UPPSALA UNIVERSITET
Matematiska institutionen
Erik Palmgren

Kompletterande material
Applied Logic
2010-10-12

1 Termination and abstract reduction systems

The following material is mainly based on

W. Klop: Term Rewriting Systems. In: S. Abramsky *et al.* (eds.) *Handbook of Logic in Computer Science,* Vol 2. Oxford University Press 1992.

1.1 Well-founded relations

A binary relation $(A, <)$ is *well-founded* if there is no infinite descending sequence

$$a_1 > a_2 > a_3 > \cdots$$

in A.

Example 1.1 The natural numbers $(\mathbb{N}, <)$ with the usual order is well-founded, while this is not the case for the integers $(\mathbb{Z}, <)$:

$$0 > -1 > -2 > -3 > \cdots$$

Example 1.2 Let $R \subseteq \mathbb{N} \times \mathbb{N}$ be the successor relation defined by

$$R(x, y) \Longleftrightarrow x + 1 = y.$$

Then $(\mathbb{N}, R)$ is well-founded. Note that R is not transitive.

Example 1.3 Consider $(\mathbb{N} \times \mathbb{N}, <')$ with the lexicographic order $(a, b) <' (c, d)$ iff $a < c$ or $a = c$ and $b < d$. We have

$$(0,0) <' (0,1) <' \cdots <' (0,n) <' \cdots <' (1,0) <' (1,1) <' \cdots (2,0) <' \cdots <' (m,0).$$

This relation is well-founded. For suppose $(a_{n+1}, b_{n+1}) <' (a_n, b_n)$ for all n. Then the sequence (a_n) is eventually constant from, say N, and onwards. Hence $b_{k+1} < b_k$ for all $k \geq N$, which is impossible. □

Example 1.4 Let Σ be a signature and let $\mathbb{X}$ be a nonempty set of variables. Order the set $\mathrm{Ter}(\Sigma, \mathbb{X})$ of terms over Σ and $\mathbb{X}$ as follows

$$t \sqsubset s \iff t \neq s \text{ and } t \text{ is a subterm of } s.$$

If $t \sqsubset s$, we say that t is a *strict subterm* of s, or that it is *structurally smaller* than s. We leave as an exercise to show that $(\mathrm{Ter}(\Sigma, \mathbb{X}, \sqsubset)$ is a well-founded relation. Example: for $\Sigma = \{0, f(\cdot), g(\cdot,\cdot)\}$, $\mathbb{X} = \{x, y, z, \ldots\}$ we have

$$x \sqsubset f(x) \qquad y \not\sqsubset f(x) \qquad f(y) \sqsubset g(f(f(y)), f(0)) \qquad g(0,z) \sqsubset f(g(g(0,z),z)) \quad \square$$

This kind of order relation is useful when proving termination of functional programs.

That a relation is well-founded is the same as saying that a certain induction principle is valid, so called *Noetherian*[1] *induction,* or *well-founded induction.* Let $(A, <)$ be a binary relation. A subset $S \subseteq A$ is *progressive* iff

$$(\forall a)[(\forall b < a) b \in S \Rightarrow a \in S].$$

Thus in a progressive set, if all the elements that lie before a are in the set, then also a is in the set. A binary relation $(A, <)$ is called *inductive* iff $S = A$ whenever $S \subseteq A$ is a progressive subset. What are the progressive subsets S of $(\mathbb{N}, <)$? Clearly, there are no elements before 0, and hence trivially $0 \in S$. Now suppose that $\{0, 1, \ldots, n\} \subseteq S$. Then all elements before $n+1$ are in S. Hence also $n+1 \in S$. By induction $S = \mathbb{N}$. Above we just showed that $(\mathbb{N}, <)$ is inductive. In fact, we have

Theorem 1.5 *A binary relation is well-founded iff it is inductive.*

Proof. Suppose that $(A, <)$ is an inductive binary relation. Define the following subset of A

$$S = \{b \in A : \text{there is no infinite sequence } b > a_1 > a_2 > a_3 \cdots\}.$$

It is easily checked that S is progressive set. Hence $S = A$, so $(A, <)$ is well-founded.

