ETH Zürich, D-INFK
HS 2023, 3. November 2023

Prof. Ueli Maurer
Giovanni Deligios

Diskrete Mathematik

Solution 6

6.1 Partial Order Relations

a) **i)** 11 and 12 are incomparable, since $11 \nmid 12$ and $12 \nmid 11$.
ii) 4 and 6 are incomparable, since $4 \nmid 6$ and $6 \nmid 4$.
iii) 5 and 15 are comparable, since $5 \mid 15$.
iv) 42 and 42 are comparable, since $42 \mid 42$.

b) The elements $(a, b) \in A$, such that $(a, b) \leq_{\mathsf{lex}} (2, 5)$ are: $(2, 1), (2, 5)$ and $(1, n)$ for all $n \in \mathbb{N} \setminus \{0\}$.

Justification: Let $(a, b) \in A$. We distinguish the following cases:

Case $a = 1$: Since $1 \mid 2$, we have $(a, b) \leq_{\mathsf{lex}} (2, 5)$ for any b.

Case $a = 2$: Since 1 and 5 are the only natural numbers which divide 5, we have $(a, b) \leq_{\mathsf{lex}} (2, 5)$ only for $b \in \{1, 5\}$.

Case $a > 2$: Since $a \nmid 2$, $(a, b) \leq_{\mathsf{lex}} (2, 5)$ cannot hold for any b.

c) $(\{1, 3, 6, 9, 12\}, \mid)$ is not a lattice, since 9 and 12 do not have a common upper bound.

d) $(A; \widehat{\preceq})$ is a poset. To prove this, we show that $\widehat{\preceq}$ is a partial order on A.

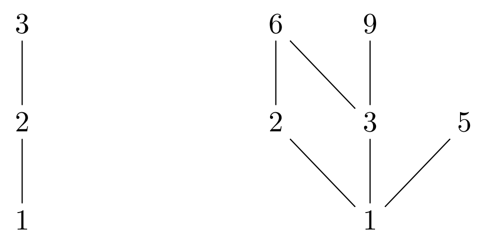
Reflexivity: For any $a \in A$, by the reflexivity of $\preceq$, we have $a \preceq a$, hence, $a \widehat{\preceq} a$.

Antisymmetry: Let $a, b \in A$ be such that $a \widehat{\preceq} b$ and $b \widehat{\preceq} a$. This means that $b \preceq a$ and $a \preceq b$ By the antisymmetry of $\preceq$, it follows that $a = b$.

Transitivity: Let $a, b, c \in A$ be such that $a \widehat{\preceq} b$ and $b \widehat{\preceq} c$. This means that $b \preceq a$ and $c \preceq b$. By the transitivity of $\preceq$, we have $c \preceq a$. Hence, $a \widehat{\preceq} c$.

6.2 Hasse Diagrams

a) The Hasse diagrams of the posets $(\{1, 2, 3\}; \leq)$ and $(\{1, 2, 3, 5, 6, 9\}; \mid)$ are as follows:



In both cases, 1 is the least and the only minimal element. In the poset $(\{1, 2, 3\}; \leq)$, the greatest and the only maximal element is 3. In the poset $(\{1, 2, 3, 5, 6, 9\}; \mid)$ there is no greatest element. The maximal elements in this poset are $5, 6$ and 9.

6.3 The Lexicographic Order

For posets $(A; \preceq)$ and $(B; \sqsubseteq)$ the lexicographic order $\leq_{\mathsf{lex}}$ on $A \times B$ is defined by

$$(a_1, b_1) \leq_{\mathsf{lex}} (a_2, b_2) \; :\Longleftrightarrow \; a_1 \prec a_2 \vee (a_1 = a_2 \wedge b_1 \sqsubseteq b_2)$$

We show that $\leq_{\mathsf{lex}}$ is a partial order relation.

Reflexivity: Take any $(a_1, b_1) \in A \times B$. Since $\sqsubseteq$ is reflexive, we have $b_1 \sqsubseteq b_1$. Hence, it is true that $(a_1 = a_1 \wedge b_1 \sqsubseteq b_1)$ and, thus, $(a_1, b_1) \leq_{\mathsf{lex}} (a_1, b_1)$.

