



# Term Rewriting

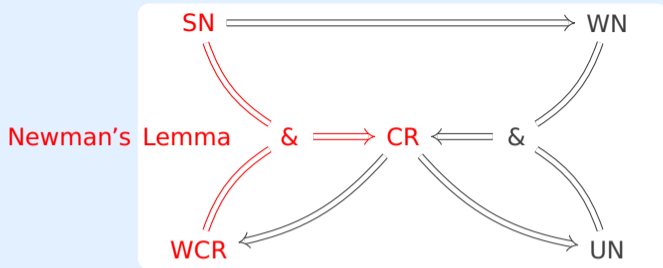
Philipp Dablander and **Aart Middeldorp**

# Outline

- 1. Summary of Lecture 2**
- 2. Multiset Orders**
- 3. Equational Reasoning**
- 4. Algebras**
- 5. Exercises**
- 6. Further Reading**

## Definitions

- ▶ **abstract rewrite system (ARS)**  $\mathcal{A}$  is set  $A$  equipped with binary relation  $\rightarrow$
- ▶ **normal form** is element  $x \in A$  such that  $x \not\rightarrow y$  for all  $y \in A$
- ▶ ARS is **terminating (SN)** if there are no infinite rewrite sequences
- ▶ ARS is **(weakly) normalizing (WN)** if every element has normal form
- ▶ ARS is **confluent (CR)** if  $*\leftarrow \cdot \rightarrow^* \subseteq \rightarrow^* \cdot *\leftarrow$  ( $\uparrow \subseteq \downarrow$ )
- ▶ ARS is **locally confluent (WCR)** if  $\leftarrow \cdot \rightarrow \subseteq \rightarrow^* \cdot *\leftarrow$
- ▶ ARS has **unique normal forms (UN)** if  $!\leftarrow \cdot \rightarrow! \subseteq =$
- ▶ ARS is **complete** if it is confluent and terminating
- ▶ ARS is **semi-complete** if it is confluent and normalizing
- ▶ ARS has **diamond property ( $\diamond$ )** if  $\leftarrow \cdot \rightarrow \subseteq \rightarrow \cdot \leftarrow$



## Lemma

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

# Outline

## 1. Summary of Lecture 2

## 2. Multiset Orders

Newman's Lemma

## 3. Equational Reasoning

## 4. Algebras

## 5. Exercises

## 6. Further Reading

## Definitions (Multisets)

- ▶ finite **multiset**  $M$  over  $A$  is function from  $A$  to  $\mathbb{N}$  such that  $M(a) \neq 0$  for 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

$$\{a, a, a, b, d, d, d\} \in \mathcal{M}(\{a, b, c, d\}) : \quad a \mapsto 3 \quad b \mapsto 1 \quad c \mapsto 0 \quad d \mapsto 3$$

## Definitions (Operations on Multisets)

- ▶ **sum**  $\forall a \quad (M_1 \uplus M_2)(a) = M_1(a) + M_2(a)$
- ▶ **difference**  $\forall a \quad (M_1 - M_2)(a) = \max\{M_1(a) - M_2(a), 0\}$

## Example

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

## Definition (Multiset Extension)

**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 there exist  $X, Y \in \mathcal{M}(A)$  such that

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

## Example

$$\begin{aligned} \{2, 3\} &>_{\text{mul}} \{0, 1, 3\} >_{\text{mul}} \{0, 1, 1, 2, 2, 2\} >_{\text{mul}} \{0, 1, 1, 0, 1, 1, 2, 2\} \\ &>_{\text{mul}} \{0, 1, 0, 1, 1, 2, 2\} >_{\text{mul}} \{0, 1, 0, 1, 0, 0, 2\} >_{\text{mul}} \{1, 1, 1, 1, 1, 1\} \\ &>_{\text{mul}} \{1, 1, 1, 1\} >_{\text{mul}} \{0, 0, 0, 0, 1, 1, 1\} >_{\text{mul}} \dots \end{aligned}$$

## Lemma

multiset extension of proper order is proper order

## Lemma

if  $M_1 >_{\text{mul}} M_2$  then  $M_1 \uplus N >_{\text{mul}} M_2 \uplus N$  for all  $N \in \mathcal{M}(A)$

## Theorem

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

## Proof (by contradiction)

- ▶ transform presupposed infinite descending sequence

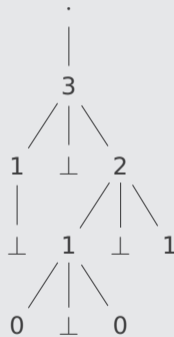
$$M_1 >_{\text{mul}} M_2 >_{\text{mul}} M_3 >_{\text{mul}} \dots$$

into infinite **finitely branching** tree  $T$

- ▶  $T$  contains infinite path by König's Lemma
- ▶ infinite path corresponds to infinite descending sequence with respect to  $>$  ⚡