Now suppose that $(A, <)$ is not inductive. Hence there is a progressive set $S \subset A$. Let $x_0 \in A \setminus S$. Since S is progressive, there must be some $x_1 < x_0$ such that $x_1 \notin S$. But then again there must be some $x_2 < x_1$ such that $x_2 \notin S$. Proceeding in this way one constructs a sequence

$$x_0 > x_1 > x_2 > \cdots$$

[1] After Emmy Noether, a pioneer in abstract algebra.

which shows that $(A, <)$ is not well-founded. $\square$

Let $(A, <)$ be a binary relation. The *transitive closure* $(A, <^+)$ of $(A, <)$ is defined by $a <^+ b$ iff there is a sequence $a_1 < \cdots < a_n$, $n \geq 1$, with $a = a_1$ and $b = a_n$. Thus, for example, $(\mathbb{N}, <)$ is the transitive closure of $(\mathbb{N}, R)$ from Example 1.2. We leave the following as an easy exercise

Proposition 1.6 *Let $(A, <)$ be a binary relation. Then $(A, <)$ is well-founded iff $(A, <^+)$ is well-founded.* $\square$

Reduction of one ordering to another. Suppose that $(A, <)$ is well-founded, $(B, <')$ a binary relation and $f : B \to A$ a function such that, for all x and y

$$x <' y \Rightarrow f(x) < f(y).$$

Then $(B, <')$ is well-founded, since if there was an infinite strictly decreasing sequence in B, we could just apply f to each term an obtain such sequence in A, which is impossible. This fact can sometimes provide an easy proof that a relation is well-founded. For instance consider Example 1.4. We know that $(\mathbb{N}, <)$ is well-founded. Let $h : \mathrm{Ter}(\Sigma, \mathbb{X}) \to \mathbb{N}$ be the height function where $h(a) = 0$ for variables and constants a, and for a function term of arity $n \geq 1$

$$h(f(t_1, \ldots, t_n)) = 1 + \max(h(t_1), \ldots, h(t_n)).$$

Clearly $t \sqsubset s$ implies $h(t) < h(s)$. This shows that the strict subterm order is well-founded.

Lexicographic orderings. Let $(A, <_A)$ and $(B, <_B)$ be two binary relation. The *lexicographic combination* of these relations $(A \times B, <_{A,B})$ is defined as

$$(x, y) <_{A,B} (u, v) \Longleftrightarrow x <_A u \text{ or } x = u \text{ and } y <_B v.$$

Proposition 1.7 *Let $(A, <_A)$ and $(B, <_B)$ be well-founded binary relations. Then their lexicographic combination $(A \times B, <_{A,B})$ is well-founded.*

Proof. Analogous to Example 1.3. $\square$

Well-quasi-orders. We introduce a notion related to that of a well-founded set. A binary relation (A, R) is a *quasi-order* if it is reflexive and transitive. A quasi-order (A, R) is a *well-quasi-order* if for every infinite sequence $a_1, a_2, a_3, \ldots$ in A there are some $m < n$ such that $R(a_m, a_n)$.

Example 1.8 $(\mathbb{N}, \leq)$ is a well-quasi-order. This is the case, since every infinite sequence in $\mathbb{N}$ has a minimum.

More generally we have:

Proposition 1.9 *Let $(A, <)$ be a linear order. Define the relation*

$$x \leq y \iff \neg y < x.$$

Then $(A, <)$ is wellfounded iff $(A, \leq)$ is a well-quasi-order.

Proof. Suppose that $(A, <)$ is wellfounded. Let $a_1, a_2, a_3, \ldots$ be an infinite sequence of elements of A. Then it is impossible that $a_{i+1} < a_i$ for all i. Hence $\neg(a_{i+1} < a_i)$ for some i. That is $a_i \leq a_{i+1}$.

Conversely, assume that $(A, \leq)$ is a well-quasi-order. Suppose that $a_1 > a_2 > a_3 > \cdots$ is an infinite, strictly decreasing sequence in A. Then since $\leq$ is a well-quasi-order, there are some $m < n$, such that $a_m \leq a_n$. By transtivity and linearity of $<$ it follows that $a_m = a_n$ — a contradiction. □

Lemma 1.10 *In any infinite sequence $a_1, a_2, a_3, \ldots$ of natural numbers there is an infinite subsequence such that $b_1 \leq b_2 \leq b_3 \leq \cdots$.*

Proof. Let b_1 be the first minimum (say a_{i_1}) of the sequence $a_1, a_2, a_3, \ldots$. Let $b_2 = a_{i_2}$ be the first minimum of the remaining sequence $a_{i_1+1}, a_{i_1+2}, a_{i_1+3}, \ldots$. Let $b_3 = a_{i_3}$ be the first minimum of the remaining sequence $a_{i_2+1}, a_{i_2+2}, a_{i_2+3}, \ldots$ and so on. Clearly $b_1, b_2, b_3, \ldots$ forms an increasing subsequence of the given sequence. □

Example 1.11 The relation $P(x, y)$: x is a substring of a permutation of y is a quasi-order on $L = \{0, 1\}^*$. We have $P(1010, 010010)$ but $\neg P(1011, 010010)$.

