COMPSCI/SFWRENG 2FA3
Discrete Mathematics with Applications II
Winter 2020

Week 03 Exercises with Solutions

Dr. William M. Farmer
McMaster University

Revised: January 25, 2020

Exercises

1. Let $\mathsf{FinSeq}_{\mathbb{N}}$ be the set of finite sequences whose members are in $\mathbb{N}$.

   a. Define $\mathsf{FinSeq}_{\mathbb{N}}$ as an inductive set.

   Solution:

   $\mathsf{FinSeq}_{\mathbb{N}}$ is the inductive set defined by the following constructors:

   - $\mathsf{Nil} : \mathsf{FinSeq}_{\mathbb{N}}$.
   - $\mathsf{Cons} : \mathbb{N} \times \mathsf{FinSeq}_{\mathbb{N}} \rightarrow \mathsf{FinSeq}_{\mathbb{N}}$.

   b. Define by pattern matching the function

   $$\mathsf{reverse} : \mathsf{FinSeq}_{\mathbb{N}} \rightarrow \mathsf{FinSeq}_{\mathbb{N}}$$

   such that $\mathsf{reverse}(s)$ is the reverse of s for all $s \in \mathsf{FinSeq}_{\mathbb{N}}$.

   Solution:

   We first need to define an auxiliary function:

   $\mathsf{revAux} : \mathsf{FinSeq}_{\mathbb{N}} \times \mathsf{FinSeq}_{\mathbb{N}} \rightarrow \mathsf{FinSeq}_{\mathbb{N}}$
   $\mathsf{revAux}(\mathsf{Nil}, y) = y$
   $\mathsf{revAux}(\mathsf{Cons}(a, x), y) = \mathsf{revAux}(x, \mathsf{Cons}(a, y))$

   $\mathsf{reverse}(x) = \mathsf{revAux}(x, \mathsf{Nil})$

   c. Write the structural induction principle for $\mathsf{FinSeq}_{\mathbb{N}}$.

   Solution:

   $$\begin{aligned}&(P(\mathsf{Nil}) \wedge (\forall s : \mathsf{FinSeq}_{\mathbb{N}} \,.\, P(s) \Rightarrow \forall x : \mathbb{N} \,.\, P(\mathsf{Cons}(x, s)))) \\ &\quad \Rightarrow \forall s : \mathsf{FinSeq}_{\mathbb{N}} \,.\, P(s).\end{aligned}$$

2. Let Nat be the natural numbers defined as an inductive set in the lecture notes, $\mathbb{B}$ be the set of boolean values true and false, $\mathsf{odd} : \mathsf{Nat} \to \mathbb{B}$ be the function that maps the odd natural numbers to true and the even natural numbers to false, and $\mathsf{even} : \mathsf{Nat} \to \mathbb{B}$ be the function that maps the even natural numbers to true and the odd natural numbers to false. Define odd and even simultaneously by pattern matching using "mutual recursion".

   Solution:

$$\mathsf{even}(0) = \mathsf{true}$$
$$\mathsf{even}(\mathsf{S}(x)) = \mathsf{odd}(x)$$

$$\mathsf{odd}(0) = \mathsf{false}$$
$$\mathsf{odd}(\mathsf{S}(x)) = \mathsf{even}(x)$$

3. Let $\mathsf{BinTree}$ be the inductive set and nodes and ht be the functions defined in the lecture notes. Let $\mathsf{leaves} : \mathsf{BinTree} \to \mathbb{N}$ be the function that maps a binary to the number of leaf nodes in it.

   a. Define leaves by pattern matching and recursion.

   Solution:

$$\mathsf{leaves}(\mathsf{Leaf}(n)) = 1.$$
$$\mathsf{leaves}(\mathsf{Branch}(t_1, n, t_2)) \quad = \mathsf{leaves}(t_1) + \mathsf{leaves}(t_2).$$

   Assuming function max is defined and returns the maximum of two numbers.

$$\mathsf{ht}(\mathsf{Leaf}(n)) = 0.$$
$$\mathsf{ht}(\mathsf{Branch}(t_1, n, t_2)) = 1 + \mathsf{max}(\mathsf{ht}(t_1), \mathsf{ht}(t_2)).$$

   b. Prove that, for all $t \in \mathsf{BinTree}$,

$$\mathsf{leaves}(t) \leq 2^{\mathsf{ht}(t)}$$

   by structural induction.

   Solution:

   Proof Let $P(t) \equiv \mathsf{leaves}(t) \leq 2^{\mathsf{ht}(t)}$ for $t \in \mathsf{BinTree}$. We will prove $P(t)$ for all $t \in \mathsf{BinTree}$ by structural induction.
   Base case: Prove $P(\mathsf{Leaf}(n))$ where $n \in \mathbb{N}$.

$$
\begin{aligned}
P(\mathsf{Leaf}(n)) &\equiv \mathsf{leaves}(\mathsf{Leaf}(n)) \leq 2^{\mathsf{ht}(\mathsf{Leaf}(n))} && \langle \text{definition of } P \rangle \\
&\equiv \mathsf{leaves}(\mathsf{Leaf}(n)) \leq 2^{0} && \langle \text{definition of } \mathsf{ht} \rangle \\
&\equiv 1 \leq 2^{0} && \langle \text{definition of } \mathsf{leaves} \rangle \\
&\equiv 1 \leq 1 && \langle \text{arithmetic} \rangle
\end{aligned}
$$

