Discrete Mathematics

Supervision 6 – Solutions with Commentary

Marcelo Fiore Ohad Kammar Dima Szamozvancev

6. On relations

6.1. Basic exercises

1. Let $A = \{1,2,3,4\}$, $B = \{a,b,c,d\}$ and $C = \{x,y,z\}$.
   Let $R = \{(1,a),(2,d),(3,a),(3,b),(3,d)\} : A \nrightarrow B$
   and $S = \{(b,x),(b,y),(c,y),(d,z)\} : B \nrightarrow C$.

   Draw the internal diagrams of the relations. What is the composition $S \circ R : A \nrightarrow C$?

2. Prove that relational composition is associative and has the identity relation as the neutral element.

3. For a relation $R : A \nrightarrow B$, let its *opposite*, or *dual relation*, $R^{\mathrm{op}} : B \nrightarrow A$ be defined by:

$$b\, R^{\mathrm{op}}\, a \iff a\, R\, b$$

   For $R, S : A \nrightarrow B$ and $T : B \nrightarrow C$, prove that:

   a) $R \subseteq S \Longrightarrow R^{\mathrm{op}} \subseteq S^{\mathrm{op}}$
   b) $(R \cap S)^{\mathrm{op}} = R^{\mathrm{op}} \cap S^{\mathrm{op}}$
   c) $(R \cup S)^{\mathrm{op}} = R^{\mathrm{op}} \cup S^{\mathrm{op}}$
   d) $(T \circ S)^{\mathrm{op}} = S^{\mathrm{op}} \circ T^{\mathrm{op}}$

6.2. Core exercises

1. Let $R, R' \subseteq A \times B$ and $S, S' \subseteq B \times C$ be two pairs of relations and assume $R \subseteq R'$ and $S \subseteq S'$. Prove that $S \circ R \subseteq S' \circ R'$.

> Assume $(a,c) \in (S \circ R)$. Hence, there exists $b \in B$ such that $(a,b) \in R$ and $(b,c) \in S$. Then, since $(a,b) \in R$ and $R \subseteq R'$, we have that $(a,b) \in R'$; similarly, $(b,c) \in S'$. By the definition of composition, this implies that $(a,c) \in S' \circ R'$, as required.

> ♪ A simple, but useful lemma which states that subset relationships can be applied on both operands of relational composition. We have seen similar properties for powersets (§5.2.2(a)), Cartesian products (§5.2.4(a)) and disjoint unions (§5.2.5(a)). As usual, special cases of this property can be derived by expanding only one of the two operands: for example, $S' \circ R$ and $S \circ R'$.

2. Let $\mathcal{F} \subseteq \mathcal{P}(A \times B)$ and $\mathcal{G} \subseteq \mathcal{P}(B \times C)$ be two collections of relations from A to B and from B to C, respectively. Prove that

$$\left(\bigcup \mathcal{G}\right) \circ \left(\bigcup \mathcal{F}\right) = \bigcup \{ S \circ R \mid R \in \mathcal{F}, S \in \mathcal{G} \} : A \nrightarrow C$$

Recall that the notation $\{ S \circ R : A \nrightarrow C \mid R \in \mathcal{F}, S \in \mathcal{G} \}$ is common syntactic sugar for the formal definition $\{ T \in \mathcal{P}(A \times C) \mid \exists R \in \mathcal{F}.\ \exists S \in \mathcal{G}.\ T = S \circ R \}$. Hence,

$$T \in \{ S \circ R \in A \nrightarrow C \mid R \in \mathcal{F}, S \in \mathcal{G} \} \iff \exists R \in \mathcal{F}.\ \exists S \in \mathcal{G}.\ T = S \circ R$$

