Notes on Discrete Structures

Kevin Sun

Preface

These notes cover topics in discrete mathematics at a standard undergraduate level. They do not assume familiarity with anything beyond elementary algebra. I recommend the textbooks below for further reading; these notes are primarily based on them:

- *Discrete Mathematics with Applications* by Epp
- *Building Blocks for Theoretical Computer Science* by Fleck
- *Discrete Mathematics: An Open Introduction* by Levin
- *Connecting Discrete Mathematics and Computer Science* by Liben-Nowell
- *Discrete Mathematics and Its Applications* by Rosen
- *A Transition to Advanced Mathematics* by Smith, Eggen, and St. Andre
- *Reasoning and Writing in the Mathematics Underlying Computation* by Snoeyink

Of course, there are many other excellent textbooks and resources not listed above, and I encourage you to seek them out.

— Kevin Sun
Last updated: January 2025

1 Logic and Proofs

One of the primary goals of mathematics is to prove true statements. To do this, we need to be familiar with the precise language and model of reasoning used in mathematics.

1.1 Propositional Logic

A *proposition* is a statement that is either true or false. For example, "$1+2=3$" and "$1+2=4$" are propositions, but "$x+2=3$" and "Is 2 an odd integer?" are not. If p is a true proposition, then its *truth value* is T; otherwise, its truth value is F. If p and q are propositions, then we can combine them to form various other propositions:

proposition	notation	truth value
not p	$\neg p$	if p is true: T; else: F
p or q	$p \vee q$	if p is true and/or q is true: T; else: F
p and q	$p \wedge q$	if p is true and q is true: T; else: F
p implies q	$p \Rightarrow q$	if p is true and q is false: F; else: T
p iff (if and only if) q	$p \Leftrightarrow q$	if p and q have the same truth value: T; else: F

There are many ways to say "p implies q," including "If p, then q," "p only if q," "p is sufficient for q," and "q is necessary for p." In the proposition $p \Rightarrow q$, the *hypothesis* is p and the *conclusion* is q. Notice that $p \Rightarrow q$ is true if p is false; in this case, we say that $p \Rightarrow q$ is *vacuously* true. For example, "If $1+1=3$, then $2+2=5$" is vacuously true.

Eequivalent Propositions

A *truth table* helps us understand complicated propositions. It has one row for each possible combination of truth values of the "base" propositions; each column lists the corresponding truth values of the complicated proposition. A proposition is a *tautology* if its entire column is T; it is a *contradiction* if its entire column is F. If propositions p and q have identical columns in a truth table, then they are *equivalent* and we write $p \equiv q$. For example, the truth table below shows that $p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$.

p	q	$p \Leftrightarrow q$	$p \Rightarrow q$	$q \Rightarrow p$	$(p \Rightarrow q) \wedge (q \Rightarrow p)$
T	T	T	T	T	T
T	F	F	F	T	F
F	T	F	T	F	F
F	F	T	T	T	T

We can similarly show that $p \Rightarrow q$ is equivalent to its *contrapositive* $\neg q \Rightarrow \neg p$. The *converse* of $p \Rightarrow q$ is $q \Rightarrow p$; it is equivalent to the *inverse* of $p \Rightarrow q$, which is $\neg p \Rightarrow \neg q$. We also note that $p \Rightarrow q \equiv \neg p \vee q$. Finally, *De Morgan's Laws* state that $\neg(p \vee q) \equiv \neg p \wedge \neg q$ and $\neg(p \wedge q) \equiv \neg p \vee \neg q$.

Practice 1.1. *Write a truth table that shows the following:*

1. $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$
2. $p \Rightarrow q \equiv \neg p \vee q$
3. $\neg(p \vee q) \equiv \neg p \wedge \neg q$
4. $\neg(p \wedge q) \equiv \neg p \vee \neg q$

Practice 1.2. *Is $p \Rightarrow q$ equivalent to $q \Rightarrow p$? Explain your answer using a truth table.*

Highlight. In ordinary English, we sometimes say $p \Rightarrow q$ when we actually mean $p \Leftrightarrow q$. For example, suppose Alice says, "If I like the book, then I'll watch the movie," and later, we find out that she watched the movie. From a logical perspective, we cannot conclude that she liked the book, but from a colloquial perspective, that might be a reasonable conclusion.

1.2 Predicates and Quantifiers

A *predicate* is a proposition whose truth value depends on the values of certain variables. Thus, one way to turn a predicate into a proposition is by setting every variable to a specific value. For example, consider the predicate $p(x) =$ "$x + 3 = 5$"; it has one variable x. Then $p(1)$ is a false proposition while $p(2)$ is a true proposition. A predicate can have multiple variables; for example, $q(x, y)$ could be the predicate "$x + y = 5$".

