universität innsbruck

26S lecture 4

Term Rewriting

Philipp Dablander and **Aart Middeldorp**

Outline

Definitions

- finite multiset M over A is function from A to $\mathbb{N}$ such that $M(a) \neq 0$ for finitely many $a \in A$
- set of all finite multisets over A is denoted by $\mathcal{M}(A)$
- 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 $M_2 = (M_1 - X) \uplus Y$, $\varnothing \neq X \subseteq M_1$ and $\forall\, y \in Y\ \exists\, x \in X\ \ x > y$

Theorem

multiset extension of well–founded order is well–founded order

Definition

equational system (ES) is pair $(\mathcal{F}, \mathcal{E})$ consisting of signature $\mathcal{F}$ and set $\mathcal{E}$ of equations between terms in $\mathcal{T}(\mathcal{F}, \mathcal{V})$

Inference Rules of Equational Logic

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

Definition

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

Definitions

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

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

- 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
- algebra $\mathcal{A}$ is model of ES $\mathcal{E}$ if $s =_\mathcal{A} t$ for all equations $s \approx t \in \mathcal{E}$
- $s =_\mathcal{E} t$ if equation $s \approx t$ is valid in all models of $\mathcal{E}$

Definition

equational theory of $\mathcal{E}$ consists of all equations $s \approx t$ such that $s =_\mathcal{E} t$

Theorem (Birkhoff)

equational reasoning is sound and complete: $\forall$ ES $\mathcal{E}$ $\quad \approx_\mathcal{E} \; = \; =_\mathcal{E}$

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

Outline

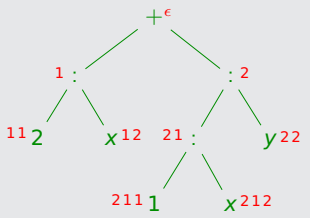
Definition (Positions)

- $\mathcal{P}\text{os}(\cdot)$ positions are strings of positive integers

$$\mathcal{P}\text{os}(t) = \begin{cases} \{\epsilon\} & \text{if } t \in \mathcal{V} \\ \{\epsilon\} \cup \{ip \mid 1 \leqslant i \leqslant n \text{ and } p \in \mathcal{P}\text{os}(t_i)\} & \text{if } t = f(t_1, \ldots, t_n) \end{cases}$$

Example

$t = (2 : x) + ((1 : x) : y)$

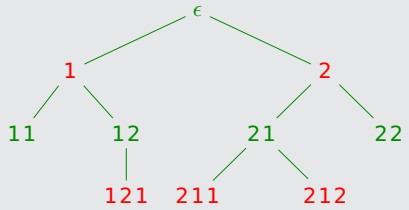


$\mathcal{P}\text{os}(t) = \{\epsilon, 1, 11, 12, 2, 21, 211, 212, 22\}$

Definitions (Relations on Positions)

- $p < q$ if $pr = q$ for some $r \neq \epsilon$ "p is strictly above q" "q is strictly below p"
- $p \leqslant q$ if $pr = q$ for some r "p is above q" "q is below p"
- $p \parallel q$ if $p \not\leqslant q$ and $q \not\leqslant p$ "p and q are parallel"

Example



- $2 < 211$
- $1 \parallel 2$
- $1 \parallel 212$
- $1 \not\parallel 121$

Definitions (Operations on Terms and Positions)

- $t|_p$ subterm of t at position p

$$t|_p = \begin{cases} t & \text{if } p = \epsilon \\ t_i|_q & \text{if } t = f(t_1, \ldots, t_n) \text{ and } p = iq \end{cases}$$

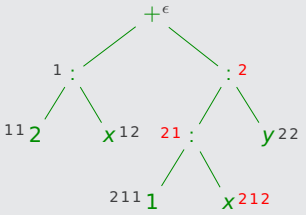
- $t(p) = \mathrm{root}(t|_p)$ symbol in t at position p
- $t[\,]_p$ context obtained by removing subterm in t at position p

$$t[\,]_p = \begin{cases} \Box & \text{if } p = \epsilon \\ f(t_1, \ldots, t_i[\,]_q, \ldots, t_n) & \text{if } t = f(t_1, \ldots, t_n) \text{ and } p = iq \end{cases}$$

