

Discrete Mathematics

Exercises 5 – Solutions with Commentary

Marcelo Fiore Ohad Kammar Dima Szamozvancev

5. On sets

5.1. Basic exercises

1. Prove that \subseteq is a partial order, that is, it is:

a) reflexive: \forall sets A . $A \subseteq A$

Let A be a set; we need to show that for all $x \in A$, x is in A , which follows immediately.

b) transitive: \forall sets A, B, C . $(A \subseteq B \wedge B \subseteq C) \implies A \subseteq C$

Let A, B, C be sets and $x \in A$ an element. We need to show that $x \in C$. Since $A \subseteq B$, $x \in B$; and since $B \subseteq C$, $x \in C$, as required.

c) antisymmetric: \forall sets A, B . $(A \subseteq B \wedge B \subseteq A) \iff A = B$

Let A, B be sets and suppose $A \subseteq B$ and $B \subseteq A$. Then, if $x \in A$ then $x \in B$, and conversely, if $x \in B$ then $x \in A$. That is, $x \in A$ if and only if $x \in B$, which implies that A and B are equal sets.

♪ Straightforward properties of the subset relation that follow from the fact that implication (in terms of which \subseteq is defined) is itself a partial order. The first two properties enable partial order reasoning to establish $A \subseteq B$ as a chain of subset relations starting at A and ending at B ; antisymmetry gives rise to a proof technique for showing that two sets are equal iff they are both subsets of each other.

2. Prove the following statements:

a) \forall sets A . $\emptyset \subseteq A$

Let A be a set. We need to show that every element of \emptyset is in A , but since there are no elements in \emptyset , this vacuously holds.

b) \forall sets A . $(\forall x. x \notin A) \iff A = \emptyset$

Let A be a set.

(\implies) Assume $\forall x. x \notin A$. We need to show that $A = \emptyset$, or equivalently, $\emptyset \subseteq A$ and $A \subseteq \emptyset$. The former holds by the previous property, and to show the latter, we need to prove that for all x , if x is in A then x is in \emptyset . But, by assumption, $x \notin A$, so the rest follows vacuously.

(\impliedby) Assume $A = \emptyset$ and x an element. We need to show that x is not in A . But A is the empty set, and by definition, it has no elements; therefore x is not in A .

♪ Properties like this are sometimes harder to prove than more complicated set-theoretic statements – they just seem *too obvious* to warrant or require a proof, and attempting one feels like circular reasoning. However, if something is obvious, it should have an accompanying formal proof built from first principles (otherwise we really can't call the property obvious)! The first part of this exercise used proof by “vacuous truth”, which is based on the logical principle that falsity implies anything. If we have an assumption which is false (such as that an element x is in the empty set), any conclusion could follow vacuously. A related principle is that every element in the empty set satisfies any property P : $\forall x \in \emptyset. P(x)$. The second part of the question could be established by simply saying that it follows from the defining property of the empty set.

3. Find the union, and intersection of:

a) $\{1, 2, 3, 4, 5\}$ and $\{-1, 1, 3, 5, 7\}$

Let $A = \{1, 2, 3, 4, 5\}$ and $B = \{-1, 1, 3, 5, 7\}$. Then:

$$A \cup B = \{-1, 1, 2, 3, 4, 5, 7\} \quad A \cap B = \{1, 3, 5\}$$

b) $\{x \in \mathbb{R} \mid x > 7\}$ and $\{x \in \mathbb{N} \mid x > 5\}$

Let $C = \{x \in \mathbb{R} \mid x > 7\}$ and $D = \{x \in \mathbb{N} \mid x > 5\}$. Then:

$$C \cup D = \{6\} \cup \{x \in \mathbb{R} \mid x \geq 7\} \quad C \cap D = \{x \in \mathbb{N} \mid x > 7\}$$

4. Find the Cartesian product and disjoint union of $\{1, 2, 3, 4, 5\}$ and $\{-1, 1, 3, 5, 7\}$.

Let $A = \{1, 2, 3, 4, 5\}$ and $B = \{-1, 1, 3, 5, 7\}$. Then:

$$\begin{aligned} A \times B = \{ & (1, -1), (1, 1), (1, 3), (1, 5), (1, 7), (2, -1), (2, 1), (2, 3), (2, 5), (2, 7), \\ & (3, -1), (3, 1), (3, 3), (3, 5), (3, 7), (4, -1), (4, 1), (4, 3), (4, 5), (4, 7), \\ & (5, -1), (5, 1), (5, 3), (5, 5), (5, 7) \} \end{aligned}$$

$$A \uplus B = \{(1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (2, -1), (2, 1), (2, 3), (2, 5), (2, 7)\}$$

5. Let $I = \{2, 3, 4, 5\}$ and for each $i \in I$, let $A_i = \{i, i + 1, i - 1, 2 \cdot i\}$.

a) List the elements of all sets A_i for $i \in I$.

$$A_2 = \{2, 3, 1, 4\} \quad A_3 = \{3, 4, 2, 6\} \quad A_4 = \{4, 5, 3, 8\} \quad A_5 = \{5, 6, 4, 10\}$$

b) Let $\{A_i \mid i \in I\}$ stand for $\{A_2, A_3, A_4, A_5\}$. Find $\bigcup\{A_i \mid i \in I\}$ and $\bigcap\{A_i \mid i \in I\}$.

$$\bigcup\{A_i \mid i \in I\} = \{1, 2, 3, 4, 5, 6, 8, 10\} \quad \bigcap\{A_i \mid i \in I\} = \{4\}$$

♪ The last three exercises are intended to make you comfortable with these important set-theoretic constructions through concrete examples – make sure you have a good intuition for them going forward.