Antisymmetry: Take any (a_1, b_1) and (a_2, b_2) in $A \times B$ such that $(a_1, b_1) \leq_{\mathsf{lex}} (a_2, b_2)$ and $(a_2, b_2) \leq_{\mathsf{lex}} (a_1, b_1)$. This means that

$$\underbrace{a_1 \prec a_2}_{(1)} \vee \underbrace{(a_1 = a_2 \wedge b_1 \sqsubseteq b_2)}_{(2)} \quad \text{and} \quad \underbrace{a_2 \prec a_1}_{(3)} \vee \underbrace{(a_2 = a_1 \wedge b_2 \sqsubseteq b_1)}_{(4)}.$$

We have to show that $(a_1, b_1) = (a_2, b_2)$. The proof proceeds by case distinction.

(1) **and** (3)**:** We have $a_1 \preceq a_2 \;\wedge\; a_1 \neq a_2$ and $a_2 \preceq a_1 \;\wedge\; a_2 \neq a_1$. But since $\preceq$ is antisymmetric, it follows that $a_1 = a_2$, which is a contradiction with $a_1 \neq a_2$. Therefore, this case cannot occur.

(1) **and** (4)**:** We have $a_1 \preceq a_2 \wedge a_1 \neq a_2$ and $a_2 = a_1 \wedge b_2 \sqsubseteq b_1$, which is a contradiction. Therefore, this case also cannot occur.

(2) **and** (3)**:** We have $a_1 = a_2 \wedge b_1 \sqsubseteq b_2$ and $a_2 \preceq a_1 \wedge a_2 \neq a_1$, which is a contradiction. Therefore, this case cannot occur as well.

(2) **and** (4)**:** We have $a_1 = a_2 \wedge b_1 \sqsubseteq b_2$ and $a_2 = a_1 \wedge b_2 \sqsubseteq b_1$. Since $\sqsubseteq$ is antisymmetric, it follows that $b_1 = b_2$. But we also have $a_1 = a_2$ and, thus, $(a_1, b_1) = (a_2, b_2)$.

Transitivity: Take any $(a_1, b_1), (a_2, b_2), (a_3, b_3)$ in $A \times B$ such that $(a_1, b_1) \leq_{\mathsf{lex}} (a_2, b_2)$ and $(a_2, b_2) \leq_{\mathsf{lex}} (a_3, b_3)$. This means that

$$\underbrace{a_1 \prec a_2}_{(1)} \vee \underbrace{(a_1 = a_2 \wedge b_1 \sqsubseteq b_2)}_{(2)} \quad \text{and} \quad \underbrace{a_2 \prec a_3}_{(3)} \vee \underbrace{(a_2 = a_3 \wedge b_2 \sqsubseteq b_3)}_{(4)}.$$

We have to show that $(a_1, b_1) \leq_{\mathsf{lex}} (a_3, b_3)$. The proof proceeds by case distinction.

(1) **and** (3)**:** We have $a_1 \prec a_2$ and $a_2 \prec a_3$. Since $\preceq$ is transitive we have $a_1 \preceq a_3$. Moreover, if we had $a_1 = a_3$, the antisymmetry of $\preceq$ would imply that $a_1 = a_2$, a contradiction to $a_1 \prec a_2$. Thus, $a_1 \neq a_3$, and therefore $a_1 \prec a_3$. Hence, $(a_1, b_1) \leq_{\mathsf{lex}} (a_3, b_3)$.

(1) **and** (4)**:** We have $a_1 \prec a_2$ and $a_2 = a_3 \wedge b_2 \sqsubseteq b_3$. Hence, $a_1 \prec a_3$ and, therefore, $(a_1, b_1) \leq_{\mathsf{lex}} (a_3, b_3)$.

(2) **and** (3)**:** We have $a_1 = a_2 \wedge b_1 \sqsubseteq b_2$ and $a_2 \prec a_3$. Hence, $a_1 \prec a_3$ and, therefore, $(a_1, b_1) \leq_{\mathsf{lex}} (a_3, b_3)$.

(2) **and** (4)**:** We have $a_1 = a_2 \wedge b_1 \sqsubseteq b_2$ and $a_2 = a_3 \wedge b_2 \sqsubseteq b_3$. It follows that $a_1 = a_3$. Since $\sqsubseteq$ is transitive, we also have $b_1 \sqsubseteq b_3$. Therefore, $(a_1, b_1) \leq_{\mathsf{lex}} (a_3, b_3)$.

6.4 Inverses of Functions

We prove the two implications separately.