- $t[s]_p = (t[\,]_p)[s]$ replace subterm in t at position p by s

Example

$t = (2 : x) + ((1 : x) : y)$



- $t|_{21} = 1 : x$
- $t(212) = x$
- $t[x + 3]_2 = (2 : x) + (x + 3)$

Definition (Rewriting)

binary relation $\to_{\mathcal{E}}$ on $\mathcal{T}(\mathcal{F}, \mathcal{V})$ for every ES $(\mathcal{F}, \mathcal{E})$:

$$s \to_{\mathcal{E}} t \iff \begin{array}{l} \exists\ p \in \mathcal{P}\mathrm{os}(s) \\ \exists\ \ell \approx r \in \mathcal{E} \\ \exists\ \text{substitution } \sigma \end{array} \quad \text{with} \quad \begin{array}{ll} s|_p = \ell\sigma & \text{redex} \\ t = s[r\sigma]_p & \end{array}$$

Example

ES $\mathcal{E} = \{0 + y \approx y,\ \mathsf{s}(x) + y \approx \mathsf{s}(x + y)\}$

	position	equation	substitution
$\mathsf{s}(\mathsf{s}(0) + \mathsf{s}(0))$			
$\downarrow_{\mathcal{E}}$	1	$\mathsf{s}(x) + y \approx \mathsf{s}(x + y)$	$\{x \mapsto 0, y \mapsto \mathsf{s}(0)\}$
$\mathsf{s}(\mathsf{s}(0 + \mathsf{s}(0)))$			
$\downarrow_{\mathcal{E}}$	11	$0 + y \approx y$	$\{y \mapsto \mathsf{s}(0)\}$
$\mathsf{s}(\mathsf{s}(\mathsf{s}(0)))$			

Lemma

$\to_{\mathcal{E}}$ is smallest relation that contains $\mathcal{E}$ and is closed under contexts and substitutions

Remark

with every ES $(\mathcal{F}, \mathcal{E})$ we associate ARS $\langle \mathcal{T}(\mathcal{F}, \mathcal{V}), \to_{\mathcal{E}} \rangle$

- notation $(\to_{\mathcal{E}}^*,\ \leftrightarrow_{\mathcal{E}}^*,\ \mathrm{NF}(\mathcal{E}),\ \dots)$
- properties $(\mathrm{SN},\ \mathrm{CR},\ \dots)$

are obtained via associated ARS

Theorem

$\forall$ ES $\mathcal{E}$ $\quad \leftrightarrow_{\mathcal{E}}^* \ = \ \approx_{\mathcal{E}} \ = \ =_{\mathcal{E}}$

Example

ES $\mathcal{E} = \{0 + y \approx y,\ \mathsf{s}(x) + y \approx \mathsf{s}(x + y)\}$

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

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

- $\mathsf{s}(\mathsf{s}(0) + \mathsf{s}(0)) \leftrightarrow_{\mathcal{E}}^* \mathsf{s}(\mathsf{s}(\mathsf{s}(0)))$: $\quad \mathsf{s}(\mathsf{s}(0) + \mathsf{s}(0)) \to_{\mathcal{E}} \mathsf{s}(\mathsf{s}(0 + \mathsf{s}(0))) \to_{\mathcal{E}} \mathsf{s}(\mathsf{s}(\mathsf{s}(0)))$

Definitions (Term Rewrite System)

- rewrite rule $\ell \to r$ is equation $\ell \approx r$ such that
  - $\ell \notin \mathcal{V}$
  - $\mathcal{V}\mathrm{ar}(r) \subseteq \mathcal{V}\mathrm{ar}(\ell)$
- term rewrite system (TRS) is pair $(\mathcal{F}, \mathcal{R})$ consisting of
  - $\mathcal{F}$ signature
  - $\mathcal{R}$ set of rewrite rules between terms in $\mathcal{T}(\mathcal{F}, \mathcal{V})$

Lemma

TRSs are ESs

Validity Problem

instance: ES $\mathcal{E}$ terms s, t

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

Theorem

validity problem is decidable for ES $\mathcal{E}$ if there exists finite TRS $\mathcal{R}$ such that

1. $\mathcal{R}$ is complete (confluent and terminating)
2. $\leftrightarrow_{\mathcal{E}}^* \ = \ \leftrightarrow_{\mathcal{R}}^*$

Example (Group Theory)

