Discrete Mathematics

Exercises 6 – Solutions with Commentary

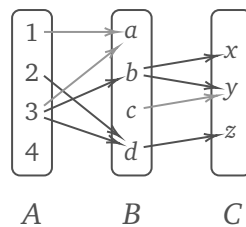Marcelo Fiore   Ohad Kammar   Dima Szamozvancev

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 $S \circ R : A \nrightarrow C$?

$$A \qquad B \qquad C$$

   The composite $S \circ R$ is the relation $\{(2, z), (3, x), (3, y), (3, z)\}$.

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

   Let $R : A \nrightarrow B$, $S : B \nrightarrow C$, and $T : C \nrightarrow D$ be three relations. We show that their composition is associative: $T \circ (S \circ R) = (T \circ R) \circ R$. Take a pair $(a, d) \in T \circ (S \circ R)$; by the definition of relational composition, there must be a $c \in C$ such that $(a, c) \in S \circ R$ and $c \, T \, d$; expanding the former, there must be a $b \in B$ such that $a \, R \, b$ and $b \, S \, c$. But then $(b, d) \in T \circ S$ via c, and $(a, d) \in (T \circ S) \circ R$ via b. The converse proof follows analogously from the definition, so we conclude that relational composition is associative.

   Let $R : A \nrightarrow B$ be a relation. We show that $\mathrm{id}_B \circ R = R = R \circ \mathrm{id}_A$. Take a pair $(a, b) \in \mathrm{id}_B \circ R$; there must exist a $b' \in B$ such that $a \, R \, b'$ and $b' \, \mathrm{id}_B \, b$, but since the identity relation is the equality, we have that $b' = b$ and therefore $(a, b) \in R$. Conversely, to show that $(a, b) \in R$ is also in $\mathrm{id}_B \circ R$, we observe that b can be used as the intermediate step in showing that $(a, b) \in R$ and $(b, b) \in \mathrm{id}_B$. The right inverse proof is analogous, so we conclude that the identity relation is the two-sided unit of relational composition.

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) $R \subseteq S \implies R^{\mathrm{op}} \subseteq S^{\mathrm{op}}$

Assume $R \subseteq S$ and show that for all $b\,R^{\text{op}}\,a$, $b\,S^{\text{op}}\,a$. By the definition of opposite relations, $b\,R^{\text{op}}\,a$ if $a\,R\,b$, but by assumption, $a\,S\,b$ and thus $b\,S^{\text{op}}\,a$, as required.

b) $(R \cap S)^{\text{op}} = R^{\text{op}} \cap S^{\text{op}}$

By the previous part and UP of intersections, we have that $(R \cap S)^{\text{op}} \subseteq R^{\text{op}}$ and $(R \cap S)^{\text{op}} \subseteq S^{\text{op}}$, so $(R \cap S)^{\text{op}} \subseteq R^{\text{op}} \cap S^{\text{op}}$. Conversely, take a pair (b, a) in R^{op} and S^{op}; then, (a, b) is both in R and S so it is in the intersection and $(b, a) \in (R \cap S)^{\text{op}}$.

c) $(R \cup S)^{\text{op}} = R^{\text{op}} \cup S^{\text{op}}$

For $(b, a) \in (R \cup S)^{\text{op}}$, we calculate as follows:

$$
\begin{aligned}
(b, a) \in (R \cup S)^{\text{op}} &\iff (a, b) \in (R \cup S) \\
&\iff (a\,R\,b \ \lor\ a\,S\,b) \\
&\iff (b\,R^{\text{op}}\,a \ \lor\ b\,S^{\text{op}}\,a) \\
&\iff (b, a) \in R^{\text{op}} \cup S^{\text{op}}
\end{aligned}
$$

d) $(T \circ S)^{\text{op}} = S^{\text{op}} \circ T^{\text{op}}$

We calculate as follows:

$$
\begin{aligned}
(T \circ S)^{\text{op}} &= \{\, (c, a) \mid (c, a) \in (T \circ S)^{\text{op}} \,\} \\
&= \{\, (c, a) \mid (a, c) \in T \circ S \,\} \\
&= \{\, (c, a) \mid \exists b \in B.\ a\,S\,b \ \land\ b\,T\,c \,\} \\
&= \{\, (c, a) \mid \exists b \in B.\ b\,S^{\text{op}}\,a \ \land\ c\,T^{\text{op}}\,b \,\} \\
&= \{\, (c, a) \mid (c, a) \in S^{\text{op}} \circ T^{\text{op}} \,\} = S^{\text{op}} \circ T^{\text{op}}
\end{aligned}
$$

As before, these questions concern the equality of sets which can be established in several ways; three possibilities (universal properties, bi-implication reasoning and set comprehension reasoning) are demonstrated here.