Another way to turn a predicate $p(x)$ into a proposition is to add a *quantifier*. There are two types of quantifiers:

quantifier	proposition	truth value
universal ($\forall$, "for all")	$\forall x\colon p(x)$	if $p(x)$ is true for all x: T; else: F
existential ($\exists$, "there exists")	$\exists x\colon p(x)$	if $p(x)$ is true for at least one x: T; else: F

For example, if $p(x)$ is the predicate "$x + 2 = 3$," then $\forall x\colon p(x)$ is false while $\exists x\colon p(x)$ is true. If $q(x)$ is the predicate "$x + 1 > x$," then $\forall x\colon q(x)$ and $\exists x\colon q(x)$ are both true.

Note that quantification only makes sense if there is a *universe of discourse*, i.e., a set of possible values for each variable. For example, the truth value of $\exists x\colon 2x = 1$ depends on whether or not x is allowed to be a fraction. In this chapter, our universe is the set of integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, in which case $\exists x\colon 2x = 1$ is false.

The concepts from propositional logic still apply to predicates and quantifiers. For example, $\forall x\colon p(x) \wedge q(x)$ is a proposition that states, "Every x satisfies both $p(x)$ and $q(x)$," and *De Morgan's Laws for Quantifiers* state $\neg(\forall x\colon p(x)) \equiv \exists x\colon \neg p(x)$ and $\neg(\exists x\colon p(x)) \equiv \forall x\colon \neg p(x)$. An x that shows $\forall x\colon p(x)$ is false is called a *counterexample*. For example, $x = 1$ (or any integer excluding 2) is a counterexample to the proposition $\forall x\colon x + 3 = 5$.

Practice 1.3. *Which of the following propositions are true (if any)?*

1. $\forall x \colon x \leq x^2$
2. $\exists x \colon x = x^2 \wedge x \geq 2$
3. $\exists x \colon x = x^2 \vee x \geq 2$
4. $\forall x \colon (x \geq 1) \Rightarrow \neg(x + 1 > 2x)$

Practice 1.4. *Express the following sentences in predicate logic:*

1. *Every integer is positive.*
2. *If we subtract an integer from itself, the result is always 0.*
3. *The square of a negative number is always positive.*
4. *At least one positive number is larger than itself.*

Nested Quantifiers

A proposition can have multiple quantifiers; the order of the quantifiers is important. For example, suppose $p(x, y)$ is the predicate "$x + y = 3$" and consider the following propositions:

proposition	truth value	explanation
$\forall x \forall y \colon p(x, y)$	F	If $x = 1$ and $y = 1$, then $x + y \neq 3$.
$\forall x \exists y \colon p(x, y)$	T	For any x, we can set $y = 3 - x$ so that $x + y = 3$.
$\exists x \forall y \colon p(x, y)$	F	There is no fixed x that satisfies $x + y = 3$ for all y.
$\exists x \exists y \colon p(x, y)$	T	One possibility is $x = 1, y = 2$.

Notice that if we're trying to prove $\forall x \exists y \colon p(x, y)$, we are allowed to let y depend on x. On the other hand, if we want to prove $\exists x \forall y \colon p(x, y)$, we must pick a single x that works for all y.

Practice 1.5. *Rewrite the following propositions such that no negation appears before a quantifier:*

1. $\neg(\forall x \exists y \colon p(x, y))$
2. $\neg(\exists x \forall y \colon p(x, y))$

Quantifiers, and nested quantifiers, allow us to state more sophisticated mathematical statements. For example, "The product of a positive integer and a negative integer is always a negative integer" can be written as $\forall x \forall y \colon (x > 0 \wedge y < 0) \Rightarrow xy < 0$. Sometimes, when the context is sufficiently clear, we omit repeated quantifiers. For example, the previous proposition can also be written as $\forall x, y \colon (x > 0 \wedge y < 0) \Rightarrow xy > 0$.

Practice 1.6. *If $p(x, y, z) =$ "$x + y = z$", which of the following are true (if any)?*

1. $\forall x \forall y \exists z \colon p(x, y, z)$

2. $\exists z \forall x \forall y \colon p(x, y, z)$

1.3 Proofs

A *proof* is an explanation of why a proposition is true. A proof starts with propositions that are known to be true, and each step in a proof should logically follow from the previous ones. When we write a proof, there is a trade-off between thoroughness (i.e., spelling out every detail) and efficiency (i.e., omitting details for brevity). Finding the "right" balance depends on the context (e.g., difficulty of the proof, background of the audience) and personal preferences. Note that proofs are generally written in complete sentences and do not use on the $\forall$ and $\exists$ symbols.

Before we see examples of proofs (and proof strategies), let's establish some definitions. Again, the universe of discourse in this chapter is the set of integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, which means that we should assume that every variable is an integer.

term	definition
"n is even"	$\exists k \colon n = 2k$
"n is odd"	$\exists k \colon n = 2k + 1$
"a divides b" $(a \mid b)$	$a \neq 0 \wedge \exists c \colon b = ac$

(If a divides b, we say that a is a *divisor* or *factor* of b, and b is a *multiple* of a. The negation of $a \mid b$ is $a \nmid b$.) We will assume, without proof, the true proposition that every integer is either even or odd (but not both).