- signature e (constant) $^{-}$ (unary, postfix) $\cdot$ (binary, infix)
- ES $\mathcal{E}$ $\mathsf{e} \cdot x \approx x$ $x^{-} \cdot x \approx \mathsf{e}$ $(x \cdot y) \cdot z \approx x \cdot (y \cdot z)$
- theorems $\mathsf{e}^{-} \downarrow_{\mathcal{R}} \mathsf{e}$ $(x \cdot y)^{-} \downarrow_{\mathcal{R}} y^{-} \cdot x^{-}$
- TRS $\mathcal{R}$

$$\begin{aligned} \mathsf{e} \cdot x &\to x & x \cdot \mathsf{e} &\to x \\ x^{-} \cdot x &\to \mathsf{e} & x \cdot x^{-} &\to \mathsf{e} \\ (x \cdot y) \cdot z &\to x \cdot (y \cdot z) & x^{--} &\to x \\ \mathsf{e}^{-} &\to \mathsf{e} & (x \cdot y)^{-} &\to y^{-} \cdot x^{-} \\ x^{-} \cdot (x \cdot y) &\to y & x \cdot (x^{-} \cdot y) &\to y \end{aligned}$$

- $\mathcal{R}$ is complete and $\leftrightarrow^{*}_{\mathcal{E}} = \leftrightarrow^{*}_{\mathcal{R}} \implies$ $\mathcal{E}$ has decidable validity problem
- how to compute $\mathcal{R}$? completion (lectures 6, 7, 8)
- how to prove termination of $\mathcal{R}$? LPO or KBO (lectures 5, 6, 8, 11, 12, 13)

Definitions (Canonicity)

- TRS $\mathcal{R}$ is reduced if for all $\ell \to r \in \mathcal{R}$
  1. r is normal form of $\mathcal{R}$
  2. ℓ is normal form of $\mathcal{R} \setminus \{\ell \to r\}$
- reduced complete TRS is canonical

Example

$$\begin{aligned} \mathsf{e} \cdot x &\to x & x \cdot \mathsf{e} &\to x \\ x^{-} \cdot x &\to \mathsf{e} & x \cdot x^{-} &\to \mathsf{e} \\ (x \cdot y) \cdot z &\to x \cdot (y \cdot z) & x^{--} &\to x \\ \mathsf{e}^{-} &\to \mathsf{e} & (x \cdot y)^{-} &\to y^{-} \cdot x^{-} \\ x^{-} \cdot (x \cdot y) &\to y & x \cdot (x^{-} \cdot y) &\to y \end{aligned}$$

canonical

Example

TRS $\mathcal{R}$ modeling Sieve of Eratosthenes for generating list of prime numbers

$$\begin{aligned} \mathsf{primes} &\to \mathsf{sieve}(\mathsf{from}(\mathsf{s}(\mathsf{s}(0)))) & \mathsf{sieve}(0 : y) &\to \mathsf{sieve}(y) \\ \mathsf{from}(x) &\to x : \mathsf{from}(\mathsf{s}(x)) & \mathsf{sieve}(\mathsf{s}(x) : y) &\to \mathsf{s}(x) : \mathsf{sieve}(\mathsf{filter}(x, y, x)) \\ \mathsf{head}(x : y) &\to x & \mathsf{filter}(0, y : z, w) &\to 0 : \mathsf{filter}(w, z, w) \\ \mathsf{tail}(x : y) &\to y & \mathsf{filter}(\mathsf{s}(x), y : z, w) &\to y : \mathsf{filter}(x, z, w) \end{aligned}$$

- $\mathcal{R}$ is confluent but not terminating:

$$\mathsf{from}(0) \to 0 : \mathsf{from}(\mathsf{s}(0)) \to 0 : (\mathsf{s}(0) : \mathsf{from}(\mathsf{s}(\mathsf{s}(0)))) \to \cdots$$

- how to prove confluence of $\mathcal{R}$? orthogonality (lectures 9, 12)
- $\exists$ non–terminating terms with (unique) normal form

$$\mathsf{head}(\mathsf{tail}(\mathsf{tail}(\mathsf{primes}))) \to^{!} \mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(0)))))$$

- how to compute normal forms in $\mathcal{R}$? strategy (lectures 10, 11)

Definitions (Constructor System)

- TRS $\mathcal{R}$ over signature $\mathcal{F}$
  - defined symbols $\mathcal{F}_{\mathcal{D}} = \{\mathsf{root}(\ell) \mid \ell \to r \in \mathcal{R}\}$
  - constructors $\mathcal{F}_{\mathcal{C}} = \mathcal{F} \setminus \mathcal{F}_{\mathcal{D}}$
- TRS is constructor system (CS) if proper subterms of left–hand sides of rewrite rules do not contain defined symbols

