Automated Theorem Proving

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

Winter Term 2024/25

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.

Proposed solution.

	1	2	3	4	5	6	7	8	9
1	6	9	3	7	8	4	5	1	2
2	4	8	7	5	1	2	9	3	6
3	1	2	5	9	6	3	8	7	4
4	9	3	2	6	5	1	4	8	7
5	5	6	8	2	4	7	3	9	1
6	7	4	1	3	9	8	6	2	5
7	3	1	9	4	7	5	2	6	8
8	8	5	6	1	2	9	7	4	3
9	2	7	4	8	3	6	1	5	9

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

Proposed solution. We take $A := \mathbb{N} = \{0, 1, 2, \dots\}$ and

$$\to := \{(n+1, n+2) \mid n \in \mathbb{N}\}.$$

Then

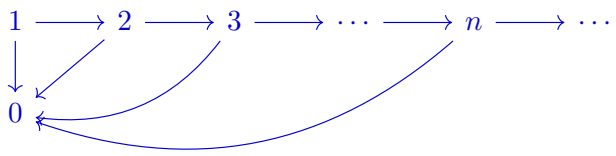
$$\begin{aligned} \leftrightarrow &:= \{(n+1, n+2) \mid n \in \mathbb{N}\} \cup \{(n+2, n+1) \mid n \in \mathbb{N}\} \\ \leftrightarrow^+ &:= \{(m+1, n+1) \mid m, n \in \mathbb{N}\}, \\ \leftrightarrow^* &:= \{(m+1, n+1) \mid m, n \in \mathbb{N}\} \cup \{(0, 0)\}. \end{aligned}$$

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

Proposed solution. We take $A := \mathbb{N}$ and

$$\to := \{(n+1, n+2) \mid n \in \mathbb{N}\} \cup \{(n+1, 0) \mid n \in \mathbb{N}\}.$$

The relation is clearly irreflexive (e.g., $1 \to 2$ but $2 \not\to 1$). It is also normalizing, with $n{\downarrow} = 0$ as the unique normal form of any number $n \in \mathbb{N}$. But it is not terminating, because it allows the infinite chain $1 \to 2 \to 3 \to 4 \to \cdots$.



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

Proposed solution. There are minimal elements; namely, the prime numbers $(2, 3, 5, 7, 11, \dots)$ are the minimal elements.

There is, however, no smallest element. A plausible candidate might be 2, but since $2 \not<_{\mathrm{d}} 3$, it does not satisfy the criterion of being smallest.

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.

Proposed solution. (1) We take $M_1 := \{0, 1, 2, \dots\}$. It is clearly well-founded, and the minimal element is 0.

(2) We take $M_2 := \{q \in \mathbb{Q} \mid 0 \leq q\}$. It admits infinite chains $1 > \frac{1}{2} > \frac{1}{3} > \frac{1}{4} > \cdots$, and the minimal element is 0.

(3) We take $M_3 := \{0, 1, 2, \dots\}$. Clearly it has no maximal element.

(4) We take $M_4 := \{q \in \mathbb{Q} \mid 0 \leq q \leq 1\}$. It admits infinite chains $1 > \frac{1}{2} > \frac{1}{3} > \frac{1}{4} > \cdots$, and the maximal element is 1.

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 $\to_1$ and $\to_2$ be two binary relations over a nonempty set M. If $\to_1$ and $\to_2$ are terminating, then $\to_1 \cup \to_2$ is also terminating.
>
> **Proof.** Since $\to_1$ is terminating, $\to_1^+$ is a well-founded ordering. Assume that there exists an infinite descending $(\to_1 \cup \to_2)$-chain. Since $\to_1^+$ is well-founded, there exists a minimal element b with respect to $\to_1^+$ such that there is an infinite descending $(\to_1 \cup \to_2)$-chain starting with b.
>
> Case 1: The $(\to_1 \cup \to_2)$-chain starts with a $\to_1$-step $b \to_1 b'$. The rest of the chain, starting with b', is still infinite. However, b' is smaller than b with respect to $\to_1^+$. This contradicts the minimality of b.
>
> Case 2: The $(\to_1 \cup \to_2)$-chain starts with a $\to_2$-step $b \to_2 b'$. Since $\to_2$ is terminating, the chain cannot consist only of $\to_2$-steps. Therefore there must be some $\to_1$-step in the chain, say $b'' \to_1 b'''$. Hence there exists an infinite $(\to_1 \cup \to_2)$-chain starting with this step. But as we have seen in Case 1, an infinite $(\to_1 \cup \to_2)$-chain cannot start with a $\to_1$-step. So there is again a contradiction.
>
> Consequently, every descending $(\to_1 \cup \to_2)$-chain must be finite, which means that $\to_1 \cup \to_2$ 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.