Proof Strategies

We already saw a proof strategy in Section 1.1: to prove that two propositions are equivalent, we can spell out their truth tables and note that they have identical columns. But this strategy only works for relatively simple statements in propositional logic; for other statements, we'll need other strategies. The ones listed below strategies are not exhaustive, and many statements can be proven in multiple ways, but they're a decent way to get started.

Strategy 1: Direct proof. Many theorems are of the form $p \Rightarrow q$. (A *theorem* is just a true proposition.) One way to prove these is directly: assume p; apply a combination of definitions, logic, and known results to construct a sequence of true propositions; and conclude with q.

Theorem 1.7. *For all n, if n is even, then $n + 1$ is odd.*

Proof. Assume n is even. By the definition of "even," there exists an integer k such that $n = 2k$. This implies $n + 1 = 2k + 1$. Since k is an integer, $n + 1$ satisfies the definition of "odd," so $n + 1$ is odd.

Highlight. A proof should not rely on any intuitions or examples. Instead, it should take logical steps from the premise (e.g., "n is even") to the goal ("n is odd"). The "correct" size of these steps is subjective; when in doubt, take smaller steps.

Practice 1.8. *Prove that for all n, if n is odd, then $n+1$ is even.*

Practice 1.9. *Prove that for all n, if $6 \mid n$, then n is even.*

When the context is clear, we sometimes omit universal quantifiers. Conventions can be useful; for example, n and k often denote integers (just as i and j often denote index variables in programming).

Theorem 1.10. *If n is odd, then n^2 is odd.*

Proof. Assume n is odd. By the definition of "odd," there exists an integer k such that $n = 2k+1$. Thus,

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Since $2k^2 + 2k$ is an integer, n^2 is odd.

Practice 1.11. *Prove that if $a \mid b$ and $b \mid c$, then $a \mid c$.*

Practice 1.12. *Prove that if m and n are odd, then mn is odd.*

Strategy 2: Split into cases. Sometimes, a proof naturally splits into multiple cases. When this happens, we can analyze each case separately.

Theorem 1.13. *If n is odd, then there exists a such that $n = 4a+1$ or there exists b such that $n = 4b-1$.*

Proof. Assume n is odd. By the definition of "odd," there exists k such that $n = 2k+1$.

- If k is even, then there exists ℓ such that $k = 2\ell$, so $n = 2(2\ell)+1 = 4\ell+1$. Thus, if we set $a = \ell$, then $n = 4a+1$.
- If k is odd, then there exists ℓ such that $k = 2\ell+1$. This implies $n = 2(2\ell+1)+1 = 4\ell+3 = 4(\ell+1)-1$. Thus, if we set $b = \ell+1$, then $n = 4b-1$.

In both cases, the conclusion of the theorem is true, so we are done.

Practice 1.14. *Prove that for all n, $n(n+1)$ is even.*

Practice 1.15. *Prove that if $5 \mid n$, then $10 \mid n$ or n is odd.*

Strategy 3: Prove the contrapositive. If we want to prove $p \Rightarrow q$, sometimes it's easier to prove its contrapositive, $\neg q \Rightarrow \neg p$. (Recall that the two propositions are equivalent.)

Theorem 1.16. *If $3n + 2$ is odd, then n is odd.*

Direct proof (failed attempt). Assume $3n + 2$ is odd, so $3n + 2 = 2k + 1$ for some integer k. This means $n = (2k - 1)/3$. It is unclear how to proceed from here...

Proof. We shall give a direct proof of the contrapositive. In particular, we'll show that if n is even, then $3n+2$ is even. If n is even, then $n = 2k$ for some integer k, so $3n+2 = 3(2k)+2 = 2(3k) + 2 = 2(3k + 1)$. Since $3k + 1$ is integer, $3n + 2$ is even.

Practice 1.17. *Prove that if $3 \nmid n^2$, then $3 \nmid n$.*

Practice 1.18. *Prove that if $n^2 - 2n + 3$ is even, then n is odd.*

Strategy 4: Proof by contradiction. One way to prove a proposition p is to prove $\neg p \Rightarrow q$, where q is something impossible (e.g., $r \wedge \neg r$ for some proposition r). In other words, we can prove that p is true by showing that $\neg p$ logically leads to an impossible conclusion.

Theorem 1.19. *There does not exist integers a, b such that $4a + 2b = 1$.*

Proof. For contradiction, we assume that the theorem is false, i.e., there exist integers a, b such that $4a+2b = 1$. Dividing by 2, we obtain $2a+b = 1/2$. However, this is a contradiction because $2a + b$ is an integer but $1/2$ is not. Thus, our assumption was false, so the theorem must be true.

