Chapter 2

Background

This chapter covers a collection of topics that are not computability theory per se, but are needed for it. They are set apart so the rest of the text reads more smoothly as a reference, but we will cover them as needed when they become relevant.

2.1 First-Order Logic

In this section we learn a vocabulary for expressing formulas, logical sentences. This is useful for brevity ($x < y$ is much shorter than "x is less than y", and the savings grows as the statement becomes more complicated) but also for clarity. Expressing a mathematical statement symbolically can make it more obvious what needs to be done with it, and however carefully words are used they may admit some ambiguity.

We use lowercase Greek letters (mostly φ and ψ, sometimes ρ and θ) to represent formulas. The simplest formula is a single symbol (or assertion) which can be either true or false. There are several ways to modify formulas, which we'll step through one at a time.

The *conjunction* of formulas φ and ψ is written "φ and ψ", "$\varphi \wedge \psi$", or "φ & ψ". It is true when both φ and ψ are true, and false otherwise. Logically "and" and "but" are equivalent, and so are φ & ψ and ψ & φ, though in natural language there are some differences in connotation.

The *disjunction* of φ and ψ is written "φ or ψ", or "$\varphi \vee \psi$". It is false when both φ and ψ are false, and true otherwise. That is, $\varphi \vee \psi$ is true when *at least one* of φ and ψ is true; it is *inclusive or*. Natural language tends to use *exclusive or*, where only one of the clauses will be true, though there are exceptions. One such: "Would you like sugar or cream in your coffee?" Again, $\varphi \vee \psi$ and $\psi \vee \varphi$ are equivalent.

The *negation* of φ is written "not(φ)", "not-φ", "$\neg\varphi$", or "$\sim\varphi$". It is true when φ is false and false when φ is true. The potential difference from natural language negation is that $\neg\varphi$ must cover all cases where φ fails to hold, and in natural language the scope of a negation is sometimes more limited. Note that $\neg\neg\varphi = \varphi$.

How does negation interact with conjunction and disjunction? $\varphi \mathbin{\&} \psi$ is false when φ, ψ, or both are false, and hence its negation is $(\neg\varphi) \vee (\neg\psi)$. $\varphi \vee \psi$ is false only when both φ and ψ are false, and so its negation is $(\neg\varphi)\&(\neg\psi)$. We might note in the latter case that this matches up with natural language's "neither...nor" construction. These two negation rules are called *DeMorgan's Laws*.

Exercise 2.1.1. Simplify the following formulas.

(i) $\varphi \mathbin{\&} ((\neg\varphi) \vee \psi)$.

(ii) $(\varphi \mathbin{\&} (\neg\psi) \mathbin{\&} \theta) \vee (\varphi \mathbin{\&} (\neg\psi) \mathbin{\&} (\neg\theta))$.

(iii) $\neg((\varphi \mathbin{\&} \neg\psi) \mathbin{\&} \varphi)$.

There are two classes of special formulas to highlight now. A *tautology* is always true; the classic example is $\varphi \vee (\neg\varphi)$ for any formula φ. A *contradiction* is always false; here the example is $\varphi \mathbin{\&} (\neg\varphi)$. You will sometimes see the former expression denoted T (or $\top$) and the latter $\perp$.

To say φ *implies* ψ ($\varphi \to \psi$ or $\varphi \Rightarrow \psi$) means whenever φ is true, so is ψ. We call φ the *antecedent* and ψ the *consequent* of the implication. We also say φ is *sufficient* for ψ (since whenever we have φ we have ψ, though we may also have ψ when φ is false), and ψ is *necessary* for φ (since it is impossible to have φ without ψ). Clearly $\varphi \to \psi$ should be true when both formulas are true, and it should be false if φ is true but ψ is false. It is maybe not so clear what to do when φ is false; this is clarified by rephrasing implication as disjunction (which is often how it is defined in the first place). $\varphi \to \psi$ means either ψ holds or φ fails; i.e., $\psi \vee (\neg\varphi)$. The truth of that statement lines up with our assertions earlier, and gives truth values for when φ is false – namely, that the implication is true. Another way to look at this is to say $\varphi \to \psi$ is only false when proven false, and that can only happen when you see a true antecedent and a false consequent. From this it is clear that $\neg(\varphi \to \psi)$ is $\varphi \mathbin{\&} (\neg\psi)$.

There is an enormous difference between implication in natural language and implication in logic. Implication in natural language tends to connote causation, whereas the truth of $\varphi \to \psi$ need not give any connection at all between the meanings of φ and ψ. It could be that φ is a contradiction, or that ψ is a tautology. Also, in natural language we tend to dismiss implications as irrelevant or meaningless when the antecedent is false, whereas to have a full and consistent logical theory we cannot throw those cases out.

Example 2.1.2. The following are true implications:

- If fish live in the water, then earthworms live in the soil.
- If rabbits are aquamarine blue, then earthworms live in the soil.

