Prof. Dr. Jürgen Giesl

Marc Brockschmidt, Carsten Fuhs, Thomas Ströder

Exercise 1 (Monotonicity): (1 + 1 + 1 + 1 = 4 points)

Consider the following relations $\sim_1, \ldots, \sim_4 \subseteq \mathcal{T}(\Sigma, \mathcal{V}) \times \mathcal{T}(\Sigma, \mathcal{V})$. Prove or disprove for each of these relations that they are monotonic.

a) $s \sim_1 t$ iff the numbers of different variables in s and t are equal, i.e., $|\mathcal{V}(s)| = |\mathcal{V}(t)|$.

b) $s \sim_2 t$ iff s is a subterm of t.

c) $s \sim_3 t$ iff s matches t.

d) $s \sim_4 t$ iff $\mathcal{V}(s) \subseteq \mathcal{V}(t)$.

Solution:

a) $\sim_1$ is not monotonic. Consider the terms $s = \mathsf{f}(x)$, $t = \mathsf{f}(y)$ and $q = \mathsf{g}(u, x)$. The number of different variables in s and t is 1 for both terms, but for $q[s]_1 = \mathsf{g}(\mathsf{f}(x), x)$ is is 1 and for $q[t]_1 = \mathsf{g}(\mathsf{f}(y), x)$, it is 2.

b) $\sim_2$ is not monotonic. Consider the terms $s = \mathsf{a}$, $t = \mathsf{h}(\mathsf{a})$ and $q = \mathsf{f}(x)$. Then $t|_1 = s$ and thus, s is a subterm of t. But for $q[s]_1 = \mathsf{f}(\mathsf{a})$ and $q[t]_1 = \mathsf{f}(\mathsf{h}(\mathsf{a}))$, there is no position π such that $q[t]_1|_\pi = q[s]_1$.

c) $\sim_3$ is not monotonic. Consider the term $s = \mathsf{f}(x)$, $t = \mathsf{f}(a)$ and $q = \mathsf{g}(x, y)$. Then $\pi = \{x/a\}$ is a matcher such that $s\sigma = t$, but $q[s]_2 = \mathsf{g}(x, \mathsf{f}(x))$ and $q[t]_2 = \mathsf{g}(x, \mathsf{f}(a))$ have no matcher.

d) $\sim_4$ is monotonic. Let s and t be terms with $\mathcal{V}(s) \subseteq \mathcal{V}(t)$, q be some context and $\pi \in Occ(q)$. Furthermore, let $x \in \mathcal{V}(q[s]_\pi)$. If $x \notin \mathcal{V}(s)$, then we have $\tau \in Occ(q)$ with $\tau \bot \pi$, $q|_\tau = x$ and thus $x \in \mathcal{V}(q[t]_\pi)$. If $x \in \mathcal{V}(s)$, we have $x \in \mathcal{V}(t)$ and thus also $x \in \mathcal{V}(q[t]_\pi)$.

Exercise 2 (Equivalence relations): ((1 + 1 + 1 + 1) + (1 + 1) = 6 points)

a) Consider the following relations $\sim_1, \ldots, \sim_4$. Prove or disprove for each of these relations that they are equivalence relations.

i) $\sim_1 \subseteq \mathcal{T}(\Sigma, \mathcal{V}) \times \mathcal{T}(\Sigma, \mathcal{V})$ with $s \sim_1 t \Leftrightarrow |\mathcal{V}(s)| = |\mathcal{V}(t)|$.

ii) $\sim_2 \subseteq \mathcal{T}(\Sigma, \mathcal{V}) \times \mathcal{T}(\Sigma, \mathcal{V})$ with $s \sim_2 t \Leftrightarrow \exists \sigma \in SUB(\Sigma, \mathcal{V}) : s\sigma = t\sigma$ (i.e., s and t unify).

iii) Let $m \in \mathbb{N}$ be some fixed natural number. Then $\sim_3^m \subseteq \mathbb{Z} \times \mathbb{Z}$ with $x \sim_3^m y \Leftrightarrow (x - y)\ mod\ m = 0$.

For example, we have $61 \sim_3^{19} 23$, as $(61 - 23)\ mod\ 19 = 38\ mod\ 19 = 0$.

