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 9: Rewrite Systems

Exercise 9.1: Let $\Sigma = (\Omega, \emptyset)$ with $\Omega = \{b/0,\ f/1,\ g/1\}$. Let E be the set of (implicitly universally quantified) equations $\{f(g(f(x))) \approx b\}$.

Give one possible derivation for the statement $E \vdash f(g(b)) \approx b$.

Exercise 9.2: Let $\Sigma = (\Omega, \emptyset)$, let $\Omega = \{f/1,\ b/0,\ c/0,\ d/0\}$. Let E be the set of equations $\{f(b) \approx d,\ f(c) \approx d,\ f(f(x)) \approx f(x)\}$. Let X be a countably infinite set of variables.

(a) Show that $f(d) \leftrightarrow_E^* d$.

(b) Sketch what the universe of $\mathrm{T}_\Sigma(\emptyset)/E$ looks like. How many elements does it have?

(c) Determine for each of the following equations whether it holds in $\mathrm{T}_\Sigma(X)/E$ and whether it holds in $\mathrm{T}_\Sigma(\emptyset)/E$. Give a very brief explanation.

$$f(b) \approx b \qquad (1)$$

$$\forall y\ f(f(f(y))) \approx f(f(y)) \qquad (2)$$

$$\forall x\, \forall y\ f(x) \approx f(y) \qquad (3)$$

Exercise 9.3: Let $\Sigma = (\Omega, \emptyset)$ with $\Omega = \{f/1,\ b/0,\ c/0,\ d/0\}$. Let E be the set of (implicitly universally quantified) equations $\{f(f(x)) \approx b\}$.

(a) Show that $b \leftrightarrow_E^* f(b)$. How does the rewrite proof look?

(b) Is the universe of the initial E-algebra $\mathrm{T}_\Sigma(\emptyset)/E$ finite or infinite? If it is finite, how many elements does it have?

Exercise 9.4: Let $\Sigma = (\Omega, \emptyset)$ be a first-order signature with $\Omega = \{f/1,\ b/0,\ c/0,\ d/0\}$. Let E be the set of Σ-equations

$$\{\forall x\,(f(x) \approx b),\ c \approx d\},$$

let $X = \{x, y, z\}$ be a set of variables. For any $t \in \mathrm{T}_\Sigma(X)$, let $[t]$ denote the congruence class of t w.r.t. E. Let $\mathcal{T} = \mathrm{T}_\Sigma(X)/E$, let $U_\mathcal{T}$ be the universe of $\mathcal{T}$, and let $\beta : X \to U_\mathcal{T}$ be the assignment that maps every variable to $[c]$. Determine for each of the following statements whether they are true or false:

(1) $[z]$ is a finite set of Σ-terms.

(2) $[f(z)]$ is a finite set of Σ-terms.

(3) $[c]$ is a set of ground Σ-terms.

(4) $[f(c)]$ is a set of ground Σ-terms.

(5) $U_\mathcal{T}$ is finite.

(6) $[b] \in U_\mathcal{T}$.

(7) $\{x, y\} \in U_\mathcal{T}$.

(8) $\mathcal{T}(\beta)(\forall z\,(z \approx f(x))) = 1$.

Exercise 9.5: Let $\Sigma = (\Omega, \emptyset)$ be a first-order signature with $\Omega = \{f/2,\ b/0,\ c/0,\ d/0\}$. Let E be the set of Σ-equations

$$\{\forall x\,(f(x, c) \approx b),\ c \approx d\},$$

let $X = \{x, y, z\}$ be a set of variables. For any $t \in \mathrm{T}_\Sigma(X)$, let $[t]$ denote the congruence class of t w.r.t. E. Let $\mathcal{T} = \mathrm{T}_\Sigma(X)/E$ let $U_\mathcal{T}$ be the universe of $\mathcal{T}$, and let $\beta : X \to U_\mathcal{T}$ be the assignment that maps every variable to $[c]$. Determine for each of the following statements whether they are true or false:

(1) $[c]$ is a finite set of Σ-terms.

(2) $[f(c, c)]$ is a set of ground Σ-terms.

(3) $[x]$ is an element of the universe of $\mathcal{T}$.

(4) $\{b, f(x, c)\}$ is a congruence class w.r.t. E.

(5) $f(c, b) \in [f(d, b)]$.

(6) $f_\mathcal{T}([y], [d]) = [f(z, c)]$.

(7) $\mathcal{T}(\beta)(y \approx d) = 1$.

(8) $\mathcal{T}(\beta)(\forall z\,(z \approx c)) = 1$.