- If rabbits are aquamarine blue, then birds drive cars.

The negation of the final statement is "Rabbits are aquamarine blue but birds do not drive cars."

The statement "If fish live in the water, then birds drive cars" is an example of a false implication.

Equivalence is two-way implication and indicated by a double-headed arrow: $\varphi \leftrightarrow \psi$ or $\varphi \Leftrightarrow \psi$. It is an abbreviation for $(\varphi \to \psi)\ \&\ (\psi \to \varphi)$, and is true when φ and ψ are either both true or both false. Verbally we might say "φ if and only if ψ", which is often abbreviated to "φ iff ψ". In terms of just conjunction, disjunction, and negation, we may write equivalence as $(\varphi\ \&\ \psi) \vee ((\neg\varphi)\ \&\ (\neg\psi))$. Its negation is *exclusive or*, $(\varphi \vee \psi)\ \&\ \neg(\varphi\ \&\ \psi)$.

Exercise 2.1.3. Negate the following statements.

(i) 56894323 is a prime number.

(ii) If there is no coffee, I drink tea.

(iii) John watches but does not play.

(iv) I will buy the blue shirt or the green one.

Exercise 2.1.4. Write the following statements using standard logical symbols.

(i) φ if ψ.

(ii) φ only if ψ.

(iii) φ unless ψ.

As an aside, let us have a brief introduction to *truth tables*. These are nothing more than a way to organize information about logical statements. The leftmost columns are generally headed by the individual propositions, and under those headings occur all possible combinations of truth and falsehood. The remaining columns are headed by more complicated formulas that are build from the propositions, and the lower rows have T or F depending on the truth or falsehood of the header formula when the propositions have the true/false values in the beginning of that row. Truth tables aren't particularly relevant to our use for this material, so I'll leave you with an example and move on.

φ	ψ	$\neg\varphi$	$\neg\psi$	$\varphi\ \&\ \psi$	$\varphi \vee \psi$	$\varphi \to \psi$	$\varphi \leftrightarrow \psi$
T	T	F	F	T	T	T	T
T	F	F	T	F	T	F	F
F	T	T	F	F	T	T	F
F	F	T	T	F	F	T	T

If we stop here, we have *propositional* (or *sentential*) logic. These formulas usually look something like $[A \vee (B\&C)] \to C$ and their truth or falsehood depends on the truth or falsehood of the assertions A, B, and C. We will continue on to *predicate* logic, which replaces these assertions with statements such as $(x < 0)$ & $(x + 100 > 0)$, which will be true or false depending on the value substituted for the variable x. We will be able to turn those formulas into statements which are true or false inherently via *quantifiers*. Note that writing $\varphi(x)$ indicates the variable x appears in the formula φ.

The *existential* quantification $\exists x$ is read "there exists x". The formula $\exists x\varphi(x)$ is true if for some value n the unquantified formula $\varphi(n)$ is true. *Universal* quantification, on the other hand, is $\forall x\varphi(x)$ ("for all x, $\varphi(x)$ holds"), true when no matter what n we fill in for x, $\varphi(n)$ is true.

Quantifiers must have a specified set of values to range over, because the truth value of a formula may be different depending on this *domain of quantification*. For example, take the formula

$$(\forall x)(x \neq 0 \to (\exists y)(xy = 1)).$$

This asserts every nonzero x has a multiplicative inverse. If we are letting our quantifiers range over the real numbers or the rational numbers, this statement is true, because the reciprocal of x is available to play the role of y. However, in the integers or natural numbers this is false, because $1/x$ is only in the domain when x is ± 1.

Introducing quantification opens us up to two kinds of logical formulas. If all variables are quantified over (*bound* variables), then the formula is called a *sentence*. If there are variables that are not in the scope of any quantifier (*free* variables), the formula is called a *predicate*. The truth value of a predicate depends on what values are plugged in for the free variables; a sentence has a truth value period. For example, $(\forall x)(\exists y)(x < y)$ is a sentence, and it is true in all our usual domains of quantification. The formula $x < y$ is a predicate, and it will be true or false depending on whether the specific values plugged in for x and y satisfy the inequality.

Exercise 2.1.5. Write the following statements as formulas, specifying the domain of quantification.

(i) 5 is prime.

(ii) For any number x, the square of x is nonnegative.

(iii) There is a smallest positive integer.

Exercise 2.1.6. Consider the natural numbers, integers, rational numbers, and real numbers. Over which domains of quantification are each of the following statements true?

(i) $(\forall x)(x \geq 0)$.

(ii) $(\exists x)(5 < x < 6)$.

(iii) $(\forall x)((x^2 = 2) \rightarrow (x = 5))$.

(iv) $(\exists x)(x^2 - 1 = 0)$.

(v) $(\exists x)(x^3 + 8 = 0)$.