Theorem 1.20. *There does not exist a largest even integer.*

Proof. For contradiction, we assume that the theorem is false, i.e., there exists a largest even integer, which we denote by n. Since n is even, there exists k such that $n = 2k$. Notice that $n + 2 = 2k + 2 = 2(k + 1)$ is even. But $n + 2 > n$, contradicting our assumption that n is the largest even integer.

For the next theorem, we need another definition: an integer n is *prime* if $n \geq 2$ and its only divisors are 1 and n. We assume, without proof, the true proposition that every integer greater than 1 has a prime divisor.

Theorem 1.21. *There are infinitely many prime numbers.*

Proof. For contradiction, we assume there are only n prime numbers for some integer n. Then we can label them as $p_1, p_2, \ldots, p_n$, where $p_1 = 2, p_2 = 3, p_3 = 5$, etc. Consider the integer $Q = p_1 p_2 \cdots p_n + 1$. By the assumption above this box, $p_i \mid Q$ for at least one p_i in the list of primes, which means $Q = kp_i$ for some integer k. Thus,

$$p_1 p_2 \cdots p_n + 1 = kp_i.$$

Dividing both sides by p_i yields a non-integer on the left (due to the $1/p_i$ term) and the integer k on the right. This is a contradiction, so our assumption was incorrect.

Practice 1.22. *Prove, by contradiction, that* $((p \Rightarrow q) \wedge q) \Rightarrow q$ *is a tautology.*

To prove an implication $p \Rightarrow q$ by contradiction, we start by assuming $p \Rightarrow q$ is false, which is equivalent to assuming $p \wedge \neg q$. From there, we try to reach an impossibility.

Theorem 1.23. *For every integer n, if n^2 is even, then n is even.*

Proof. For contradiction, assume that the theorem is false, i.e., there exists an integer n such that n^2 is even but n is odd. Then there exists an integer k such that $n = 2k + 1$, which means $n^2 = (2k+1)^2 = 4k^2 + 2k + 1 = 2(2k^2 + k) + 1$. Since $2k^2 + k$ is an integer, n^2 satisfies the definition of "odd." However, this contradicts our assumption, so the theorem must be true.

A proof of the contrapositive of $p \Rightarrow q$ can be straightforwardly convert to a proof by contradiction of $p \Rightarrow q$: assume $p \wedge \neg q$, insert the proof of the contrapositive $\neg q \Rightarrow \neg p$, note that $\neg p$ contradicts our assumption $p \wedge \neg q$, and conclude that $p \Rightarrow q$ must be true. On the other hand, not every proof by contradiction can be straightforwardly converted to a proof of the contrapositive.

Theorem 1.24. *There does not exist an integer n such that $4n + 1 = 21$ and $n - 3 = 1$.*

Proof. For contradiction, assume that there exists an integer n such that $4n + 1 = 21$ and $n - 3 = 1$. The first equality implies $n = 5$, so $n - 3 = 2$. However, this contradicts the second equality. Thus, our assumption was incorrect, i.e., the theorem must be true.

Practice 1.25. *Prove that if $6 \mid n$, then $2 \mid n$.*

Practice 1.26. *Prove that if $a + b \geq 20$, then $a \geq 10$ or $b \geq 10$.*

2 Sets, Relations, and Functions

The previous chapter introduced the fundamentals of mathematical reasoning; this chapter introduces the core building blocks: sets, relations, and functions.

2.1 Sets

A *set*, commonly denoted by a capital letter, is a collection of objects called *elements*. If A is a set, then "$x \in A$" means x is an element of A and "$x \notin A$" means x is not an element of A. We let $|A|$ denote the *size* of A (i.e., the number of elements in A), and we let $\emptyset$ denote the empty set. (For now, we will not consider what $|A|$ means if A has infinitely many elements.) If every element in A is also in another set B, then A is a *subset* of B, and we write $A \subseteq B$. A useful fact is $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$. Sets A and B are *disjoint* if they have no elements in common.

One way to specify a set is to list its elements in curly braces, e.g., $A = \{2, 3, 5\}$. We can also use *set builder* notation, which has the following format: $A = \{x \mid p(x)\}$, where $p(x)$ is a predicate. This notation indicates that A is the set of elements x such that $p(x)$ is true. For example, $\{2, 3, 5\} = \{x \mid x < 7 \wedge x \text{ is prime}\}$.

Just as we can combine propositions to form other propositions (e.g., $p \vee q$), we can combine sets A and B to form other sets:

term	notation	definition
union of A and B	$A \cup B$	$\{x \mid x \in A \vee x \in B\}$
intersection of A and B	$A \cap B$	$\{x \mid x \in A \wedge x \in B\}$
difference of A and B	$A \setminus B$	$\{x \mid x \in A \wedge x \notin B\}$
complement of A	$\overline{A}$	$\{x \mid x \notin A\}$
power set of A	$\mathcal{P}(A)$	$\{X \mid X \subseteq A\}$

As mentioned in the previous chapter, we need a universe of discourse for some things (e.g., $\overline{A}$) to make sense.