> ($\subseteq$) We show: $\left(\bigcup \mathcal{G}\right) \circ \left(\bigcup \mathcal{F}\right) \subseteq \bigcup \{ S \circ R \mid R \in \mathcal{F}, S \in \mathcal{G} \}$.
>
> Assume $(a,c) \in \left(\bigcup \mathcal{G}\right) \circ \left(\bigcup \mathcal{F}\right)$. Hence, there exists $b \in B$ such that $(a,b) \in \bigcup \mathcal{F}$ and $(b,c) \in \bigcup \mathcal{G}$. Then, by the definition of big unions, we have $(a,b) \in R$ for some $R \in \mathcal{F}$ and $(b,c) \in S$ for some $S \in \mathcal{G}$ so it follows that $(a,c) \in S \circ R$ for some $R \in \mathcal{F}$ and $S \in \mathcal{G}$. That is, $(a,c) \in \bigcup \{ S \circ R \mid R \in \mathcal{F}, S \in \mathcal{G} \}$.
>
> ($\supseteq$) By the universal property of unions, we have that $\bigcup \{ S \circ R \mid R \in \mathcal{F}, S \in \mathcal{G} \} \subseteq \left(\bigcup \mathcal{G}\right) \circ \left(\bigcup \mathcal{F}\right)$ if and only if $S \circ R \subseteq \left(\bigcup \mathcal{G}\right) \circ \left(\bigcup \mathcal{F}\right)$ for all $R \in \mathcal{F}$ and $S \in \mathcal{G}$. This is the case by §6.2.1 and the fact that $R \subseteq \bigcup \mathcal{F}$ for all $S \in \mathcal{F}$ and $S \subseteq \bigcup \mathcal{G}$ for all $S \in \mathcal{G}$, since the big unions are upper bounds.
>
> $\boxed{♪}$ One direction required a direct proof of membership, but the other direction was of the form $\bigcup \mathcal{U} \subseteq X$ and therefore could be approached via the universal property of big unions as the least upper bound of a family of sets; to show that it is below X, it is sufficient to show that every element of the family $\mathcal{U}$ is below X.

What happens in the case of big intersections?

> One direction follows in both cases from the universal property of intersections:
>
> $$\left(\bigcap \mathcal{G}\right) \circ \left(\bigcap \mathcal{F}\right) \subseteq \bigcap \{ S \circ R \mid R \in \mathcal{F}, S \in \mathcal{G} \}$$
>
> However, the other inclusion fails. Consider a pair $(a,c) \in \bigcap \{ S \circ R \mid R \in \mathcal{F}, S \in \mathcal{G} \}$: it means that for all $R \in \mathcal{F}$ and $S \in \mathcal{G}$, there exists a $b_{R,S} \in B$ such that $(a, b_{R,S}) \in R$ and $(b_{R,S}, c) \in S$. We need to show that $(a,c) \in \left(\bigcap \mathcal{G}\right) \circ \left(\bigcap \mathcal{F}\right)$, that is, there exists a $b \in B$ such that for all $R \in \mathcal{F}$, $(a,b) \in R$, and for all $S \in \mathcal{G}$, $(b,c) \in S$. Note the order of quantification: our assumption produces an intermediate $b_{R,S}$ for any choices of S and R (and the $b_{R,S}$s may be different depending on the choice), while the goal asks for a single $b \in B$ that acts as an intermediate for every relation in $\mathcal{F}$ and $\mathcal{G}$. Since we won't be able to find such a single b in general, this direction cannot hold. Abstractly, we only have the implication $\exists x.\ \forall y.\ P(x,y) \Longrightarrow \forall y.\ \exists x.\ P(x,y)$ but not the other direction; this was not an issue with union since existentials can be swapped.

3. Suppose R is a relation on a set A. Prove that
   a) R is reflexive iff $\mathrm{id}_A \subseteq R$
   b) R is symmetric iff $R = R^{\mathrm{op}}$
   c) R is transitive iff $R \circ R \subseteq R$
   d) R is antisymmetric iff $R \cap R^{\mathrm{op}} \subseteq \mathrm{id}_A$
4. Let R be an arbitrary relation on a set A, for example, representing an undirected graph. We are interested in constructing the smallest transitive relation (graph) containing R, called the

transitive closure of R.

a) We define the family of relations which are transitive supersets of R:

$$\mathcal{T}_R \triangleq \{ Q : A \rightarrow\!\!\!\!\!\!\rightarrow A \mid R \subseteq Q \text{ and } Q \text{ is transitive} \}$$

R is not necessarily going to be an element of this family, as it might not be transitive. However, R is a *lower bound* for $\mathcal{T}_R$, as it is a subset of every element of the family.

Prove that the set $\bigcap \mathcal{T}_R$ is the transitive closure for R.