Induction step: Assume $P(t_1)$ and $P(t_2)$ hold for $t_1, t_2 \in \mathsf{BinTree}$. We will prove $P(\mathsf{Branch}(t_1, n, t_2)$ where $n \in \mathbb{N}$. Let $t = \mathsf{Branch}(t_1, n, t_2)$.

$$
\begin{aligned}
P(t) &\equiv \mathsf{leaves}(t) \leq 2^{\mathsf{ht}(t)} && \langle \text{definition of } P \rangle \\
&\equiv \mathsf{leaves}(t_1) + \mathsf{leaves}(t_2) \leq 2^{\mathsf{ht}(t)} && \langle \text{definition of } \mathsf{leaves} \rangle \\
&\equiv 2^{\mathsf{ht}(t_1)} + 2^{\mathsf{ht}(t_2)} \leq 2^{\mathsf{ht}(t)} && \langle \text{induction hypothesis} \rangle \\
&\equiv 2^{\mathsf{ht}(t_1)} + 2^{\mathsf{ht}(t_2)} \leq 2^{1+\mathsf{max}(\mathsf{ht}(t_1),\mathsf{ht}(t_2))} && \langle \text{definition of } \mathsf{ht} \rangle \\
&\equiv 2^{\mathsf{ht}(t_1)} + 2^{\mathsf{ht}(t_2)} \leq 2 * 2^{\mathsf{max}(\mathsf{ht}(t_1),\mathsf{ht}(t_2))} && \langle \text{arithmetic} \rangle
\end{aligned}
$$

$\square$

4. Let $\mathsf{BinTree}$ be the inductive set defined in the lecture notes. Let $\mathsf{mirror} : \mathsf{BinTree} \to \mathsf{BinTree}$ be the function that maps a binary tree to its "mirror image".

   a. Define mirror by pattern matching.

   Solution:

   $\mathsf{mirror}\ (\mathsf{Leaf}(n)) = \mathsf{Leaf}(n)$
   $\mathsf{mirror}\ (\mathsf{Branch}(t_1, n, t_2)) = \mathsf{Branch}(\mathsf{mirror}(t_2), n, \mathsf{mirror}(t1))$

   b. Prove that, for all $t \in \mathsf{BinTree}$,

   $$\mathsf{mirror}(\mathsf{mirror}(t)) = t$$

   by structural induction.

   Solution:

   Proof Let $P(t) \equiv \mathsf{mirror}(\mathsf{mirror}(t)) = t$. We will prove that $P(t)$ for all $t \in \mathsf{BinTree}$ by structural induction.

   Base case: Prove $P(\mathsf{Leaf(n)})$.

$$
\begin{aligned}
P(\mathsf{Leaf}(n)) &\equiv \mathsf{mirror}(\mathsf{mirror}(\mathsf{Leaf}(n))) = \mathsf{Leaf}(n) && \langle \text{definition of } P \rangle \\
&\equiv \mathsf{mirror}(\mathsf{Leaf}(n)) = \mathsf{Leaf}(n) && \langle \text{definition of mirror} \rangle \\
&\equiv \mathsf{Leaf}(n) = \mathsf{Leaf}(n) && \langle \text{definition of mirror} \rangle
\end{aligned}
$$

Induction step: Assume $P(t_1)$ and $P(t_2)$. Prove $P(\mathsf{Branch}(t_1, n, t_2))$
To save space let $\mathsf{mir} \equiv \mathsf{mirror}$.

$$\begin{aligned}
P(\mathsf{Branch}(t_1, n, t_2)) &\equiv \mathsf{mir}(\mathsf{mir}(\mathsf{Branch}(t_1, n, t_2))) = \mathsf{Branch}(t_1, n, t_2) \\
&\quad \langle \text{definition of } P \rangle \\
&\equiv \mathsf{mir}(\mathsf{Branch}(\mathsf{mir}(t_2), n, \mathsf{mir}(t_1))) = \mathsf{Branch}(t_1, n, t_2) \\
&\quad \langle \text{definition of mirror} \rangle \\
&\equiv \mathsf{Branch}(\mathsf{mir}(\mathsf{mir}(t_1)), n, \mathsf{mir}(\mathsf{mir}(t_2))) = \mathsf{Branch}(t_1, n, t_2) \\
&\quad \langle \text{definition of mirror} \rangle \\
&\equiv \mathsf{Branch}(t_1, n, t_2) = \mathsf{Branch}(t_1, n, t_2) \\
&\quad \langle \text{inductive hypothesis} \rangle
\end{aligned}$$

$\square$

5. Let $\mathsf{BinTree}$ be the inductive set defined in the lectures. A *subtree* of $t \in \mathsf{BinTree}$ is t itself or a subcomponent of t that is a member of $\mathsf{BinTree}$.

   a. Define a function $\mathsf{subtrees} : \mathsf{BinTree} \to \mathsf{set}(\mathsf{BinTree})$ that maps each $t \in \mathsf{BinTree}$ to the set of subtrees of t.