Example

$$\begin{aligned} \mathsf{primes} &\to \mathsf{sieve}(\mathsf{from}(\mathsf{s}(\mathsf{s}(0)))) & \mathsf{sieve}(0 : y) &\to \mathsf{sieve}(y) \\ \mathsf{from}(x) &\to x : \mathsf{from}(\mathsf{s}(x)) & \mathsf{sieve}(\mathsf{s}(x) : y) &\to \mathsf{s}(x) : \mathsf{sieve}(\mathsf{filter}(x, y, x)) \\ \mathsf{head}(x : y) &\to x & \mathsf{filter}(0, y : z, w) &\to 0 : \mathsf{filter}(w, z, w) \\ \mathsf{tail}(x : y) &\to y & \mathsf{filter}(\mathsf{s}(x), y : z, w) &\to y : \mathsf{filter}(x, z, w) \end{aligned}$$

CS

- defined symbols primes from head tail sieve filter
- constructors 0 s :

Example (Combinatory Logic)

$$\mathsf{I} \cdot x \to x \qquad \mathsf{I}x \to x \qquad \mathsf{I}x \to x$$
$$(\mathsf{K} \cdot x) \cdot y \to x \qquad (\mathsf{K}x)y \to x \qquad \mathsf{K}xy \to x$$
$$((\mathsf{S} \cdot x) \cdot y) \cdot z \to (x \cdot z) \cdot (y \cdot z) \qquad ((\mathsf{S}x)y)z \to (xz)(yz) \qquad \mathsf{S}xyz \to xz(yz)$$

- applicative notation: suppress $\cdot$ and adopt left–association
- CL is confluent but not terminating:

$$\mathsf{SII}(\mathsf{SII}) \to \mathsf{I}(\mathsf{SII})(\mathsf{I}(\mathsf{SII})) \to \mathsf{SII}(\mathsf{I}(\mathsf{SII})) \to \mathsf{SII}(\mathsf{SII})$$

- CL is consistent: $\mathsf{S} \leftrightarrow^* \mathsf{K}$ does not hold

Remark

CL is Turing–complete

Definition (String Rewrite System)

string rewrite system (SRS) is TRS over signature consisting of unary function symbols

Example

Example (Cola Gene Puzzle)

- signature $\mathsf{A}\,\mathsf{C}\,\mathsf{G}\,\mathsf{T}$ (unary)
- ES $\mathcal{E}$ $\mathsf{TCAT} \approx \mathsf{T}$ $\mathsf{GAG} \approx \mathsf{AG}$ $\mathsf{CTC} \approx \mathsf{TC}$ $\mathsf{AGTA} \approx \mathsf{A}$ $\mathsf{TAT} \approx \mathsf{CT}$
- theorem $\mathsf{TAGCTAGCTAGCT} \downarrow_{\mathcal{R}} \mathsf{CTGACTGACT}$
- SRS $\mathcal{R}$ $\mathsf{GA} \to \mathsf{A}$ $\mathsf{AGT} \to \mathsf{AT}$ $\mathsf{ATA} \to \mathsf{A}$ $\mathsf{CT} \to \mathsf{T}$ $\mathsf{TAT} \to \mathsf{T}$ $\mathsf{TCA} \to \mathsf{TA}$
- $\mathcal{R}$ is canonical and $\leftrightarrow^*_{\mathcal{E}} = \leftrightarrow^*_{\mathcal{R}} \implies \mathcal{E}$ has decidable validity problem

Outline

Theorem

term rewriting is Turing–complete hence all non–trivial questions are undecidable

Undecidable Problems

instance: (finite) TRS $\mathcal{R}$
question: is $\mathcal{R}$ terminating ?

instance: TRS $\mathcal{R}$
question: is $\mathcal{R}$ confluent ?

instance: TRS $\mathcal{R}$, term t
question: is t terminating ?

...

Theorem

- confluence is decidable for terminating TRSs (lecture 6)
- termination is undecidable for confluent TRSs

Outline

Post Correspondence Problem (PCP)

instance: finite subset P of $\Gamma^+ \times \Gamma^+$ over some alphabet Γ
question: $\exists\ (\alpha_1, \beta_1), \ldots, (\alpha_n, \beta_n) \in P$ with $n > 0$ such that $\alpha_1 \cdots \alpha_n = \beta_1 \cdots \beta_n$?

Examples

1.

	1	2	3
α_i	1	10111	10
β_i	11	101	01

solution

	2	1	1	
α	10111	1	1	$= 1011111$
β	101	11	11	$= 1011111$

2.

	1	2	3
α_i	10	011	101
β_i	101	11	011

no solution

solution must start with 1, followed by 3, followed by 3, ...