(vi) $(\exists x)(x^2 - 2 = 0)$.

When working with multiple quantifiers the order of quantification can matter a great deal. For example, take the two formulas

$$\varphi = (\forall x)(\exists y)(x \cdot x = y);$$

$$\psi = (\exists y)(\forall x)(x \cdot x = y).$$

φ says "every number has a square" and is true in our typical domains. However, ψ says "there is a number which is all other numbers' square" and is true only if you are working over the domain containing only 0 or only 1.

Exercise 2.1.7. Over the real numbers, which of the following statements are true? Over the natural numbers?

(i) $(\forall x)(\exists y)(x + y = 0)$.

(ii) $(\exists y)(\forall x)(x + y = 0)$.

(iii) $(\forall x)(\exists y)(x \leq y)$.

(iv) $(\exists y)(\forall x)(x \leq y)$.

(v) $(\exists x)(\forall y)(x < y^2)$.

(vi) $(\forall y)(\exists x)(x < y^2)$.

(vii) $(\forall x)(\exists y)(x \neq y \rightarrow x < y)$.

(viii) $(\exists y)(\forall x)(x \neq y \rightarrow x < y)$.

The order of operations when combining quantification with conjunction or disjunction can also make the difference between truth and falsehood.

Exercise 2.1.8. Over the real numbers, which of the following statements are true? Over the natural numbers?

(i) $(\forall x)(x \geq 0 \vee x \leq 0)$.

(ii) $(\forall x)(x \geq 0) \vee (\forall x)(x \leq 0)$.

(iii) $(\exists x)(x \leq 0 \mathbin{\&} x \geq 5)$.

(iv) $(\exists x)(x \leq 0) \mathbin{\&} (\exists x)(x \geq 5)$.

How does negation work for quantifiers? If $\exists x \varphi(x)$ fails, it means no matter what value we fill in for x the formula obtained is false – i.e., $\neg(\exists x \varphi(x)) \leftrightarrow \forall x(\neg\varphi(x))$. Likewise, $\neg(\forall x \varphi(x)) \leftrightarrow \exists x(\neg\varphi(x))$: if φ does not hold for all values of x, there must be an example for which it fails. If we have multiple quantifiers, the negation walks in one by one, flipping each quantifier and finally negating the predicate inside. For example:

$$\neg[(\exists x)(\forall y)(\forall z)(\exists w)\varphi(x,y,z,w)] \leftrightarrow (\forall x)(\exists y)(\exists z)(\forall w)(\neg\varphi(x,y,z,w)).$$

Exercise 2.1.9. Negate the following sentences.

(i) $(\forall x)(\exists y)(\forall z)((z < y) \rightarrow (z < x))$.

(ii) $(\exists x)(\forall y)(\exists z)(xz = y)$.

(iii) $(\forall x)(\forall y)(\forall z)(y = x \ \vee \ z = x \ \vee \ y = z)$.
(bonus: over what domains of quantification would this be true?)

A final notational comment: you will sometimes see the symbols $\exists^\infty$ and $\forall^\infty$. The former means "there exist infinitely many"; $\exists^\infty x\varphi(x)$ is shorthand for $\forall y \exists x(x > y \mathbin{\&} \varphi(x))$ (no matter how far up we go, there are still examples of φ above us). The latter means "for all but finitely-many"; $\forall^\infty x \varphi(x)$ is shorthand for $\exists y \forall x((x > y) \rightarrow \varphi(x))$ (we can get high enough up to bypass all the failed cases of φ). Somewhat common in predicate logic but less so in computability theory is $\exists! x$, which means "there exists a unique x." The sentence $(\exists! x)\varphi(x)$ expands into $(\exists x)(\forall y)(\varphi(x) \mathbin{\&} (\varphi(y) \rightarrow (x = y)))$.

2.2 Sets

A *set* is a collection of objects. If x is an element of a set A, we write $x \in A$, and otherwise $x \notin A$. Two sets are *equal* if they have the same elements; if they have no elements in common they are called *disjoint*. The set A is a *subset* of a set B if all of the elements of A are also elements of B; this is notated $A \subseteq B$. If we know that A is not equal to B, we may write $A \subset B$ or (to emphasize the non-equality) $A \subsetneq B$. The collection of all subsets of A is denoted $\mathcal{P}(A)$ and called the *power set* of A.

We may write a set using an explicit list of its elements, such as {red, blue, green} or $\{5, 10, 15, \ldots\}$. When writing down sets, order does not matter and repetitions do not count. That is, $\{1,2,3\}$, $\{2,3,1\}$, and $\{1,1,2,2,3,3\}$ are all representations of the same set. We may also write it in notation that may be familiar to you from calculus:

$$A = \{x : (\exists y)(y^2 = x)\}$$

This is the set of all values we can fill in for x that make the logical predicate $(\exists y)(y^2 = x)$ true. We are always working within some fixed *universe*, a set which contains all of our sets. The domain of quantification is all elements of the universe, and hence the contents of the set above will vary depending on what our universe is. If we are living in the integers it is the set of perfect squares; if we are living in the real numbers it is the set of all non-negative numbers.