> We need to prove that $\bigcap \mathcal{T}_R$ is the ③ smallest ② transitive relation ① containing R.
>
> ① By the UP of intersections, $R \subseteq \bigcap \mathcal{T}_R$ holds iff $R \subseteq Q$ for all $Q \in \mathcal{T}_R$; but by definition of $\mathcal{T}_R$ we have that R must be a subset of all its elements.
>
> ② To show that $\bigcap \mathcal{T}_R$ is transitive, it is sufficient to show that $\bigcap \mathcal{T}_R \circ \bigcap \mathcal{T}_R \subseteq \bigcap \mathcal{T}_R$ by §6.2.3. By the UP of intersections (similar to §6.2.2), $\bigcap \mathcal{T}_R \circ \bigcap \mathcal{T}_R \subseteq \bigcap \{ Q \circ Q \mid Q \in \mathcal{T}_R \}$, but since all $Q \in \mathcal{T}_R$ are transitive, $Q \circ Q \subseteq Q$ and thus $\bigcap \{ Q \circ Q \mid Q \in \mathcal{T}_R \} \subseteq \bigcap \{ Q \mid Q \in \mathcal{T}_R \} = \bigcap \mathcal{T}_R$.
>
> ③ To show that $\bigcap \mathcal{T}_R$ is the smallest transitive superset of R, we let S be a transitive relation with $R \subseteq S$ and prove that $\bigcap \mathcal{T}_R \subseteq S$. Since S is transitive and $R \subseteq S$, it must also be an element of T_R, and by the UP of intersections, $\bigcap \mathcal{T}_R$ is a subset of every element of T_R, in particular S.

b) $\bigcap \mathcal{T}_R$ is the intersection of an infinite number of relations so it's difficult to compute the transitive closure this way. A better approach is to start with R, and keep adding the missing connections until we get a transitive graph. This can be done by repeatedly composing R with itself: after n compositions, all paths of length n in the graph represented by R will have a transitive connection between their endpoints.

Prove that the (at least once) iterated composition $R^{\circ+} \triangleq R \circ R^{\circ*}$ is the transitive closure for R, i.e. it coincides with the greatest lower bound of $\mathcal{T}_R$: $R^{\circ+} = \bigcap \mathcal{T}_R$. *Hint*: show that $R^{\circ+}$ is both an element and a lower bound of $\mathcal{T}_R$.

> By the definition of $R^{\circ*}$ and §6.2.2 (with $\mathcal{F} = \left\{ R^{\circ k} \mid k \in \mathbb{N} \right\}$ and $\mathcal{G} = \{ R \}$), we have that
>
> $$R^{\circ+} = R \circ R^{\circ*} = R \circ \bigcup \left\{ R^{\circ k} \mid k \in \mathbb{N} \right\} = \bigcup \left\{ R \circ R^{\circ k} \mid k \in \mathbb{N} \right\} = \bigcup_{n \in \mathbb{N}^+} R^{\circ n}$$
>
> where $\mathbb{N}^+$ is the set of positive natural numbers. Again, we show that $\bigcup_{n \in \mathbb{N}^+} R^{\circ n}$ is the ③ smallest ② transitive relation ① containing R, where ① and ② amounts to proving that $R^{\circ+} \in \mathcal{T}_R$ and ③ that it is a lower bound of $\mathcal{T}_R$.
>
> ① We have that $R \subseteq \bigcup_{n \in \mathbb{N}^+} R^{\circ n}$ since $R = R^{\circ 1}$ is an element of the indexed family and big unions are upper bounds.
>
> ② To show that $R^{\circ+}$ it is transitive, it is sufficient to show that $R^{\circ+} \circ R^{\circ+} \subseteq R^{\circ+}$. By

§6.2.2, we have the following:

$$R^{\circ+} \circ R^{\circ+} = \left(\bigcup_{n\in\mathbb{N}^+} R^{\circ n} \right) \circ \left(\bigcup_{m\in\mathbb{N}^+} R^{\circ m} \right) = \bigcup_{n\in\mathbb{N}^+} \bigcup_{m\in\mathbb{N}^+} R^{\circ n} \circ R^{\circ m}$$

To proceed, we prove the following lemma: for all $k, l \in \mathbb{N}$, $R^{\circ k} \circ R^{\circ l} = R^{\circ(k+l)}$.

Base case: $k = 0$. Then, $R^{\circ 0} \circ R^{\circ l} = \mathrm{id}_A \circ R^{\circ l} = R^{\circ(0+l)}$ since the identity relation is a left unit for composition.

Inductive step: $k+1$. Assume the ⒾⒽ: $R^{\circ k} \circ R^{\circ l} = R^{\circ(k+l)}$. By definition of iterated composition, $R^{\circ(k+1)} \circ R^{\circ l} = \left(R \circ R^{\circ k}\right) \circ R^{\circ l}$, but since relational composition is associative, this equals $R \circ \left(R^{\circ k} \circ R^{\circ l}\right)$ which, by the ⒾⒽ, is $R \circ R^{\circ(k+l)} = R^{\circ((k+1)+l)}$, as required.