It is more difficult to see that P is actually a well-quasi-order. Let $s(a, x)$ denote the number of occurrences of a in x. Note that $P(x, y)$ iff $s(0, x) \leq s(0, y)$ and $s(1, x) \leq s(1, y)$. The relation is then expressed in terms of occurence count. Suppose now that $u_1, u_2, u_3, \ldots$ is a given sequence strings in L. Consider the sequence $s(0, u_1), s(0, u_2), s(0, u_3), \ldots$ of natural numbers. Then by Lemma 1.10 there is a subsequence $v_1, v_2, v_3, \ldots$ of the given sequence such that

$$s(0, v_1) \leq s(0, v_2) \leq s(0, v_3) \leq \cdots$$

Since $(\mathbb{N}, \leq)$ is a well-quasi-order there is in this sequence some $m < n$ such that $s(1, v_m) \leq s(1, v_n)$. But then $P(v_m, v_n)$ which was to be proven. □

This result can be generalised to arbitrary finite alphabets (See Exercises). Thus if you have an infinite row of books (which may arbitrary thick) there

is always some book whose text may be obtained by cutting out letters from another book and rearranging them. Even more amazingly, you do not have to rearrange the letters:

Proposition 1.12 *Let Σ be a finite alphabet. Define the relation on the set Σ^* of strings:*

$$K(u,v) \Longleftrightarrow u \text{ is obtained by removing zero or more symbols from } v.$$

Then K is a well-quasi-order.

Proof. A sequence $u_1, u_2, u_3, \ldots$ of strings in Σ^* is called *bad* if $\neg K(u_m, u_n)$ for all $m < n$. Suppose that K is not a well-quasi-order. Thus there is at least one bad sequence. In a bad sequence there are no empty strings, and any subsequence is obviously still bad. Let v_1 be a shortest string which is the first term of a bad sequence. Then let v_2 be a shortest string such that v_1, v_2 are the first two terms of a bad sequence. More generally, let v_n be a shortest string such that $v_1, v_2, \ldots, v_n$ are the first n terms of a bad sequence. Each v_i is a non-empty string, so we may write $v_i = a_i w_i$ where $a_i \in \Sigma$. Since Σ is finite, some symbol occurs as initial symbol in infinitely many of the strings v_i. Let k_1 be the least such that a_{k_1} occurs infinitely often as initial symbol. Suppose that $k_1 < k_2 < k_3 < \ldots$ are the indices of strings that begin with a_{k_1}. Then

$$a_1 w_1, a_2 w_2, \ldots, a_{k_1-1} w_{k_1-1}, w_{k_1}, w_{k_2}, w_{k_3}, \ldots$$

is a bad sequence, since all v_{k_i} begin with the same symbol a_{k_1} which is different from $a_1, \ldots, a_{k_1-1}$. But now w_{k_1} is one symbol shorter than v_{k_1}, contradicting the construction of v_{k_1}.

Hence there are no bad sequences. □

Kruskal's Theorem

This theorem is very useful proving termination of term rewriting systems. We refer to Dershowitz and Jouannaud (1990).

Let S be a set. Let $\mathcal{T}(S)$ be the set of terms formed in the following way:

(a) $m \in \mathcal{T}(S)$ for any $m \in S$,

(b) If $m \in S$, and $t_1, \ldots, t_k \in \mathcal{T}(S)$ then $m(t_1, \ldots, t_k) \in \mathcal{T}(S)$.

For $S = \mathbb{N}$, the expressions are thus 3, $0(1, 0(2))$, $2(1, 3(2, 2, 1(0)))$ some examples of such terms.

Suppose that $\leq$ is a quasi-order on S. Define the following quasi-order on $\mathcal{T}(S)$: $t \preceq s$ if t can be obtained from s by zero or more of the following operations

(a) replace $m(t_1, \ldots, t_n)$ by t_i where $1 \leq i \leq n$

(b) replace $m(t_1, \ldots, t_n)$ by $p(t_1, \ldots, t_n)$ for $p < m$

(c) replace $m(t_1, \ldots, t_i, \ldots, t_n)$ by $q(t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n)$ for $1 \leq i \leq n$ and $q \leq m$.