($\Longrightarrow$) Let g be a function such that $g \circ f = \mathrm{id}$. We show that f is injective. Assume that $f(a) = f(b)$ for some $a, b \in A$. Then

$$\begin{aligned} a &= (g \circ f)(a) && (g \circ f = \mathrm{id}) \\ &= g(f(a)) && (\text{def. } \circ) \\ &= g(f(b)) && (f(a) = f(b)) \\ &= (g \circ f)(b) && (\text{def. } \circ) \\ &= b && (g \circ f = \mathrm{id}) \end{aligned}$$

($\Longleftarrow$) Assume that f is injective. We construct a function g such that $g \circ f = \mathrm{id}$ as follows. For any $b \in \mathrm{Im}(f)$, by the injectivity of f, there exists a unique a such that $f(a) = b$, and we define $g(b) = a$. For $b \notin \mathrm{Im}(f)$, we define $g(b) = b$. We have $g \circ f = \mathrm{id}$, because for any $a \in A$, $f(a) \in \mathrm{Im}(f)$, so $g(f(a)) = a$.

Note: The choice $g(b) = b$ in case $b \notin \mathrm{Im}(f)$ is irrelevant. For example, we could set $g(b) = a_0$ for some fixed $a_0 \in A$.

6.5 Countability and Uncountability

a) We prove the implication indirectly. Assume that B is countable. Then $B \preceq \mathbb{N}$ (Definition 3.42). Since $A \preceq B$ (by assumption) and $B \preceq \mathbb{N}$, we get $A \preceq \mathbb{N}$ (Lemma 3.15 (a)), that is, A is countable (Definition 3.42).

b) We show an injection from $\{0,1\}^\infty$ into S. Consider the function[1]

$$\begin{aligned} \psi : \{0,1\}^\infty &\to S \\ f &\mapsto g \end{aligned}$$

where $g : \{0,1\} \to \{0,1\}^\infty$ is the (constant) function such that $g(0) = g(1) = f$. We show that ψ is injective, that is, for all $f, f' \in \{0,1\}^\infty$ if $\psi(f) = \psi(f')$ then $f = f'$ (the indirect implication of Definition 3.39-1). Let $g = \psi(f)$ and $g' = \psi(f')$ and suppose $g = g'$. We have $f = g(0) = g'(0) = f'$. Therefore ψ is an injection from the uncountable set $\{0,1\}^\infty$ (Theorem 3.18) into S. This means $\{0,1\}^\infty \preceq S$ (Definition 3.42-(ii)) and the claim follows from subtask (a).

6.6 The Hunt for the Red October

The set $\mathbb{Z} \times \mathbb{Z}$ of possible parameters (v, s_0) is countable due to the fact that $\mathbb{Z}$ is countable (see Example 3.57) and Corollary 3.20. Thus, due to Theorem 3.17 there exists a bijection $\psi : \mathbb{N} \to \mathbb{Z} \times \mathbb{Z}$. The strategy is to attempt the parameters in the sequence

$$\psi(0), \psi(1), \psi(2), \ldots$$

[1] We interpret the set $\{0,1\}^\infty$ as the set of functions $\mathbb{N} \to \{0,1\}$.

Since ψ is a bijection, Svetlana will find the correct values $(\widehat{v}, \widehat{s_0}) \in \mathbb{Z} \times \mathbb{Z}$ in the i-th attempt (we start to count from zero), where

$$i = \psi^{-1}(\widehat{v}, \widehat{s_0}).$$

Hence, Svetlana only needs finitely many attempts, so she is guaranteed to find the correct parameters in a finite time.

6.7 More Countability

a) The set of all Java programs is countable. Every Java program can be seen as a finite binary sequence. That is, there is an injection from the set of all Java programs to the set $\{0,1\}^*$ of finite binary sequences. By Theorem 3.18, this set is countable.

b) This set is uncountable. To prove this, we notice that $\{0,1\}^\infty \subseteq A$, which implies that $\{0,1\}^\infty \preceq A$ (Lemma 3.15). Since $\{0,1\}^\infty$ is uncountable, A must be uncountable as well (if A was countable, the transitivity of $\preceq$ would imply that $\{0,1\}^\infty$ is countable, which is a contradiction).

An alternative proof. We can also apply directly the diagonalization argument.