   Solution:

$$\begin{aligned}
\mathsf{subtrees}(\mathsf{Leaf}(a)) &= \{\mathsf{Leaf}(a)\} \\
\mathsf{subtrees}(\mathsf{Branch}(t_1, n, t_2)) &= \{(\mathsf{Branch}(t_1, n, t_2))\} \cup \mathsf{subtrees}(t_1) \cup \mathsf{subtrees}(t_2)
\end{aligned}$$

   b. Prove by structural induction that, if $t \in \mathsf{BinTree}$ contains n Branch nodes, then t has at most $2n + 1$ subtrees.

   Solution:

   Proof
   Base case: Prove $P(\mathsf{Leaf(a)})$ i.e., $n = 0$

$$\begin{aligned}
P(\mathsf{Leaf(a)}) &\equiv |\mathsf{subtrees}(\mathsf{Leaf(a)})| \leq 2n + 1 && \langle \text{definition of P} \rangle \\
&\equiv |\{\mathsf{Leaf(a)}\}| \leq 2n + 1 && \langle \text{definition of subtrees} \rangle \\
&\equiv 1 \leq 2n + 1 && \langle \text{cardinality of set} \rangle \\
&\equiv 1 \leq 2 * (0) + 1 && \langle \text{n} = 0 \rangle \\
&\equiv 1 \leq 1 && \langle \text{arithmetic} \rangle
\end{aligned}$$

   Induction step: Assume Pt holds for all trees with k branch nodes. Prove Pt for trees with $(k + 1)$ branch nodes. There are two scenarios:

- The tree consists of a root node and a subtree t1 that has k branch nodes.

$$\begin{aligned}
P(t) &\equiv |\mathsf{subtrees}(t)| \leq 2(k+1)+1 && \langle \text{definition of P} \rangle \\
&\equiv 1 + |\mathsf{subtrees}(t1)| \leq 2(k+1)+1 && \langle \text{definition of subtrees and cardinality} \rangle \\
&\equiv 1 + (2k+1) \leq 2(k+1)+1 && \langle \text{induction hypothesis} \rangle \\
&\equiv 2k+2 \leq 2k+3 && \langle \text{arithmetic} \rangle
\end{aligned}$$

- The tree consists of a root node and two subtrees t1 and t2, with each having $k1$ and $k2$ nodes, respectively. Moreover, $k1$+$k2$ = k branch nodes.

$$\begin{aligned}
P(t) &\equiv |\mathsf{subtrees}(t)| \leq 2(k+1)+1 && \langle \text{definition of P} \rangle \\
&\equiv 1 + |\mathsf{subtrees}(t1)| + |\mathsf{subtrees}(t2)| \leq 2(k+1)+1 && \langle \text{definition of subtrees} \rangle \\
& && \langle \text{and set cardinality} \rangle \\
&\equiv 1 + (2k1+1) + (2k2+1) \leq 2(k+1)+1 && \langle \text{induction hypothesis} \rangle \\
&\equiv 2(k1+k2)+3 \leq 2(k+1)+1 && \langle \text{arithmetic} \rangle \\
&\equiv 2k+3 \leq 2k+3 && \langle \text{addition of nodes} \rangle
\end{aligned}$$

□

6. Let S be the set of bit strings defined inductively by:

   a. `"0"` $\in S$.
   b. If $s \in S$, then `"0"` $+ s \in S$ and $s +$ `"0"` $\in S$.
   c. If $s \in S$, then , `"0"` $+ s +$ `"1"` $\in S$ and `"1"` $+ s +$ `"0"` $\in S$.

   $s + t$ denotes the concatenation of s and t. Prove by structural induction that, for all strings $s \in S$, the number of 1s in s is less than or equal to the number of 0s in s.

   Solution:

   Let us consider the set S as the inductive type defined by the following constructors:

   a. $\mathsf{0} : S$
   b. $\mathsf{0\text{-}left} : S \to S$.
   c. $\mathsf{0\text{-}right} : S \to S$.
   d. $\mathsf{0\text{-}1} : S \to S$.

e. $\mathsf{1\text{-}0} : S \to S$.

Define $\mathsf{zeros} : S \to \mathbb{N}$ and $\mathsf{ones} : S \to \mathbb{N}$ by pattern matching as follows:

$\mathsf{zeros}\,\mathsf{0} = 1.$
$\mathsf{zeros}\,(\mathsf{0\text{-}left}\,s) = 1 + \mathsf{zeros}\,s.$
$\mathsf{zeros}\,(\mathsf{0\text{-}right}\,s) = 1 + \mathsf{zeros}\,s.$
$\mathsf{zeros}\,(\mathsf{0\text{-}1}\,s) = 1 + \mathsf{zeros}\,s.$
$\mathsf{zeros}\,(\mathsf{1\text{-}0}\,s) = 1 + \mathsf{zeros}\,s.$
$\mathsf{ones}\,\mathsf{0} = 1.$
$\mathsf{ones}\,(\mathsf{0\text{-}left}\,s) = \mathsf{ones}\,s.$
$\mathsf{ones}\,(\mathsf{0\text{-}right}\,s) = \mathsf{ones}\,s.$
$\mathsf{ones}\,(\mathsf{0\text{-}1}\,s) = 1 + \mathsf{ones}\,s.$
$\mathsf{ones}\,(\mathsf{1\text{-}0}\,s) = 1 + \mathsf{ones}\,s.$

Theorem. $\mathsf{ones}(s) \le \mathsf{zeros}(s)$ for $s \in S$.