By this lemma, $\bigcup_{n\in\mathbb{N}^+} \bigcup_{m\in\mathbb{N}^+} R^{\circ n} \circ R^{\circ m} = \bigcup_{n\in\mathbb{N}^+} \bigcup_{m\in\mathbb{N}^+} R^{\circ(n+m)}$. Now, to show that $\bigcup_{n\in\mathbb{N}^+} \bigcup_{m\in\mathbb{N}^+} R^{\circ(n+m)} \subseteq R^{\circ+}$, we can use the UP of big unions twice and equivalently establish

$$\forall n \in \mathbb{N}^+.\ \forall m \in \mathbb{N}^+.\ R^{\circ(n+m)} \subseteq R^{\circ+}$$

but this is the case because $R^{\circ(n+m)} \in \left\{ R^{\circ k} \,\middle|\, k \in \mathbb{N}^+ \right\}$ and big unions are upper bounds. Thus, we have shown that $R^{\circ+} \circ R^{\circ+} \subseteq R^{\circ+}$, and by §6.2.3, it is transitive.

③ We need to show that $R^{\circ+}$ is the smallest such relation, i.e. it is a lower bound of $\mathcal{T}_R$. By the UP of unions, we equivalently have

$$\bigcup_{n\in\mathbb{N}^+} R^{\circ n} \subseteq \bigcap \mathcal{T}_R \iff \forall n \in \mathbb{N}^+.\ \forall Q \in \mathcal{T}_R.\ R^{\circ n} \subseteq Q$$

The latter statement can be proved by induction on n.

Base case: $n = 1$. We need to show that for all $Q \in \mathcal{T}_R$, $R^{\circ 1} = R \subseteq Q$; but this is the case since $R \subseteq Q$ by the definition of $\mathcal{T}_R$.

Inductive step: $n = k+1$. Assume the ⒾⒽ: $\forall Q \in \mathcal{T}_R.\ R^{\circ k} \subseteq Q$. We need to prove that $\forall Q \in \mathcal{T}_R.\ R^{\circ(k+1)} \subseteq Q$. Let $Q \in \mathcal{T}_R$ be such a relation, and show that $R^{\circ(k+1)} = R \circ R^{\circ k} \subseteq Q$. By the induction hypothesis, $R^{\circ k} \subseteq Q$ and $R \subseteq Q$ by assumption on Q, so §6.2.1 implies that

$$R \circ R^{\circ k} \subseteq Q \circ Q \subseteq Q$$

where the last step follows from the fact that Q is transitive. Thus, $R^{\circ(k+1)} \subseteq Q$. By the principle of mathematical induction, we have that $\forall n \in \mathbb{N}^+.\ R^{\circ n} \subseteq Q$ for all $Q \in \mathcal{T}_R$, so $R^{\circ+}$ is indeed a lower bound of $\mathcal{T}_R$.

Putting everything together, we have that $R^{\circ+}$ is the transitive closure of R, as required.

$\boxed{♪}$ A rather involved proof with many distinct steps, references to established properties and several proof techniques. Notice, however, that at no point did we have to reason about elements of the relations: we got to the end without ever having to say “take $(a, a') \in R^{\circ+}$”, for example. It would have been possible to get a low-level

> proof like this, but expanding all definitions and resorting to purely logical reasoning is often lengthier and more error-prone. Gaining the fluency to work with universal properties and recognising common patterns (sufficient conditions for transitivity, operand-wise application of subsets in composition, etc.) is a worthwhile, time-saving skill to learn for discrete mathematics and other mathematical subjects.

7. On partial functions

7.1. Basic exercises

1. Let $A_2 = \{1, 2\}$ and $A_3 = \{a, b, c\}$. List the elements of the sets $\mathrm{PFun}(A_i, A_j)$ for $i, j \in \{2, 3\}$.
2. Prove that a relation $R\colon A \nrightarrow B$ is a partial function iff $R \circ R^{\mathrm{op}} \subseteq \mathrm{id}_B$.
3. Prove that the identity relation is a partial function, and that the composition of partial functions is a partial function.