Given two sets, we may obtain a third from them in several ways. First there is *union*: $A \cup B$ is the set containing all elements that appear in at least one of A and B. Next *intersection*: $A \cap B$ is the set containing all elements that appear in both A and B. We can subtract: $A - B$ contains all elements of A that are *not* also elements of B. You will often see $A \setminus B$ for set subtraction, but we will use ordinary minus because the slanted minus is sometimes given a different meaning in computability theory. Finally, we can take their *Cartesian product*: $A \times B$ consists of all ordered pairs that have their first entry an element of A and their second an element of B. We may take the product of more than two sets to get ordered triples, quadruples, quintuples, and in general *n-tuples*. If we take the Cartesian product of n copies of A, we may abbreviate $A \times A \times \ldots \times A$ as A^n. A generic ordered n-tuple from A^n will be written $(x_1, x_2, \ldots, x_n)$, where x_i are all elements of A.

Example 2.2.1. Let $A = \{x, y\}$ and $B = \{y, z\}$. Then $A \cup B = \{x, y, z\}$, $A \cap B = \{y\}$, $A - B = \{x\}$, $B - A = \{z\}$, $A \times B = \{(x, y), (x, z), (y, y), (y, z)\}$, and $\mathcal{P}(A) = \{\emptyset, \{x\}, \{y\}, \{x, y\}\}$.

The sets we will use especially are $\emptyset$ and $\mathbb{N}$. The former is the *empty set*, the set with no elements. The latter is the *natural numbers*, the set $\{0, 1, 2, 3, \ldots\}$. In computability, we often use lowercase omega, ω, to denote the natural numbers, but in these notes we will be consistent with $\mathbb{N}$. On occasion we may also refer to $\mathbb{Z}$ (the integers), $\mathbb{Q}$ (the rational numbers), or $\mathbb{R}$ (the real numbers).

We will assume unless otherwise specified that all of our sets are subsets of $\mathbb{N}$. That is, we assume $\mathbb{N}$ is our universe. When a universe is fixed we can define *complement*. The complement of A, denoted $\overline{A}$, is all the elements of $\mathbb{N}$ that are not in A; i.e., $\overline{A} = \mathbb{N} - A$.

Exercise 2.2.2. Convert the list or description of each of the following sets into notation using a logical predicate. Assume the domain of quantification is $\mathbb{N}$.

(i) $\{2, 4, 6, 8, 10, \ldots\}$.

(ii) $\{4, 5, 6, 7, 8\}$.

(iii) The set of numbers that are cubes.

(iv) The set of pairs of numbers such that one is twice the other (in either order).

(v) The intersection of the set of square numbers and the set of numbers that are divisible by 3.

(vi) [For this and the next two, you'll need to use $\in$ in your logical predicate.] $A \cup B$ for sets A and B.

(vii) $A \cap B$ for sets A and B.

(viii) $A - B$ for sets A and B.

Exercise 2.2.3. For each of the following sets, list (a) the elements of X, and (b) the elements of $\mathcal{P}(X)$.

(i) $X = \{1, 2\}$

(ii) $X = \{1, 2, \{1, 2\}\}$

(iii) $X = \{1, 2, \{1, 3\}\}$

Exercise 2.2.4. Work inside the finite universe $\{1, 2, \ldots, 10\}$. Define the following sets:

$A = \{1, 3, 5, 7, 9\}$
$B = \{1, 2, 3, 4, 5\}$
$C = \{2, 4, 6, 8, 10\}$
$D = \{7, 9\}$
$E = \{4, 5, 6, 7\}$

(i) Find all the subset relationships between pairs of the sets above.

(ii) Which pairs, if any, are disjoint?

(iii) Which pairs, if any, are complements?

(iv) Find the following unions and intersections: $A \cup B$, $A \cup D$, $B \cap D$, $B \cap E$.

Exercise 2.2.5. Prove that $A \cup B = (A - B) \cup (B - A) \cup (A \cap B)$ for any sets A and B.

When sets are given by descriptions instead of explicit lists, we must prove one set is a subset of another by taking an arbitrary element of the first set and showing it is also a member of the second set. For example, to show the set of people eligible for President of the United States is a subset of the set of people over 30, we might say: Consider a person in the first set. That person must meet the criteria listed in the US Constitution, which includes being at least 35 years of age. Since 35 is more than 30, the person we chose is a member of the second set.

We can further show that this containment is proper, by demonstrating a member of the second set who is not a member of the first set. For example, a 40-year-old Japanese citizen.

Exercise 2.2.6. Prove that the set of squares of even numbers, $\{x : \exists y(x = (2y)^2)\}$, is a proper subset of the set of multiples of 4, $\{x : \exists y(x = 4y)\}$.