Just as many theorems are of the form $p \Rightarrow q$, many theorems are of the form $A \subseteq B$. (In fact, $A \subseteq B$ is equivalent to $\forall x\colon x \in A \Rightarrow x \in B$.) To show $A \subseteq B$, we start with any element $a \in A$ and show that a must also be in B.

Theorem 2.1. *For any sets A and B, if $A \cap B = A$, then $A \subseteq B$.*

Proof. Consider any element $a \in A$. Since $A = A \cap B$, a must also be in $A \cap B$, so $a \in B$. Thus, $A \subseteq B$, as desired.

In the proof above, we should technically include the case where $A = \emptyset$. However, $\emptyset \subseteq B$ for every set B, so it is reasonable to omit this case. (In other words, $x \in \emptyset \Rightarrow x \in B$ is vacuously true for every set B.)

Practice 2.2. *Prove that if $A \cup B = B$, then $A \subseteq B$.*

Practice 2.3. *Prove that* $(A \setminus B) \cup (B \setminus C) \subseteq (A \cup B) \setminus (A \cap B \cap C)$.

The next theorem has the form $p \Leftrightarrow q$; we'll prove it by proving $p \Rightarrow q$ and $q \Rightarrow p$ separately.

Theorem 2.4. *For any sets* A *and* B, $A \subseteq B$ *iff* $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Proof. Suppose $A \subseteq B$ and consider any $S \in \mathcal{P}(A)$. Since $S \subseteq A$ and $A \subseteq B$, $S \subseteq B$. Thus, $S \in \mathcal{P}(B)$. Conversely, suppose $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. Since $A \subseteq A$, $A \in \mathcal{P}(A)$, so $A \in \mathcal{P}(B)$. This means $A \subseteq B$, as desired.

Similarly, to prove $A = B$, we often prove $A \subseteq B$ and $B \subseteq A$ separately. We'll illustrate this method by proving one of *De Morgan's Laws for Sets* (and leaving the other for practice).

Theorem 2.5. *For any sets* A *and* B, $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Proof. We first prove $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$. If $x \in \overline{A \cup B}$, then $x \notin A$ and $x \notin B$. This means $x \in \overline{A}$ and $x \in \overline{B}$, so $x \in \overline{A} \cap \overline{B}$.

Now we prove $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$. If $x \in \overline{A} \cap \overline{B}$, then $x \in \overline{A}$ and $x \in \overline{B}$. This means $x \notin A$ and $x \notin B$, so $x \notin A \cup B$, which implies $x \in \overline{A \cup B}$.

Practice 2.6. *Prove* $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Practice 2.7. *Prove that* $A \cup B = A \cap B$ *iff* $A = B$.

2.2 Relations

For any non-negative integer k, a *k-tuple* is an ordered collection (or *sequence*) of k objects called *components* (or *terms*); we write tuples in parentheses. A 2-tuple is also called an *ordered pair* (or just *pair*). Now we can define another set operation: $A \times B$ (read as "the Cartesian product of A and B," or "A cross B") is a set of pairs, where the first element is in A and the second is in B. In other words, $A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$. Notice that $|A \times B| = |A| \cdot |B|$. For example,

$$\{2, 3, 5\} \times \{2, 4\} = \{(2, 2), (2, 4), (3, 2), (3, 4), (5, 2), (5, 4)\}.$$

We let $A^2 = A \times A$, $A^3 = A \times A \times A$, etc.

Theorem 2.8. *If* $A \neq \emptyset$ *and* $A \times B = B \times C$, *then* $B = C$.

Proof. We'll only show $B \subseteq C$; the proof of $C \subseteq B$ is nearly identical. Consider any $b \in B$ and $a \in A$. Then $(a, b) \in A \times B$, so $(a, b) \in B \times C$, which implies $b \in C$.

A *relation* R from a set A to another set B is a subset of $A \times B$. Instead of writing "$(a, b) \in R$", we often write "$a \, R \, b$". The *domain* of R is $\mathrm{Dom}(R) = \{x \in A \mid \exists y \in B \colon x \, R \, y\}$, and the *range* of R is $\mathrm{Rng}(r) = \{y \in B \mid \exists x \in A \colon x \, R \, y\}$.

If A is a set, a *relation on* A is a relation from A to A. For example, $<$ ("is less than"), $=$ ("is equal to"), and "divides" are three relations on $\mathbb{Z}$. The table below, in which the universe of discourse is $\mathbb{Z}$, lists various properties that a relation on a set can satisfy. Note that a "×" indicates that the relation satisfies that property.

property	definition	$<$	$=$	"divides"
reflexive	$\forall a\colon a\,R\,a$		×	
symmetric	$\forall a, b\colon a\,R\,b \Rightarrow b\,R\,a$		×	
transitive	$\forall a, b, c\colon a\,R\,b \wedge b\,R\,c \Rightarrow a\,R\,c$	×	×	×

(The only reason "divides" is not reflexive is because 0 does not divide anything.)