Proof Let $P(s) \equiv \mathsf{ones}(s) \le \mathsf{zeros}(s)$. We will prove $P(s)$ for all $s \in S$ by structure induction for S.

Base case: Prove $P(\mathsf{0})$.

$$\begin{aligned} \mathsf{ones}(\mathsf{0}) &= 0 && \langle \text{definition of } \mathsf{ones} \rangle \\ &< 1 && \langle \text{arithmetic} \rangle \\ &= \mathsf{zeros}(\mathsf{0}) && \langle \text{definition of } \mathsf{zeros} \rangle \end{aligned}$$

This shows that $P(\mathsf{0})$ holds.

Induction step 1: Assume $P(s)$. Prove $P(\mathsf{0\text{-}left}(s))$.

$$\begin{aligned} \mathsf{ones}(\mathsf{0\text{-}left}(s)) &= \mathsf{ones}(s) && \langle \text{definition of } \mathsf{ones} \rangle \\ &\le \mathsf{zeros}(s) && \langle \text{induction hypothesis} \rangle \\ &< \mathsf{zeros}(\mathsf{0\text{-}left}(s)) && \langle \text{definition of } \mathsf{zeros} \rangle \end{aligned}$$

This shows that $P(\mathsf{0\text{-}left}(s))$ holds.

Induction step 2: Assume $P(s)$. Prove $P(\mathsf{0\text{-}right}(s))$. The proof is similar to the previous case.

Induction step 3: Assume $P(s)$. Prove $P(\mathsf{0\text{-}1}(s))$.

$$\begin{aligned} \mathsf{ones}(\mathsf{0\text{-}1}(s)) &= 1 + \mathsf{ones}(s) && \langle \text{definition of } \mathsf{ones} \rangle \\ &\le 1 + \mathsf{zeros}(s) && \langle \text{induction hypothesis} \rangle \\ &= \mathsf{zeros}(\mathsf{0\text{-}left}(s)) && \langle \text{definition of } \mathsf{zeros} \rangle \end{aligned}$$

This shows that $P(\mathsf{0\text{-}1}(s))$ holds.

Induction step 4: Assume $P(s)$. Prove $P(\mathsf{1\text{-}0}(s))$. The proof is similar to the previous case.

$\square$

7. Suppose $(S_1, \leq_1)$ and $(S_2, \leq_2)$ are weak partial orders. Prove that $(S_1 \times S_2, \leq)$ is a weak partial order where $(s_1, s_2) \leq (s_1', s_2')$ iff $s_1 \leq_1 s_1'$ and $s_2 \leq_2 s_2'$.

Solution:

Proof If $(S_1 \times S_2, \leq)$ is reflexive, antisymmetric, and transitive, then it is a weak partial order. We already know that $(S_1, \leq_1)$ and $(S_2, \leq_2)$ are weak partial orders so they are reflexive, antisymmetric, and transitive. Definitions for a weak partial order, $(S, \leq)$, are given below:

$$\begin{aligned} \forall x \in S.\ x \leq x & \qquad \langle\text{reflexive}\rangle \\ \forall x, y \in S.\ x \leq y \wedge y \leq x \Rightarrow x = y & \qquad \langle\text{antisymmetric}\rangle \\ \forall x, y, z \in S.\ x \leq y \wedge y \leq z \Rightarrow x \leq z & \qquad \langle\text{transitive}\rangle \end{aligned}$$

We also have the given property of $(S_1 \times S_2, \leq)$:

$$\forall s_1 \in S_1, \forall s_2 \in S_2.\ (s_1, s_2) \leq (s_1', s_2') \iff s_1 \leq_1 s_1' \wedge s_2 \leq_2 s_2'$$

Reflexivity of $(S_1 \times S_2, \leq)$**:** For any $x_1 \in S_1$ and $x_2 \in S_2$ we see that:

$$\begin{aligned} & x_1 \leq_1 x_1 \wedge x_2 \leq_2 x_2 & \qquad \langle S_1 \text{ and } S_2 \text{ are reflexive}\rangle \\ \iff & (x_1, x_2) \leq (x_1, x_2) & \qquad \langle\text{given property}\rangle \end{aligned}$$

Therefore $\forall (x_1, x_2) \in S_1 \times S_2\ .\ (x_1, x_2) \leq (x_1, x_2)$. This shows that $(S_1 \times S_2, \leq)$ is reflexive.

Antisymmetry of $(S_1 \times S_2, \leq)$**:** For any $x_1, y_1 \in S_1$ and $x_2, y_2 \in S_2$ we see that:

$$\begin{aligned} & (x_1, x_2) \leq (y_1, y_2) \wedge (y_1, y_2) \leq (x_1, x_2) & \\ \Rightarrow\ & x_1 \leq_1 y_1 \wedge x_2 \leq_2 y_2 \wedge y_1 \leq_1 x_1 \wedge y_2 \leq_2 x_2 & \qquad \langle\text{given property}\rangle \\ \Rightarrow\ & x_1 = y_1 \wedge x_2 = y_2 & \qquad \langle S_1 \text{ and } S_2 \text{ are antisymmetric}\rangle \\ \Rightarrow\ & (x_1, x_2) = (y_1, y_2) & \end{aligned}$$

By transitivity of $\Rightarrow$, $\forall (x_1, x_2), (y_1, y_2) \in S_1 \times S_2\ .\ (x_1, x_2) \leq (y_1, y_2) \wedge (y_1, y_2) \leq (x_1, x_2) \Rightarrow (x_1, x_2) = (y_1, y_2)$. This shows that $(S_1 \times S_2, \leq)$ is antisymmetric.

