26S lecture 1

Term Rewriting

Philipp Dablander and **Aart Middeldorp**

Initial Remarks

- Term Rewriting is part of compulsory module 20 ("Ausgewählte Kapitel") in bachelor program Computer Science
- Term Rewriting is part of elective module 20 ("individual choice of specialization") in master program Computer Science
- any course offered by MIP can be used for "Ausgewählte Kapitel"
- other master courses with theory content (Logic and Learning specialization):
  - WM 2: Constraint Solving
  - WM 7: Interactive Theorem Proving in Isabelle / HOL
  - WM 7: Current Challenges in Probabilistic Learning, Inference, and their Applications
  - WM 8: Advanced Logic and Quantum Logic
  - WM 9: Research Seminar CL / TCS

Outline

Organisation

- LVA 703141 VU 3 – 5 ECTS 15:30 – 18:00 in HS 11
- http://cl-informatik.uibk.ac.at/teaching/ss26/trs OLAT

Consultation Hours

Philipp Dablander	3M03	Wednesday	10:00 – 11:30
Aart Middeldorp	3M07	Monday	12:00 – 13:30

Schedule

lecture 1	March 2	lecture 6	April 20	lecture 11	June 1
lecture 2	March 9	lecture 7	April 27	lecture 12	June 8
lecture 3	March 16	lecture 8	May 4	lecture 13	June 15
lecture 4	March 23	lecture 9	May 11	lecture 14	June 22 (test)
lecture 5	April 13	lecture 10	May 18		

Grading

$$\text{score} = \min\left(\max\left(\tfrac{50}{69}(E+P) + \tfrac{1}{3}T + B,\ T+B\right),\ 100\right)$$

- E: points for solved exercises (at most 84)
- P: points for presentation of solutions (at most 8)
- T: points for test (at most 100)
- B: points for bonus exercises (at most 20)

$$\text{grade} = \text{score} \in (-50) \to 5 \quad [50-63) \to 4 \quad [63-75) \to 3 \quad [75-88) \to 2 \quad [88-) \to 1$$

- solved exercises must be marked and solutions (PDF format) must be uploaded in OLAT before 10 am on Monday
- presentations are optional
- (optional) test on June 22

Grading (cont'd)

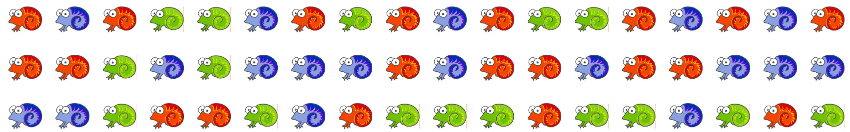
- VU $\Longrightarrow$ attendance is mandatory
- unexcused attendance is allowed twice $\Longrightarrow$ zero points
- dropping out without grade is possible until March 16

Presentations

- solutions will be presented in first part of every subsequent lecture
- scheduling of presentations in OLAT

evaluation 25S

Outline



A colony of chameleons includes 20 red, 18 blue, and 16 green individuals. Whenever two chameleons of different color meet, each changes to the third color. Some time passes during which no chameleons are born or die nor do any enter or leave the colony. Is it possible that at the end of this period, all 54 chameleons are the same color?

A team of genetic engineers decides to create cows that produce cola instead of milk. To that end they have to transform the DNA of the milk gene

TAGCTAGCTAGCT

in every fertilized egg into the cola gene

CTGACTGACT

Techniques exist to perform the following DNA substitutions

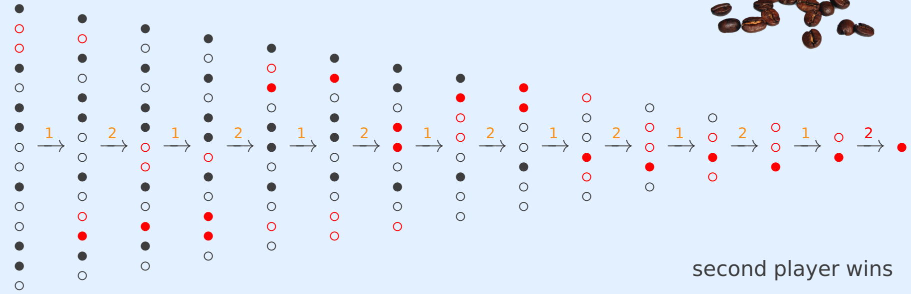
TCAT ↔ T   GAG ↔ AG   CTC ↔ TC   AGTA ↔ A   TAT ↔ CT