Assume towards a contradiction that there is a bijection $f : \mathbb{N} \to A$. Let $\beta_{i,j}$ denote the j-th number in the i-th sequence. We define a new sequence as follows:

$$\alpha \stackrel{\text{def}}{=} R_{10}(\beta_{0,0}+1), R_{10}(\beta_{1,1}+1), R_{10}(\beta_{2,2}+1), \dots ,$$

where $R_{10}(a)$ denotes the remainder when a is divided by 10. Of course, $\alpha \in A$. Moreover, there is no $n \in \mathbb{N}$ such that $\alpha = f(n)$, since α disagrees with a sequence $f(n)$ on position n.

c) This set is uncountable. We can define an injective function $f : [0,1] \to C$ by $f(x) = \left(x, \sqrt{1-x^2}\right)$. Hence, we have $[0,1] \preceq C$. Since $[0,1]$ is uncountable, C must be uncountable as well (if C was countable, the transitivity of $\preceq$ would imply that $[0,1]$ is countable as well, which is a contradiction).

Note: The fact that the interval $[0,1]$ is uncountable follows from Theorem 3.23 and the fact that any element of $\{0,1\}^\infty$ can be interpreted as the binary expansion of a number in the interval $[0,1]$, and vice versa.

d) To begin, consider the subset $\mathbb{P} \subseteq \mathbb{N}$ of prime numbers and consider the inclusion function

$$\begin{aligned} i : \mathbb{P} &\to \mathbb{N}, \\ p &\mapsto p. \end{aligned} \tag{1}$$

The function i is injective, as $i(p) = i(p')$ clearly implies $p = p'$. This means $\mathbb{P} \preceq \mathbb{N}$ (Definition 3.42). Since $\mathbb{P}$ is infinite (hint), then $\mathbb{P} \sim \mathbb{N}$ (Theorem 3.17), or equivalently there exists a bijection between $\mathbb{N}$ and $\mathbb{P}$. Let $\phi : \mathbb{N} \to \mathbb{P}$ be such a bijective function. We prove that S is uncountable by exhibiting an injection from $\{0,1\}^\infty$ to S. In what follows, we understand the set $\{0,1\}^\infty$ as the set of functions $\mathbb{N} \to \{0,1\}$. Consider the following function

$$\begin{aligned} \psi : \{0,1\}^\infty &\to S, \\ f &\mapsto g \end{aligned} \tag{2}$$

where g is defined as follows:

$$g(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \neq 1 \text{ and } n \text{ is not prime }, \\ f(\phi^{-1}(n)) & \text{otherwise.} \end{cases} \tag{3}$$

First of all, we prove that ψ is well defined, that is, for all $f \in \{0,1\}^\infty$ it holds that $\psi(f) \in S$. Let $f \in \{0,1\}^\infty$ and let $g = \psi(f)$. Let $n \in \mathbb{N}$ such that $g(n) = 0$. There are three cases to consider.

- The first case is that $n = 0$. In this case, for all $m \in \mathbb{N}$ we have $0 \nmid m$ so that there is nothing to check.
- The second case is that $n \notin \{0,1\}$ and n is not prime. In this case, if $n \mid m$ then $m \neq 1$ and m is not prime, so that $g(m) = 0$.
- The last case is that n is prime. In this case, if $n \mid m$ then m is not prime, so that $g(m) = 0$.

This shows that $g \in S$.

Next, we show that ψ is injective. Suppose that $\psi(f) = \psi(f')$ for some $f, f' \in \{0,1\}^\infty$. Let $g = \psi(f)$ and $g' = \psi(f')$. This means that for all $n \in \mathbb{N}$ it holds that $g(n) = g'(n)$. We want to show that $f(n) = f'(n)$ for all $n \in \mathbb{N}$. Let $n \in \mathbb{N}$. Since ϕ is bijective we have $n = \phi^{-1}(p)$ for some $p \in \mathbb{P}$. Therefore

$$\begin{aligned} f(n) &= f(\phi^{-1}(p)) && (n = \phi^{-1}(p)) \\ &= g(p) && (\text{Definition of } g) \\ &= g'(p) && (g(n) = g'(n) \text{ for all } n \in \mathbb{N}) \\ &= f'(\phi^{-1}(p)) && (\text{Definition of } g) \\ &= f'(n) && (n = \phi^{-1}(p)). \end{aligned} \tag{4}$$

This shows that ψ is injective.