Our final topic in the realm of sets is *cardinality.* The cardinality of a finite set is the number of elements in it. For example, the cardinality of the set of positive integer divisors of 6 is 4: $|\{1, 2, 3, 6\}| = 4$. When we get to infinite sets, cardinality separates them by "how infinite" they are. We'll get to its genuine definition in §2.3, but it is fine now and later to think of cardinality as a synonym for size. The way to tell whether set A is bigger than set B is to look for a one-to-one function from A into B. If no such function exists, then A is bigger than B, and we write $|B| < |A|$. The most important result is that $|A| < |\mathcal{P}(A)|$ for *any* set A.

If we know there is a one-to-one function from A into B but we don't know about the reverse direction, we write $|A| \leq |B|$. If we have injections both ways, $|A| = |B|$. It is a significant theorem of set theory that having injections from A to B and from B to A is equivalent to having a bijection between A and B; the fact that this is difficult is a demonstration of the fact that things get weird when you work in the infinite world. Another key fact (for set theorist; not so much for us) is *trichotomy*: for any two sets A and B, exactly one of $|A| < |B|$, $|A| > |B|$, or $|A| = |B|$ is true.

Infinite cardinalities are divided into two categories. A set is *countably infinite* if it has the same cardinality as the natural numbers. The integers and the rational numbers are important examples of countably infinite sets. The term *countable* is used by some authors to mean "countably infinite", and by others to mean "finite or countably infinite", so you often have to rely on context. To prove that a set is countable, you must demonstrate it is in bijection with the natural numbers – that is, that you can count the objects of your set 1, 2, 3, 4, . . . , and not miss any. We'll come back to this in §4.1; for now you can look in the appendices to find Cantor's proofs that the rationals are countable and the reals are not (§A.3).

The rest of the infinite cardinalities are called *uncountable*, and for our purposes that's about as fine-grained as it gets. The fundamental notions of computability theory live in the world of countable sets, and the only uncountable ones we get to are those which can be approximated in the countable world.

2.3 Relations

The following definition is not the most general case, but we'll start with it.

Definition 2.3.1. A *relation* $R(x, y)$ on a set A is a logical formula that is true or false of any pair $(x, y) \in A^2$, never undefined.

We also think of relations as subsets of A^2 consisting of the pairs for which the relation is true. For example, in the set $A = \{1, 2, 3\}$, the relation $<$ consists of $\{(1, 2), (1, 3), (2, 3)\}$ and the relation $\leq$ is the union of $<$ with $\{(1, 1), (2, 2), (3, 3)\}$. Note that the order matters: although $1 < 2$, $2 \not< 1$, so $(2, 1)$ is not in $<$. The first definition shows you why these are called *relations*; we think of R as being true when the values filled in for x and y have some relationship to each other. The set-theoretic definition is generally more useful, however.

More generally, we may define *n-ary* relations on a set A as logical formulas that are true or false of any n-tuple (ordered set of n elements) of A, or alternatively as subsets of A^n. For $n = 1, 2, 3$ we refer to these relations as *unary*, *binary*, and *ternary*, respectively.

Exercise 2.3.2. Prove the two definitions of relation are equivalent. That is, prove that every logical predicate corresponds to a unique set, and vice-versa.

Exercise 2.3.3. Let $A = \{a, b, c, d, e\}$.

(i) What is the ternary relation R on A defined by $(x, y, z) \in R \;\Leftrightarrow\; (xyz$ is an English word)?

(ii) What is the unary relation on A which is true of elements of A that are vowels?

(iii) What is the complement of the relation in (2)? We may describe it in two ways: as "the negation of the relation in (2)", and how?

(iv) How many elements are in the 5-ary relation R defined by $(v, w, x, y, z) \in R$ $\Leftrightarrow$ (v, w, x, y, z are all *distinct* elements of A)?

(v) How many unary relations are possible on A? What other collection associated with A does the collection of all unary relations correspond to?

Exercise 2.3.4. How many n-ary relations are possible on an m-element set?

We tend to focus on binary relations, since most of our common, useful examples are binary: $<, \leq, =, \neq, \subset, \subseteq$. Binary relations may have certain properties:

- Reflexivity: $(\forall x)R(x, x)$
- Symmetry: $(\forall x, y)[R(x, y) \rightarrow R(y, x)]$
  i.e., $(\forall x, y)[(R(x, y)\ \&\ R(y, x)) \;\vee\; (\neg R(x, y)\ \&\ \neg R(y, x))]$
- Antisymmetry: $(\forall x, y)[(R(x, y)\ \&\ R(y, x)) \rightarrow x = y]$

- Transitivity: $(\forall x, y, z)[(R(x,y)\ \&\ R(y,z)) \rightarrow R(x,z)]$

I want to point out that reflexivity is a property of possession: R must have the reflexive pairs (the pairs (x,x)). Antisymmetry is, loosely, a property of nonpossession. Symmetry and transitivity, on the other hand, are *closure* properties: **if** R has certain pairs, **then** it must also have other pairs. Those conditions may be met either by adding in the pairs that are consequences of the pairs already present, or omitting the pairs that are requiring such additions. In particular, the empty relation is symmetric and transitive, though it is not reflexive.