(d) replace $m(t_1, \ldots, t_n)$ by $q(t_1, \ldots, t_n)$ if $m \leq q$ and $q \leq m$.

Example 1.13 Consider the standard order $(\mathbb{N}, \leq)$. On $\mathcal{T}(\mathbb{N})$ we have $0(1, 0(2)) \preceq 2(1, 0(2)) \preceq 2(1, 3(2)) \preceq 2(1, 3(2, 2)) \preceq 2(1, 3(2, 2, 1)) \preceq 2(1, 3(2, 2, 1(0)))$. But $1(1, 1) \not\preceq 1(1, 0)$.

Theorem 1.14 (Kruskal) *$\preceq$ is a well-quasi-order on $\mathcal{T}(S, \leq)$ whenever $(S, \leq)$ is a well-quasi-order.*

The proof is difficult and beyond the scope of this course. However, as much can be said that it uses the technique of *minimal bad sequences* illustrated in Lemma 1.10 and Proposition 1.12.

Exercises

1. Show that the following program $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ terminates by using a lexicographic combination

$$\begin{aligned} f(0, y) &= y \\ f(S(x), 0) &= S(x) \\ f(S(x), S(y)) &= S(f(x, f(S(x), y))). \end{aligned}$$

2. Prove Proposition 1.6.

3. Show that $\sqsubset$ is the transitive closure of the immediate subterm relation on $\mathrm{Ter}(\Sigma, \mathbb{X})$.

4. Extend Example 1.11 to strings over any finite alphabet. (What does Proposition 1.12 say here?)

5. Prove that the substring relation over $\{0, 1\}^*$ is not a well-quasi-order.

6. Find all $t \in \mathcal{T}$ such that $t \preceq 2(1, 1(2, 1(0)))$.

1.2 Abstract reduction systems

An *Abstract Reduction System* (ARS) is a set A together with a binary relation $\rightarrow$. Further on we will mostly be interested in the case where A is a set of terms and $\rightarrow$ is a one-step computation, or reduction, relation. However we treat the general case first, so $(A, \rightarrow)$ could be any directed graph, finite or infinite.

An element a in A of an ARS $(A, \rightarrow)$ is said to be a *normal form*, if there is no $b \in A$ such that $a \rightarrow b$. (Intuitively a cannot be computed further, and can be considered as the *value* of a computation.)

Example 1.15 Let $A = \{0, 1, 2, 3\}$ and $\rightarrow = \{(1, 0), (1, 2), (2, 1), (2, 3)\}$. (Draw the graph of this ARS!) It is easy to see that the elements of normal form are exactly 0 and 3.

Example 1.16 The ARS given by $A_2 = \{0, 1\}$ and $\rightarrow = \{(1, 0), (0, 1)\}$ has no elements of normal form.

Let $(A, \rightarrow)$ be an ARS. Denote by $\twoheadrightarrow$ the reflexive and transitive closure of $\rightarrow$, that is, $a \twoheadrightarrow b$ holds iff there is a sequence $a = a_1, \ldots, a_n = b$, $n \geq 1$, such that

$$a_1 \rightarrow a_2 \rightarrow \cdots \rightarrow a_n.$$

Write $a \rightarrow^+ b$ if this holds for a sequence where $n \geq 2$. An ARS $(A, \rightarrow)$ is *weakly normalizing (WN)* if for every $a \in A$ there is some normal form $b \in B$ with $a \twoheadrightarrow b$. It is easily checked that the ARS of Example 1.15 is weakly normalizing. Note however that $1 \twoheadrightarrow 0$ and $1 \twoheadrightarrow 3$ so that 1 has two distinct normal forms.

Two elements a and b of an ARS $(A, \rightarrow)$ are said to be *convergent* (in symbols: $a \downarrow b$) if there is some c such that $a \twoheadrightarrow c$ and $b \twoheadrightarrow c$. An ARS $(A, \rightarrow)$ is *confluent* or *Church-Rosser (CR)* if $b \downarrow c$ for any $a, b, c \in A$ such that $a \twoheadrightarrow b$ and $a \twoheadrightarrow c$ The following simple result shows the importance of this property.