6. Let U be a set. For all $A, B \in \mathcal{P}(U)$, prove that:

a) $A^c = B \iff (A \cup B = U \wedge A \cap B = \emptyset)$

(\Rightarrow) Let $A, B \in \mathcal{P}(U)$ be sets and assume $A^c = B$. We show that $A \cup B = U$ and $A \cap B = \emptyset$. By definition, $A \cup A^c = \{a \in U \mid a \in A \vee a \in A^c\} = \{x \in U \mid x \in A \vee x \notin A\} = \{x \in U \mid \top\} = U$, since every element of U is either in A or not in A . Dually, $A \cap A^c = \{x \in U \mid x \in A \wedge x \in A^c\} = \{x \in U \mid x \in A \wedge x \notin A\} = \{x \in U \mid \perp\} = \emptyset$, since no element can be both in A and not in A .

 This direction proves that $(\cdot)^c$ satisfies the complementation laws on [Slide 300](#).

(\Leftarrow) Let $A, B \in \mathcal{P}(U)$ be sets and assume $A \cup B = U$; that is, every $x \in U$ is in A or B . This is logically equivalent to

$$\forall x \in U. x \notin A \implies x \in B$$

so $A \cup B = U$ implies that $A^c \subseteq B$. Similarly, assume $A \cap B = \emptyset$; that is, for every $x \in U$, it is not the case that x is in both A and B . This is logically equivalent to

$$\forall x \in U. x \in B \implies x \notin A$$

so $A \cap B = \emptyset$ implies that $B \subseteq A^c$. By the antisymmetry of \subseteq , we conclude that $A^c = B$.

b) Double complement elimination: $(A^c)^c = A$

Presented are two different arguments.

(A) We reason using part (a): to show $(A^c)^c = A$, it is sufficient to show that $A^c \cup A = U$ and $A^c \cap A = \emptyset$. Both of these follow from the complementation laws and the commutativity of union and intersection.

(B) We can prove the equality of the sets directly via equational reasoning.

$$\begin{aligned} (A^c)^c &= \{x \in U \mid \neg(x \in A^c)\} \\ &= \{x \in U \mid \neg(x \in \{y \in U \mid y \notin A\})\} \\ &= \{x \in U \mid \neg(x \notin A)\} \\ &= \{x \in U \mid x \in A\} && \text{(double negation elimination)} \\ &= A \end{aligned}$$

 This self-inverse property of complementation (and negation) is called *involution*.

c) The de Morgan laws: $(A \cup B)^c = A^c \cap B^c$ and $(A \cap B)^c = A^c \cup B^c$

Presented are two different arguments.

(A) We reason using part (a). To show the de Morgan law $(A \cup B)^c = A^c \cap B^c$, it is enough to show that

$$(A \cup B) \cup (A^c \cap B^c) = U \quad \text{and} \quad (A \cup B) \cap (A^c \cap B^c) = \emptyset$$

We calculate as follows:

$$\begin{aligned}
 & (A \cup B) \cup (A^c \cap B^c) \\
 &= ((A \cup B) \cup A^c) \cap ((A \cup B) \cup B^c) && (\cup \text{ distributes over } \cap) \\
 &= (B \cup (A \cup A^c)) \cap (A \cup (B \cup B^c)) && (\text{commutativity and associativity of } \cup) \\
 &= (B \cup U) \cap (A \cup U) && (\text{complementation laws}) \\
 &= U \cap U && (U \text{ annihilates } \cup) \\
 &= U && (\text{idempotence of } \cap)
 \end{aligned}$$

$$\begin{aligned}
 & (A \cup B) \cap (A^c \cap B^c) \\
 &= (A \cap (A^c \cap B^c)) \cup (B \cap (A^c \cap B^c)) && (\cap \text{ distributes over } \cup) \\
 &= ((A \cap A^c) \cap B^c) \cup ((B \cap B^c) \cap A^c) && (\text{commutativity and associativity of } \cap) \\
 &= (\emptyset \cap B^c) \cup (\emptyset \cap A^c) && (\text{complementation laws}) \\
 &= \emptyset \cup \emptyset && (\emptyset \text{ annihilates } \cap) \\
 &= \emptyset && (\text{idempotence of } \cup)
 \end{aligned}$$

To show the other de Morgan law $(A \cap B)^c = A^c \cup B^c$, one proceeds analogously or derives it from the previous de Morgan law and part (b):

$$\begin{aligned}
 A^c \cup B^c &= ((A^c \cup B^c)^c)^c && (\text{complement is an involution}) \\
 &= ((A^c)^c \cap (B^c)^c)^c && (\text{previous de Morgan law}) \\
 &= (A \cap B)^c && (\text{complement is an involution})
 \end{aligned}$$

ⓑ We can work with iff-reasoning, where the crucial third step uses the propositional de Morgan laws $\neg(P \vee Q) \iff \neg P \wedge \neg Q$ and $\neg(P \wedge Q) \iff \neg P \vee \neg Q$.

$$\begin{array}{ll}
 x \in (A \cup B)^c \iff \neg(x \in A \cup B) & x \in (A \cap B)^c \iff \neg(x \in A \cap B) \\
 \iff \neg(x \in A \vee x \in B) & \iff \neg(x \in A \wedge x \in B) \\
 \iff \neg(x \in A) \wedge \neg(x \in B) & \iff \neg(x \in A) \vee \neg(x \in B) \\
 \iff x \in A^c \wedge x \in B^c & \iff x \in A^c \vee x \in B^c \\
 \iff x \in A^c \cap B^c & \iff x \in A^c \cup B^c
 \end{array}$$

♪ Many set-theoretic proofs involve establishing the equality of two sets, and there are several ways of formulating such proofs. Two sets A and B are equal if they have the same elements: $\forall x. x \in A \iff x \in B$. Separating the bi-implication into two directions gives rise to a derived proof technique: to prove $A = B$, it is sufficient to prove $A \subseteq B$ and $B \subseteq A$. These individual subset relation may be established element-wise ($\forall x \in A. x \in B$ and $\forall x \in B. x \in A$), or via a transitive chain of subset relations. The equality $A = B$ itself can be shown via equivalence reasoning, either by equating set comprehensions, or using a

collection of known equalities (such as the ones proved in this exercise) and “algebraic manipulation” of sets. Finally, a way to combine element-wise and calculational reasoning is via a chain of bi-implications between membership predicates, which often reduces the proof to a purely logical argument, treating “ $x \in A$ ” as an atomic proposition. All of these proof techniques are perfectly appropriate (as long as the nontrivial calculational steps are all justified): one may be easier or harder than another, depending on the problem.