## Example

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



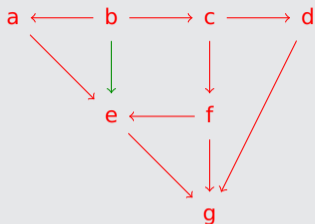
SN & WCR  $\implies$  CR

## Third Proof

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

## Example

### ► ARS



### ► conversion

$a \leftarrow b \rightarrow c \rightarrow d$

$\{a, b, c, d\}$

$a \rightarrow e \leftarrow f \leftarrow c \rightarrow d$

$\{a, e, f, c, d\}$

$a \rightarrow e \leftarrow f \rightarrow g \leftarrow d$

$\{a, e, f, g, d\}$

$a \rightarrow e \rightarrow g \leftarrow d$

$\{a, e, g, d\}$

rewrite proof

# Outline

1. Summary of Lecture 2
2. Multiset Orders
- 3. Equational Reasoning**
4. Algebras
5. Exercises
6. Further Reading

## Definition (Equational System)

**equational system (ES)** is pair  $(\mathcal{F}, \mathcal{E})$  consisting of

- ▶  $\mathcal{F}$  signature
- ▶  $\mathcal{E}$  set of equations between terms in  $\mathcal{T}(\mathcal{F}, \mathcal{V})$

## Example

ES  $(\mathcal{F}, \mathcal{E})$  with signature  $\mathcal{F}$

$0$  (constant)     $s$  (unary)     $+$  (binary, infix)

and equations  $\mathcal{E}$

$$0 + y \approx y$$

$$s(x) + y \approx s(x + y)$$

## Notation

$\mathcal{E}$  instead of  $(\mathcal{F}, \mathcal{E})$  if  $\mathcal{F}$  can be inferred from context

## Inference Rules of Equational Logic

**r** reflexivity

$$\frac{}{t \approx t}$$

$\forall t$

**s** symmetry

$$\frac{s \approx t}{t \approx s}$$

$\forall s, t$

**t** transitivity

$$\frac{s \approx t \quad t \approx u}{s \approx u}$$

$\forall s, t, u$

**a** application

$$\frac{}{l\sigma \approx r\sigma}$$

$\forall l \approx r \in \mathcal{E} \quad \forall \sigma$

**c** congruence

$$\frac{s_1 \approx t_1 \quad \dots \quad s_n \approx t_n}{f(s_1, \dots, s_n) \approx f(t_1, \dots, t_n)}$$

$\forall n\text{-ary } f \quad \forall s_1, t_1, \dots, s_n, t_n$

## Definition (Derivability)

$s \approx_{\mathcal{E}} t$  if equation  $s \approx t$  is derivable from equations in  $\mathcal{E}$

## Example

ES  $\mathcal{E}$

$$0 + y \approx y$$

$$s(x) + y \approx s(x + y)$$

$$\begin{array}{c} \frac{\frac{\frac{}{s(0) + s(0) \approx s(0 + s(0))}{} \quad \frac{\frac{\frac{}{0 + s(0) \approx s(0)}{} \quad \frac{}{s(0 + s(0)) \approx s(s(0))}}{} \quad \frac{}{s(0) + s(0) \approx s(s(0))}}{} \quad \frac{}{s(s(0) + s(0)) \approx s(s(s(0)))}}{} \end{array}$$

$$s(s(0) + s(0)) \approx_{\mathcal{E}} s(s(s(0)))$$

# Outline

1. Summary of Lecture 2
2. Multiset Orders
3. Equational Reasoning
- 4. Algebras**
5. Exercises
6. Further Reading

## Definition (Algebra)

$\mathcal{F}$ -algebra  $\mathcal{A} = (A, \{f_{\mathcal{A}}\}_{f \in \mathcal{F}})$  consists of

- ▶ carrier  $A$
- ▶ interpretations  $f_{\mathcal{A}}: \underbrace{A \times \cdots \times A}_n \rightarrow A$  if  $f \in \mathcal{F}$  has arity  $n$

## Example

two  $\{0, s, +\}$ -algebras

- ▶  $\mathcal{A} = (\mathbb{N}, \{0_{\mathcal{A}}, s_{\mathcal{A}}, +_{\mathcal{A}}\})$  with  $0_{\mathcal{A}} = 0$   $s_{\mathcal{A}}(x) = x + 1$   $+_{\mathcal{A}}(x, y) = x + y$
- ▶  $\mathcal{B} = (\mathbb{N}, \{0_{\mathcal{B}}, s_{\mathcal{B}}, +_{\mathcal{B}}\})$  with  $0_{\mathcal{B}} = 1$   $s_{\mathcal{B}}(x) = x + 1$   $+_{\mathcal{B}}(x, y) = 2x + y$