Recently it has been discovered that the mad cow disease is caused by a retrovirus with the following DNA sequence CTGCTACTGACT. What now, if accidentally cows with this virus are created? According to the engineers there is little risk because this never happened in their experiments, but various action groups demand absolute assurance.

Coffee beans come in two kinds called black (•) and white (○). A two−player game starts with a random sequence of black and white beans. In a move, a player must take two adjacent beans and put back one bean, according to the following set of rules:

• • → ○   ○ ○ → ○   • ○ → •   ○ • → •

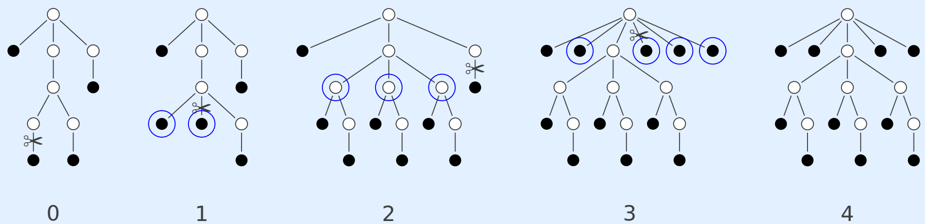
The player who puts the last black bean wins.



second player wins

Does the game terminate? Does one of the players have a winning strategy? What if the rules are changed to • • → ○ ○ ○ ○   ○ ○ → ○   • ○ → ○ ○ ○ •   ○ • → •   ?

The mythological monster Hydra is a dragon−like creature with multiple heads. Whenever Hercules in his fight chops off a head, more and more new heads can grow instead, since the beast gets increasingly angry. Hydra dies and Hercules wins if there are no heads left. Here we model a Hydra as an unordered tree. If Hercules cuts off a leaf l that has a grandparent g, the branch from g to the parent of l gets multiplied, with the number of copies depending on the number of decapitations so far.



Can Hercules win the battle?

Example (Addition on Natural Numbers in Unary Notation)

signature   0 (constant)   s (unary)   a (binary)

terms   0   s(0)   s(s(0))   a(s(0), s(0))   s(a(s(0), s(a(0, s(s(0))))))

rewrite rules
$$\mathsf{a}(0, y) \to y$$
$$\mathsf{a}(\mathsf{s}(x), y) \to \mathsf{s}(\mathsf{a}(x, y))$$

rewriting
$$\begin{aligned} \mathsf{a}(\mathsf{s}(\mathsf{s}(\mathsf{s}(0))), \mathsf{s}(\mathsf{s}(0))) &\to \mathsf{s}(\mathsf{a}(\mathsf{s}(\mathsf{s}(0)), \mathsf{s}(\mathsf{s}(0)))) \\ &\to \mathsf{s}(\mathsf{s}(\mathsf{a}(\mathsf{s}(0), \mathsf{s}(\mathsf{s}(0))))) \\ &\to \mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{a}(0, \mathsf{s}(\mathsf{s}(0)))))) \\ &\to \mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(0))))) \end{aligned}$$
normal form

Example (Addition on Natural Numbers in Decimal Notation)

signature 0 1 ... 9 (constants) $+$ $:$ (binary, infix)