Exercise 2.3.5. Is $=$ reflexive? Symmetric? Antisymmetric? Transitive? How about $\neq$?

Exercise 2.3.6. For finite relations we may check these properties by hand. Let $A = \{1, 2, 3, 4\}$.

(a) What is the smallest binary relation on A that is reflexive?

(b) Define the following binary relations on A:

$$R_1 = \{(2,3), (3,4), (4,2)\}$$

$$R_2 = \{(1,1), (1,2), (2,1), (2,2)\}$$

$$R_3 = \{(1,1), (1,2), (2,2), (2,3), (3,3), (3,4), (4,4)\}$$

For each of those relations, answer the following questions.

(i) Is the relation reflexive? Symmetric? Antisymmetric? Transitive?

(ii) If the relation is not reflexive, what pairs need to be added to make it reflexive?

(iii) If the relation is not symmetric, what pairs need to be added to make it symmetric?

(iv) If the relation is not transitive, what pairs need to be added to make it transitive?

(v) If the relation is not antisymmetric, which pairs violate the antisymmetry?

Exercise 2.3.7. Let $A = \{1, 2, 3\}$. Define binary relations on A with the following combinations of properties:

(i) Reflexive but neither symmetric nor transitive.

(ii) Symmetric but neither reflexive nor transitive.

(iii) Transitive but neither reflexive nor symmetric.

(iv) Symmetric and transitive but not reflexive.

(v) Reflexive and transitive but not symmetric.

(vi) Reflexive and symmetric but not transitive.

(vii) Reflexive, symmetric, and transitive.

(viii) None of reflexive, symmetric, or transitive.

Exercise 2.3.8. Suppose R and S are binary relations on A. For each of the following properties, if R and S possess the property, must $R \cup S$ possess it? $R \cap S$?

(i) Reflexivity

(ii) Symmetry

(iii) Antisymmetry

(iv) Transitivity

Graphically, if the elements of A are vertices of a graph, and a directed edge (arrow) from vertex x to vertex y means $R(x, y)$, these properties may be stated as:

- Reflexivity: every vertex has a loop.
- Symmetry: for any pair of vertices, either there are edges in both directions or there are no edges between them.
- Antisymmetry: for two distinct vertices there is at most one edge connecting them.
- Transitivity: if there is a path of edges from one vertex to another (always proceeding in the direction of the edge), there is an edge directly connecting them, in the same direction as the path.

Certain subsets of these properties define classes of relations which are of particular importance. We'll consider two, starting with equivalence relations.

Definition 2.3.9. An *equivalence relation* is a binary relation that is reflexive, symmetric, and transitive.

The quintessential equivalence relation is equality, which is the relation consisting of only the reflexive pairs. What is special about an equivalence relation? We can take a *quotient structure* whose elements are *equivalence classes*.

Definition 2.3.10. Let R be an equivalence relation on A. The *equivalence class* of some $x \in A$ is the set $[x] = \{y \in A : R(x, y)\}$.

Exercise 2.3.11. Let R be an equivalence relation on A and let x, y be elements of A. Prove that either $[x] = [y]$ or $[x] \cap [y] = \emptyset$.

In short, an equivalence relation puts all the elements of the set into boxes so that each element is unambiguously assigned to a single box. Then we can consider the boxes themselves as elements.

Definition 2.3.12. Given a set A and an equivalence relation R on A, the *quotient of A by R*, A/R, is the set whose elements are the equivalence classes of A under R.

Now we can define cardinality more correctly. The cardinality of a set is the equivalence class it belongs to under the equivalence relation of bijectivity, so cardinalities are elements of the quotient of the collection of all sets under that relation.

Exercise 2.3.13. Let A be the set $\{1, 2, 3, 4, 5\}$, and let R be the binary relation on A that consists of the reflexive pairs together with $(1, 2)$, $(2, 1)$, $(3, 4)$, $(3, 5)$, $(4, 3)$, $(4, 5)$, $(5, 3)$, $(5, 4)$.

(i) Represent R as a graph.

(ii) How many elements does A/R have?

(iii) Write out the sets $[1]$, $[2]$, and $[3]$.

Exercise 2.3.14. A *partition* of a set A is a collection of disjoint subsets of A with union equal to A. Prove that any partition of A determines an equivalence relation on A.

Exercise 2.3.15. Let $R(m, n)$ be the relation on $\mathbb{Z}$ that holds when $m - n$ is a multiple of 3.

