

Automated Reasoning*

Uwe Waldmann

Summer Term 2011

Topics of the Course

Preliminaries

- abstract reduction systems
- well-founded orderings

Propositional logic

- syntax, semantics
- calculi: DPLL-procedure, ...
- implementation: 2-watched literal, clause learning

First-order predicate logic

- syntax, semantics, model theory, ...
- calculi: resolution, tableaux, ...
- implementation: sharing, indexing

First-order predicate logic with equality

- term rewriting systems
- calculi: Knuth-Bendix completion, dependency pairs

*This document contains the text of the lecture slides (almost verbatim) plus some additional information, mostly proofs of theorems that are presented on the blackboard during the course. It is not a full script and does not contain the examples and additional explanations given during the lecture. Moreover it should not be taken as an example how to write a research paper – neither stylistically nor typographically.

1 Preliminaries

Literature: Franz Baader and Tobias Nipkow: *Term rewriting and all that*, Cambridge Univ. Press, 1998, Chapter 2.

Throughout the lecture, we will have to work with reduction systems,

on the object level, in particular in the section on equality,

and on the meta level, i. e., to describe deduction calculi.

1.1 Abstract Reduction Systems

An *abstract reduction system* is a pair (A, \rightarrow) , where

A is a set,

$\rightarrow \subseteq A \times A$ is a binary relation on A .

The relation \rightarrow is usually written in infix notation, i. e., $a \rightarrow b$ instead of $(a, b) \in \rightarrow$.

Let $\rightarrow' \subseteq A \times B$ and $\rightarrow'' \subseteq B \times C$ be two binary relations. Then the binary relation $(\rightarrow' \circ \rightarrow'') \subseteq A \times C$ is defined by

$$a (\rightarrow' \circ \rightarrow'') c \quad \text{if and only if} \quad a \rightarrow' b \text{ and } b \rightarrow'' c \text{ for some } b \in B.$$

\rightarrow^0	$= \{ (a, a) \mid a \in A \}$	<i>identity</i>
\rightarrow^{i+1}	$= \rightarrow^i \circ \rightarrow$	<i>i + 1-fold composition</i>
\rightarrow^+	$= \bigcup_{i>0} \rightarrow^i$	<i>transitive closure</i>
\rightarrow^*	$= \bigcup_{i \geq 0} \rightarrow^i = \rightarrow^+ \cup \rightarrow^0$	<i>reflexive transitive closure</i>
$\rightarrow^=$	$= \rightarrow \cup \rightarrow^0$	<i>reflexive closure</i>
\rightarrow^{-1}	$= \leftarrow = \{ (b, c) \mid c \rightarrow b \}$	<i>inverse</i>
\leftrightarrow	$= \rightarrow \cup \leftarrow$	<i>symmetric closure</i>
\leftrightarrow^+	$= (\leftrightarrow)^+$	<i>transitive symmetric closure</i>
\leftrightarrow^*	$= (\leftrightarrow)^*$	<i>refl. trans. symmetric closure</i>

$b \in A$ is *reducible*, if there is a c such that $b \rightarrow c$.

b is *in normal form (irreducible)*, if it is not reducible.

c is a *normal form of b* , if $b \rightarrow^* c$ and c is in normal form.

Notation: $c = b \downarrow$ (if the normal form of b is unique).

A relation \rightarrow is called

terminating, if there is no infinite descending chain $b_0 \rightarrow b_1 \rightarrow b_2 \rightarrow \dots$

normalizing, if every $b \in A$ has a normal form.

Lemma 1.1 *If \rightarrow is terminating, then it is normalizing.*

Note: The reverse implication does not hold.

1.2 Well-Founded Orderings

Termination of reduction systems is strongly related to the concept of well-founded orderings.

Partial Orderings

A *strict partial ordering* \succ on a set M is a transitive and irreflexive binary relation on M .

An $a \in M$ is called *minimal*, if there is no b in M such that $a \succ b$.

An $a \in M$ is called *smallest*, if $b \succ a$ for all $b \in M$ different from a .

Notation:

\prec for the inverse relation \succ^{-1}

\succeq for the reflexive closure ($\succ \cup =$) of \succ

Well-Foundedness

A strict partial ordering \succ on M is called *well-founded* (*Noetherian*), if there is no infinite descending chain $a_0 \succ a_1 \succ a_2 \succ \dots$ with $a_i \in M$.

Well-Foundedness and Termination

Lemma 1.2 *If \succ is a well-founded partial ordering and $\rightarrow \subseteq \succ$, then \rightarrow is terminating.*

Lemma 1.3 *If \rightarrow is a terminating binary relation over A , then \rightarrow^+ is a well-founded partial ordering.*

Proof. Transitivity of \rightarrow^+ is obvious; irreflexivity and well-foundedness follow from termination of \rightarrow . □

Well-Founded Orderings: Examples

Natural numbers. $(\mathbb{N}, >)$

Lexicographic orderings. Let $(M_1, \succ_1), (M_2, \succ_2)$ be well-founded orderings. Then let their *lexicographic combination*

$$\succ = (\succ_1, \succ_2)_{lex}$$

on $M_1 \times M_2$ be defined as

$$(a_1, a_2) \succ (b_1, b_2) \quad :\Leftrightarrow \quad a_1 \succ_1 b_1 \text{ or } (a_1 = b_1 \text{ and } a_2 \succ_2 b_2)$$

(analogously for more than two orderings)

This again yields a well-founded ordering (proof below).