Hints:

- To save work, you may write $x - y \equiv_m 0$ instead of $(x - y)\ mod\ m = 0$.

iv) Let $\mathbb{Z}_{\neq 0} = \mathbb{Z} \setminus \{0\}$ and $(p, q), (u, v) \in \mathbb{Z} \times \mathbb{Z}_{\neq 0}$. Then $\sim_4 \subseteq (\mathbb{Z} \times \mathbb{Z}_{\neq 0}) \times (\mathbb{Z} \times \mathbb{Z}_{\neq 0})$ with $(p, q) \sim_4 (u, v) \Leftrightarrow p \cdot v = u \cdot q$.

For example, we have $(3, 6) \sim_4 (2, 4)$, as $3 \cdot 4 = 12 = 2 \cdot 6$.

b) For each of the relations $\sim_1$ and $\sim_2$, give the smallest equivalence relation (i.e., the transitive-reflexive-symmetric closure) that includes them.

i) Let $M = \{0, 1, 2, 3, 4\}$ and $0 \sim_1 2$, $3 \sim_1 1$, $4 \sim_1 2$ and $2 \sim_1 0$.

ii) Let $\mathbb{Z}_{\neq 0} = \mathbb{Z} \setminus \{0\}$. Then $\sim_2 \subseteq \mathbb{Z}_{\neq 0} \times \mathbb{Z}_{\neq 0}$ with $x \sim_2 y \Leftrightarrow x + 1 = y$.

Solution:

a) i) $\sim_1$ is an equivalence relation. Let $t, s, q \in \mathcal{T}(\Sigma, \mathcal{V})$. Then, we have $t \sim_1 t$, as $|\mathcal{V}(t)| = |\mathcal{V}(t)|$ and thus, $\sim_1$ is reflexive. Furthermore, if $t \sim_1 s$, then $|\mathcal{V}(t)| = |\mathcal{V}(s)|$ and consequently also $s \sim_1 t$. Thus, $\sim_1$ is symmetrical. Finally, if $t \sim_1 s$ and $s \sim_1 q$, then $|\mathcal{V}(t)| = |\mathcal{V}(s)| = |\mathcal{V}(q)|$ and thus $s \sim_1 q$ (i.e., $\sim_1$ is transitive).

ii) $\sim_2$ is not an equivalence relation. Consider the terms $t = \mathsf{f}(\mathsf{a})$, $s = \mathsf{f}(x)$ and $q = \mathsf{f}(\mathsf{b})$. Then, $t \sim_2 s$ with $\sigma_1 = \{x/\mathsf{a}\}$ and $s \sim_2 q$ with $\sigma_2 = \{x/\mathsf{b}\}$, but there is no substitution μ such that $\mathsf{f}(\mathsf{a})\mu = \mathsf{f}(\mathsf{b})\mu$ and thus, $\sim_2$ is not transitive.

iii) $\sim_3$ is an equivalence relation. Let $x, y, z \in \mathbb{Z}$. Then, we have $x \sim_3 x$, as $x - x = 0 \Rightarrow x - x \equiv_m 0$ and thus, $\sim_3$ is reflexive. Futhermore, if $x \sim_3 y$, then $x - y \equiv_m 0$, thus there is a $k \in \mathbb{Z}$ such that $x - y = k \cdot m \Leftrightarrow y - x = -k \cdot m \Leftrightarrow y - x \equiv_m 0$. Thus, $\sim_3$ is symmetric. Finally, if $x \sim_3 y$ and $y \sim_3 z$, then $x - y \equiv_m 0$ and $y - z \equiv_m 0$. Therefore, $x - y + y - z \equiv_m 0 \Leftrightarrow x - z \equiv_m 0$ and thus, $\sim_3$ is transitive.

iv) $\sim_4$ is an equivalence relation. Let $(p, q), (u, v), (a, b) \in \mathbb{Z} \times \mathbb{Z}_{\neq 0}$. Then, we have $(p, q) \sim_4 (p, q)$, as $p \cdot q = p \cdot q$ and thus, $\sim_4$ is reflexive. Futhermore, if $(p, q) \sim_4 (u, v)$, then $p \cdot v = u \cdot q$ and thus obviously also $(u, v) \sim_4 (p, q)$. Thus, $\sim_3$ is symmetric. Finally, if $(p, q) \sim_4 (u, v)$ and $(u, v) \sim_4 (a, b)$, then