terms $1+3$ $2+(7:3)$ $(2:(3:x))+((1+7):2)$

rewrite rules

$0+0 \to 0$	$1+0 \to 1$	$\cdots$	$9+0 \to 9$	$0:x \to x$
$0+1 \to 1$	$1+1 \to 2$	$\cdots$	$9+1 \to 1:0$	$x+(y:z) \to y:(x+z)$
$0+2 \to 2$	$1+2 \to 3$	$\cdots$	$9+2 \to 1:1$	$(x:y)+z \to x:(y+z)$
$0+3 \to 3$	$1+3 \to 4$	$\cdots$	$9+3 \to 1:2$	$x:(y:z) \to (x+y):z$
$0+4 \to 4$	$1+4 \to 5$	$\cdots$	$9+4 \to 1:3$	
$0+5 \to 5$	$1+5 \to 6$	$\cdots$	$9+5 \to 1:4$	
$0+6 \to 6$	$1+6 \to 7$	$\cdots$	$9+6 \to 1:5$	
$0+7 \to 7$	$1+7 \to 8$	$\cdots$	$9+7 \to 1:6$	
$0+8 \to 8$	$1+8 \to 9$	$\cdots$	$9+8 \to 1:7$	
$0+9 \to 9$	$1+9 \to 1:0$	$\cdots$	$9+9 \to 1:8$	

rewriting $(2:3)+(7:7) \to^* (1:0):0$ normal form

Example (Group Theory)

signature e (constant) $^-$ (unary, postfix) $\cdot$ (binary, infix)

axioms $\mathsf{e} \cdot x \approx x$ $x^- \cdot x \approx \mathsf{e}$ $(x \cdot y) \cdot z \approx x \cdot (y \cdot z)$ $\mathcal{E}$

theorems $\mathsf{e}^- \approx_{\mathcal{E}} \mathsf{e}$ $(x \cdot y)^- \approx_{\mathcal{E}} y^- \cdot x^-$

rewrite rules $\mathcal{R}$

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

1. $s \approx t$ is valid in $\mathcal{E}$ ($s \approx_{\mathcal{E}} t$) $\iff$ s and t have same normal form with respect to $\mathcal{R}$
2. $\mathcal{R}$ admits no infinite computations

1 & 2 $\implies$ $\mathcal{E}$ has decidable validity problem

Example (Combinatory Logic)

signature S K I (constants) $\cdot$ (application, binary, infix)

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

rewrite rules

$$\begin{array}{rcl} \mathsf{I} \cdot x & \to & x \\ (\mathsf{K} \cdot x) \cdot y & \to & x \\ ((\mathsf{S} \cdot x) \cdot y) \cdot z & \to & (x \cdot z) \cdot (y \cdot z) \end{array}$$

rewriting $((\mathsf{S} \cdot \mathsf{K}) \cdot \mathsf{K}) \cdot x \to (\mathsf{K} \cdot x) \cdot (\mathsf{K} \cdot x) \to x$

inventor Moses Schönfinkel (1924)

Combinatory Logic is Turing–complete

Outline

Definitions (Terms)

- signature $\mathcal{F}$ function symbols with arities
- variables $\mathcal{V}$ $\mathcal{F} \cap \mathcal{V} = \varnothing$ infinitely many
- terms $\mathcal{T}(\mathcal{F},\mathcal{V})$ smallest set such that
  - $\mathcal{V} \subseteq \mathcal{T}(\mathcal{F},\mathcal{V})$
  - if $f \in \mathcal{F}$ has arity $n \geqslant 0$ and $t_1, \ldots, t_n \in \mathcal{T}(\mathcal{F},\mathcal{V})$ then $f(t_1, \ldots, t_n) \in \mathcal{T}(\mathcal{F},\mathcal{V})$
- ground terms $\mathcal{T}(\mathcal{F})$ smallest set such that
  - if $f \in \mathcal{F}$ has arity $n \geqslant 0$ and $t_1, \ldots, t_n \in \mathcal{T}(\mathcal{F})$ then $f(t_1, \ldots, t_n) \in \mathcal{T}(\mathcal{F})$

Definitions (Operations on Terms)

- $\mathcal{V}\mathrm{ar}(\cdot)$ $\mathcal{V}\mathrm{ar}((2:x)+((1:x):y)) = \{x, y\}$

$$\mathcal{V}\mathrm{ar}(t) = \begin{cases} \{t\} & \text{if } t \in \mathcal{V} \\ \bigcup_{i=1}^{n} \mathcal{V}\mathrm{ar}(t_i) & \text{if } t = f(t_1, \ldots, t_n) \end{cases}$$

