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 6: General Resolution

Exercise 6.1: Using the (a) standard and the (b) polynomial unification rules, compute most general unifiers of $P(g(x_1, x_1), g(x_3, h(x_4)))$ and $P(g(h(x_2), h(h(x_6))), g(h(x_5), x_5))$, if they exist.

Proposed solution. (a)

$$
\begin{aligned}
& P(g(x_1, x_1), g(x_3, h(x_4))) \doteq P(g(h(x_2), h(h(x_6))), g(h(x_5), x_5)) \\
\Rightarrow_{SU}\ & g(x_1, x_1) \doteq g(h(x_2), h(h(x_6))),\ g(x_3, h(x_4)) \doteq g(h(x_5), x_5) \\
\Rightarrow_{SU}\ & x_1 \doteq h(x_2),\ x_1 \doteq h(h(x_6)),\ g(x_3, h(x_4)) \doteq g(h(x_5), x_5) \\
\Rightarrow_{SU}\ & x_1 \doteq h(x_2),\ x_1 \doteq h(h(x_6)),\ x_3 \doteq h(x_5),\ h(x_4) \doteq x_5 \\
\Rightarrow_{SU}\ & x_1 \doteq h(x_2),\ x_1 \doteq h(h(x_6)),\ x_3 \doteq h(x_5),\ x_5 \doteq h(x_4) \\
\Rightarrow_{SU}\ & x_1 \doteq h(x_2),\ h(x_2) \doteq h(h(x_6)),\ x_3 \doteq h(x_5),\ x_5 \doteq h(x_4) \\
\Rightarrow_{SU}\ & x_1 \doteq h(x_2),\ x_2 \doteq h(x_6),\ x_3 \doteq h(x_5),\ x_5 \doteq h(x_4) \\
\Rightarrow_{SU}\ & x_1 \doteq h(x_2),\ x_2 \doteq h(x_6),\ x_3 \doteq h(h(x_4)),\ x_5 \doteq h(x_4) \\
\Rightarrow_{SU}\ & x_1 \doteq h(h(x_6)),\ x_2 \doteq h(x_6),\ x_3 \doteq h(h(x_4)),\ x_5 \doteq h(x_4)
\end{aligned}
$$

The last set is in solved form. Hence

$$\{x_1 \mapsto h(h(x_6)),\ x_2 \mapsto h(x_6),\ x_3 \mapsto h(h(x_4)),\ x_5 \mapsto h(x_4)\}$$

is a most general unifier.

(b)

$$
\begin{aligned}
& P(g(x_1,x_1),g(x_3,h(x_4))) \doteq P(g(h(x_2),h(h(x_6))),g(h(x_5),x_5)) \\
\Rightarrow_{PU}\ & g(x_1,x_1) \doteq g(h(x_2),h(h(x_6))),\ g(x_3,h(x_4)) \doteq g(h(x_5),x_5) \\
\Rightarrow_{PU}\ & x_1 \doteq h(x_2),\ x_1 \doteq h(h(x_6)),\ g(x_3,h(x_4)) \doteq g(h(x_5),x_5) \\
\Rightarrow_{PU}\ & x_1 \doteq h(x_2),\ x_1 \doteq h(h(x_6)),\ x_3 \doteq h(x_5),\ h(x_4) \doteq x_5 \\
\Rightarrow_{PU}\ & x_1 \doteq h(x_2),\ x_1 \doteq h(h(x_6)),\ x_3 \doteq h(x_5),\ x_5 \doteq h(x_4) \\
\Rightarrow_{PU}\ & x_1 \doteq h(x_2),\ h(x_2) \doteq h(h(x_6)),\ x_3 \doteq h(x_5),\ x_5 \doteq h(x_4) \\
\Rightarrow_{PU}\ & x_1 \doteq h(x_2),\ x_2 \doteq h(x_6),\ x_3 \doteq h(x_5),\ x_5 \doteq h(x_4) \\
=\ & x_5 \doteq h(x_4),\ x_3 \doteq h(x_5),\ x_2 \doteq h(x_6),\ x_1 \doteq h(x_2)
\end{aligned}
$$

The last set is in solved form. Hence

$$
\begin{aligned}
& \{x_5 \mapsto h(x_4)\} \circ \{x_3 \mapsto h(x_5)\} \circ \{x_2 \mapsto h(x_6)\} \circ \{x_1 \mapsto h(x_2)\} \\
=\ & \{x_1 \mapsto h(h(x_6)),\ x_2 \mapsto h(x_6),\ x_3 \mapsto h(h(x_4)),\ x_5 \mapsto h(x_4)\}
\end{aligned}
$$

is a most general unifier.

Exercise 6.2: Using the (a) standard and the (b) polynomial unification rules, compute most general unifiers of $P(g(x_1,g(f(x_3),x_3)),g(h(x_4),x_3))$ and $P(g(x_2,x_2),g(x_3,h(x_1)))$, if they exist.