(i) Prove that R is an equivalence relation.

(ii) What are the equivalence classes of 1, 2, and 3?

(iii) What are the equivalence classes of -1, -2, and -3?

(iv) Prove that $\mathbb{Z}/R$ has three elements.

Exercise 2.3.16. Let $R(m, n)$ be the relation on $\mathbb{N}$ that holds when $m - n$ is even.

(i) Prove that R is an equivalence relation.

(ii) What are the equivalence classes of R? Give a concise verbal description of each.

The two exercises above are examples of *modular arithmetic*, also sometimes called *clock-face arithmetic* because its most widespread use in day-to-day life is telling what time it will be some hours from now. This is a notion that is used only in $\mathbb{N}$ and $\mathbb{Z}$. The idea of modular arithmetic is that it is only the number's remainder upon division by a fixed value that matters. For clock-face arithmetic that value is 12; we say we are working *modulo 12*, or just *mod 12*, and the equivalence classes are represented by the numbers 0 through 11 (in mathematics; 1 through 12 in usual life). The fact that if it is currently 7:00 then in eight hours it will be 3:00 would be written as the equation

$$7 + 8 = 3 \pmod{12},$$

where $\equiv$ is sometimes used in place of the equals sign.

Exercise 2.3.17. (i) Exercises 2.3.14 and 2.3.15 consider equivalence relations that give rise to arithmetic mod k for some k. For each, what is the correct value of k?

(ii) Describe the equivalence relation on $\mathbb{Z}$ that gives rise to arithmetic mod 12.

(iii) Let m, n, and p be integers. Prove that

$$n = m \pmod{12} \implies n + p = m + p \pmod{12}.$$

That is, it doesn't matter which representative of the equivalence class you pick to do your arithmetic.

The second important class of relations we will look at is partial orders.

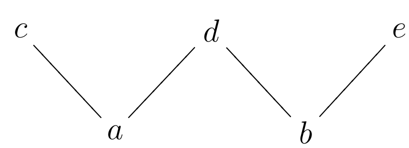
Definition 2.3.18. A *partial order* $\leq$ on a set A is a binary relation that is reflexive, antisymmetric, and transitive. A with $\leq$ is called a *partially ordered set*, or *poset*.

In a poset, given two nonequal elements of A, either one is strictly greater than the other or they are incomparable. If all pairs of elements are comparable, the relation is called a *total order* or *linear order* on A.

Example 2.3.19. Let $A = \{a, b, c, d, e\}$ and define $\leq$ on A as follows:

- $(\forall x \in A)(x \leq x)$
- $a \leq c$, $a \leq d$
- $b \leq d$, $b \leq e$

We could graph this as follows:



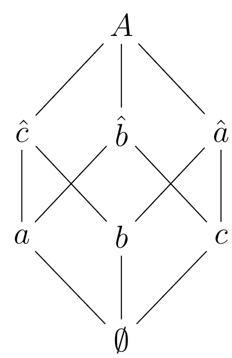
Example 2.3.20. $\mathcal{P}(\mathbb{N})$ ordered by subset inclusion is a partially ordered set.

It is easy to check the relation $\subseteq$ is reflexive, transitive, and antisymmetric. Not every pair of elements is comparable: for example, neither $\{1,2,3\}$ nor $\{4,5,6\}$ is a subset of the other. This poset actually has some very nice properties that not every poset has: it has a top element ($\mathbb{N}$) and a bottom element ($\emptyset$), and every pair of elements has both a least upper bound (here, the union) and a greatest lower bound (the intersection).

If we were to graph this, it would look like an infinitely-faceted diamond with points at the top and bottom.

Example 2.3.21. Along the same lines as Example 2.3.19, we can consider the power set of a finite set, and then we can graph the poset that results.

Let $A = \{a, b, c\}$. Denote the set $\{a\}$ by a and the set $\{b, c\}$ by $\hat{a}$, and likewise for the other three elements. The graph is then as follows:



You could think of this as a cube standing on one corner.

Exercise 2.3.22. How many partial orders are possible on a set of two elements? Three elements?

Our final note is to point out relations generalize functions. The function $f : A \to A$ may be written as a binary relation on A consisting of the pairs $(x, f(x))$. A binary relation R, conversely, represents a function whenever $[(x, y) \in R \ \& \ (x, z) \in R] \to y = z$ (the vertical line rule for functions).[1] We can ramp this up even further to multivariable functions, functions from A^n to A, by considering $(n+1)$-ary relations. The first n places represent the input and the last one the output. The advantage to this is consolidation; we can prove many things about functions by proving them for relations in general.

[1]You might object that this does not require every element of A be in the domain of the function. We will not be concerned by that; see §2.5.