- $\mathcal{F}\mathrm{un}(\cdot)$ $\mathcal{F}\mathrm{un}((2:x)+((1:x):y)) = \{2, :, +, 1\}$

$$\mathcal{F}\mathrm{un}(t) = \begin{cases} \varnothing & \text{if } t \in \mathcal{V} \\ \{f\} \cup \bigcup_{i=1}^{n} \mathcal{F}\mathrm{un}(t_i) & \text{if } t = f(t_1, \ldots, t_n) \end{cases}$$

- size $|\cdot|$ $|(2:x)+((1:x):y)| = 9$

$$|t| = \begin{cases} 1 & \text{if } t \in \mathcal{V} \\ 1 + \sum_{i=1}^{n} |t_i| & \text{if } t = f(t_1, \ldots, t_n) \end{cases}$$

Definitions (Operations on Terms)

- root$(\cdot)$

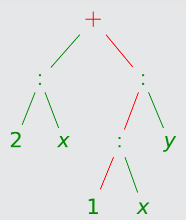
$$\mathrm{root}(t) = \begin{cases} t & \text{if } t \in \mathcal{V} \\ f & \text{if } t = f(t_1, \ldots, t_n) \end{cases}$$

- height$(\cdot)$

$$\mathrm{height}(t) = \begin{cases} 0 & \text{if } t \in \mathcal{V} \text{ or } t \text{ is constant} \\ 1 + \max_{1 \leqslant i \leqslant n} \mathrm{height}(t_i) & \text{if } t = f(t_1, \ldots, t_n) \text{ with } n \geqslant 1 \end{cases}$$

Example

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



$\mathrm{root}((2:x)+((1:x):y)) = +$

$\mathrm{height}((2:x)+((1:x):y)) = 3$

Definitions (Subterms)

- $s \trianglelefteq t$ s is subterm of t
  - $s = t$ or
  - $t = f(t_1, \ldots, t_n)$ and $s \trianglelefteq t_i$ for some $1 \leqslant i \leqslant n$
- $s \vartriangleleft t$ s is proper subterm of t
  - $t = f(t_1, \ldots, t_n)$ and $s \trianglelefteq t_i$ for some $1 \leqslant i \leqslant n$

Example

term $(2:x)+((1:x):y)$ has subterms

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

Outline

Definitions (Context)

- 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

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

Examples

- $\square$ $\quad \mathsf{s}(0) + \mathsf{s}(\mathsf{s}(\square))$ $\quad \square + x$
- $\square[\mathsf{s}(0)] = \mathsf{s}(0)$ $\quad (\square + x)[0 + x] = (0 + x) + x$
- subterm relation is not closed under contexts: $0 \trianglelefteq \mathsf{s}(0)$ but $0 + 0 \ntrianglelefteq \mathsf{s}(0) + 0$

Lemmata

- $s \trianglelefteq t \quad \Longleftrightarrow \quad t = C[s]$ for some context C
- $s \triangleleft t \quad \Longleftrightarrow \quad t = C[s]$ for some context $C \neq \square$

Outline

Definitions (Substitution)

- 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
- (unique) substitution with empty domain is denoted by ε
- application of substitution σ to term t

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

Example

$t = x + \mathsf{s}(y + z)$ $\qquad \sigma = \{x \mapsto \mathsf{s}(y),\ y \mapsto x + \mathsf{s}(0)\}$ $\qquad t\sigma = \mathsf{s}(y) + \mathsf{s}((x + \mathsf{s}(0)) + z)$

Definition (Closure under Substitutions)

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

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

Lemma

subterm relation is closed under substitutions

Definition (Matching Problem)

instance: terms s, t

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

Examples

1. $\mathsf{e}^- \cdot \mathsf{e}^{--}$ is instance of $x \cdot x^-$: $(x \cdot x^-)\sigma = \mathsf{e}^- \cdot \mathsf{e}^{--}$ for $\sigma = \{x \mapsto \mathsf{e}^-\}$
2. $\mathsf{e}^- \cdot (\mathsf{e}^- \cdot \mathsf{e}^-)$ is no instance of $x^- \cdot (x \cdot y)$

Remarks

- term t can be rewritten if subterm of t is instance of left–hand side of rewrite rule
- matching problem is decidable (in linear time)

Definition (Matching Problem)

instance: terms s, t

question: $\exists$ substitution σ: $s\sigma = t$?