Practice 2.9. *Prove that the last three columns in the table above are correct.*

Practice 2.10. *How many relations on* $\{0, 1\}$ *contain the pair* $(0, 1)$*?*

Practice 2.11. *Suppose* R *is a symmetric, transitive relation on* A *and* $\operatorname{Dom}(R) = A$*. Prove that* R *is reflexive.*

Since a relation is a set, we can combine relations together to form new relations by taking their union, intersection, etc.

Theorem 2.12. *The intersection of two symmetric relations is symmetric.*

Proof. Let R and S be symmetric relations and suppose $(a, b) \in R \cap S$; we want to show $(b, a) \in R \cap S$. Since $(a, b) \in R \cap S$, we have $a\,R\,b$ and $a\,S\,b$. Since R and S are symmetric, $b\,R\,a$ and $b\,S\,a$. Thus, $(b, a) \in R \cap S$, so $R \cap S$ is symmetric.

Practice 2.13. *Prove that the intersection of two transitive relations is transitive.*

Practice 2.14. *Prove or disprove: The union of two transitive relations is transitive.*

We can also construct other relations as follows:

- Suppose R is a relation from A to B and S is a relation from B to C. The *composition* of R and S is a relation from A to C defined by $S \circ R = \{(a, c) \mid \exists b\colon a\,R\,b \wedge b\,S\,c\}$.
- Suppose R is a relation from A to B. The *inverse* of R is a relation from B to A defined by $R^{-1} = \{(b, a) \mid (a, b) \in R\}$.

Intuitively, $S \circ R$ consists of R and S "linked" together and R^{-1} is the "flipped" version of R.

Theorem 2.15. *If R and S are relations, then $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.*

Proof. As usual, to prove $A = B$, we prove $A \subseteq B$ and $B \subseteq A$ separately. First, suppose $(a, b) \in (S \circ R)^{-1}$. This means $(b, a) \in (S \circ R)$, so there exists c such that $b \mathrel{R} c$ and $c \mathrel{S} a$, which is equivalent to $(c, b) \in R^{-1}$ and $(a, c) \in S^{-1}$. This implies $(a, b) \in R^{-1} \circ S^{-1}$.

The other part is similar: suppose $(a, b) \in R^{-1} \circ S^{-1}$. This means there exists c such that $(a, c) \in S^{-1}$ and $(c, b) \in R^{-1}$, which is equivalent to $c \mathrel{S} a$ and $b \mathrel{R} c$. This implies $(b, a) \in S \circ R$, so $(a, b) \in (R \circ S)^{-1}$.

Alternative Proof. Consider any (a, b). Notice the following:

$$\begin{aligned}
&(a, b) \in (S \circ R)^{-1} \\
&\text{iff } (b, a) \in S \circ R \\
&\text{iff } \exists c\colon b \mathrel{R} c \wedge c \mathrel{S} a \\
&\text{iff } \exists c\colon c \mathrel{R^{-1}} b \wedge a \mathrel{S^{-1}} c \\
&\text{iff } (a, b) \in R^{-1} \circ S^{-1}.
\end{aligned}$$

Thus, $(a, b) \in (S \circ R)^{-1}$ if and only if $(a, b) \in R^{-1} \circ S^{-1}$, which implies the theorem.

Highlight. The alternative proof above illustrates that we can sometimes prove $A = B$ using a one-part, rather than two-part, proof. But often, the proof of $A \subseteq B$ looks quite different from the proof of $B \subseteq A$, making it tricky to write a one-part proof.

Practice 2.16. *Prove that R is symmetric if and only if $R = R^{-1}$.*

Practice 2.17. *Prove that $T \circ (S \circ R) = (T \circ S) \circ R$.*

Equivalence Relations and Partitions

An *equivalence relation* is a relation that is reflexive, symmetric, and transitive. If R is an equivalence relation on A and $a \in A$, the set $[a]_R = \{b \mid a \mathrel{R} b\}$ is the *equivalence class* of a. (When R is clear from the context, we often write $[a]$ instead of $[a]_R$.)

Practice 2.18. *Consider the following relation on $\mathbb{Z}$:*

$$R = \{(a, b) \mid a + b \text{ is even}\}.$$

Prove that R is an equivalence relation, and describe each equivalence class.

A *partition* P of a set A is a collection (i.e., set) of sets such that (1) each $S \in P$ is a non-empty subset of A, (2) any two distinct sets in P are disjoint, and (3) the union of all the sets in P is equal to A. For example, $P = \{\{1\}, \{2, 5\}, \{3, 4\}\}$ is a partition of $A = \{1, 2, 3, 4, 5\}$.

Like a theorem, a *lemma* is just a true proposition. However, mathematicians typically use the word "lemma" to describe a proposition that helps them prove a theorem.

