Exercise 1 (Monotonicity): 

(1 + 1 + 1 + 1 = 4 points)

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

a) \( s \sim t \) iff the numbers of different variables in \( s \) and \( t \) are equal, i.e., \( |\cal V(s)| = |\cal V(t)| \).

b) \( s \sim t \) iff \( s \) is a subterm of \( t \).

c) \( s \sim t \) iff \( s \) matches \( t \).

d) \( s \sim t \) iff \( \cal V(s) \subseteq \cal V(t) \).

Solution:

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

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

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

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

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) \( \sim_1 \subseteq T(\Sigma, \cal V) \times T(\Sigma, \cal V) \) with \( s \sim_1 t \iff |\cal V(s)| = |\cal V(t)| \).

ii) \( \sim_2 \subseteq T(\Sigma, \cal V) \times T(\Sigma, \cal V) \) with \( s \sim_2 t \iff \exists \sigma \in \text{SUB}(\Sigma, \cal V) \cdot s\sigma = t\sigma \) (i.e., \( s \) and \( t \) unify).

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

For example, we have \( 61 \sim_3 23 \) 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 \( (p, q) \sim_4 (u, v) \iff p \cdot v = u \cdot q \).

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.
Solution:

\[ a) \]

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

ii) \( \sim_2 \) is not an equivalence relation. Consider the terms \( t = f(a) \), \( s = f(x) \) and \( q = f(b) \). Then, \( t \sim_2 s \) with \( \sigma_1 = \{x/a\} \) and \( s \sim_2 q \) with \( \sigma_2 = \{x/b\} \), but there is no substitution \( \mu \) such that \( f(a) \mu = f(b) \mu \) 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. Furthermore, 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, \( x - y + y - z \equiv_m 0 \Rightarrow x - z \equiv_m 0 \) and thus, \( \sim_3 \) is transitive.

iv) \( \sim_4 \) is an equivalence relation. Let \( (p, q), (u, v), (a, b) \in \mathbb{Z} \times \mathbb{Z} \). Then, we have \( (p, q) \sim_4 (u, q) \), as \( p \cdot q = u \cdot q \) and thus, \( \sim_4 \) is reflexive. Furthermore, 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, \( \sim_4 \) is symmetric. Finally, if \( (p, q) \sim_4 (u, v) \) and \( (u, v) \sim_4 (a, b) \), then

\[
\begin{align*}
    p \cdot v &= u \cdot q & \land & & u \cdot b &= a \cdot v \\
    \Leftrightarrow \quad p \cdot v \cdot b &= u \cdot q \cdot b & \land & & u \cdot b \cdot q &= a \cdot v \cdot q \\
    \Leftrightarrow \quad p \cdot b \cdot v &= u \cdot q \cdot b & \land & & u \cdot q \cdot b &= a \cdot q \cdot v \\
    \Rightarrow \quad v \cdot (p \cdot b - a \cdot q) &= 0 \\
    \Leftrightarrow \quad p \cdot b - a \cdot q &= 0 \\
    \Rightarrow \quad p \cdot b &= a \cdot q
\end{align*}
\]

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 \( \sim_2 = \{(x, y) \mid x, y \in \mathbb{Z} \land x < 0 \land y < 0\} \cup \{(x, y) \mid x, y \in \mathbb{Z} \land x > 0 \land y > 0\} \).

---

**Exercise 3 (Equivalence classes):**

\( (2 + 4 = 6 \text{ points}) \)

\[ a) \]

Let \( s \sim t \) hold for two terms \( s \) and \( t \) if \( V(s) = V(t) \) 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 $E$ over $\Sigma = \Sigma_2 \cup \Sigma_0$ with $\Sigma_2 = \{, \cup\}$ and $\Sigma_0 = \{a\}$.

\[
\begin{align*}
(x : y) \cup z &\equiv x : (y \cup z) \\
x \cup (y \cup z) &\equiv (x \cup y) \cup z \\
x \cup y &\equiv y \cup x \\
x : (y : z) &\equiv y : (x : z) \\
x : (y \cup z) &\equiv y \cup (x : z)
\end{align*}
\]

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 $|V(s)|^{n \cdot k} \cdot |\Sigma|^k$ different terms having $k$ function symbols and the variable set $V(s)$. Hence, $[s]_{\sim}$ is finite.

b) We see that all equations $s \equiv t \in E$ satisfy $s \sim t$. Thus, the equivalence classes w.r.t. $\equiv_E$ are subsets of the equivalence classes w.r.t. $\sim$ and, therefore, finite. Knowing that all equivalence classes w.r.t. $\equiv_E$ are finite, for two given terms $s$ and $t$ we can decide whether $s \equiv_E t$ holds by computing the finite equivalence class $[s]_{\equiv_E}$ and return yes if $t \in [s]_{\equiv_E}$ 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):

Consider the following set of equations\(^1\) $E$:

\[
\begin{align*}
f(x, f(y, z)) &\equiv f(f(x, y), z) \\
f(x, e) &\equiv x \\
f(x, i(x)) &\equiv e \\
f(i(x), x) &\equiv e
\end{align*}
\]

\(^1\) They correspond to the group axioms from the lecture and an additional equation for the operation of inverse elements from the right hand side. (1 + 4 = 5 points)
a) Prove $f(e, x) \equiv x$ 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 $f(i(v), i(u)) \equiv i(f(u, v))$ 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)

$$f(e, x)$$

$$\begin{array}{c}
\langle 3 \rangle_{\mathcal{E}} f(f(x, i(x)), x) \\
\langle 1 \rangle_{\mathcal{E}} f(x, f(i(x), x)) \\
\langle 3' \rangle_{\mathcal{E}} f(x, e) \\
\langle 2 \rangle_{\mathcal{E}} x
\end{array}$$

b)

$$f(i(v), i(u))$$

$$\begin{array}{c}
\langle 2 \rangle_{\mathcal{E}} f(f(i(v), i(u)), e) \\
\langle 3 \rangle_{\mathcal{E}} f(f(i(v), i(u)), f(f(u, v), i(f(u, v)))) \\
\langle 1 \rangle_{\mathcal{E}} f(f(i(v), i(u)), f(u, f(v, i(f(u, v))))) \\
\langle 1 \rangle_{\mathcal{E}} f(f(i(v), i(u)), u, f(v, f(u, v)))) \\
\langle 1 \rangle_{\mathcal{E}} f(f(i(v), f(i(u), u), f(v, i(f(u, v))))) \\
\langle 3' \rangle_{\mathcal{E}} f(f(i(v), e), f(v, i(f(u, v)))) \\
\langle 2 \rangle_{\mathcal{E}} f(i(v), f(v, i(f(u, v)))) \\
\langle 1 \rangle_{\mathcal{E}} f(f(i(v), v), i(f(u, v))) \\
\langle 3' \rangle_{\mathcal{E}} f(e, i(f(u, v))) \\
\langle 2 \rangle_{\mathcal{E}} i(f(u, v))
\end{array}$$