

Automated Theorem Proving

Prof. Dr. Jasmin Blanchette, Yiming Xu, PhD,
Tanguy Bozec, and Lydia Kondylidou
based on exercises by Dr. Uwe Waldmann

Winter Term 2025/26

Exercises 1: Motivation and Preliminaries

More difficult exercises are identified with an asterisk (*). These are included because they can be fun and instructive, but they are not typical exam questions.

Exercise 1.1: Solve the sudoku puzzle presented in the lecture.

Exercise 1.2: Find an abstract reduction system $(A, \rightarrow)$ such that the relations $\rightarrow$, $\leftrightarrow$, and $\leftrightarrow^*$ are all different.

Exercise 1.3: Find an abstract reduction system $(A, \rightarrow)$ such that $\rightarrow^+$ is irreflexive and $\rightarrow$ is normalizing but not terminating.

Exercise 1.4: Let $(\mathbb{N} \setminus \{0, 1\}, <_d)$ be the set of natural numbers larger than 1 ordered by the divisibility ordering $<_d$ that is defined by $a <_d b$ if a divides b and $a \neq b$. Are there minimal elements? Is there a smallest element? What do they look like?

Exercise 1.5: Let $(\mathbb{Q}, <)$ be the set of rational numbers with the usual ordering $<$. Construct infinite subsets M_1 , M_2 , M_3 , and M_4 of $\mathbb{Q}$ with the following properties:

- (1) M_1 is well-founded and has a minimal element.
- (2) M_2 is not well-founded and has a minimal element.
- (3) M_3 is well-founded and does not have a maximal element.

- (4) M_4 is not well-founded and has a maximal element.

Exercise 1.6 (*): You are asked to review a scientific article that has been submitted to a conference on automated reasoning. On page 3 of the article, the authors write the following:

Theorem 2. Let $\rightarrow_1$ and $\rightarrow_2$ be two binary relations over a nonempty set M . If $\rightarrow_1$ and $\rightarrow_2$ are terminating, then $\rightarrow_1 \cup \rightarrow_2$ is also terminating.

Proof. Since $\rightarrow_1$ is terminating, $\rightarrow_1^+$ is a well-founded ordering. Assume that there exists an infinite descending $(\rightarrow_1 \cup \rightarrow_2)$ -chain. Since $\rightarrow_1^+$ is well-founded, there exists a minimal element b with respect to $\rightarrow_1^+$ such that there exists an infinite descending $(\rightarrow_1 \cup \rightarrow_2)$ -chain starting with b .

Case 1: The $(\rightarrow_1 \cup \rightarrow_2)$ -chain starts with a $\rightarrow_1$ -step $b \rightarrow_1 b'$. The rest of the chain, starting with b' , is still infinite. However, b' is smaller than b with respect to $\rightarrow_1^+$. This contradicts the minimality of b .

Case 2: The $(\rightarrow_1 \cup \rightarrow_2)$ -chain starts with a $\rightarrow_2$ -step $b \rightarrow_2 b'$. Since $\rightarrow_2$ is terminating, the chain cannot consist only of $\rightarrow_2$ -steps. Therefore there must be some $\rightarrow_1$ -step in the chain, say $b'' \rightarrow_1 b'''$. Hence there exists an infinite $(\rightarrow_1 \cup \rightarrow_2)$ -chain starting with this step. But as we have seen in Case 1, an infinite $(\rightarrow_1 \cup \rightarrow_2)$ -chain cannot start with a $\rightarrow_1$ -step. So there is again a contradiction.

Consequently, every descending $(\rightarrow_1 \cup \rightarrow_2)$ -chain must be finite, which means that $\rightarrow_1 \cup \rightarrow_2$ is terminating.

- (1) Is the “proof” correct?
- (2) If the “proof” is not correct:
 - (a) Which step is incorrect?
 - (b) Does the “theorem” hold? If yes, give a correct proof; otherwise, give a counterexample.

Exercise 1.7 (*): (1) Prove: If $>$ is a well-founded strict partial ordering on a set M and if b is the only element of M that is minimal in M , then b is the smallest element of M .

(2) Give an example of a strict partial ordering $>$ on a set M and an element $b \in M$ such that b is the only element of M that is minimal in M but not the smallest element of M .

Exercise 1.8 (*): Let $(A, \rightarrow)$ be an abstract reduction system such that every element of A has exactly one normal form w.r.t. $\rightarrow$. For every $b \in A$, define $L(b)$ as the minimal $n \in \mathbb{N}$ such that $b \rightarrow^n b'$ and b' is in normal form w.r.t. $\rightarrow$. Define the binary relation $\Rightarrow$ over A by $b \Rightarrow c$ if and only if $b \rightarrow c$ and $L(b) > L(c)$.

- (1) Give an example that shows that $\rightarrow \neq \Rightarrow$.
- (2) Show that for every $b \in A$ we have $b \Rightarrow^* b'$, where b' is the normal form of b w.r.t. $\rightarrow$.
- (3) Use part (2) to show that $\leftrightarrow^* = \Leftrightarrow^*$.