Exercise 9.6 (∗)**:** Find a signature Σ containing at least one constant symbol, a set E of Σ-equations, and two terms $s, t \in \mathrm{T}_\Sigma(X)$ such that

$$\mathrm{T}_\Sigma(\{x_1\})/E \ \models\ \forall \vec{x}\,(s \approx t),$$

but

$$\mathrm{T}_\Sigma(\{x_1, x_2\})/E \ \not\models\ \forall \vec{x}\,(s \approx t),$$

where $\vec{x}$ consists of all the variables occurring in s and t. (The variables in $\vec{x}$ need not be contained in $\{x_1, x_2\}$.)

Exercise 9.7: Let R be the following term rewrite system over $\Sigma = (\{f/1,\ g/2,\ h/1,\ c/0\}, \emptyset)$.

$$\begin{aligned} f(f(x)) &\to h(h(x)) && (1) \\ g(f(y), x) &\to g(y, x) && (2) \\ h(g(z, f(c))) &\to f(z) && (3) \end{aligned}$$

Give all critical pairs between the three rules.

Exercise 9.8: Let

$$\{f(b) \to f(c),\ f(c) \to f(d),\ f(d) \to f(b),\ f(x) \to x\}$$

be a rewrite system over $\Sigma = (\{f/1,\ b/0\, c/0,\ d/0\},\ \emptyset)$. Is it (a) terminating? (b) normalizing? (c) locally confluent? (d) confluent? Justify your answers.

Exercise 9.9 (*)**:** Let $\Sigma = (\Omega, \emptyset)$ with $\Omega = \{f/1, g/1, h/1, b/0, c/0\}$. Let R be the following term rewrite system over Σ:

$$\{g(f(x)) \to h(x),\ h(f(x)) \to g(x),\ g(b) \to c,\ h(c) \to b\}$$

Prove: If $s, t \in \mathrm{T}_\Sigma(X)$ and $R \models \forall \vec{x}\,(s \approx t)$, then there exists a rewrite derivation $s \leftrightarrow_R^* t$ with at most $|s| + |t| - 2$ rewrite steps.

Exercise 9.10 (*)**:** Let $\Sigma = (\Omega, \emptyset)$ be a signature. Let R be a term rewrite system.

(a) Prove: If $s \to_R t$, then $\mathrm{var}(s) \supseteq \mathrm{var}(t)$.

(b) Prove: If $x \in X$ is a variable, $s \in \mathrm{T}_\Sigma(X)$ is a term such that $x \notin \mathrm{var}(s)$, and $R \models x \approx s$, then R is not confluent.

Exercise 9.11 (*)**:** Let $\Sigma = (\Omega, \emptyset)$ be a first-order signature, let E be a set of Σ-equations such that for every equation $s \approx s'$ in E neither s nor s' is a variable. For any term $t \in \mathrm{T}_\Sigma(X)$, let $[t]$ denote the congruence class of t w.r.t. E.

Prove or refute: For every variable $x \in X$ we have $[x] = \{x\}$.

Exercise 9.12 (*)**:** A friend asks you to proofread her master thesis. On page 15 of the thesis, your friend writes the following:

Lemma 5. Let $\succ$ be a well-founded ordering over a set A, let $\to$ be a binary relation such that $\to \subseteq \succ$. Let r be an element of A that is irreducible with respect to $\to$, and define $A_r = \{t \in A \mid t \to^* r\}$. If for every $u_0, u_1, u_2 \in A$ such that $u_1 \leftarrow u_0 \to u_2 \to^* r$ there exists a $u_3 \in A$ such that $u_1 \to^* u_3 \leftarrow^* u_2$, then for every $t_0 \in A_r$ and $t_1 \in A$, $t_0 \to^* t_1$ implies $t_1 \in A_r$.

Proof. We use well-founded induction over t_0 with respect to $\succ$. Let $t_0 \in A_r$ and $t_1 \in A$ such that $t_0 \to^* t_1$. If this derivation is empty, the result is trivial, so suppose that $t_0 \to t_1' \to^* t_1$. Since $t_0 \in A_r$ is reducible, it is different from r, hence there is a nonempty derivation $t_0 \to t_2 \to^* r$. By assumption, there exists a $t_3 \in A$ such that $t_1' \to^* t_3 \leftarrow^* t_2$. Now $t_0 \succ t_2$ and $t_2 \in A_r$, hence $t_3 \in A_r$ by the induction hypothesis, and thus $t_1' \in A_r$. Since $t_0 \succ t_1'$, we can use the induction hypothesis once more and obtain $t_1 \in A_r$ as required.

(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.