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 $a\,R\,b$ and $b\,S\,c$. 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 $a \, R \, b$ for some $R \in \mathcal{F}$ and $b \, S \, c$ 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.

♪ 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 $R \in \mathcal{F}$, $a \, R \, b$, and for all $S \in \mathcal{G}$, $b \, S \, c$. 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 $\mathrm{id}_A \subseteq R$

R is reflexive iff for all $a \in A$, $a\,R\,a$. Equivalently, for all $a, a' \in A$, if $a = a'$ then $a\,R\,a'$. Since the identity relation is equality, this is equivalent to id_A being a subset of R.

b) R is symmetric iff $R = R^{\mathrm{op}}$

R is symmetric iff for all $a, b \in A$, if $a\,R\,b$ then $b\,R\,a$. Equivalently, we can express this as $a\,R\,b$ implying $a\,R^{\mathrm{op}}\,b$, or $b\,R^{\mathrm{op}}\,a$ implying $b\,R\,a$. These conditions in turn say that $R \subseteq R^{\mathrm{op}}$ and $R^{\mathrm{op}} \subseteq R$, so $R = R^{\mathrm{op}}$ is equivalent to R being symmetric.

c) R is transitive iff $R \circ R \subseteq R$

R is transitive iff for all $a, b, c \in A$, if $(a, b) \in R$ and $(b, c) \in R$ then $(a, c) \in R$. We first assume R is transitive and prove that $R \circ R \subseteq R$ by taking a pair $(a, c) \in R \circ R$. By the definition of relation composition, there exists a $b \in A$ such that $a\,R\,b$ and $b\,R\,c$, but R is transitive, so $a\,R\,c$. Conversely, assume $R \circ R \subseteq R$ and suppose $a\,R\,b$ and $b\,R\,c$ for three elements $a, b, c \in A$. Then, $(a, c) \in R \circ R$ via b, and by assumption, $a\,R\,c$, proving that R is transitive.

♪ The calculational proof of this property would depend on the equivalence

$$\forall a, c \in A. \, (\exists b \in A. \, a\,R\,b \,\wedge\, b\,R\,c) \Longrightarrow a\,R\,c$$
$$\Longleftrightarrow \quad \forall a, c \in A. \, \forall b \in A. \, (a\,R\,b \,\wedge\, b\,R\,c) \Longrightarrow a\,R\,c$$

which is precisely an instance of the equivalence of the formulae $(\exists x. \, P(x)) \Rightarrow Q$ and $\forall x. \, (P(x) \Rightarrow Q)$ way back from §1.3.2.

d) R is antisymmetric iff $R \cap R^{\mathrm{op}} \subseteq \mathrm{id}_A$

R is antisymmetric iff for all $a, b \in A$, $a\,R\,b$ and $b\,R\,a$ implies $a = b$. This is equivalent to the statement that $a\,R\,b$ and $a\,R^{\mathrm{op}}\,b$ implies $a = b$, that is, $(a, b) \in R \cap R^{\mathrm{op}}$ implies $(a, b) \in \mathrm{id}_A$. This, in turn, is equivalent to $R \cap R^{\mathrm{op}} \subseteq \mathrm{id}_A$.

♪ These are sufficient and necessary conditions for establishing properties of relations in terms of set-theoretic operators rather than element-wise proofs. As before, having the ability to reason without "going down to the level of elements" often results in more direct and elegant proofs that capture the algebraic nature of set-level calculations; in addition, not having to introduce a lot of new variable names for elements make such proofs less finicky and error-prone as well.

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:

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

   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 (IH): $R^{\circ k} \circ R^{\circ l} = R^{\circ(k+l)}$. 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 (IH), 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 $R^{\circ(n+m)} \in \left\{ R^{\circ k} \mid k \in \mathbb{N}^+ \right\}$ 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 (IH): $\forall Q \in \mathcal{T}_R.\ R^{\circ k} \subseteq Q$. 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.