Proposed solution. (a)

$$
\begin{aligned}
& P(g(x_1,g(f(x_3),x_3)),g(h(x_4),x_3)) \doteq P(g(x_2,x_2),g(x_3,h(x_1))) \\
\Rightarrow_{SU}\ & g(x_1,g(f(x_3),x_3)) \doteq g(x_2,x_2),\ g(h(x_4),x_3) \doteq g(x_3,h(x_1)) \\
\Rightarrow_{SU}\ & x_1 \doteq x_2,\ g(f(x_3),x_3) \doteq x_2,\ g(h(x_4),x_3) \doteq g(x_3,h(x_1)) \\
\Rightarrow_{SU}\ & x_1 \doteq x_2,\ g(f(x_3),x_3) \doteq x_2,\ h(x_4) \doteq x_3,\ x_3 \doteq h(x_1) \\
\Rightarrow_{SU}\ & x_1 \doteq x_2,\ x_2 \doteq g(f(x_3),x_3),\ h(x_4) \doteq x_3,\ x_3 \doteq h(x_1) \\
\Rightarrow_{SU}\ & x_1 \doteq x_2,\ x_2 \doteq g(f(x_3),x_3),\ x_3 \doteq h(x_4),\ x_3 \doteq h(x_1) \\
\Rightarrow_{SU}\ & x_1 \doteq x_2,\ x_2 \doteq g(f(x_3),x_3),\ x_3 \doteq h(x_4),\ x_3 \doteq h(x_2) \\
\Rightarrow_{SU}\ & x_1 \doteq g(f(x_3),x_3),\ x_2 \doteq g(f(x_3),x_3),\ x_3 \doteq h(x_4),\ x_3 \doteq h(g(f(x_3),x_3)) \\
\Rightarrow_{SU}\ & x_1 \doteq g(f(h(x_4)),h(x_4)),\ x_2 \doteq g(f(h(x_4)),h(x_4)),\ x_3 \doteq h(x_4), \\
& h(x_4) \doteq h(g(f(h(x_4)),h(x_4))) \\
\Rightarrow_{SU}\ & x_1 \doteq g(f(h(x_4)),h(x_4)),\ x_2 \doteq g(f(h(x_4)),h(x_4)),\ x_3 \doteq h(x_4), \\
& x_4 \doteq g(f(h(x_4)),h(x_4)) \\
\Rightarrow_{SU}\ & \bot
\end{aligned}
$$

There exist no most general unifiers.

(b)

$$
\begin{array}{ll}
& P(g(x_1, g(f(x_3), x_3)), g(h(x_4), x_3)) \doteq P(g(x_2, x_2), g(x_3, h(x_1))) \\
\Rightarrow_{PU} & g(x_1, g(f(x_3), x_3)) \doteq g(x_2, x_2),\ g(h(x_4), x_3) \doteq g(x_3, h(x_1)) \\
\Rightarrow_{PU} & x_1 \doteq x_2,\ g(f(x_3), x_3) \doteq x_2,\ g(h(x_4), x_3) \doteq g(x_3, h(x_1)) \\
\Rightarrow_{PU} & x_1 \doteq x_2,\ g(f(x_3), x_3) \doteq x_2,\ h(x_4) \doteq x_3,\ x_3 \doteq h(x_1) \\
\Rightarrow_{PU} & x_1 \doteq x_2,\ x_2 \doteq g(f(x_3), x_3),\ h(x_4) \doteq x_3,\ x_3 \doteq h(x_1) \\
\Rightarrow_{PU} & x_1 \doteq x_2,\ x_2 \doteq g(f(x_3), x_3),\ x_3 \doteq h(x_4),\ x_3 \doteq h(x_1) \\
\Rightarrow_{PU} & x_1 \doteq x_2,\ x_2 \doteq g(f(x_3), x_3),\ x_3 \doteq h(x_4),\ h(x_4) \doteq h(x_1) \\
\Rightarrow_{PU} & x_1 \doteq x_2,\ x_2 \doteq g(f(x_3), x_3),\ x_3 \doteq h(x_4),\ x_4 \doteq x_1 \\
\Rightarrow_{PU} & \bot
\end{array}
$$

There exist no most general unifiers.

Exercise 6.3: In the lecture notes, standard unification ($\Rightarrow_{SU}$) is proved to be terminating based on a lexicographic combination of orderings. Can the same combination be used to prove the termination of polynomial unification ($\Rightarrow_{PU}$)?

Proposed solution. No, because the last rule for $\Rightarrow_{PU}$ does not decrease the ordering. The first component stays the same, but the second component may increase if t is larger than x.

Exercise 6.4: (a) Give an example of a most general unifier of $f(g(x, y))$ and $f(z)$ that is idempotent.

(b) Give an example of a most general unifier of $f(g(x, y))$ and $f(z)$ that is not idempotent.