α	10101101
β	101011011

Theorem (Post)

PCP is undecidable

Definition (PCP Encoding 1, Signature)

PCP instance $P \subseteq \Gamma^+ \times \Gamma^+$

- signature $\mathcal{F}_P$ consists of
  - binary function symbol f
  - unary function symbol a for every $a \in \Gamma$
  - constants start, stop, c
- mapping $\varphi\colon \Gamma^* \times \mathcal{T}(\mathcal{F}_P, \mathcal{V}) \to \mathcal{T}(\mathcal{F}_P, \mathcal{V})$

$$\varphi(x,t) = \begin{cases} t & \text{if } x = \epsilon \\ a(\varphi(y,t)) & \text{if } x = ay \end{cases}$$

Notation

$x(t) = \varphi(x,t)$

Definition (PCP Encoding 1, Rewrite Rules)

PCP instance $P \subseteq \Gamma^+ \times \Gamma^+$

- TRS $\mathcal{R}_P$ over signature $\mathcal{F}_P$ consists of

$$\mathsf{start} \to \mathsf{f}(\alpha(\mathsf{c}),\beta(\mathsf{c})) \quad \forall\ (\alpha,\beta) \in P \qquad \mathsf{f}(x,x) \to \mathsf{stop}$$
$$\mathsf{f}(x,y) \to \mathsf{f}(\alpha(x),\beta(y)) \quad \forall\ (\alpha,\beta) \in P \qquad \mathsf{f}(x,y) \to \mathsf{start}$$

Lemma

$\forall$ PCP instance P $\quad \mathcal{R}_P$ is CR $\iff$ $\mathsf{f}(\mathsf{c},\mathsf{c})$ is CR $\iff$ $\mathcal{R}_P$ is WN
$\iff$ start is WN $\iff$ $\mathcal{R}_P$ is WCR
$\iff$ $\mathsf{f}(\mathsf{c},\mathsf{c})$ is WCR $\iff$ P has solution

Example

- PCP instance P

	1	2	3
α	1	10111	10
β	11	101	01

- TRS $\mathcal{R}_P$

$$\mathsf{start} \to \mathsf{f}(1(\mathsf{c}),11(\mathsf{c})) \qquad \mathsf{f}(x,y) \to \mathsf{f}(1(x),11(y)) \qquad \mathsf{f}(x,x) \to \mathsf{stop}$$
$$\mathsf{start} \to \mathsf{f}(10111(\mathsf{c}),101(\mathsf{c})) \qquad \mathsf{f}(x,y) \to \mathsf{f}(10111(x),101(y)) \qquad \mathsf{f}(x,y) \to \mathsf{start}$$
$$\mathsf{start} \to \mathsf{f}(10(\mathsf{c}),01(\mathsf{c})) \qquad \mathsf{f}(x,y) \to \mathsf{f}(10(x),01(y))$$

- $\mathsf{start} \to^*_{\mathcal{R}_P} \mathsf{stop}$:

$$\mathsf{start} \xrightarrow{1} \mathsf{f}(1(\mathsf{c}),11(\mathsf{c})) \xrightarrow{1} \mathsf{f}(11(\mathsf{c}),1111(\mathsf{c})) \xrightarrow{2} \mathsf{f}(1011111(\mathsf{c}),1011111(\mathsf{c})) \to \mathsf{stop}$$

Corollary

CR, WCR, WN are undecidable properties of (terms in) TRSs

Definition (PCP Encoding 2)

PCP instance $P \subseteq \Gamma^+ \times \Gamma^+$

- TRS $\mathcal{S}_P$ consists of

$$\mathsf{f}(\alpha(x),\beta(y),z) \to \mathsf{f}(x,y,z) \qquad \mathsf{f}(\alpha(\mathsf{c}),\beta(\mathsf{c}),z) \to \mathsf{f}(z,z,z)$$

$\forall\ (\alpha,\beta) \in P$

Lemma

$\forall$ PCP instance P $\quad \mathcal{S}_P$ is SN $\iff$ P has no solution

Outline

Homework Exercises for April 13

① Exercise 2.6. 1

② Exercise 3.3. 2

③ Exercise 3.4. 3

④ Exercise 3.12. 1

⑤ Exercise 2.36. ☆☆☆

Outline

Lecture Notes

- Section 2.1 (from Definition 2.1.14)
- Section 3.1
- Section 3.2 (until Theorem 3.2.4)
- Section 3.3 (from Definition 3.3.14)

Important Concepts

- canonical
- combinatory logic (CL)
- constructor
- constructor system (CS)
- defined symbol
- position
- rewrite rule
- string rewrite system (SRS)
- term rewrite system (TRS)
- term rewriting
- reduced