♪ The non-calculational proofs in parts (A) of (b) and (c) may seem rather contrived: they are longer and fiddlier than the alternative proofs, and proceed in a very roundabout way compared to directly calculating with elements. But this is precisely what makes them illuminating: they make no reference whatsoever to notions and constructions specific to sets, like the membership relation or set comprehension. The reasoning is carried out entirely using the abstract properties of unions, intersections, and complementation, such as commutativity, distributivity, annihilation, etc. Thus, the proofs can be directly translated to any setting that supports operators with similar properties; namely order-theoretic structures called *Boolean algebras*^a. Powersets of a set form a Boolean algebra (see §5.3.2), but so does the familiar set of truth values with conjunction, disjunction and negation. If logical negation is only characterised via the properties $P \vee \neg P \iff \top$ and $P \wedge \neg P \iff \perp$, the proofs above show that negation must also satisfy the property $\neg(\neg P) \iff P$ and the familiar de Morgan dualities (that we used as a *given* in the alternative proofs in part (c)).

Why bother with all this, you may ask? We can already *obviously* see that $\neg(\neg P) \iff P$ and the de Morgan laws hold from the truth tables. The guiding principle here (and most of mathematics) is simple: results that have fewer assumptions are stronger than results that have more. The fact that these propositions follow from a small, discrete set of algebraic properties makes them stronger than if we had to rely on notions like truth tables, set comprehensions, etc., which would restrict them to the particular area of mathematics we are working with. Sure, the proofs are more cumbersome than using these “domain-specific” concepts, but they are possible and therefore need not be reproved as long as we are working with a Boolean algebra. Much of mathematics is about proving more abstract and general results than what one actually needs, because relying on fewer assumptions makes them more widely applicable.

^a You should be familiar with the notion of Boolean algebra as a branch of “normal” algebra which uses truth values instead of numbers – this is what you used in Digital Electronics. Thus it may seem weird to refer to the plural “algebras” in this context. The name clash is unfortunate, but here we are discussing the *algebraic structure* known as “a Boolean algebra”, similarly to how we would discuss “a monoid” or “a field” – and Boolean algebras are the setting in which you can do Boolean algebra (the calculational process). There are other kinds of algebras too, like Heyting algebras and Lindenbaum–Tarski algebras, all with slightly different operations and properties.

5.2. Core exercises

1. Prove that for all for all sets U and subsets $A, B \subseteq U$:

$$\text{a) } \forall X. A \subseteq X \wedge B \subseteq X \iff (A \cup B) \subseteq X \quad \text{b) } \forall Y. Y \subseteq A \wedge Y \subseteq B \iff Y \subseteq (A \cap B)$$

a) Let $X \subseteq U$ be a set.

(\Rightarrow) Assume that ① $A \subseteq X$ and ② $B \subseteq X$. We need show that for all $x \in U$, $x \in A \vee x \in B$ implies $x \in X$. So, let $x \in U$ and assume ③ $x \in A \vee x \in B$. Then, if $x \in A$ we have $x \in X$ by assumption ①; and, if $x \in B$ we also have $x \in X$, by assumption ③. Thus, assumption ③ yields $x \in X$ as required.

(\Leftarrow) Assume $A \cup B \subseteq X$. Then, since $A \subseteq A \cup B$ and $B \subseteq A \cup B$, we have by transitivity of \subseteq (Lemma 84) both that $A \subseteq X$ and $B \subseteq X$.

b) Let $Y \subseteq U$ be a set.

(\Rightarrow) Assume that ① $Y \subseteq A$ and ② $Y \subseteq B$. We need show that for all $y \in U$, $y \in Y$ implies $y \in A \wedge y \in B$. So, let $y \in U$ and assume $y \in Y$. Then, by assumption ①, $y \in A$ and, by assumption ②, $y \in B$, as required.

(\Leftarrow) Assume $Y \subseteq A \cap B$. Then, since $A \cap B \subseteq A$ and $A \cap B \subseteq B$, we have by transitivity of \subseteq (Lemma 84) both that $Y \subseteq A$ and $Y \subseteq B$.

♪ These properties are also given in Proposition 86, but they are reproduced here to highlight their importance. Once again, these are if-and-only-if characterisations of unions and intersections, which usually hints at an underlying universal property that uniquely describes what it means for something to be a union/intersection. In other words, these properties are the *specification* for the set-theoretic concept of a union/intersection, and the proofs above verify that the specific way we define them (via disjunction/conjunction of membership) satisfies the specification. As Corollary 87 suggests, this gives rise to a proof strategy for showing that a set C is the union of A and B : if C is a superset of both A and B , and it is a subset of any other set X that is a superset of A and B , then C must equal $A \cup B$ (and there is a dual pair of conditions for intersections). The benefit of this formulation is that some properties about unions/intersections are easier to approach via this universal property, rather than directly unwrapping the set-theoretic definitions of the operators. Moreover, just like with the complement proofs above, it gives us a way of proving properties with minimal reference to set-theoretic constructions like membership or comprehension, making them more general.