Proposed solution. No, the "proof" is not correct.

The step "But as we have seen in Case 1, an infinite $(\to_1 \cup \to_2)$-chain cannot start with a $\to_1$-step" is incorrect. What we have seen in Case 1 is that an infinite $(\to_1 \cup \to_2)$-chain cannot start with a $\to_1$-step of the form $b \to_1 b'$, where b is the minimal element w.r.t. $\to_1^+$. Nothing prevents the step from having the form $b'' \to_1 b'''$, where $b'' \neq b$.

In fact, the "theorem" does not hold. A counterexample is $M := \mathbb{N}$ and

$$\begin{aligned} \to_1 &:= \{(2n+1, 2n) \mid n \in \mathbb{N}\}, \\ \to_2 &:= \{(2n, 2n+1) \mid n \in \mathbb{N}\}. \end{aligned}$$

Each relation $\to_i$ admits only chains of length at most 1 (e.g., $5 \to_1 4$ or $4 \to_2 5$), but the two relations in combination admit infinite chains $5 \to_1 4 \to_2 5 \to_1 4 \to_2 5 \to_1 \cdots$. Methodologically, a good way to locate the flaw in the "proof" is to analyze where the proof goes wrong for this 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.

Proposed solution. (1) Assume that $>$ is well-founded and that b is the only element of M that is minimal in M, but that b is not the smallest element of M. Let $X = \{x \in M \mid b \leq x\}$ and let $Y = M \setminus X$. Since b is not the smallest element of M, we know that $Y \neq \emptyset$. Since $>$ is well-founded, this implies that there exists some $c \in Y$ that is minimal in Y. By assumption, b is the only element of M that is minimal in M, so c is not minimal in M. Therefore, there exists some $d \in M$ such that $d < c$. Since c is minimal in Y, d cannot be contained in Y. But then $d \in X$, which implies $b \leq d < c$ and thus $c \in X$, contradicting the fact that $c \in Y$.

(2) Let $M = \{x \in \mathbb{Z} \mid x \leq 0\} \cup \{b\}$, where $>$ is the usual ordering on integer numbers and b is incomparable with all integer numbers. Then b is minimal in M (since no element of M is smaller), and it is the only minimal element of M (since for every other $x \in M$ there exists a smaller element $x - 1 \in M$, but b is not the smallest element of M, since the other elements of M are not larger than b.

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

(1) Give an example that shows that $\to \neq \Rightarrow$.

(2) Show that for every $b \in A$ we have $b \Rightarrow^* b'$, where b' is the normal form of b w.r.t. $\to$.

(3) Use part (2) to show that $\leftrightarrow^* = \Leftrightarrow^*$.

Proposed solution. (1) Let $A = \{a, b\}$ with $\to = \{(a, a), (a, b)\}$. Every element of A has exactly one normal form, namely b. We get $L(a) = 1$ and $L(b) = 0$, so $a \to a$ but not $a \Rightarrow a$.

(2) We use induction over $L(b)$. If $L(b) = 0$, then the normal form of b with respect to $\to$ is b itself. Obviously, $b \Rightarrow^0 b$ and therefore $b \Rightarrow^* b$.

If $L(b) = n{+}1$, then there is a derivation with $n{+}1$ steps $b \to b'' \to^n b'$, where b' is the normal form of both b and b''. Clearly, there cannot exist any shorter derivation $b'' \to^m b'$ with $m < n$, since otherwise there would be a derivation $b \to^{m+1} b'$, contradicting the minimality assumption. So $L(b'') = n$, and therefore $b \Rightarrow b''$. By induction, $b'' \Rightarrow^* b'$, so $b \Rightarrow^* b'$.

(3) Since $\to \supseteq \Rightarrow$, we get $\leftrightarrow^* \supseteq \Leftrightarrow^*$. To prove the reverse inclusion, we first show that $\to \subseteq \Leftrightarrow^*$. Assume that $a \to b$. Let c be the normal form of b. Clearly, c is also the normal form of a. By part (2), $a \Rightarrow^* c \Leftarrow^* b$, so $a \Leftrightarrow^* b$ as required. Since $\Leftrightarrow^*$ is reflexive, symmetric, and transitive, $\to \subseteq \Leftrightarrow^*$ implies $\leftrightarrow^* \subseteq \Leftrightarrow^*$.