Transitivity of $(S_1 \times S_2, \leq)$**:** For any $x_1, y_1, z_1 \in S_1$ and $x_2, y_2, z_2 \in S_2$ we see that:

$$\begin{aligned} & (x_1, x_2) \leq (y_1, y_2) \wedge (y_1, y_2) \leq (z_1, z_2) & \\ \Rightarrow\ & x_1 \leq_1 y_1 \wedge x_2 \leq_2 y_2 \wedge y_1 \leq_1 z_1 \wedge y_2 \leq_2 z_2 & \qquad \langle\text{given property}\rangle \\ \Rightarrow\ & x_1 \leq_1 z_1 \wedge x_2 \leq_2 z_2 & \qquad \langle S_1 \text{ and } S_2 \text{ are transitive}\rangle \\ \Rightarrow\ & (x_1, x_2) \leq (z_1, z_2) & \qquad \langle\text{given property}\rangle \end{aligned}$$

By transitivity of $\Rightarrow$, $\forall (x_1, x_2), (y_1, y_2), (z_1, z_2) \in S_1 \times S_2 \,.\, (x_1, x_2) \leq (y_1, y_2) \wedge (y_1, y_2) \leq (z_1, z_2) \Rightarrow (x_1, x_2) \leq (z_1, z_2)$. This shows that $(S_1 \times S_2, \leq)$ is transitive.

Therefore $(S_1 \times S_2, \leq)$ is a weak partial order. $\square$

8. Let $<_{\text{lex}} \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ be lexicographical order, i.e.,

$$(x_1, y_1) <_{\text{lex}} (x_2, y_2)$$

iff $x_1 < x_2$ or ($x_1 = x_2$ and $y_1 < y_2$).

a. Prove that $(\mathbb{N} \times \mathbb{N}, <_{\text{lex}})$ is a well-order.

Solution:

Proof A well-order is a strict total order that contains no infinite descending sequences. Strict total orders are irreflexive, asymmetric, transitive, and trichotomous.
Irreflexive: $\forall (x, y) \in (\mathbb{N} \times \mathbb{N}) \,.\, \neg((x, y) <_{\text{lex}} (x, y))$
Prove by contradiction: Assume $(x, y) <_{\text{lex}} (x, y)$

$$\begin{aligned}
& (x, y) <_{\text{lex}} (x, y) \\
& \qquad \langle \text{definition of } <_{\text{lex}} \rangle \\
\iff & x < x \vee (x = x \wedge y < y) \\
& \qquad \langle < \text{ is irreflexive: } \neg(x < x) \text{ and } \neg(y < y) \rangle \\
\iff & \mathit{False} \vee (x = x \wedge \mathit{False}) \\
& \qquad \langle \text{basic logic} \rangle \\
\iff & \mathit{False}
\end{aligned}$$

Our assumption implies false therefore the assumption was false; $(\mathbb{N} \times \mathbb{N}, <_{\text{lex}})$ is irreflexive.

Asymmetric: $\forall (x_1, y_1), (x_2, y_2) \in (\mathbb{N} \times \mathbb{N}) \,.\, (x_1, y_1) <_{\text{lex}} (x_2, y_2) \Rightarrow \neg((x_2, y_2) <_{\text{lex}} (x_1, y_1))$
Prove by contradiction: Assume $\neg((x_1, y_1) <_{\text{lex}} (x_2, y_2) \Rightarrow \neg(x_2, y_2) <_{\text{lex}} (x_1, y_1))$

$$
\begin{aligned}
& \neg((x_1, y_1) <_{\text{lex}} (x_2, y_2) \Rightarrow \neg((x_2, y_2) <_{\text{lex}} (x_1, y_1))) \\
& \qquad \langle p \Rightarrow q \equiv \neg p \vee q \rangle \\
\iff & \neg(\neg((x_1, y_1) <_{\text{lex}} (x_2, y_2)) \vee \neg((x_2, y_2) <_{\text{lex}} (x_1, y_1))) \\
& \qquad \langle \text{De Morgan's} \rangle \\
\iff & ((x_1, y_1) <_{\text{lex}} (x_2, y_2)) \wedge ((x_2, y_2) <_{\text{lex}} (x_1, y_1)) \\
& \qquad \langle \text{definition of } <_{\text{lex}} \rangle \\
\iff & (x_1 < x_2 \vee (x_1 = x_2 \wedge y_1 < y_2)) \wedge (x_2 < x_1 \vee (x_2 = x_1 \wedge y_2 < y_1)) \\
& \qquad \langle \vee \text{ and } \wedge \text{ rules to expand} \rangle \\
\iff & (x_1 < x_2 \wedge x_2 < x_1) \vee (x_1 < x_2 \wedge x_2 = x_1 \wedge y_2 < y_1) \\
& \qquad \vee (x_1 = x_2 \wedge y_1 < y_2 \wedge x_2 < x_1) \\
& \qquad \vee (x_1 = x_2 \wedge y_1 < y_2 \wedge x_2 = x_1 \wedge y_2 < y_1) \\
& \qquad \langle < \text{ is asymmetric} \rangle \\
\Rightarrow & \mathit{False} \vee (x_1 < x_2 \wedge x_2 = x_1 \wedge y_2 < y_1) \\
& \qquad \vee (x_1 = x_2 \wedge y_1 < y_2 \wedge x_2 < x_1) \\
& \qquad \vee \mathit{False} \\
& \qquad \langle \text{if } x_1 = x_2 \text{, then } x_1 < x_2 \Rightarrow x_1 < x_1 \text{ (contradicting that } < \text{ is irreflexive} \rangle \\
\Rightarrow & \mathit{False} \vee \mathit{False} \vee \mathit{False} \vee \mathit{False} \\
\iff & \mathit{False}
\end{aligned}
$$