Now, you may have recognised similar formulations from last term, in an entirely different field of mathematics: number theory. Indeed, if we spell out the universal property of intersections:

$$\textcircled{1} A \cap B \subseteq A \wedge A \cap B \subseteq B \quad \textcircled{2} \forall Y \in \mathcal{P}(U). (Y \subseteq A \wedge Y \subseteq B) \implies Y \subseteq A \cap B$$

and compare it with the universal property of greatest common divisors:

$$\textcircled{1} \gcd(m, n) \mid m \wedge \gcd(m, n) \mid n \quad \textcircled{2} \forall d \in \mathbb{Z}^+. (d \mid m \wedge d \mid n) \implies d \mid \gcd(m, n)$$

we can notice a clear and striking similarity. The secret is that both intersections and gcds are instances of a more general construction called a *greatest lower bound*, which is a

concept that can be defined (but doesn't necessarily have to exist) in any partially ordered set (poset), i.e. a set with a reflexive, transitive and antisymmetric ordering relation.

Intuitively, a greatest lower bound of two elements of a poset is the largest element that is smaller than both (it is “just below” both of them, but not smaller than necessary). For an abstract poset (P, \sqsubseteq) , the greatest lower bound of two elements x and y in P is usually denoted $x \sqcap y$ (also an element of P , if it exists) and often called their *(binary) meet*. It has the properties that it is a lower bound of both x and y :

$$\textcircled{1} \quad x \sqcap y \sqsubseteq x \quad \wedge \quad x \sqcap y \sqsubseteq y$$

and it is greater than any lower bound of both x and y :

$$\textcircled{2} \quad \forall l \in P. (l \sqsubseteq x \wedge l \sqsubseteq y) \implies l \sqsubseteq x \sqcap y$$

Binary meets (just like all concepts defined via an universal property) are unique, if they exist; an important consequence is that *any* element that satisfies these two properties will be equal to $x \sqcap y$. This lets us prove results about $x \sqcap y$ completely abstractly, without knowing how it is defined in a particular poset.

The properties $\textcircled{1}$ and $\textcircled{2}$ of intersections and gcds exactly align with those of the abstract definition of a binary meet: they are the exact same concept, manifested in different partially ordered sets. In the case of intersections, the poset is the powerset $\mathcal{P}(U)$ with the subset ordering relation, which we proved in §5.1.1 to be a partial order. In the case of gcds, the poset is that of natural numbers, with divisibility as the ordering relation: d is “less than” n if $d \mid n$. This may seem like a peculiar way of ordering (in particular, 0 becomes the “greatest element” since $d \mid 0$ for any $d \in \mathbb{N}$, and 1 becomes the “least element” since $1 \mid n$ for any $n \in \mathbb{N}$), but it satisfies all the required properties of being a partial order. In the divisibility poset, “lower bounds” of two numbers are their common divisors, so the “greatest lower bound” is indeed the greatest common divisor.

With this abstract understanding, we can consider binary meets in other known posets. What would the meet of two natural numbers m and n be in the standard \leq ordering? It would be the number that is less than (or equal to) both m and n , but not “too small”; the obvious choice would simply be the minimum of the two numbers, the greatest number that is not larger than either m or n . Slightly more esoteric is the partial order of Boolean truth values, $\{\top, \perp\}$, whose intuitive ordering (reflexive and \perp less than \top) coincides with the Boolean operator of implication. Then, the binary meet of propositions P and Q is a proposition that implies both P and Q , and is implied by anything that implies both P and Q . It is easy to see that the conjunction $P \wedge Q$ satisfies this characterisation: it clearly implies both P and Q , and if $R \implies P$ and $R \implies Q$, we can conclude that $R \implies P \wedge Q$.

And of course, by dualising everything, we get two concepts for the price of one: the dual notion of a greatest lower bound is the *least upper bound*, also called the *(binary) join* and

denoted $x \sqcup y$, with universal properties:

$$\textcircled{1} x \sqsubseteq x \sqcup y \wedge y \sqsubseteq x \sqcup y \quad \textcircled{2} \forall u \in P. (x \sqsubseteq u \wedge y \sqsubseteq u) \implies x \sqcup y \sqsubseteq u$$

All the posets described above have binary joins given by the “expected” dual constructions: union, least common multiple, minimum, disjunction.

One important point to highlight is the “unique, if it exists” nature of meets and joins: they are not guaranteed to exist for any pair of elements in a poset. This is different from saying that in any monoid $(M, \bullet, \varepsilon)$, we can combine any two elements a and b into $a \bullet b \in M$. The monoid product $a \bullet b$ is guaranteed to exist because $\bullet: M \times M \rightarrow M$ is a binary operator, mapping two elements a and b to a new element of M – it “generates” the element $a \bullet b$, and since it is an operator on M , asking if $a \bullet b$ exists in M or not is uninteresting. The symbols \sqcap and \sqcup are *not* operators: they are simply used to denote the unique meet/join of two elements of a poset, if it happens to exist. The family of sets $\mathcal{F} = \{\emptyset, \{1\}, \{2\}\}$ is a poset under subset inclusion, and \emptyset is indeed the meet (intersection) of $\{1\}$ and $\{2\}$; but their union $\{1, 2\}$ is not an element of \mathcal{F} and there is no other common upper bound that could be called the join, so the elements $\{1\}$ and $\{2\}$ in \mathcal{F} have no binary join.

Having said that, we *can* analyse sets which have binary meets and joins for all pairs of elements; such posets are called *lattices*. It so happens that all of the above examples are lattices, and some are moreover *bounded* lattices with greatest and least elements (with the exception being that (\mathbb{N}, \leq) has no greatest element). A consequence of this is that the meet and join can indeed be presented as binary operators in a lattice, since $x \sqcap y$ and $x \sqcup y$ are guaranteed to exist for any $x, y \in P$. The binary operators $\sqcap: P \times P \rightarrow P$ and $\sqcup: P \times P \rightarrow P$ satisfy several properties “for free”: they are associative, commutative, and idempotent. These follow – unsurprisingly – from the universal properties of the corresponding (order-theoretic) concepts: for example, to show that $x \sqcap x = x$, it is sufficient to show that $x \sqsubseteq x$ (by reflexivity), and for any $y \in P$ such that $y \sqsubseteq x$, $y \sqsubseteq x$ holds (sure). Similar proofs of commutativity and associativity are actually demonstrated in the notes, following the statements of these properties for gcds in [Lemma 63](#). Since the arguments are done purely by universal properties, they can be adapted directly to binary meets in any poset, and then specialised to other lattices like $(\mathcal{P}(U), \subseteq)$ or (\mathbb{N}, \leq) .