♪ 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 $i, j \in \{2, 3\}$.
   Hint: there may be quite a few, so you can think of ways of characterising all of them without giving an explicit listing.

> $\mathrm{PFun}(A_2, A_2)$. We have 4 possible total functions: $\{(1,1),(2,1)\}$, $\{(1,1),(2,2)\}$, $\{(1,2),(2,1)\}$, $\{(1,2),(2,2)\}$. All singleton subsets of these are also partial functions, of which there are 4 more: $\{(1,1)\}$, $\{(1,2)\}$, $\{(2,1)\}$, $\{(2,2)\}$. Finally we have the totally undefined function $\{\}$, giving the expected number of $(2+1)^2 = 9$ of partial functions.
>
> $\mathrm{PFun}(A_2, A_3)$. We have 9 possible total functions: $\{\{(1,x),(2,y)\} \mid x, y \in A_3\}$. The singletons map 1 or 2 to any of a, b, c, so there are 6 of those: $\{\{(1,x)\} \mid x \in A_3\} \cup \{\{(2,y)\} \mid y \in A_3\}$. With $\{\}$, we have $16 = (3+1)^2$ partial functions, as expected.
>
> $\mathrm{PFun}(A_3, A_2)$. We have 8 possible total functions: $\{\{(a,x),(b,y),(c,z)\} \mid x, y, z \in A_2\}$. There are $3 \cdot 2 \cdot 2 = 12$ partial functions undefined at one argument (where the notation $\{A_i\}_{i \in I}$ for an indexed family of sets stands for $\{A_i \mid i \in I\}$):
>
> $$\{\{(a,x),(b,y)\}\}_{x,y \in A_2} \cup \{\{(a,x),(c,z)\}\}_{x,z \in A_2} \cup \{\{(b,y),(c,z)\}\}_{y,z \in A_2}$$
>
> There are $3 \cdot 2 = 6$ partial functions undefined at two arguments:
>
> $$\{\{(a,x)\}\}_{x \in A_2} \cup \{\{(b,y)\}\}_{y \in A_2} \cup \{\{(c,z)\}\}_{z \in A_2}$$
>
> With $\{\}$, we have $27 = (2+1)^3$ partial functions, as expected.
>
> $\mathrm{PFun}(A_3, A_3)$. We have 27 possible total functions: $\{\{(a,x),(b,y),(c,z)\} \mid x, y, z \in A_3\}$. There are $3 \cdot 3 \cdot 3 = 27$ partial functions undefined at one argument:
>
> $$\{\{(a,x),(b,y)\}\}_{x,y \in A_3} \cup \{\{(a,x),(c,z)\}\}_{x,z \in A_3} \cup \{\{(b,y),(c,z)\}\}_{y,z \in A_3}$$
>
> There are $3 \cdot 3 = 9$ partial functions undefined at two arguments:
>
> $$\{\{(a,x)\}\}_{x \in A_3} \cup \{\{(b,y)\}\}_{y \in A_3} \cup \{\{(c,z)\}\}_{z \in A_3}$$
>
> With $\{\}$, we have $64 = (3+1)^3$ partial functions, as expected.

2. Prove that a relation $R: A \nrightarrow B$ is a partial function iff $R \circ R^{\mathrm{op}} \subseteq \mathrm{id}_B$.

> ($\Rightarrow$) Assume $R: A \nrightarrow B$ is a partial function: that is, for all $a \in A$ and $b_1, b_2 \in B$, if $a \, R \, b_1$ and $a \, R \, b_2$ then $b_1 = b_2$. We need to show that if $(b_1, b_2) \in R \circ R^{\mathrm{op}}$, $b_1 = b_2$. By the definition of relational composition and the opposite relation, there exists a $a \in A$ such that $a \, R \, b_1$ and $a \, R \, b_2$; but since R is functional, $b_1 = b_2$.
>
> ($\Leftarrow$) Assume $R \circ R^{\mathrm{op}} \subseteq \mathrm{id}_B$ and take $a \in A$, $b_1, b_2 \in B$ with $a \, R \, b_1$ and $a \, R \, b_2$. Then, $b_1 \, R^{\mathrm{op}} \, a$ and therefore $(b_1, b_2) \in R \circ R^{\mathrm{op}}$ through a. By assumption, this implies that $b_1 = b_2$, as required.