Lemma 2.19. *For any equivalence relation R, $x \mathrel{R} y$ if and only if $[x] = [y]$.*

Proof. Suppose $x \mathrel{R} y$; we will show $[x] \subseteq [y]$. (The proof of $[y] \subseteq [x]$ is similar.) Let $z \in [x]$, so $x \mathrel{R} z$. Since R is symmetric, we have $y \mathrel{R} x$; since R is transitive, $y \mathrel{R} z$. Thus, $z \in [y]$. Conversely, if $[x] = [y]$, then $y \in [x]$ (since $y \in [y]$), so $x \mathrel{R} y$.

Now we are ready to prove a theorem that connects equivalence relations and partitions:

Theorem 2.20. *For any equivalence relation R on a set A, the set of equivalence classes of R form a partition of A.*

Proof. Let P be the set of equivalence classes of R. First, since R is reflexive, $a \in [a]$ for all $a \in A$. Thus, every equivalence class is a non-empty subset of A, and the union of all the sets in P is equal to A.

Now suppose $[x]$ and $[y]$ are distinct equivalence classes; we need to show that $[x]$ and y are disjoint. By Lemma 2.19, $(x, y) \notin R$. For contradiction, assume there exists $z \in [x] \cap [y]$. This means $x \mathrel{R} z$ and $y \mathrel{R} z$; since R is symmetric and transitive, this implies $x \mathrel{R} y$, contradicting the fact that $(x, y) \notin R$.

The converse of the theorem is also true; we leave its proof for practice.

Practice 2.21. *Suppose P is a partition of A, and we define a relation R such that $a \mathrel{R} b$ if a and b are in the same set in P. Prove that R is an equivalence relation on A.*

2.3 Functions

Suppose A and B are sets. A *function* f from A to B is a relation from A to B that satisfies the following property: for every $a \in A$, there exists exactly one element $b \in B$ such that $(a, b) \in f$. In other words, f is a function if, for every input $a \in A$, f produces exactly one output in B.

If f is a function from A to B, we write $f \colon A \to B$, and $f(a) = b$ instead of $(a, b) \in f$. Recall that A is the domain of f; we refer to B as the *codomain*. If the domain contains a tuple $(a_1, \ldots, a_n)$, we typically omit a pair of parentheses by writing $f(a_1, \ldots, a_n)$ instead of $f((a_1, \ldots, a_n))$.

The table below, in which $A = B = \mathbb{Z}$, lists a few properties that a function can satisfy.

property	definition	$f(a) = a + 1$	$f(a) = 2a$
surjective ("onto")	$\forall b \exists a \colon f(a) = b$	×	
injective ("one-to-one")	$\forall a_1, a_2 \colon a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$	×	×
bijective	surjective and injective	×	

(A bijection is also known as a "one-to-one correspondence.")

Theorem 2.22. *The function $f\colon \mathbb{Z}^2 \to \mathbb{Z}$ defined by $f(x, y) = x + y$ is surjective but not injective.*

Proof. We first show that f is surjective by considering any $z \in \mathbb{Z}$. Notice that if $x = 0$ and $y = z$, then $f(x, y) = 0 + z = z$, so f is surjective. There are infinitely many counterexamples that show f is not injective; for example, $(1, 1) \neq (0, 2)$ but $f(1, 1) = 2 = f(0, 2)$.

Practice 2.23. *For each of the following functions from $\mathbb{Z}$ to $\mathbb{Z}$, determine if the function is surjective, injective, both, or neither. Explain your answers.*

1. $f(x) = 2$
2. $f(x) = 2x + 1$
3. $f(x) = x^2$

Practice 2.24. *Does there exist a function from $\mathbb{Z}$ to $\mathbb{Z}$ that is surjective but not injective? If so, describe an example; if not, explain why.*

Recall that if R is a relation from A to B and S is a relation from B to C, then their composition is a relation from A to C defined by $S \circ R = \{(a, c) \mid \exists b\colon a\,R\,b \wedge b\,S\,c\}$. Since every function is a relation, this also applies to functions: if $f\colon A \to B$ and $g\colon B \to C$ are functions, then $h = g \circ f$ is a function from A to C defined as $h = \{(a, c) \mid \exists b\colon f(a) = b \wedge g(b) = c\}$. Before we continue, let's verify that h is indeed a function (not just a relation):

Theorem 2.25. *If $f\colon A \to B$ and $g\colon B \to C$ are functions, then $h = g \circ f$ is a function from A to C.*

Proof. For all $a \in A$, there exists $b \in B$ such that $(a, b) \in f$ since f is a function, and there exists c such that $(b, c) \in g$ since g is a function, so $(a, c) \in h$.

Now suppose $(a, c_1) \in h$ and $(a, c_2) \in h$ for some $c_1, c_2 \in C$; we want to show that $c_1 = c_2$. By the definition of h, there exist $b_1, b_2 \in B$ such that

$$\begin{aligned} f(a) &= b_1 & g(b_1) &= c_1 \\ f(a) &= b_2 & g(b_2) &= c_2 \end{aligned}$$

Since f is a function, we must have $b_1 = b_2$, and since g is a function, we must have $c_1 = c_2$.