Proposition 1.17 *Let $(A, \rightarrow)$ be a confluent, weakly normalizing ARS. Then every element of A has a unique normal form.*

Proof. Suppose that b and c are normal forms and $a \twoheadrightarrow b$ and $a \twoheadrightarrow c$. By confluency, for some $d \in A$ with $b \twoheadrightarrow d$ and $c \twoheadrightarrow d$. Since b is normal, $b = d$ and likewise $c = d$. Hence $b = c$. □

An ARS $(A, \rightarrow)$, where there are no infinite sequences $a_1 \rightarrow a_2 \rightarrow a_3 \rightarrow \cdots$ is called *strongly normalizing (SN)*, i.e. $(A, \leftarrow)$ is a wellfounded relation. Clearly, in this case any strategy of performing the reductions will lead to a

normal form. The ARS of Example 1.15 is does not have this property since there is the sequence $1 \to 2 \to 1 \to 2 \to \cdots$.

Example 1.18 The ARS given by $A = \{0, 1, 2, 3\}$ and $\to = \{(1, 0), (1, 2), (2, 3)\}$ is strongly normalizing but not confluent.

The following theorem is often useful when proving confluency. An ARS $(A, \to)$ is *weakly confluent* or *Weakly Church-Rosser (WCR)* if $b \downarrow c$ for any $a, b, c \in A$ such that $a \to b$ and $a \to c$. (Note the one-step computation relations from a.)

Theorem 1.19 *(Newman's lemma) A weakly confluent, strongly normalizing ARS is confluent.*

Proof. Let $(A, \to)$ be an ARS. That it is confluent is equivalent to $P(u)$ for all u, where

$$P(u) \Leftrightarrow_{\text{def}} (\forall x, y)[u \twoheadrightarrow x \wedge u \twoheadrightarrow y \Rightarrow x \downarrow y]$$

Since the ARS is strongly normalizing, we can prove $(\forall u)\, P(u)$ by Noetherian induction. For this it suffices to show that $S = \{u \in A : P(u)\}$ is a progressive set, i.e.

$$(\forall u)[(\forall t)\, (u \to t \Rightarrow P(t)) \Rightarrow P(u)].$$

So assume that $u \in A$ is arbitrary, and as induction hypothesis $(\forall t)\, (u \to t \Rightarrow P(t))$. In case u is normal, we are done. Otherwise, suppose that $u \to b \twoheadrightarrow x$ and $u \to c \twoheadrightarrow y$. By weak confluency there is some d such that $b \twoheadrightarrow d$ and $c \twoheadrightarrow d$. By the induction hypothesis $P(b)$, so there is a z with $x \twoheadrightarrow z$ and $d \twoheadrightarrow z$. By transitivity, $c \twoheadrightarrow z$. Using the induction hypothesis again, $P(c)$ holds, so there is some v with $z \twoheadrightarrow v$ and $y \twoheadrightarrow v$. Thus by transitivity, $x \twoheadrightarrow v$. The induction step is finished. □

The following result can sometimes be used to prove that an ARS is strongly normalising.

Theorem 1.20 *Let $(A, \to)$ be an ARS such that $(A, \to^+)$ is irreflexive. Suppose that there is a well-quasi-order $(A, \preceq)$ such that for all $s \neq t \in A$:*

$$s \preceq t \Longrightarrow t \to^+ s.$$

Then $(A, \to)$ is strongly normalising.

Proof. Suppose to the contrary that the ARS is not strongly normalising. Then there is an infinite sequence in A so that

$$s_1 \to s_2 \to s_3 \to \cdots$$

Hence since $\preceq$ is a well-quasi-order, there are $m < n$ such that $s_m \preceq s_n$, and $s_m \neq s_n$. Hence $s_n \to^+ s_m$ by the assumption. By transtivitity it follows that $s_n \to^+ s_n$, contradicting the irreflexivity assumption. □

References

N. Dershowitz and J.P. Jouannaud. Rewrite Systems. In: J. van Leeuwen (ed.) *Handbook of Theoretical Computer Science.* North-Holland 1990.

J.A. Goguen and G. Malcolm. *Algebraic Semantics of Imperative Programming Languages.* MIT Press, 1996.

K. Meinke and J.V. Tucker. Universal Algebra. In: S. Abramsky *et al.* (eds.): *Handbook of Logic in Computer Science, Vol. 1.* Oxford University Press 1992.

W. Wechler. *Universal Algebra for Computer Scientists.* Springer 1992.