3. Prove that the identity relation is a partial function, and that the composition of partial functions is a partial function.

> We show that for all $a, a_1, a_2 \in A$, if $a \operatorname{id}_A a_1$ and $a \operatorname{id}_A a_2$, $a_1 = a_2$. Since id_A is the equality relation, we haven that $a = a_1$ and $a = a_2$, so $a_1 = a_2$.
>
> Let $f : A \rightharpoonup B$ and $g : B \rightharpoonup C$ be two partial functions. To show that $g \circ f$ is a partial function, it is sufficient to show that $(g \circ f) \circ (g \circ f)^{\mathrm{op}} \subseteq \operatorname{id}_C$ (§7.1.2). By §6.1.3(d), we have that $(g \circ f) \circ (g \circ f)^{\mathrm{op}} = g \circ f \circ f^{\mathrm{op}} \circ g^{\mathrm{op}}$. Since f is a partial function, $f \circ f^{\mathrm{op}} \subseteq \operatorname{id}_B$ and $g \circ g^{\mathrm{op}} \subseteq \operatorname{id}_C$; thus, by §6.2.1, we have:
>
> $$g \circ (f \circ f^{\mathrm{op}}) \circ g^{\mathrm{op}} \subseteq g \circ \operatorname{id}_A \circ g^{\mathrm{op}} = g \circ g^{\mathrm{op}} \subseteq \operatorname{id}_C .$$
>
> ♪ We could of course prove the latter by unwrapping the definition of partial functions and composition, or doing case analysis on when the functions are defined. But approaching it via a sufficient condition is quite neat too!

7.2. Core exercises

1. Show that $(\mathrm{PFun}(A, B), \subseteq)$ is a partial order. What is its least element, if it exists?

> Any subset of a partial function is itself a partial function, since it may be defined on fewer elements of the domain, but functionality is not violated. The set of partial functions between two sets therefore has the standard subset ordering $f \subseteq g$ which is reflexive, transitive and antisymmetric as shown in §5.1.1. The least element is the empty set seen as the totally undefined partial function from A to B.

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.

   > By §7.1.2, it is sufficient to show that $\left(\bigcap \mathcal{F}\right) \circ \left(\bigcap \mathcal{F}\right)^{\mathrm{op}} \subseteq \operatorname{id}_B$. We calculate as follows:
   >
   > $$\begin{aligned} \left(\bigcap \mathcal{F}\right) \circ \left(\bigcap \mathcal{F}\right)^{\mathrm{op}} &= \left(\bigcap \mathcal{F}\right) \circ \left(\bigcap \{F^{\mathrm{op}} \mid F \in \mathcal{F}\}\right) & \text{(by §6.1.3(b))} \\ &\subseteq \bigcap \{F \circ F^{\mathrm{op}} \mid F \in \mathcal{F}\} & \text{(by UP of intersections)} \\ &\subseteq \bigcap \{\operatorname{id}_B \mid F \in \mathcal{F}\} = \operatorname{id}_B & \text{(by §7.1.2 and assumption)} \end{aligned}$$

   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.

   > We can simply have $f = \{(1, a)\}$ and $g = \{(1, b)\}$ for $A = \{1\}$ and $B = \{a, b\}$. Both are partial (in fact total) functions, but the union $\{(1, a), (1, b)\}$ maps 1 to both a and b, violating functionality.

   c) Let $h : A \rightharpoonup B$ be a partial function. Show that if every element of $\mathcal{F}$ is below h then $\bigcup \mathcal{F}$ is a partial function.

If for all $f \in \mathcal{F}$, $f \subseteq h$, then h is an upper bound of $\mathcal{F}$ and therefore we have $\bigcup \mathcal{F} \subseteq h$. But subsets of partial functions are themselves partial functions, since they cannot have more mappings from any particular element of A than h.