7.2. Core exercises

1. Show that $(\mathrm{PFun}(A, B), \subseteq)$ is a partial order. What is its least element, if it exists?
2. Let $\mathcal{F} \subseteq \mathrm{PFun}(A, B)$ be a non-empty collection of partial functions from A to B.
   a) Show that $\bigcap \mathcal{F}$ is a partial function.
   b) Show that $\bigcup \mathcal{F}$ need not be a partial function by defining two partial functions $f, g : A \rightharpoonup B$ such that $f \cup g : A \nrightarrow B$ is a non-functional relation.
   c) Let $h\colon A \rightharpoonup B$ be a partial function. Show that if every element of $\mathcal{F}$ is below h then $\bigcup \mathcal{F}$ is a partial function.

8. On functions

8.1. Basic exercises

1. Let $A_2 = \{1, 2\}$ and $A_3 = \{a, b, c\}$. List the elements of the sets $\mathrm{Fun}(A_i, A_j)$ for $i, j \in \{2, 3\}$.
2. Prove that the identity partial function is a function, and the composition of functions yields a function.
3. Prove or disprove that $(\mathrm{Fun}(A, B), \subseteq)$ is a partial order.
4. Find endofunctions $f, g : A \to A$ such that $f \circ g \neq g \circ f$.

8.2. Core exercises

1. A relation $R\colon A \nrightarrow B$ is said to be *total* if $\forall a \in A.\ \exists b \in B.\ a\,R\,b$. Prove that this is equivalent to $\mathrm{id}_A \subseteq R^{\mathrm{op}} \circ R$. Conclude that a relation $R\colon A \nrightarrow B$ is a function iff $R \circ R^{\mathrm{op}} \subseteq \mathrm{id}_B$ and $\mathrm{id}_A \subseteq R^{\mathrm{op}} \circ R$.
2. Let $\chi : \mathcal{P}(U) \to (U \Rightarrow [2])$ be the function mapping subsets $S \subseteq U$ to their characteristic functions $\chi_S : U \to [2]$.
   a) Prove that for all $x \in U$,
      - $\chi_{A \cup B}(x) = (\chi_A(x) \vee \chi_B(x)) = \max(\chi_A(x), \chi_B(x))$
      - $\chi_{A \cap B}(x) = (\chi_A(x) \wedge \chi_B(x)) = \min(\chi_A(x), \chi_B(x))$
      - $\chi_{A^{\mathrm{c}}}(x) = \neg(\chi_A(x)) = (1 - \chi_A(x))$

b) For what construction $A?B$ on sets A and B does it hold that

$$\chi_{A?B}(x) = (\chi_A(x) \oplus \chi_B(x)) = (\chi_A(x) +_2 \chi_B(x))$$

for all $x \in U$, where $\oplus$ is the *exclusive or* operator? Prove your claim.

8.3. Optional advanced exercises

Consider a set A together with an element $a \in A$ and an endofunction $f : A \to A$. \ Say that a relation $R \colon \mathbb{N} \nrightarrow A$ is (a, f)-*closed* whenever

$$R(0,a) \quad \text{and} \quad \forall n \in \mathbb{N}, x \in A.\ R(n,x) \Longrightarrow R(n+1, f(x))$$

Define the relation $F : \mathbb{N} \nrightarrow A$ as

$$F \triangleq \bigcap \{ R \colon \mathbb{N} \nrightarrow A \mid R \text{ is } (a,f)\text{-closed} \}$$

a) Prove that F is (a, f)-closed.
b) Prove that F is total, that is: $\forall n \in \mathbb{N}.\ \exists y \in A.\ F(n, y)$.
c) Prove that F is a function $\mathbb{N} \to A$, that is: $\forall n \in \mathbb{N}.\ \exists! y \in A. F(n, y)$. \ *Hint*: Proceed by induction. Observe that, in view of the previous item, to show that $\exists! y \in A. F(k, y)$ it suffices to exhibit an (a, f)-closed relation R_k such that $\exists! y \in A. R_k(k, y)$. (Why?) For instance, as the relation $R_0 = \{(m, y) \in \mathbb{N} \times A \mid m = 0 \Longrightarrow y = a\}$ is (a, f)-closed one has that $F(0, y) \Longrightarrow R_0(0, y) \Longrightarrow y = a$.
d) Show that if h is a function $\mathbb{N} \to A$ with $h(0) = a$ and $\forall n \in \mathbb{N}.\ h(n+1) = f(h(n))$ then $h = F$.

Thus, for every set A together with an element $a \in A$ and an endofunction $f : A \to A$ there exists a unique function $F : \mathbb{N} \to A$, typically said to be *inductively defined*, satisfying the recurrence relation

$$F(n) = \begin{cases} a & \text{for } n = 0 \\ f(F(n-1)) & \text{for } n \geq 1 \end{cases}$$