$$
\begin{array}{rrcr}
 & p \cdot v = u \cdot q & \wedge & u \cdot b = a \cdot v \\
\Leftrightarrow & p \cdot v \cdot b = u \cdot q \cdot b & \wedge & u \cdot b \cdot q = a \cdot v \cdot q \\
\Leftrightarrow & p \cdot b \cdot v = u \cdot q \cdot b & \wedge & u \cdot q \cdot b = a \cdot q \cdot v \\
\Rightarrow & p \cdot b \cdot v = a \cdot q \cdot v & & \\
\Leftrightarrow & v \cdot (p \cdot b - a \cdot q) = 0 & & \\
\overset{v \neq 0}{\Leftrightarrow} & p \cdot b - a \cdot q = 0 & & \\
\Leftrightarrow & p \cdot b = a \cdot q & &
\end{array}
$$

Therefore, $\sim_4$ is transitive.

b) i) We have $\sim_1 = \{(0, 0), (0, 2), (0, 4), (2, 0), (2, 2), (2, 4), (4, 0), (4, 2), (4, 4), (1, 1), (1, 3), (3, 1), (3, 3)\}$.

ii) We have $\sim_2 = \{(x, y) \mid x, y \in \mathbb{Z} \wedge x < 0 \wedge y < 0\} \cup \{(x, y) \mid x, y \in \mathbb{Z} \wedge x > 0 \wedge y > 0\}$.

Exercise 3 (Equivalence classes): (2 + 4 = 6 points)

a) Let $s \sim t$ hold for two terms s and t iff $\mathcal{V}(s) = \mathcal{V}(t)$ and the number of function symbols in s is the same as the number of function symbols in t.

Please show that $\sim$ is an equivalence relation and that all equivalence classes w.r.t. $\sim$ are finite.

b) Please show that the word problem is decidable for the following set of equations $\mathcal{E}$ over $\Sigma = \Sigma_2 \cup \Sigma_0$ with $\Sigma_2 = \{:, \cup\}$ and $\Sigma_0 = \{a\}$.

$$\begin{aligned}(x : y) \cup z &\equiv x : (y \cup z)\\ x \cup (y \cup z) &\equiv (x \cup y) \cup z\\ x \cup y &\equiv y \cup x\\ x : (y : z) &\equiv y : (x : z)\\ x : (y \cup z) &\equiv y \cup (x : z)\end{aligned}$$

Hints:

- You may use part a) of this exercise.
- Consider how finite equivalence classes may have an impact on the decidability of the word problem.

Solution:

a) $\sim$ is an equivalence relation as both conditions are equalities and $=$ is an equivalence relation. Let s be an arbitrary term. Furthermore, let k be the number of function symbols in s. We now show that the equivalence class $[s]_\sim$ is finite. This implies that all equivalence classes w.r.t. $\sim$ are finite, since s is an arbitrary term. Let n be the maximal arity of function symbols in our signature. Then any term t with k function symbols cannot contain more than $n \cdot k$ variables. Moreover, there are at most $|\Sigma|^k$ possibilities which function symbols are used in t. Thus, there are not more than $|\mathcal{V}(s)|^{n \cdot k} \cdot |\Sigma|^k$ different terms having k function symbols and the variable set $\mathcal{V}(s)$. Hence, $[s]_\sim$ is finite.

b) We see that all equations $s \equiv t \in \mathcal{E}$ satisfy $s \sim t$. Thus, the equivalence classes w.r.t. $\equiv_\mathcal{E}$ are subsets of the equivalence classes w.r.t. $\sim$ and, therefore, finite. Knowing that all equivalence classes w.r.t. $\equiv_\mathcal{E}$ are finite, for two given terms s and t we can decide whether $s \equiv_\mathcal{E} t$ holds by computing the finite equivalence class $[s]_{\equiv_\mathcal{E}}$ and return yes if $t \in [s]_{\equiv_\mathcal{E}}$ and no otherwise. The computation of the equivalence class can for example be done by building the search tree starting from s and pruning this tree every time we reach a node which already occurred before. This tree must be finite due to the finite equivalence class of s and contain this whole equivalence class.