Our assumption implies false therefore the assumption was false; $(\mathbb{N} \times \mathbb{N}, <_{\text{lex}})$ is asymmetric.

Transitive: $\forall (x_1, y_1), (x_2, y_2), (x_3, y_3) \in (\mathbb{N} \times \mathbb{N})\ .\ (x_1, y_1) <_{\text{lex}} (x_2, y_2) \wedge (x_2, y_2) <_{\text{lex}} (x_3, y_3) \Rightarrow (x_1, y_1) <_{\text{lex}} (x_3, y_3)$

$$
\begin{aligned}
& (x_1, y_1) <_{\text{lex}} (x_2, y_2) \wedge (x_2, y_2) <_{\text{lex}} (x_3, y_3) \\
& \qquad \langle \text{definition of } <_{\text{lex}} \rangle \\
\iff & (x_1 < x_2 \vee (x_1 = x_2 \wedge y_1 < y_2)) \wedge (x_2 < x_3 \vee (x_2 = x_3 \wedge y_2 < y_3)) \\
& \qquad \langle \vee \text{ and } \wedge \text{ rules to expand} \rangle \\
\iff & (x_1 < x_2 \wedge x_2 < x_3) \\
& \qquad \vee (x_1 < x_2 \wedge x_2 = x_3 \wedge y_2 < y_3) \\
& \qquad \vee (x_1 = x_2 \wedge y_1 < y_2 \wedge x_2 < x_3) \\
& \qquad \vee (x_1 = x_2 \wedge y_1 < y_2 \wedge x_2 = x_3 \wedge y_2 < y_3) \\
& \qquad \langle < \text{ is transitive} \rangle \\
\Rightarrow & (x_1 < x_3) \\
& \qquad \vee (x_1 < x_2 \wedge x_2 = x_3 \wedge y_2 < y_3) \\
& \qquad \vee (x_1 = x_2 \wedge y_1 < y_2 \wedge x_2 < x_3) \\
& \qquad \vee (x_1 = x_2 \wedge x_2 = x_3 \wedge y_1 < y_3) \\
& \qquad \langle \text{use } x_i = x_j \text{ terms to trivially rewrite} \rangle \\
\Rightarrow & (x_1 < x_3) \\
& \qquad \vee (x_1 < x_3 \wedge y_2 < y_3) \\
& \qquad \vee (y_1 < y_2 \wedge x_1 < x_3) \\
& \qquad \vee (x_1 = x_3 \wedge y_1 < y_3) \\
& \qquad \langle A \wedge B \Rightarrow A \rangle \\
\Rightarrow & (x_1 < x_3) \\
& \qquad \vee (x_1 < x_3) \\
& \qquad \vee (x_1 < x_3) \\
& \qquad \vee (x_1 = x_3 \wedge y_1 < y_3) \\
& \qquad \langle A \vee A \iff A \rangle \\
\iff & (x_1 < x_3) \vee (x_1 = x_3 \wedge y_1 < y_3) \\
& \qquad \langle \text{definition of } <_{\text{lex}} \rangle \\
\iff & (x_1, y_1) <_{\text{lex}} (x_3, y_3)
\end{aligned}
$$

By transitivity of implication we now have:

$$(x_1, y_1) <_{\text{lex}} (x_2, y_2) \wedge (x_2, y_2) <_{\text{lex}} (x_3, y_3) \Rightarrow (x_1, y_1) <_{\text{lex}} (x_3, y_3)$$

Therefore $(\mathbb{N} \times \mathbb{N}, <_{\text{lex}})$ is transitive.

Trichotomous: $\forall (x_1, y_1), (x_2, y_2) \in (\mathbb{N} \times \mathbb{N})\ .\ (x_1, y_1) <_{\text{lex}} (x_2, y_2) \vee (x_2, y_2) <_{\text{lex}} (x_1, y_1) \vee (x_1, y_1) = (x_2, y_2)$