2. Either prove or disprove that, for all sets A and B ,

a) $A \subseteq B \implies \mathcal{P}(A) \subseteq \mathcal{P}(B)$

Assume $A \subseteq B$ and let $X \in \mathcal{P}(A)$. Then, $X \subseteq A$ and $A \subseteq B$. Hence, $X \subseteq B$ and so $X \in \mathcal{P}(B)$.

b) $\mathcal{P}(A \cup B) \subseteq \mathcal{P}(A) \cup \mathcal{P}(B)$

One can disprove it by taking two different singleton sets A and B and noticing that $(A \cup B) \in \mathcal{P}(A \cup B)$ while it is not the case that $(A \cup B) \in \mathcal{P}(A) \cup \mathcal{P}(B)$. For instance, $\{1\} \cup \{2\} = \{1, 2\} \in \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$, but $\{1, 2\} \notin \{\emptyset, \{1\}, \{2\}\}$.

c) $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$

Assume $X \in \mathcal{P}(A) \cup \mathcal{P}(B)$; that is, either ① $X \in \mathcal{P}(A)$ or ② $X \in \mathcal{P}(B)$.

In case ①, $X \subseteq A$ and since $A \subseteq (A \cup B)$ we have $X \subseteq (A \cup B)$; and hence $X \in \mathcal{P}(A \cup B)$.

In case ②, $X \subseteq B$ and since $B \subseteq (A \cup B)$ we have $X \subseteq (A \cup B)$; and hence $X \in \mathcal{P}(A \cup B)$.

d) $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$

Assume $X \in \mathcal{P}(A \cap B)$; that is $X \subseteq (A \cap B)$ or, equivalently, $X \subseteq A$ and $X \subseteq B$. Hence, $X \in \mathcal{P}(A)$ and $X \in \mathcal{P}(B)$; so that $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$.

e) $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$

Assume $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$; that is, $X \in \mathcal{P}(A)$ and $X \in \mathcal{P}(B)$. Then, $X \subseteq A$ and $X \subseteq B$; so that $X \subseteq (A \cap B)$ and hence $X \in \mathcal{P}(A \cap B)$.

♪ Parts (d) and (e) used the universal property of intersections from §5.2.1. We could have formulated the proof for (c) entirely using universal properties: to show $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$, it is sufficient to show that $\mathcal{P}(A \cup B)$ is an upper bound of $\mathcal{P}(A)$ and $\mathcal{P}(B)$; but both follow from the fact that $A \subseteq A \cup B$, $B \subseteq A \cup B$, and part (a) which lifts these subset relations to powersets. A UP proof for (d) is very similar: to show $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$, it is sufficient to show that $\mathcal{P}(A \cap B)$ is a common subset of $\mathcal{P}(A)$ and $\mathcal{P}(B)$, both of which follow from lifting $A \cap B \subseteq A$ and $A \cap B \subseteq B$ to powersets. It is not necessarily the case that a UP proof is shorter or simpler than one done from first principles, but it often allows for higher-level reasoning than going down to element-wise definitions. The rule of thumb should be: if the proof goal is of the form $A \cup B \subseteq X$ or $Y \subseteq A \cap B$, a UP proof may be possible since it is sufficient to show that X is a common superset or Y is a common subset.

3. Let U be a set. For all $A, B \in \mathcal{P}(U)$ prove that the following statements are equivalent.

$$\text{a) } A \cup B = B \quad \text{b) } A \subseteq B \quad \text{c) } A \cap B = A \quad \text{d) } B^c \subseteq A^c$$

Let U be a set and consider $A, B \in \mathcal{P}(U)$. To prove that the statements are equivalent, it is sufficient that they cyclically imply each other.

(a) \Rightarrow (b) Assume $A \cup B = B$. Then, $A \subseteq (A \cup B) = B$ and we are done.

(b) \Rightarrow (c) Assume $A \subseteq B$. Since, $(A \cap B) \subseteq A$ we need only show $A \subseteq (A \cap B)$ or, by §5.2.1, that $A \subseteq A$ and $A \subseteq B$; which respectively hold by reflexivity of \subseteq and assumption.

(c) \Rightarrow (d) Assume $(A \cap B) = A$ and let $x \in U$. Then, $x \notin B$ implies $x \notin (A \cap B) = A$.

(d) \Rightarrow (b) Because $B^c \subseteq A^c$ stands for $x \notin B \implies x \notin A$ for all $x \in U$ which is the contrapositive of $x \in A \implies x \in B$ for all $x \in U$.

(b) \Rightarrow (a) Assume $A \subseteq B$. Since also $B \subseteq B$, by §5.2.1 above, we have $(A \cup B) \subseteq B$; and as $B \subseteq (A \cup B)$ we are done.

♪ Questions of the form “prove that the following n statements are equivalent” require one to prove (at least) n implications that form a cycle; thanks to the transitivity and symmetry of implication, this is sufficient to take care of a bi-implication between any two statements. The order and number of implications proved is not important, as long as there is a way to get from any statement to another. In this question we could have done the chain $(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (d) \Rightarrow (a)$, but (d) is simply a contrapositive of (b) so the implication $(d) \Rightarrow (b)$ is easier. However, this only results in one outgoing implication from (a) , so that needed to be “patched” up with an extra (straightforward) proof.