Exercise 4 (Syntactic Proofs): (1 + 4 = 5 points)

Consider the following set of equations[1] $\mathcal{E}$:

$$\mathsf{f}(x, \mathsf{f}(y, z)) \equiv \mathsf{f}(\mathsf{f}(x, y), z) \quad (1)$$
$$\mathsf{f}(x, \mathsf{e}) \equiv x \quad (2)$$
$$\mathsf{f}(x, \mathsf{i}(x)) \equiv \mathsf{e} \quad (3)$$
$$\mathsf{f}(\mathsf{i}(x), x) \equiv \mathsf{e} \quad (3)'$$

[1] They correspond to the group axioms from the lecture and an additional equation for the operation of inverse elements from the right hand side.

a) Prove $\mathsf{f}(e, x) \equiv x$ using $\leftrightarrow_{\mathcal{E}}^{*}$. Mark in each step which part of your term you are replacing and which equation you used for it.

b) Prove $\mathsf{f}(\mathsf{i}(v), \mathsf{i}(u)) \equiv \mathsf{i}(\mathsf{f}(u, v))$ using $\leftrightarrow_{\mathcal{E}}^{*}$. Mark in each step which part of your term you are replacing and which equation you used for it.

Solution:

a)

$$
\begin{aligned}
& \mathsf{f}(\underline{\mathsf{e}}, x) \\
\overset{(3)}{\leftrightarrow}_{\mathcal{E}}\ & \underline{\mathsf{f}(\mathsf{f}(x, \mathsf{i}(x)), x)} \\
\overset{(1)}{\leftrightarrow}_{\mathcal{E}}\ & \mathsf{f}(x, \underline{\mathsf{f}(\mathsf{i}(x), x)}) \\
\overset{(3)'}{\leftrightarrow}_{\mathcal{E}}\ & \underline{\mathsf{f}(x, \mathsf{e})} \\
\overset{(2)}{\leftrightarrow}_{\mathcal{E}}\ & \underline{x}
\end{aligned}
$$

b)

$$
\begin{aligned}
& \underline{\mathsf{f}(\mathsf{i}(v), \mathsf{i}(u))} \\
\overset{(2)}{\leftrightarrow}_{\mathcal{E}}\ & \mathsf{f}(\mathsf{f}(\mathsf{i}(v), \mathsf{i}(u)), \underline{\mathsf{e}}) \\
\overset{(3)}{\leftrightarrow}_{\mathcal{E}}\ & \mathsf{f}(\mathsf{f}(\mathsf{i}(v), \mathsf{i}(u)), \underline{\mathsf{f}(\mathsf{f}(u, v), \mathsf{i}(\mathsf{f}(u, v)))}) \\
\overset{(1)}{\leftrightarrow}_{\mathcal{E}}\ & \underline{\mathsf{f}(\mathsf{f}(\mathsf{i}(v), \mathsf{i}(u)), \mathsf{f}(u, \mathsf{f}(v, \mathsf{i}(\mathsf{f}(u, v)))))} \\
\overset{(1)}{\leftrightarrow}_{\mathcal{E}}\ & \mathsf{f}(\underline{\mathsf{f}(\mathsf{f}(\mathsf{i}(v), \mathsf{i}(u)), u)}, \mathsf{f}(v, \mathsf{i}(\mathsf{f}(u, v)))) \\
\overset{(1)}{\leftrightarrow}_{\mathcal{E}}\ & \mathsf{f}(\mathsf{f}(\mathsf{i}(v), \underline{\mathsf{f}(\mathsf{i}(u), u)}), \mathsf{f}(v, \mathsf{i}(\mathsf{f}(u, v)))) \\
\overset{(3)'}{\leftrightarrow}_{\mathcal{E}}\ & \mathsf{f}(\underline{\mathsf{f}(\mathsf{i}(v), \mathsf{e})}, \mathsf{f}(v, \mathsf{i}(\mathsf{f}(u, v)))) \\
\overset{(2)}{\leftrightarrow}_{\mathcal{E}}\ & \underline{\mathsf{f}(\mathsf{i}(v), \mathsf{f}(v, \mathsf{i}(\mathsf{f}(u, v))))} \\
\overset{(1)}{\leftrightarrow}_{\mathcal{E}}\ & \mathsf{f}(\underline{\mathsf{f}(\mathsf{i}(v), v)}, \mathsf{i}(\mathsf{f}(u, v))) \\
\overset{(3)'}{\leftrightarrow}_{\mathcal{E}}\ & \underline{\mathsf{f}(\mathsf{e}, \mathsf{i}(\mathsf{f}(u, v)))} \\
\overset{(a)}{\leftrightarrow}_{\mathcal{E}}\ & \mathsf{i}(\mathsf{f}(u, v))
\end{aligned}
$$