$$
\begin{aligned}
&(x_1, y_1) <_{\text{lex}} (x_2, y_2) \lor (x_2, y_2) <_{\text{lex}} (x_1, y_1) \lor (x_1, y_1) = (x_2, y_2) \\
&\qquad \langle \text{definition of } <_{\text{lex}} \rangle \\
\iff &(x_1 < x_2 \lor (x_1 = x_2 \land y_1 < y_2)) \\
&\qquad \lor (x_2 < x_1 \lor (x_2 = x_1 \land y_2 < y_1)) \\
&\qquad \lor (x_1, y_1) = (x_2, y_2) \\
&\qquad \langle \text{expanding the } = \rangle \\
\iff &(x_1 < x_2 \lor (x_1 = x_2 \land y_1 < y_2)) \\
&\qquad \lor (x_2 < x_1 \lor (x_2 = x_1 \land y_2 < y_1)) \\
&\qquad \lor (x_1 = x_2 \land y_1 = y_2) \\
&\qquad \langle \text{rearranging terms} \rangle \\
\iff &x_1 < x_2 \lor x_2 < x_1 \\
&\qquad \lor (x_1 = x_2 \land y_1 < y_2) \\
&\qquad \lor (x_2 = x_1 \land y_2 < y_1) \\
&\qquad \lor (x_1 = x_2 \land y_1 = y_2) \\
&\qquad \langle (A \land B) \lor (A \land C) \iff A \land (B \lor C) \rangle \\
\iff &x_1 < x_2 \lor x_2 < x_1 \\
&\qquad \lor (x_1 = x_2 \land (y_1 < y_2 \lor y_2 < y_1 \lor y_1 = y_2)) \\
&\qquad \langle < \text{ is trichotomous} \rangle \\
\iff &x_1 < x_2 \lor x_2 < x_1 \\
&\qquad \lor (x_1 = x_2 \land True) \\
&\qquad \langle \text{reducing} \rangle \\
\iff &x_1 < x_2 \lor x_2 < x_1 \lor x_1 = x_2 \\
&\qquad \langle < \text{ is trichotomous} \rangle \\
\iff &True
\end{aligned}
$$

Looking at the above in reverse we see that true implies $(x_1, y_1) <_{\text{lex}} (x_2, y_2) \lor (x_2, y_2) <_{\text{lex}} (x_1, y_1) \lor (x_1, y_1) = (x_2, y_2)$. Therefore $(\mathbb{N} \times \mathbb{N}, <_{\text{lex}})$ is trichotomous.

Moving on...
Next, we will prove by contradiction that $(\mathbb{N} \times \mathbb{N}, <_{\text{lex}})$ contains no infinite descending sequences. Assume there is an infinite descending sequence:

$$... <_{\text{lex}} (x_2, y_2) <_{\text{lex}} (x_1, y_1) <_{\text{lex}} (x_0, y_0)$$

We observe two cases:

i. There is an infinite number of distinct x_i.
This contradicts that $(\mathbb{N}, <)$ is a well-order as the sequence of distinct x_i would form an infinite descending sequence.

ii. There is a finite number of distinct x_i.
Then $\exists k . \forall i, i \geq k \Rightarrow x_i = x_{i+1}$. But then the sequence of y_i for $i \geq k$ would form an infinite descending sequence which again contradicts that $(\mathbb{N}, <)$ is a well-order.

Therefore $(\mathbb{N} \times \mathbb{N}, <_{\text{lex}})$ has no infinite descending sequence.

□

b. Write the ordinal induction principle for $(\mathbb{N} \times \mathbb{N}, <_{\text{lex}})$.

Solution:

Proof The ordinal induction principle for $(\mathbb{N} \times \mathbb{N}, <_{\text{lex}})$ is:

$$\begin{aligned}&\forall (x, y) \in \mathbb{N} \times \mathbb{N} \ . \\ &\qquad ((\forall (x', y') \in \mathbb{N} \times \mathbb{N} \ . \ (x', y') <_{\text{lex}} (x, y) \Rightarrow P(x', y')) \\ &\qquad \Rightarrow P(x, y))\end{aligned}$$

for any property P of $\mathbb{N} \times \mathbb{N}$. □

c. Prove by the ordinal induction principle for $(\mathbb{N} \times \mathbb{N}, <_{\text{lex}})$ that the version of the Ackermann function presented in the lecture notes is defined on all members of $\mathbb{N} \times \mathbb{N}$.

Solution:

Proof Let $A : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be the Ackermann function defined by:

- $A(0, n) = n + 1$
- $A(m, 0) = A(m - 1, 1), if m > 0$
- $A(m, n) = A(m - 1, A(m, n - 1)), if m, n > 0$

Let $P(m, n)$ hold iff $A(m, n)$ exists.

Base Case: $(m, n) = (0, 0)$

$$A(0, 0) = 0 + 1 = 1$$

Therefore $A(0, 0)$ is defined and $P(0, 0)$ holds.
Inductive Step: $(0, 0) <_{\text{lex}} (m, n)$. Assume $P(m', n')$ for all $(m', n') <_{\text{lex}} (m, n)$. Prove $P(m, n)$.

We have three cases for the inductive step:

i. $m = 0$

$$A(0, n) = n + 1$$

Therefore $A(0, n)$ is defined.

ii. $m \neq 0$, $n = 0$

$$A(m,0) = A(m-1,1)$$

Since $(m-1,1) <_{\text{lex}} (m,0)$, $A(m-1,1)$ is defined by the induction hypothesis.
Therefore $A(m,0)$ is defined.

iii. $m \neq 0$, $n \neq 0$

$$A(m,n) = A(m-1, A(m,n-1))$$

Since: $A(m,n-1) <_{\text{lex}} A(m,n)$
Therefore, by the induction hypothesis, $A(m,n-1)$ is defined.
Also: $A(m-1, A(m,n-1)) <_{\text{lex}} A(m,n)$
Therefore, by the induction hypothesis, $A(m-1, A(m,n-1))$ is defined.
Therefore $A(m,n)$ is defined for $m,n \neq 0$.