♪ You may wonder why the high-level proof we used for intersections doesn't work for unions. The issue is that the UP of unions only allows the inclusion

$$\bigcup \{ \mathcal{F} \circ \mathcal{F}^{\mathrm{op}} \mid F \in \mathcal{F} \} \subseteq \left(\bigcup \mathcal{F} \right) \circ \left(\bigcup \{ F^{\mathrm{op}} \mid F \in \mathcal{F} \} \right)$$

and while a seemingly more general property

$$\bigcup \{ F \circ F' \mid F, F' \in \mathcal{F} \} = \left(\bigcup \mathcal{F} \right) \circ \left(\bigcup \mathcal{F} \right)$$

holds in both directions (see §6.2.2), the F and F' are independent (since they come from two existential assumptions) and F' cannot be specialised to F^{op}.

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 $i, j \in \{ 2, 3 \}$.

The total functions have already been listed amongst the partial functions in §7.1.1:

$$\mathrm{Fun}(A_2, A_2) = \{ \{ (1, x), (2, y) \} \mid x, y \in A_2 \}$$
$$\mathrm{Fun}(A_2, A_2) = \{ \{ (1, x), (2, y) \} \mid x, y \in A_3 \}$$
$$\mathrm{Fun}(A_3, A_2) = \{ \{ (a, x), (b, y), (c, z) \} \mid x, y, z \in A_2 \}$$
$$\mathrm{Fun}(A_3, A_3) = \{ \{ (a, x), (b, y), (c, z) \} \mid x, y, z \in A_3 \}$$

2. Prove that the identity partial function is a function, and the composition of functions yields a function.

We need to show that for all $a \in A$ there exists a unique $a' \in A$ such that $\mathrm{id}_A(a) = a'$. Of course, a is the witness of the existence, and it is unique since sets have no duplicate elements.

Let $f : A \to B$ and $g : B \to C$ be functions. We show that the composite $g \circ f$ is also a function, that is, for all $a \in A$, there exists a unique $c \in C$ such that $(g \circ f)(a) = c$. By the definition of function composition, $(g \circ f)(a) = g(f(a))$, where $f(a) = b$ for a unique $b \in B$ and $g(b) = c$ for a unique $c \in C$. Thus, a unique c does exist, and $g \circ f$ is a function.

3. Prove or disprove that $(\mathrm{Fun}(A, B), \subseteq)$ is a partial order.

Unlike partial functions, functions are not closed under taking subsets or supersets: the number of mappings (i.e. the graph) of a function must be equal to the size of the domain (or, more precisely, isomorphic), so we can't add or remove mappings without breaking functionality or totality. We may be tempted to conclude that $(\mathrm{Fun}(A, B), \subseteq)$ is not a partial

order, but we should remember that there is still an ordering on the set even if different functions can't be compared: $f \subseteq g$ if and only if $f = g$. Thus, the subset ordering on functions simply restricts to equality, which is trivially a partial order: we have reflexivity since $f \subseteq f$, and antisymmetry and transitivity hold because the hypotheses like $f \subseteq g$ and $g \subseteq h$ simply become $f = g = h$.

4. Find endofunctions $f, g : A \to A$ such that $f \circ g \neq g \circ f$.

Let $f : \mathbb{N} \to \mathbb{N}$ be the successor function $n \mapsto n+1$, and $g : \mathbb{N} \to \mathbb{N}$ be the squaring function $m \mapsto m^2$. Then, for all n, $(g \circ f)(n) = (n+1)^2 = n^2 + 2n + 1$, but $(f \circ g)(n) = n^2 + 1$.

♪ Many other examples exist of course. This is merely a reminder that function composition (and relational composition in general) is not commutative, and it doesn't have many other properties that we tend to expect from binary operators: for example, $f \circ g = f \circ h$ does not imply $g = h$ in general.

8.2. Core exercises

1. A relation $R : A \nrightarrow B$ is said to be *total* if $\forall a \in A. \exists b \in B. \, a \, R \, b$. Prove that this is equivalent to $\text{id}_A \subseteq R^{\text{op}} \circ R$. Conclude that a relation $R : A \nrightarrow B$ is a function iff $R \circ R^{\text{op}} \subseteq \text{id}_B$ and $\text{id}_A \subseteq R^{\text{op}} \circ R$.