Length-based ordering on words. For alphabets Σ with a well-founded ordering $>_\Sigma$, the relation \succ defined as

$$w \succ w' \quad :\Leftrightarrow \quad |w| > |w'| \text{ or } (|w| = |w'| \text{ and } w >_{\Sigma, lex} w')$$

is a well-founded ordering on Σ^* (Exercise).

Counterexamples:

$(\mathbb{Z}, >)$

$(\mathbb{N}, <)$

the lexicographic ordering on Σ^*

Basic Properties of Well-Founded Orderings

Lemma 1.4 (M, \succ) is well-founded if and only if every $\emptyset \subset M' \subseteq M$ has a minimal element.

Lemma 1.5 (M_1, \succ_1) and (M_2, \succ_2) are well-founded if and only if $(M_1 \times M_2, \succ)$ with $\succ = (\succ_1, \succ_2)_{lex}$ is well-founded.

Proof. (i) “ \Rightarrow ”: Suppose $(M_1 \times M_2, \succ)$ is not well-founded. Then there is an infinite sequence $(a_0, b_0) \succ (a_1, b_1) \succ (a_2, b_2) \succ \dots$

Let $A = \{a_i \mid i \geq 0\} \subseteq M_1$. Since (M_1, \succ_1) is well-founded, A has a minimal element a_n . But then $B = \{b_i \mid i \geq n\} \subseteq M_2$ can not have a minimal element, contradicting the well-foundedness of (M_2, \succ_2) .

(ii) “ \Leftarrow ”: obvious. □

Monotone Mappings

Let $(M_1, >_1)$ and $(M_2, >_2)$ be strict partial orderings. A mapping $\varphi : M_1 \rightarrow M_2$ is called *monotone*, if $a >_1 b$ implies $\varphi(a) >_2 \varphi(b)$ for all $a, b \in M_1$.

Lemma 1.6 *If φ is a monotone mapping from $(M_1, >_1)$ to $(M_2, >_2)$ and $(M_2, >_2)$ is well-founded, then $(M_1, >_1)$ is well-founded.*

Noetherian Induction

Theorem 1.7 (Noetherian Induction) *Let (M, \succ) be a well-founded ordering, let Q be a property of elements of M .*

If for all $m \in M$ the implication

*if $Q(m')$ for all $m' \in M$ such that $m \succ m'$,¹
then $Q(m)$.²*

is satisfied, then the property $Q(m)$ holds for all $m \in M$.

Proof. Let $X = \{m \in M \mid Q(m) \text{ false}\}$. Suppose, $X \neq \emptyset$. Since (M, \succ) is well-founded, X has a minimal element m_1 . Hence for all $m' \in M$ with $m' \prec m_1$ the property $Q(m')$ holds. On the other hand, the implication which is presupposed for this theorem holds in particular also for m_1 , hence $Q(m_1)$ must be true so that m_1 can not be in X . *Contradiction.* □

Multisets

Let M be a set. A *multiset* S over M is a mapping $S : M \rightarrow \mathbb{N}$. Hereby $S(m)$ specifies the number of occurrences of elements m of the base set M within the multiset S .

Example. $S = \{a, a, a, b, b\}$ is a multiset over $\{a, b, c\}$, where $S(a) = 3$, $S(b) = 2$, $S(c) = 0$.

We say that m is an *element* of S , if $S(m) > 0$.

We use set notation (\in , \subset , \subseteq , \cup , \cap , etc.) with analogous meaning also for multisets, e. g.,

$$\begin{aligned}(S_1 \cup S_2)(m) &= S_1(m) + S_2(m) \\ (S_1 \cap S_2)(m) &= \min\{S_1(m), S_2(m)\}\end{aligned}$$

¹induction hypothesis

²induction step

A multiset S is called *finite*, if

$$|\{m \in M \mid S(m) > 0\}| < \infty.$$

From now on we only consider finite multisets.

Multiset Orderings

Lemma 1.8 (König's Lemma) *Every finitely branching tree with infinitely many nodes contains an infinite path.*

Let (M, \succ) be a strict partial ordering. The *multiset extension* of \succ to multisets over M is defined by

$$\begin{aligned} S_1 \succ_{\text{mul}} S_2 &\Leftrightarrow \\ &S_1 \neq S_2 \text{ and} \\ &\forall m \in M: (S_2(m) > S_1(m) \\ &\quad \Rightarrow \exists m' \in M: m' \succ m \text{ and } S_1(m') > S_2(m')) \end{aligned}$$

Theorem 1.9

- (a) \succ_{mul} is a strict partial ordering.
- (b) \succ well-founded $\Rightarrow \succ_{\text{mul}}$ well-founded.
- (c) \succ total $\Rightarrow \succ_{\text{mul}}$ total.

Proof. see Baader and Nipkow, page 22–24. □