## Definition (Interpretation of Ground Terms)

interpretation function  $[ ]_{\mathcal{A}}(\cdot) : \mathcal{T}(\mathcal{F}) \rightarrow A$

$$[ ]_{\mathcal{A}}(f(t_1, \dots, t_n)) = f_{\mathcal{A}}([ ]_{\mathcal{A}}(t_1), \dots, [ ]_{\mathcal{A}}(t_n))$$

## Example

- ▶  $\mathcal{A} = (\mathbb{N}, \{0_{\mathcal{A}}, s_{\mathcal{A}}, +_{\mathcal{A}}\})$  with  $0_{\mathcal{A}} = 0$   $s_{\mathcal{A}}(x) = x + 1$   $+_{\mathcal{A}}(x, y) = x + y$
- ▶  $\mathcal{B} = (\mathbb{N}, \{0_{\mathcal{B}}, s_{\mathcal{B}}, +_{\mathcal{B}}\})$  with  $0_{\mathcal{B}} = 1$   $s_{\mathcal{B}}(x) = x + 1$   $+_{\mathcal{B}}(x, y) = 2x + y$

$$[ ]_{\mathcal{A}}(s(s(s(s(0)))))) = 4$$

$$[ ]_{\mathcal{A}}(s(s(0)) + s(0 + s(0))) = 4$$

$$[ ]_{\mathcal{B}}(s(s(s(s(0)))))) = 5$$

$$[ ]_{\mathcal{B}}(s(s(0)) + s(0 + s(0))) = 11$$

## Definitions (Interpretation of Terms)

- ▶ **assignment**  $\alpha: \mathcal{V} \rightarrow A$
- ▶ **interpretation function**  $[\alpha]_{\mathcal{A}}(\cdot): \mathcal{T}(\mathcal{F}, \mathcal{V}) \rightarrow A$

$$[\alpha]_{\mathcal{A}}(t) = \begin{cases} \alpha(t) & \text{if } t \in \mathcal{V} \\ f_{\mathcal{A}}([\alpha]_{\mathcal{A}}(t_1), \dots, [\alpha]_{\mathcal{A}}(t_n)) & \text{if } t = f(t_1, \dots, t_n) \end{cases}$$

## Example

- ▶  $\mathcal{A} = (\mathbb{N}, \{0_{\mathcal{A}}, s_{\mathcal{A}}, +_{\mathcal{A}}\})$  with  $0_{\mathcal{A}} = 0$   $s_{\mathcal{A}}(x) = x + 1$   $+_{\mathcal{A}}(x, y) = x + y$
- ▶  $\mathcal{B} = (\mathbb{N}, \{0_{\mathcal{B}}, s_{\mathcal{B}}, +_{\mathcal{B}}\})$  with  $0_{\mathcal{B}} = 1$   $s_{\mathcal{B}}(x) = x + 1$   $+_{\mathcal{B}}(x, y) = 2x + y$
- ▶  $t = s(s(x) + s(x + y))$   $\alpha(x) = 2$   $\alpha(y) = 3$   $\beta(x) = 1$   $\beta(y) = 4$

$$[\alpha]_{\mathcal{A}}(t) = 10$$

$$[\alpha]_{\mathcal{B}}(t) = 15$$

$$[\beta]_{\mathcal{A}}(t) = 9$$

$$[\beta]_{\mathcal{B}}(t) = 12$$

## Definitions (Model)

- ▶ equation  $s \approx t$  is **valid** in algebra  $\mathcal{A}$  ( $s =_{\mathcal{A}} t$ ) if

$$[\alpha]_{\mathcal{A}}(s) = [\alpha]_{\mathcal{A}}(t)$$

for all assignments  $\alpha$

- ▶  $\mathcal{F}$ -algebra  $\mathcal{A}$  is **model** of ES  $(\mathcal{F}, \mathcal{E})$  if  $s =_{\mathcal{A}} t$  for all equations  $s \approx t \in \mathcal{E}$

## Example

- ▶  $\mathcal{A} = (\mathbb{N}, \{0_{\mathcal{A}}, s_{\mathcal{A}}, +_{\mathcal{A}}\})$  with  $0_{\mathcal{A}} = 0$   $s_{\mathcal{A}}(x) = x + 1$   $+_{\mathcal{A}}(x, y) = x + y$
- ▶  $\mathcal{B} = (\mathbb{N}, \{0_{\mathcal{B}}, s_{\mathcal{B}}, +_{\mathcal{B}}\})$  with  $0_{\mathcal{B}} = 1$   $s_{\mathcal{B}}(x) = x + 1$   $+_{\mathcal{B}}(x, y) = 2x + y$
- ▶  $\mathcal{E} = \{0 + y \approx y, s(x) + y \approx s(x + y)\}$
- ▶  $\mathcal{A}$  is model of  $\mathcal{E}$
- ▶  $\mathcal{B}$  is no model of  $\mathcal{E}$