($\Rightarrow$) Assume that $R : A \nrightarrow B$ is a total relation, that is, for all $a \in A$ there exists a $b \in B$ such that $a \, R \, b$. We need to show that for all $(a, a') \in \text{id}_A$, $(a, a') \in R^{\text{op}} \circ R$ – that is, that $R^{\text{op}} \circ R$ is reflexive. A pair (a, a) for $a \in A$ is in $R^{\text{op}} \circ R$ if there exists a $b \in B$ such that $a \, R \, b$ and $b \, R^{\text{op}} \, a$, i.e. $a \, R \, b$, which is satisfied if there exists a $b \in B$ such that $a \, R \, b$. But this follows from the assumption that R is total.

($\Leftarrow$) Assume that $R^{\text{op}} \circ R$ is reflexive and show that R is total. Take $a \in A$; as $R^{\text{op}} \circ R$ is reflexive, $(a, a) \in R^{\text{op}} \circ R$, so there exists a $b \in B$ such that $a \, R \, b$. Taking this b as the witness of existence, we conclude that R is a total relation.

A total function is both a total relation and a partial function, so a relation R is total if and only if it satisfies both $\text{id}_A \subseteq R^{\text{op}} \circ R$ (from above) and $R \circ R^{\text{op}} \subseteq \text{id}_B$ (from §7.1.2).

♪ This question establishes that partial functions are in some sense dual to total relations: instead of asking for uniqueness (functionality), they require an existence (totality). Consequently, we can dualise several results from the previous section. For example, we have that the union of total relations is total, but the intersection is not, with the proofs being the duals of the arguments in §7.2.2 (and the proof attempt for intersections failing because their universal property is the "wrong way around").

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 $x \in U$,

   • $\chi_{A \cup B}(x) = (\chi_A(x) \lor \chi_B(x)) = \max(\chi_A(x), \chi_B(x))$

Let $x \in U$. Then,

$$\chi_{A \cup B}(x) \iff x \in (A \cup B) \iff (x \in A) \vee (x \in B) \iff (\chi_A(x) \vee \chi_B(x))$$

and the latter holds iff $\chi_A(x) = 1$ or $\chi_B(x) = 1$, so $\max(\chi_A(x), \chi_B(x)) = 1$.

- $\chi_{A \cap B}(x) = (\chi_A(x) \wedge \chi_B(x)) = \min(\chi_A(x), \chi_B(x))$

  Let $x \in U$. Then,

  $$\chi_{A \cap B}(x) \iff x \in (A \cap B) \iff (x \in A) \wedge (x \in B) \iff (\chi_A(x) \wedge \chi_B(x))$$

  and the latter holds iff $\chi_A(x) = 1$ and $\chi_B(x) = 1$, so $\min(\chi_A(x), \chi_B(x)) = 1$.

- $\chi_{A^c}(x) = \neg(\chi_A(x)) = (1 - \chi_A(x))$

  Let $x \in U$. Then,

  $$\chi_{A^c}(x) \iff x \notin A \iff \neg(x \in A) \iff \neg(\chi_A(x))$$

  and the latter holds iff $\chi_A(x) = 0$, so $1 - \chi_A(x) = 1$.

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.

The element x must be exactly in one of A or B, not their intersection. This leads to the definition

$$A?B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$$

which is known as the *symmetric difference* and written $A \triangle B$. Then, for $x \in U$,

$$
\begin{aligned}
\chi_{A \triangle B}(x) &\iff x \in (A \triangle B) \\
&\iff (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A) \\
&\iff (\chi_A(x) \wedge \neg\chi_B(x)) \vee (\chi_B(x) \wedge \neg\chi_A(x)) \\
&\iff \chi_A(x) \oplus \chi_B(x)
\end{aligned}
$$

and the latter doesn't hold iff $\chi_A(x) = \chi_B(x) = 0$ or $\chi_A(x) = \chi_B(x) = 1$. Adding $\chi_A(x)$ and $\chi_B(x)$ can give the values of 0, 1 or 2, but we only want the case where the sum is 1 and use the addition modulo 2 to route the other possibilities to 0.

8.3. Optional advanced exercise

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

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

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

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

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 $R_0 = \{ (m, y) \in \mathbb{N} \times A \mid m = 0 \implies y = a \}$ is (a, f)-closed one has that $F(0, y) \implies R_0(0, y) \implies y = a$.

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

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