26S lecture 3

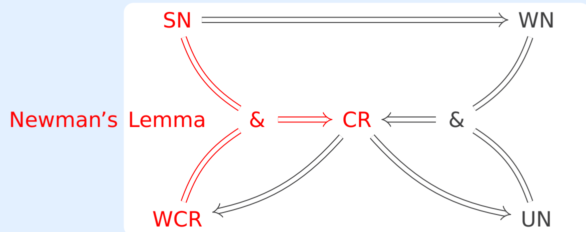
Term Rewriting

Philipp Dablander and **Aart Middeldorp**

Outline

Definitions

- abstract rewrite system (ARS) $\mathcal{A}$ is set A equipped with binary relation $\to$
- normal form is element $x \in A$ such that $x \not\to y$ 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 ${}^*\!\leftarrow \cdot \to^* \subseteq \to^* \cdot {}^*\!\leftarrow$ $(\uparrow \subseteq \downarrow)$
- ARS is locally confluent (WCR) if $\leftarrow \cdot \to \subseteq \to^* \cdot {}^*\!\leftarrow$
- ARS has unique normal forms (UN) if ${}^!\!\leftarrow \cdot \to^! \subseteq =$
- 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 $\leftarrow \cdot \to \subseteq \to \cdot \leftarrow$



Lemma

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

Outline

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

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

Definitions (Operations on Multisets)

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

Example

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

Definition (Multiset Extension)

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

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

Lemma

multiset extension of proper order is proper order

Lemma

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

Theorem

multiset extension of well–founded order is well–founded

Proof (by contradiction)

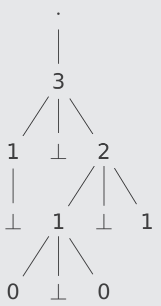
- transform presupposed infinite descending sequence

$$M_1 >_{\mathsf{mul}} M_2 >_{\mathsf{mul}} M_3 >_{\mathsf{mul}} \cdots$$

  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

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



Newman's Lemma

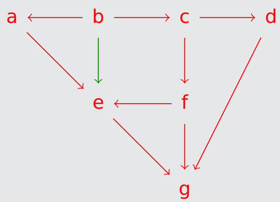
SN & WCR $\Longrightarrow$ CR

Third Proof

- given $b \; {}^*{\leftarrow} \; a \to^* c$
- construct sequence of conversions $(C_i)_{i \geqslant 0}$ between b and c
  - C_0 is initial conversion $b \; {}^*{\leftarrow} \; a \to^* c$
  - C_{i+1} is obtained from C_i by replacing peak $e \leftarrow d \to f$ in C_i by valley $e \to^* \cdot \; {}^*{\leftarrow} \; f$
- $M(C_i)$ is multiset of elements appearing in C_i
- $M(C_i) \; (\to^+)_{\mathrm{mul}} \; M(C_{i+1})$
- $(\to^+)_{\mathrm{mul}}$ is well–founded
- hence C_n has no peaks for some $n \geqslant 0 \quad \Longrightarrow \quad C_n\colon \; b \to^* \cdot \; {}^*{\leftarrow} \; c$

Example

- ARS



- conversion — multiset

conversion	multiset	
a ← b → c → d	{a, b, c, d}	
a → e ← f ← c → d	{a, e, f, c, d}	
a → e ← f → g ← d	{a, e, f, g, d}	
a → e → g ← d	{a, e, g, d}	rewrite proof

Outline

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 $\mathcal{F}$

$$0 \text{ (constant)} \qquad \mathsf{s} \text{ (unary)} \qquad + \text{ (binary, infix)}$$

and equations $\mathcal{E}$

$$0 + y \approx y \qquad \mathsf{s}(x) + y \approx \mathsf{s}(x + y)$$

Notation

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

Inference Rules of Equational Logic

- **r** reflexivity $\dfrac{}{t \approx t}$ $\quad \forall\ t$
- **s** symmetry $\dfrac{s \approx t}{t \approx s}$ $\quad \forall\ s, t$
- **t** transitivity $\dfrac{s \approx t \quad t \approx u}{s \approx u}$ $\quad \forall\ s, t, u$
- **a** application $\dfrac{}{\ell\sigma \approx r\sigma}$ $\quad \forall\ \ell \approx r \in \mathcal{E}\ \ \forall\ \sigma$
- **c** congruence $\dfrac{s_1 \approx t_1 \quad \cdots \quad s_n \approx t_n}{f(s_1, \dots, s_n) \approx f(t_1, \dots, t_n)}$ $\quad \forall\ n\text{-ary } f\ \ \forall\ s_1, t_1, \dots, s_n, t_n$

Definition (Derivability)