4. For sets A, B, C, D , prove or disprove at least three of the following statements:

a) $(A \subseteq C \wedge B \subseteq D) \implies A \times B \subseteq C \times D$

Assume $A \subseteq C$ and $B \subseteq D$, and let (a, b) be an element of $A \times B$. We need to show that (a, b) is also an element of $C \times D$. Since $a \in A$ and $A \subseteq C$, we have that $a \in C$; similarly, $b \in D$. Thus, $(a, b) \in C \times D$, as required.

♪ We slightly glossed over a few formal steps here, but this is rarely an issue. What we mean by “let (a, b) be an element of $A \times B$ ” is that we consider an element $x \in A \times B$ and use the fact that all elements of $A \times B$ are pairs; so x must be of the form (a, b) for an $a \in A$ and $b \in B$. Such “pattern-matching” is very common in formal proofs and needs not be elaborated on too much, unless the patterns are interesting in their own right or the relationships between the sets are more complex.

b) $(A \cup C) \times (B \cup D) \subseteq (A \times B) \cup (C \times D)$

This statement is false. As a counterexample, consider $A = \{1\}$, $C = \{2\}$ and $B = D = \emptyset$. $A \cup C = \{1, 2\}$ and $B \cup D = \emptyset$; the first Cartesian product is thus $\{(1, 2)\}$. However, $A \times B = C \times D = \emptyset$, so their union is also the empty set, not a superset of $\{(1, 2)\}$.

c) $(A \times C) \cup (B \times D) \subseteq (A \cup B) \times (C \cup D)$

By the universal property of unions it is sufficient to prove that $A \times C \subseteq (A \cup B) \times (C \cup D)$ and $B \times D \subseteq (A \cup B) \times (C \cup D)$. Part (a) implies the former with $A \subseteq A \cup B$ and $C \subseteq C \cup D$, as well as the latter with $B \subseteq A \cup B$ and $D \subseteq C \cup D$.

♪ Again we notice that the question asks us to prove that the union of two sets X and Y is below another set Z , for which it is sufficient to prove that Z is a common superset of both X and Y so the least common superset (a.k.a. the union) is necessarily going to be below it. The requirements can be discharged using property (a), that lets us “apply” subset relations within components of a Cartesian product. Note how we do not need to refer to elements of the sets at all.

d) $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$

Let (a, x) be an element of $A \times (B \cup C)$. By the definition of unions, x is either in B or in C ; in the former case the tuple (a, x) is in $A \times B$, which is a subset of $(A \times B) \cup (A \times C)$; in the latter, $(a, x) \in A \times C$ which is again a subset of the union $(A \cup B) \times (C \cup D)$, as required.

e) $(A \times B) \cup (A \times D) \subseteq A \times (B \cup D)$

By the universal property of unions it is sufficient to prove that $A \times B \subseteq A \times (B \cup D)$ and $A \times D \subseteq A \times (B \cup D)$. Both follow from property (a) and the fact that $B \cup D$ is a common superset of both B and D .

5. For sets A, B, C, D , prove or disprove at least three of the following statements:

a) $(A \subseteq C \wedge B \subseteq D) \implies A \uplus B \subseteq C \uplus D$

Assume $A \subseteq C$ and $B \subseteq D$, and let x be an element of $A \uplus B$. We need to prove that x is in $C \uplus D$. By the definition of disjoint union, x is either of the form $(1, a)$ for $a \in A$, or $(2, b)$ for $b \in B$. In the first case we use the assumption $A \subseteq C$ to derive that $a \in C$, but then $(1, a)$ is in $C \uplus D$. In the second case we use the assumption $B \subseteq D$ to derive that $b \in D$, so $(2, b)$ is in $C \uplus D$, as required.

b) $(A \cup B) \uplus C \subseteq (A \uplus C) \cup (B \uplus C)$

Let x be an element of $(A \cup B) \uplus C$. By the definition of unions and disjoint unions, we consider three cases: x is of the form $(1, a)$ with $a \in A$, or $(1, b)$ for $b \in B$, or $(2, c)$ for $c \in C$. In the first case, $(1, a)$ is in $A \uplus C$ and therefore in $(A \uplus C) \cup (B \uplus C)$; similarly, in the second case, $(1, b)$ is in $B \uplus C$ so in $(A \uplus C) \cup (B \uplus C)$. Finally, in the third case, $(2, c)$ is in both $A \uplus C$ and $B \uplus C$, so it will certainly be in $(A \uplus C) \cup (B \uplus C)$.

c) $(A \uplus C) \cup (B \uplus C) \subseteq (A \cup B) \uplus C$

By the UP of unions it is sufficient to prove that $A \uplus C \subseteq (A \cup B) \uplus C$ and $B \uplus C \subseteq (A \cup B) \uplus C$. Both follow using part (a) and the fact that $A \cup B$ is a superset of both A and B .

d) $(A \cap B) \uplus C \subseteq (A \uplus C) \cap (B \uplus C)$

By the UP of intersections it is sufficient to prove that $(A \cap B) \uplus C$ is in $A \uplus C$ and in $B \uplus C$. Both follow using part (a) and the fact that $A \cap B$ is a common subset of both A and B .

e) $(A \uplus C) \cap (B \uplus C) \subseteq (A \cap B) \uplus C$

Let x be an element of $(A \uplus C) \cap (B \uplus C)$. By definition of intersections it must be both in $A \uplus C$ and $B \uplus C$, which is possible if it has the same tag: either x is of the form $(1, y)$ where y is both in A and B , or of the form $(2, c)$ with $c \in C$. In the first case $(1, y)$ is the first injection of $(A \cap B) \uplus C$, and in the second case $(2, c)$ is the second injection of $(A \cap B) \uplus C$.

6. Prove the following properties of the big unions and intersections of a family of sets $\mathcal{F} \subseteq \mathcal{P}(A)$:

$$\text{a) } \forall U \subseteq A. (\forall X \in \mathcal{F}. X \subseteq U) \iff \bigcup \mathcal{F} \subseteq U$$

Let U be a subset of A .