Now that we know $g \circ f$ is a function, let's prove a few theorems about it.

Theorem 2.26. *If $f\colon A \to B$ and $g\colon B \to C$ are surjective, then $g \circ f$ is surjective.*

Proof. Consider any $c \in C$; we want to show that there exists $a \in A$ such that $g(f(a)) = c$. Since g is surjective, there exists $b \in B$ such that $g(b) = c$. Moreover, since f is surjective, there exists $a \in A$ such that $f(a) = b$. Thus, we have $g(f(a)) = g(b) = c$, as desired.

Practice 2.27. *Prove that if f and g are injective, then $g \circ f$ is injective.*

Practice 2.28. *Prove that if f and g are bijective, then $g \circ f$ is bijective.*

Practice 2.29. *Prove or disprove: If f and g are functions, then $g \circ f = f \circ g$.*

If $f\colon A \to B$ is a function, then the *inverse* of f is the relation $f^{-1} = \{(b,a) \mid (a,b) \in f\} \subseteq B \times A$. The following theorem states that f^{-1} is a function if and only if f is injective.

Theorem 2.30. *Suppose f is a function with domain A. Then f is injective if and only if f^{-1} is a function from* $\operatorname{Rng}(f)$ *to A.*

Proof. Suppose f is injective and consider any $b \in \operatorname{Rng}(f)$. If there exist $a_1, a_2 \in A$ such that $(b, a_1) \in f^{-1}$ and $(b, a_2) \in f^{-1}$, then we must have $(a_1, b) \in f$ and (a_2, b) in f. Since f is injective, $a_1 = a_2$, so f^{-1} is a function from $\operatorname{Rng}(f)$ to A.

Now assume f^{-1} is a function from $\operatorname{Rng}(f)$ to A, and for contradiction, assume f is not injective. This means there exist $a_1, a_2 \in A$ such that $a_1 \neq a_2$ and $f(a_1) = f(a_2)$. If we let $b = f(a_1)$, this means $(b, a_1) \in f^{-1}$ and $(b, a_2) \in f^{-1}$, contradicting our assumption that f^{-1} is a function. Thus, f must be injective.

Practice 2.31. *Prove that if f is injective, then f^{-1} is also injective.*

Sequences and Summations

Recall that a *sequence* is an ordered collection of objections; repetitions are allowed in a sequence. We can define a sequence more formally as a function a whose domain is (1) $\{i, \ldots, j\}$ for some $i, j \in \mathbb{Z}$ such that $i < j$, or (2) $\{i, i+1, \ldots\}$ for some $i \in \mathbb{Z}$. In the first case, a is a finite sequence of length $j - i + 1$; in the second and third cases, a is an infinite sequence. If a is a sequence, we often refer to a_i instead of $a(i)$.

For example, one sequence of length 5 is $(2, 4, 6, 8, 10)$. Under our formal definition, we can describe this sequence as a function $a\colon \{1, 2, 3, 4, 5\} \to \mathbb{Z}$ defined by

$$a = \{(1,2), (2,4), (3,6), (4,8), (5,10)\},$$

but informally, we can write $a = (2, 4, 6, 8, 10)$. An example of an infinite sequence is the *Fibonacci sequence*, which is defined recursively:

$$a_1 = 1, \quad a_2 = 1$$
$$\forall n \geq 3\colon a_n = a_{n-1} + a_{n-2}$$

So the first few terms of the Fibonacci sequence are $(1, 1, 2, 3, 5, \ldots)$.

Practice 2.32. *Suppose the first few terms of an infinite sequence a are $(1, 7, 25, 79, \ldots)$. What is a simple formula for a_n?*

If a is a sequence, we can use *summation notation* to express the sum of the terms in a from a_i through a_j as follows:

$$\sum_{k=i}^{j} a_k = a_i + a_{i+1} + \cdots + a_j.$$

If S is a set (or sequence) of numbers, $\sum_{a \in S} a$ refers to the sum of every number $a \in S$. Similarly, we can denote the product from a_i through a_j by

$$\prod_{k=i}^{j} a_k = a_i \times a_{i+1} \times \cdots \times a_j,$$

and $\prod_{a \in S} a$ refers to the product of every number $a \in S$.

Practice 2.33. *What are the values of $\sum_{i=1}^{5} 2i$, $\sum_{i=1}^{5} i^2$, and $\prod_{i=3}^{5}(i+1)$?*

In Chapter 4, we will prove the following classic theorem:

Theorem 2.34. *For every positive integer n, $\sum_{i=1}^{n} i = n(n+1)/2$.*

3 Graphs

[unfinished]

4 Induction

[unfinished]

5 Cardinality

[unfinished]

6 Counting

[unfinished]

7 Probability

[unfinished]