Proposed solution. (a) $\{z \mapsto g(x, y)\}$ is an idempotent mgu.

(b) $\{y \mapsto z,\ z \mapsto g(x, z)\}$ is a nonidempotent mgu.

Exercise 6.5: Let $\Sigma = (\Omega, \Pi)$ with $\Omega = \{b/0,\ c/0,\ f/2\}$ and $\Pi = \{P/1,\ Q/1,\ R/0\}$. Use the general resolution calculus *Res* to check whether the following clause set is satisfiable:

$$\neg P(f(x, c)) \lor Q(x) \quad (1)$$
$$\neg P(f(b, b)) \lor R \quad (2)$$
$$\neg Q(b) \lor \neg R \quad (3)$$
$$Q(c) \lor R \quad (4)$$
$$P(f(b, y)) \quad (5)$$
$$\neg P(c) \quad (6)$$

Proposed solution. From (5) and (1), we obtain via "Resolution" $Q(b)$ (7). From (5) and (2) we obtain via "Resolution" R (8). From (7) and (3) we obtain via "Resolution" $\neg R$ (9). From (8) and (9) we obtain via "Resolution" $\bot$. Since resolution is sound, the clause set is unsatisfiable.

Exercise 6.6: Let $\Sigma = (\Omega, \Pi)$ with $\Omega = \{b/0,\ f/1\}$ and $\Pi = \{P/1\}$. Use the general resolution calculus *Res* to determine whether the following clause set is satisfiable:

$$P(x) \lor \neg P(f(x)) \quad (1)$$
$$\neg P(b) \quad (2)$$

Proposed solution. From (1) and (2), we obtain via "Resolution" $\neg P(f(b))$ (3). From (1) and (3) we obtain via "Resolution" $\neg P(f(f(b)))$ (4). From (1) and (4) we obtain via "Resolution" $\neg P(f(f(f(b))))$ (5). And so on. We never derive $\bot$. At the limit, we have a saturated set that does not contain $\bot$. By refutational completeness of resolution, this means that the clause set is satisfiable. A model of all the clauses is given by the algebra $\mathcal{A}$ such as $U_{\mathcal{A}} = \{0\}$, $a_{\mathcal{A}} = 0$, $f_{\mathcal{A}}(0) = 0$, and $P_{\mathcal{A}} = \emptyset$.

Exercise 6.7 (*)**:** For inferences with more than one premise, we implicitly assume that the variables in the premises are renamed such that they become different to any variable in the other premises. Show that the resolution calculus *without* this renaming is incomplete by exhibiting a saturated unsatisfiable clause set that does not contain the empty clause.

Proposed solution. We take the set $N := \{P(x, c),\ \neg P(b, x)\}$. If variables are not renamed apart, a "Resolution" inference from the two clauses is impossible because x cannot be unified with both b and c. The set is saturated.

Yet the set is unsatisfiable, because the resolution calculus *with* variable renaming can be used to derive the empty clause, and that calculus is sound. If we rename the variable x to y in the second clause, we get $\neg P(b, y)$, whose atom can be unified with $P(x, c)$ by taking the mgu $\{x \mapsto b,\ y \mapsto c\}$. This means that a "Resolution" inference is possible, yielding the empty clause.

Exercise 6.8 (*)**:** (a) Let N be a set of (not necessarily ground) first-order clauses. Let $D = \neg A$ be a negative unit clause such that no "Resolution" inference between any clause $C \in N$ and D is possible. Prove that no "Resolution" inference between any clause $C' \in \mathit{Res}^*(N)$ and D is possible.

(b) Does the property also hold if D is a positive unit clause or an arbitrary clause? Give a brief explanation.

Proposed solution. (a) We will first show that no resolution inference between any clause $C' \in \mathit{Res}(N)$ and D is possible. By induction, this property extends to $\mathit{Res}^*(N)$.

First, we note the following key invariant: If no "Resolution" inference between a clause $C \in N$ and D is possible, then C contains no positive literals unifiable with A.

If $C' \in \mathit{Res}(N)$ is the conclusion of a "Resolution" inference, then it was derived from two premises $D, E \in N$ that contain no positive literal unifiable with A. As a result, C'—which consists of a subset of the literals of D and E to which a substitution is applied—contains no positive literals unifiable with A. (Applying a substitution can never turn a nonunifiable literal into a unifiable one.)

If C' is the conclusion of a "Factorization" inference, then it was derived from a premise $D \in N$ that contains no positive literals unifiable with A. As a result, C'—which consists of a subset of the literals of D to which a substitution is applied—contains no positive literals unifiable with A.

(b) Yes, it holds. If D is a positive literal, clauses in N contain no negative literals unifiable with $\neg A$. And if D is an arbitrary clause, clauses in N contain no literals whose complement are unifiable with any literals from D. The proof that these two properties are preserved by inferences is analogous to part (a).