(\Rightarrow) Assume that U is a superset of every element of \mathcal{F} and let x be a member of $\bigcup \mathcal{F}$. We need to show that x is also in U . By the definition of big unions, there exists a set $F \in \mathcal{F}$ such that $x \in F$; but since U is a superset of every set in \mathcal{F} , we know that $F \subseteq U$ and therefore that $x \in U$.


(\Leftarrow) Assume $\bigcup \mathcal{F} \subseteq U$ and let X be a set in \mathcal{F} . Since $\bigcup \mathcal{F}$ is the union of all sets in \mathcal{F} , we know that $X \subseteq \bigcup \mathcal{F}$, and by transitivity with the first assumption we can conclude that $X \subseteq U$, as required.

$$\text{b) } \forall L \subseteq A. (\forall X \in \mathcal{F}. L \subseteq X) \iff L \subseteq \bigcap \mathcal{F}$$

Let L be a subset of A .

(\Rightarrow) Assume that L is a subset of every element of \mathcal{F} and let x be a member of L . We need to show that x is also in $\bigcap \mathcal{F}$, that is, it is a member of every set in \mathcal{F} . To this end, let F be an arbitrary element of \mathcal{F} . By assumption, we know that $L \subseteq F$, but then $x \in L$ must also be in F . Since F was arbitrary, this holds for every element of \mathcal{F} , so indeed $x \in \bigcap \mathcal{F}$.

(\Leftarrow) Assume $L \subseteq \bigcap \mathcal{F}$ and let X be a set in \mathcal{F} . Since $\bigcap \mathcal{F}$ is the intersection of all sets in \mathcal{F} , we know that $\bigcap \mathcal{F} \subseteq X$, and by transitivity with the first assumption we can conclude that $L \subseteq X$, as required.

 These two propositions generalise the universal properties of unions and intersections. The union of a family of sets \mathcal{F} is the least common superset of all the sets in the family:

$$\textcircled{1} \forall X \in \mathcal{F}. X \subseteq \bigcup \mathcal{F} \quad \textcircled{2} \forall U \subseteq A. (\forall X \in \mathcal{F}. X \subseteq U) \implies \bigcup \mathcal{F} \subseteq U$$

Dually, the intersection is the greatest common subset of all sets in \mathcal{F} :

$$\textcircled{1} \forall X \in \mathcal{F}. \bigcap \mathcal{F} \subseteq X \quad \textcircled{2} \forall L \subseteq A. (\forall X \in \mathcal{F}. L \subseteq X) \implies L \subseteq \bigcap \mathcal{F}$$

You should be able to read such properties with relative ease: the first one says that the big union is an upper bound of all elements in \mathcal{F} , and the second one characterises it as the smallest such set. As in the binary case, the real power of universal properties comes when proving statements of the form $\bigcup \mathcal{F} \subseteq U$ or $L \subseteq \bigcap \mathcal{F}$, since all one needs to show next is that U and L are upper and lower bounds, respectively.

7. Let A be a set.

a) For a family $\mathcal{F} \subseteq \mathcal{P}(A)$, let $\mathcal{U} \triangleq \{U \subseteq A \mid \forall S \in \mathcal{F}. S \subseteq U\}$. Prove that $\bigcup \mathcal{F} = \bigcap \mathcal{U}$.

The family \mathcal{U} is the set of upper bounds of \mathcal{F} , i.e. the family of sets which are all supersets of every set in \mathcal{F} .

(\subseteq) By the universal property of big unions (§5.2.6), it is sufficient to prove that $\forall X \in \mathcal{F}. X \subseteq \bigcap \mathcal{U}$. By the universal property of intersections, for this it is sufficient to prove that $\forall X \in \mathcal{F}. \forall U \in \mathcal{U}. X \subseteq U$, and this holds by the definition of \mathcal{U} as the set of upper bounds of \mathcal{F} .

(\supseteq) We know from the universal property of big unions that $\bigcup \mathcal{F}$ is an upper bound, so $\forall S \in \mathcal{F}. S \subseteq \bigcup \mathcal{F}$. But then $\bigcup \mathcal{F}$ must be in \mathcal{U} , the set of upper bounds. By the UP of intersections, $\bigcap \mathcal{U}$ is a subset of every element of \mathcal{U} , and in particular, $\bigcap \mathcal{U} \subseteq \bigcup \mathcal{F}$, as required.

b) Analogously, define the family $\mathcal{L} \subseteq \mathcal{P}(A)$ such that $\bigcap \mathcal{F} = \bigcup \mathcal{L}$. Also prove this statement.

The family \mathcal{L} is the set of lower bounds of \mathcal{F} , that is,

$$\mathcal{L} \triangleq \{L \subseteq A \mid \forall S \in \mathcal{F}. L \subseteq S\}$$

We prove that $\bigcap \mathcal{F} = \bigcup \mathcal{L}$.

(\subseteq) We know from the universal property of big intersections that $\bigcap \mathcal{F}$ is a lower bound, so $\forall S \in \mathcal{F}. \bigcap \mathcal{F} \subseteq S$. But then $\bigcap \mathcal{F}$ must be in \mathcal{L} , the set of lower bounds. By the UP of unions, $\bigcup \mathcal{L}$ is a superset of every element of \mathcal{L} , and in particular, $\bigcap \mathcal{F} \subseteq \bigcup \mathcal{L}$, as required.

(\supseteq) By the universal property of big unions (§5.2.6), it is sufficient to prove that $\forall L \in \mathcal{L}. L \subseteq \bigcap \mathcal{F}$. By the universal property of intersections, for this it is sufficient to prove that $\forall L \in \mathcal{L}. \forall X \in \mathcal{F}. L \subseteq X$, and this holds by the definition of \mathcal{L} as the set of lower bounds of \mathcal{F} .