In each case we found that $A(m,n)$ was defined, therefore $P(m,n)$ holds given the inductive hypothesis.
Therefore $A(m,n)$ is defined on all members of $\mathbb{N} \times \mathbb{N}$.

$\square$

9. Let $(S,<)$ be a partial order such that S is finite. Prove that $(S,<)$ is well-founded.

Solution:

Proof $(S,<)$ is a strict partial order and is therefore irreflexive $(\neg x < x)$, and transitive $(x < y \wedge y < z \Rightarrow x < z)$. For this question we won't need the asymmetry of strict partial orders.

We know that $(S,<)$ is well-founded iff $(S,<)$ is Noetherian iff every descending $<$-sequence of members of S is finite.
We proceed by contradiction. Assume there exists an infinite descending $<$-sequence:

$$... < x_2 < x_1 < x_0$$

Choose n such that $x_n = x_i$ for some $i < n$. We know that such an n exists because this is an infinite sequence of members of S, but there is only a finite number of members of S.
Trivially, with transitivity, we can see that for any member of the sequence, a, and every earlier member in the sequence, b: $a < b$ (i.e. the n_{th} member of the sequence is less than all earlier members).
Thus $x_n < x_i$, and since $x_n = x_i$, this means that $x_n < x_n$, but then $(S,<)$ is not irreflexive and is not a strict partial order. Therefore by contradiction, there is no infinite descending $<$-sequence, every descending $<$-sequence of members of S is finite, and $(S,<)$ is well-founded. $\square$

10. Let $(\mathbb{N}, R_{\mathsf{suc}})$ be the mathematical structure where

$$m \; R_{\mathsf{suc}} \; n \text{ iff } n = m + 1.$$

Prove that $(\mathbb{N}, R_{\mathsf{suc}})$ is well-founded.

Solution:

Proof As in question 8 we will prove by contradiction by assuming there exists an infinite descending R_{suc}-sequence:

$$\ldots \; R_{\mathsf{suc}} \; x_2 \; R_{\mathsf{suc}} \; x_1 \; R_{\mathsf{suc}} \; x_0$$

Because $m \; R_{\mathsf{suc}} \; n \iff n = m + 1$, we can rewrite the sequence as:

$$\ldots \; R_{\mathsf{suc}} \; x_0 - (x_0 + 1) \; R_{\mathsf{suc}} \; x_0 - x_0 \ldots \; R_{\mathsf{suc}} \; x_0 - 2 \; R_{\mathsf{suc}} \; x_0 - 1 \; R_{\mathsf{suc}} \; x_0$$

But here we see that one of the members of the sequence is $x_0 - (x_0 + 1) = -1$ and $-1 \notin \mathbb{N}$ so the sequence cannot continue. Therefore, by contradiction, $(\mathbb{N}, R_{\mathsf{suc}})$ is well-founded.

□

11. The Ackermann function was originally defined as the ternary function $B : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that:

   a. $B(m, n, 0) = m + n$.
   b. $B(m, 0, 1) = 0$.
   c. $B(m, 0, 2) = 1$.
   d. $B(m, 0, p) = m$ for $p > 2$.
   e. $B(m, n, p) = B(m, B(m, n - 1, p), p - 1)$ for $n > 0$ and $p > 0$.

Prove that B is defined on all members of $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ using well-founded induction.

Solution:

Proof Let $U = \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ and $R \subseteq U$ be the relation defined by

$$(m, n, p) \; R \; (m', n', p') \text{ iff (1) } p' < p \text{ or (2) } p' = p \text{ and } n' < n.$$

Every nonempty subset of U has an R-minimal element since $(\mathbb{N}, <)$ is a well-order; hence (U, R) is well founded. Let $P(m, n, p)$ mean that $B(m, n, p)$ is defined. We will prove that $P(m, n, p)$ holds for all $(m, n, p) \in U$ by the well-founded induction principle for (U, R):

$$\begin{array}{l} (\forall \, (m, n, p) \in U \, . \\ \quad (\forall \, (m', n', p') \in U \, . \, (m', n', p') \; R \; (m, n, p) \Rightarrow P(m', n', p')) \\ \qquad \Rightarrow P(m, n, p)) \\ \quad \Rightarrow \forall \, (m, n, p) \in U \, . \, P(m, n, p). \end{array}$$

Let $(m, n, p) \in U$. Assume that, for all $(m', n', p') \in U$ with

$$(m', n', p') \; R \; (m, n, p),$$

$P(m', n', p')$ holds. We must show that $P(m, n, p)$ holds.

Case 1: $n = 0$ or $p = 0$. Then $B(m, n, p)$ is clearly defined and thus $P(m, n, p)$ holds.

Case 2: $n > 0$ and $p > 0$. Then $B(m, n-1, p)$ is defined by $P(m, n-1, p)$ since $(m, n-1, p) \; R \; (m, n, p)$ and $B(m, B(m, n-1, p), p-1)$ is defined by $P(m, B(m, n-1, p), p-1)$ since $(m, B(m, n-1, p), p-1) \; R \; (m, n, p)$. Then $B(m, n, p)$ is clearly defined and thus $P(m, n, p)$ holds.

Therefore, B is total. $\square$