- $b \rightarrow^! n_1$ and $b \rightarrow^! n_2$ with $n_1 \neq n_2$
- $\text{SN} \implies \exists n \ b_3 \rightarrow^! n$
- $b_1 \notin B \implies \text{UN}(b_1) \implies n_1 = n$
- $b_2 \notin B \implies \text{UN}(b_2) \implies n = n_2$ ↯



# Outline

# Homework Exercises for March 16

1. Exercise 1.4. 2
2. Exercise 1.5. 2
3. Complete the table on slide 18. Motivate your answers. 2
4. Download FORT–s and execute the following commands

```
./fort-s -S "a 0 b 0 c 0" "UN & ~CR"
./fort-s -a "0 0" "WN & ~SN"
./fort-s -a "0 0 0 0" -r 4 "WCR & ~CR"
```

   and compare the output with the ARSs on slide 16. 1
5. Exercise 1.19. ☆☆

# Outline

1. Summary of Lecture 1
2. Abstract Rewrite Systems
3. Newman's Lemma
4. Exercises
5. **Further Reading**

## Lecture Notes

- Section 1.1
- Section 1.2 (until Lemma 1.2.13)
- Section 1.3
- Appendix A.1
- Appendix A.2

## Important Concepts

- abstract rewrite system
- completeness
- confluence
- conversion
- diamond property
- joinability
- local confluence
- Newman's Lemma
- normal form
- normalization
- reduct
- semi–completeness
- termination
- unique normal forms
- well–founded induction