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

Example

ES $\mathcal{E}$

$$0 + y \approx y \qquad \mathsf{s}(x) + y \approx \mathsf{s}(x + y)$$

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

$$\dfrac{\dfrac{\dfrac{}{\mathsf{s}(0) + \mathsf{s}(0) \approx \mathsf{s}(0 + \mathsf{s}(0))}\,\mathsf{a} \qquad \dfrac{\dfrac{}{0 + \mathsf{s}(0) \approx \mathsf{s}(0)}\,\mathsf{a}}{\mathsf{s}(0 + \mathsf{s}(0)) \approx \mathsf{s}(\mathsf{s}(0))}\,\mathsf{c}}{\mathsf{s}(0) + \mathsf{s}(0) \approx \mathsf{s}(\mathsf{s}(0))}\,\mathsf{t}}{\mathsf{s}(\mathsf{s}(0) + \mathsf{s}(0)) \approx \mathsf{s}(\mathsf{s}(\mathsf{s}(0)))}\,\mathsf{c}$$

Outline

Definition (Algebra)

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

- carrier A
- interpretations $f_\mathcal{A} \colon \underbrace{A \times \cdots \times A}_{n} \to A$ if $f \in \mathcal{F}$ has arity n

Example

two $\{0, \mathsf{s}, +\}$–algebras

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

Definition (Interpretation of Ground Terms)

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

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

Example

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

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

$[\,]_\mathcal{B}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(0))))) = 5$ $\qquad [\,]_\mathcal{B}(\mathsf{s}(\mathsf{s}(0)) + \mathsf{s}(0 + \mathsf{s}(0))) = 11$

Definitions (Interpretation of Terms)

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

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

Example

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

$[\alpha]_\mathcal{A}(t) = 10$ $\qquad [\alpha]_\mathcal{B}(t) = 15$ $\qquad [\beta]_\mathcal{A}(t) = 9$ $\qquad [\beta]_\mathcal{B}(t) = 12$

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 α
- $\mathcal{F}$–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

- $\mathcal{A} = (\mathbb{N}, \{0_\mathcal{A}, \mathsf{s}_\mathcal{A}, +_\mathcal{A}\})$ with $0_\mathcal{A} = 0$ $\mathsf{s}_\mathcal{A}(x) = x + 1$ $+_\mathcal{A}(x, y) = x + y$
- $\mathcal{B} = (\mathbb{N}, \{0_\mathcal{B}, \mathsf{s}_\mathcal{B}, +_\mathcal{B}\})$ with $0_\mathcal{B} = 1$ $\mathsf{s}_\mathcal{B}(x) = x + 1$ $+_\mathcal{B}(x, y) = 2x + y$
- $\mathcal{E} = \{0 + y \approx y,\ \mathsf{s}(x) + y \approx \mathsf{s}(x + y)\}$
- $\mathcal{A}$ 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 $s =_{\mathcal{E}} t$

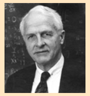
Example

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

$$\mathsf{s}(\mathsf{s}(0) + \mathsf{s}(0)) =_{\mathcal{E}} \mathsf{s}(\mathsf{s}(\mathsf{s}(0))) \qquad\qquad x + y \neq_{\mathcal{E}} y + x$$

Theorem (Birkhoff)

equational reasoning is sound and complete



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

Example (Cola Gene Puzzle)

$$\mathcal{E} \qquad \mathsf{TCAT} \approx \mathsf{T} \qquad \mathsf{GAG} \approx \mathsf{AG} \qquad \mathsf{CTC} \approx \mathsf{TC} \qquad \mathsf{AGTA} \approx \mathsf{A} \qquad \mathsf{TAT} \approx \mathsf{CT}$$

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

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

- (milk gene) $\mathsf{TAGCTAGCTAGCT} \neq_{\mathcal{E}} \mathsf{CTGCTACTGACT}$ (mad cow retrovirus) because

$$[\alpha]_{\mathcal{A}}(\mathsf{TAGCTAGCTAGCT}(x)) = \alpha(x) + 1$$
$$[\alpha]_{\mathcal{A}}(\mathsf{CTGCTACTGACT}(x)) = \alpha(x) + 2$$

for all assignments α

- (milk gene) $\mathsf{TAGCTAGCTAGCT} \not\approx_{\mathcal{E}} \mathsf{CTGCTACTGACT}$ (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

$$\mathsf{I} \cdot x \approx x \qquad (\mathsf{K} \cdot x) \cdot y \approx x \qquad ((\mathsf{S} \cdot x) \cdot y) \cdot z \approx (x \cdot z) \cdot (y \cdot z)$$

Outline

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

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