## Definition (Equational Theory)

- ▶  $s =_{\mathcal{E}} t$  if equation  $s \approx t$  is valid in all models of  $\mathcal{E}$
- ▶ **equational theory** of  $\mathcal{E}$  consists of all equations  $s \approx t$  such that  $s =_{\mathcal{E}} t$

## Example

- ▶ ES  $\mathcal{E} = \{0 + y \approx y, s(x) + y \approx s(x + y)\}$
- ▶ model  $\mathcal{C} = (\mathbb{N}, \{0_{\mathcal{C}}, s_{\mathcal{C}}, +_{\mathcal{C}}\})$  with  $0_{\mathcal{C}} = 0$   $s_{\mathcal{C}}(x) = x + 1$   $+_{\mathcal{C}}(x, y) = x + y$

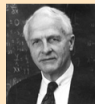
$$s(s(0) + s(0)) =_{\mathcal{E}} s(s(s(0)))$$

$$x + y \neq_{\mathcal{E}} y + x$$

## Theorem (Birkhoff)

equational reasoning is **sound** and **complete**

$$\forall \text{ ES } \mathcal{E} \quad \approx_{\mathcal{E}} = =_{\mathcal{E}}$$



## Example (Cola Gene Puzzle)

$\varepsilon$        $\text{TCAT} \approx \text{T}$        $\text{GAG} \approx \text{AG}$        $\text{CTC} \approx \text{TC}$        $\text{AGTA} \approx \text{A}$        $\text{TAT} \approx \text{CT}$

- ▶ model  $\mathcal{A} = (\mathbb{Z}, \{\mathbf{A}_{\mathcal{A}}, \mathbf{C}_{\mathcal{A}}, \mathbf{G}_{\mathcal{A}}, \mathbf{T}_{\mathcal{A}}\})$  with

$$\mathbf{A}_{\mathcal{A}}(x) = x - 1 \qquad \mathbf{C}_{\mathcal{A}}(x) = \mathbf{G}_{\mathcal{A}}(x) = x \qquad \mathbf{T}_{\mathcal{A}}(x) = x + 1$$

- ▶ (milk gene)  $\text{TAGCTAGCTAGCT} \not\approx_{\varepsilon} \text{CTGCTACTGACT}$  (mad cow retrovirus) because

$$[\alpha]_{\mathcal{A}}(\text{TAGCTAGCTAGCT}(x)) = \alpha(x) + 1$$

$$[\alpha]_{\mathcal{A}}(\text{CTGCTACTGACT}(x)) = \alpha(x) + 2$$

for all assignments  $\alpha$

- ▶ (milk gene)  $\text{TAGCTAGCTAGCT} \not\approx_{\varepsilon} \text{CTGCTACTGACT}$  (mad cow retrovirus) by Birkhoff

## Definition (Consistency)

ES  $\mathcal{E}$  is **consistent** if  $s \neq_{\mathcal{E}} t$  for some terms  $s, t$

## Validity Problem

instance: ES  $(\mathcal{F}, \mathcal{E})$  terms  $s, t \in \mathcal{T}(\mathcal{F}, \mathcal{V})$

question:  $s =_{\mathcal{E}} t$ ?

## Theorem

validity problem is **undecidable** for Combinatory Logic

## Combinatory Logic

$$I \cdot x \approx x$$

$$(K \cdot x) \cdot y \approx x$$

$$((S \cdot x) \cdot y) \cdot z \approx (x \cdot z) \cdot (y \cdot z)$$

# Outline

1. Summary of Lecture 2
2. Multiset Orders
3. Equational Reasoning
4. Algebras
- 5. Exercises**
6. Further Reading

## Homework Exercises for March 23

① Exercise A.23.

1

② Exercise A.29.

1

③ Exercise 2.17.

1

④ Exercise 2.29.

2

⑤ Exercise 2.30.

2

# Outline

1. Summary of Lecture 2
2. Multiset Orders
3. Equational Reasoning
4. Algebras
5. Exercises
- 6. Further Reading**

## Lecture Notes

- ▶ Section A.3
- ▶ Section 2.2 (until Example 2.2.10)
- ▶ Section 2.4

## Important Concepts

- ▶ algebra
- ▶ equation
- ▶ equational reasoning
- ▶ equational system (ES)
- ▶ equational theory
- ▶ model
- ▶ multiset
- ▶ multiset order
- ▶ validity problem