Matching Algorithm

① start with $\{s \mapsto t\}$

② repeatedly apply following transformation rules

$$\{f(s_1, \dots, s_n) \mapsto f(t_1, \dots, t_n)\} \uplus S \implies \{s_1 \mapsto t_1, \dots, s_n \mapsto t_n\} \cup S$$

$$\{f(s_1, \dots, s_n) \mapsto g(t_1, \dots, t_m)\} \uplus S \implies \bot \quad \text{if } f \neq g$$

$$\{f(s_1, \dots, s_n) \mapsto x\} \uplus S \implies \bot$$

$$\{x \mapsto t\} \uplus S \implies \bot \quad \text{if } S \text{ contains } x \mapsto u \text{ with } t \neq u$$

Examples

1. $\mathsf{s}(y) + \mathsf{s}((x + \mathsf{s}(0)) + z)$ is instance of $x + \mathsf{s}(y + z)$:

$$\begin{aligned} & \{x + \mathsf{s}(y+z) \mapsto \mathsf{s}(y) + \mathsf{s}((x + \mathsf{s}(0)) + z)\} \\ \implies & \{x \mapsto \mathsf{s}(y), \mathsf{s}(y+z) \mapsto \mathsf{s}((x + \mathsf{s}(0)) + z)\} \\ \implies & \{x \mapsto \mathsf{s}(y), y + z \mapsto (x + \mathsf{s}(0)) + z\} \\ \implies & \{x \mapsto \mathsf{s}(y), y \mapsto x + \mathsf{s}(0), z \mapsto z\} \end{aligned}$$

2. $(\mathsf{e} \cdot x)^- \cdot ((\mathsf{e} \cdot \mathsf{e}) \cdot x)$ is no instance of $x^- \cdot (x \cdot y)$:

$$\begin{aligned} & \{x^- \cdot (x \cdot y) \mapsto (\mathsf{e} \cdot x)^- \cdot ((\mathsf{e} \cdot \mathsf{e}) \cdot x)\} \\ \implies & \{x^- \mapsto (\mathsf{e} \cdot x)^-, x \cdot y \mapsto (\mathsf{e} \cdot \mathsf{e}) \cdot x\} \\ \implies & \{x \mapsto \mathsf{e} \cdot x, x \cdot y \mapsto (\mathsf{e} \cdot \mathsf{e}) \cdot x\} \\ \implies & \{x \mapsto \mathsf{e} \cdot x, x \mapsto \mathsf{e} \cdot \mathsf{e}, y \mapsto x\} \\ \implies & \bot \end{aligned}$$

Definition

- solution of matching problem $\{s_1 \mapsto t_1, \ldots, s_n \mapsto t_n\}$ is substitution σ such that $s_i\sigma = t_i$ for all $1 \leqslant i \leqslant n$
- $\bot$ has no solutions

Lemmata

- there are no infinite derivations $T_1 \implies T_2 \implies \cdots$
- if $S \implies^* T$ then S and T have same solutions
- if $S \implies^* T$ is maximal derivation and $T \neq \bot$ then T is solution of S

Definition

term is linear if it does not contain multiple occurrences of same variable

Outline

Homework Exercises for March 9

① Exercise 2. ❶
② Exercise 3(b). ❷
③ Exercise 2.5. ❷
④ Exercise 2.15. ❶
⑤ Exercise 2.16. ❶
⑥ Exercise 4. ☆☆☆

Starred Exercises

. . . are optional; solutions give bonus points

Outline

Lecture Notes

- Section 2.1 (except Definition 2.1.14 — Example 2.1.17 and Definition 2.1.19)

Important Concepts

- closure under contexts
- closure under substitutions
- context
- ground term
- instance
- matching algorithm
- substitution
- term