♪ One could approach such questions from first principles, by expanding all definitions and reasoning purely by logic. However, it would be rather cumbersome, and the higher-level proof techniques derived from universal properties have a clear advantage. They may take some getting used to, but it's worth the practice.

5.3. Optional advanced exercises

1. Prove that for all families of sets \mathcal{F}_1 and \mathcal{F}_2 ,

$$(\bigcup \mathcal{F}_1) \cup (\bigcup \mathcal{F}_2) = \bigcup (\mathcal{F}_1 \cup \mathcal{F}_2)$$

State and prove the analogous property for intersections of non-empty families of sets.

The stated identity for unions is a special case of the associativity law for big unions, so let us just consider the case of intersections; that is: for non-empty collections of sets \mathcal{F}_1

and \mathcal{F}_2 ,

$$\left(\bigcap \mathcal{F}_1\right) \cap \left(\bigcap \mathcal{F}_2\right) = \bigcap (\mathcal{F}_1 \cup \mathcal{F}_2)$$

Indeed, for all x , we have


$$\begin{aligned} x \in \left(\bigcap \mathcal{F}_1\right) \cap \left(\bigcap \mathcal{F}_2\right) &\iff (x \in \bigcap \mathcal{F}_1) \wedge (x \in \bigcap \mathcal{F}_2) \\ &\iff (\forall X \in \mathcal{F}_1. x \in X) \wedge (\forall X \in \mathcal{F}_2. x \in X) \\ &\iff \forall X. (X \in \mathcal{F}_1 \Rightarrow x \in X) \wedge (X \in \mathcal{F}_2 \Rightarrow x \in X) \\ &\iff \forall X. (X \in \mathcal{F}_1 \vee X \in \mathcal{F}_2) \Rightarrow x \in X \\ &\iff \forall X. X \in (\mathcal{F}_1 \cup \mathcal{F}_2) \Rightarrow x \in X \\ &\iff x \in \bigcap (\mathcal{F}_1 \cup \mathcal{F}_2) \end{aligned}$$

2. For a set U , prove that $(\mathcal{P}(U), \subseteq, \cup, \cap, U, \emptyset, (\cdot)^c)$ is a **Boolean algebra**.

Let U be a set. We have the following:

- $\subseteq: \mathcal{P}(U) \times \mathcal{P}(U) \rightarrow \mathbb{B}$ is a partial order, as shown in §5.1.1.
- Every two sets A and B have a union $A \cup B$ which is their least upper bound, as well as an intersection $A \cap B$ which is their greatest lower bound (§5.2.1). It follows from the universal properties that both operations are commutative, associative, and idempotent.
- The full set U is the neutral element of intersection: given any set $A \subseteq U$, it is the case that $A \cap U = A$ by §5.2.3.
- The empty set \emptyset is the neutral element of union: given any set $A \subseteq U$, we know that $\emptyset \subseteq A$ so §5.2.3 implies that $A \cup \emptyset = A$.
- Similarly using §5.2.3 we can deduce that U is the annihilator for union (since $A \subseteq U$ implies $A \cup U = U$) and \emptyset is the annihilator for intersection (since $\emptyset \subseteq A$ implies $\emptyset \cap A = \emptyset$).
- To show the absorption laws, we let A and B be subsets of U and prove that $A \cup (A \cap B) = A$. Let x be an element of $A \cup (A \cap B)$; by definition, it has to be either in A or in $A \cap B$, i.e. in A or in both A and B . In both cases x must be in A . Conversely, assume $x \in A$; then it is clearly in $A \cup (A \cap B)$, as required. The second absorption law is similar.
- To show distributivity, we let A, B and C be subsets of U and prove that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. Let x be an element of $A \cap (B \cup C)$; by definition, it has to be both in A and either in B or in C . If it is in B , then it is also in $A \cap B$ and hence in $(A \cap B) \cup (A \cap C)$. Otherwise, if it is in C , then it is in $A \cap C$ and hence in $(A \cap B) \cup (A \cap C)$. The other distributive law is similar.

Thus we can conclude that $(\mathcal{P}(U), \subseteq, \cup, \cap, U, \emptyset, (\cdot)^c)$ is indeed a Boolean algebra.

 As the name implies, a Boolean algebra is an algebraic (or order-theoretic) structure that generalises Boolean truth values and operators. As an algebraic structure, it is a carrier set with two idempotent, commutative and associative operators that distribute over each other and are absorptive; two elements that are units for one operator and annihilators

for the other; and a unary complement operator. As an order-theoretic structure, it is a complemented, distributive lattice; that is, a poset in which every element has a meet and a join (i.e. a lattice, see §5.3.2) which distribute over each other, and every element has a complement.

As this exercise shows, powersets of a set also form a Boolean algebra – this underlies the intuitive similarity between logical operators (conjunction, disjunction) and set operators (intersection, union). An interesting question to ponder is the status of *implication*: it does not form part of the algebraic structure and is instead defined as $P \Rightarrow Q \triangleq \neg P \vee Q$. Set-theoretically the corresponding notion would be $A^c \cup B$, i.e. all the elements of the universe except the ones that are exclusively in A – not a particularly common or useful notion! We can also choose to axiomatise logic in terms of implication, and define negation as $\neg P \triangleq P \Rightarrow \perp$. A lattice with least and greatest elements and an appropriately characterised “implication” operator is called a *Heyting algebra*. Every Boolean algebra is a Heyting algebra with the implication defined as above, but not every Heyting algebra is a Boolean algebra – as a consequence, some logical tautologies like double negation elimination $\neg(\neg P) \Rightarrow P$ or the law of excluded middle $P \vee \neg P$ do not in general hold in a Heyting algebra. The distinction between Boolean and Heyting algebras is the distinction between *classical* and *intuitionistic* logic, the latter of which is particularly important in computer science and will be covered in much detail in future courses.