2.4 Recursion and Induction

Recursive definitions and proofs by induction are essentially opposite sides of the same coin. Both have some specific starting point, and then a way to extend from there via a small set of operations. For induction, you might be proving some property P holds of all the natural numbers. To do so, you prove that P holds of 0, and then prove that *if* P holds of some $n \geq 0$, *then* P also holds of $n+1$. To recursively define a class of objects C, you give certain simple examples of objects in C, and then combination and extension operations such that applying those operations to elements of C gives results still in C. They relate more deeply than just appearance, though. We'll tackle induction, then recursion, then induction again.

Induction on $\mathbb{N}$

The basic premise of induction is that if you can start, and once you start you know how to keep going, then you will get all the way to the end. If I can get on the ladder, and I know how to get from one rung to the next, I can get to the top of the ladder.

Principle of Mathematical Induction, basic form:

If S is a subset of the positive integers such that $1 \in S$ and $n \in S$ implies $n+1 \in S$ for all n, then S contains all of the positive integers. [We may need the beginning to be 0 or another value depending on context.]

In general you want to use induction to show that some property holds no matter what integer you feed it, or no matter what size finite set you are dealing with. The proofs always have a *base case*, the case of 1 (or wherever you're actually starting). Then they have the *inductive step*, the point where you assume the property holds for some unspecified n and then show it holds for $n+1$.

Example 2.4.1. Prove that for every positive integer n, the equation

$$1 + 3 + 5 + \ldots + (2n-1) = n^2$$

holds.

Proof. Base case: For $n = 1$, the equation is $1 = 1^2$, which is true.
Inductive step: Assume that $1 + 3 + 5 + \ldots + (2n-1) = n^2$ for some $n \geq 1$. To show that it holds for $n+1$, add $2(n+1) - 1$ to each side, in the simplified form $2n+1$:

$$1 + 3 + 5 + \ldots + (2n-1) + (2n+1) = n^2 + 2n + 1 = (n+1)^2.$$

Since the equation above is that of the theorem, for $n+1$, by induction the equation holds for all n. $\square$

For the next example we need to know a *convex* polygon is one where all the corners point out. The outline of a big block-printed V is a polygon, but not a convex one. The importance of this will be that if you connect two corners of a convex polygon with a straight line segment, the segment will lie entirely within the polygon.

As you get more comfortable with induction, you can write it in a more natural way, without segmenting off the base case and inductive step portions of the argument. We'll do that here. Notice the base case is not 0 or 1 for this proof.

Example 2.4.2. For $n > 2$, the sum of angle measures of the interior angles of a convex polygon of n vertices is $(n-2) \cdot 180°$.

Proof. We work by induction. For $n = 3$, the polygon in question is a triangle, and it has interior angles which sum to $180° = (3-2) \cdot 180°$.

Assume the theorem holds for some $n \geq 3$ and consider a convex polygon with $n+1$ vertices. Let one of the vertices be named x, and pick a vertex y such that along the perimeter from x in one direction there is a single vertex between x and y, and in the opposite direction, $(n+1)-3 = n-2$ vertices. Join x and y by a new edge, dividing our original polygon into two polygons. The new polygons' interior angles together sum to the sum of the original polygon's interior angles. One of the new polygons has 3 vertices and the other n vertices (x, y, and the $n-2$ vertices between them). The triangle has interior angle sum $180°$, and by the inductive hypothesis the n-gon has interior angle sum $(n-2) \cdot 180°$. The $n+1$-gon therefore has interior angle sum $180° + (n-2)180° = (n+1-2) \cdot 180°$, as desired. $\square$

Notice also in this example that we used the base case as part of the inductive step, since one of the two polygons was a triangle. This is not uncommon.

Exercise 2.4.3. Prove the following statements by induction.

(i) For every positive integer n,

$$1 + 4 + 7 + \ldots + (3n-2) = \frac{1}{2}n(3n-1).$$

(ii) For every positive integer n,

$$2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 2.$$

(iii) For every positive integer n, $\dfrac{n^3}{3} + \dfrac{n^5}{5} + \dfrac{7n}{15}$ is an integer.

(iv) For every positive integer n, $4^n - 1$ is divisible by 3.

(v) The sequence $a_0, a_1, a_2, \ldots$ defined by $a_0 = 0$, $a_{n+1} = \frac{a_n+1}{2}$ is bounded above by 1.

(vi) Recall that for a binary operation $*$ on a set A associativity is defined as "for any x, y, z, $(x * y) * z = x * (y * z)$." Use induction to prove that for any collection of n elements from A put together with $*$, $n \geq 3$, any grouping of the elements which preserves order will give the same result.

Exercise 2.4.4. A *graph* consists of *vertices* and *edges*. Each edge has a vertex at each end (they may be the same vertex). Each vertex has a *degree*, which is the number of edge endpoints at that vertex (so if an edge connects two distinct vertices, it contributes 1 to each of their degrees, and if it is a loop on one vertex, it contributes 2 to that vertex's degree). It is possible to prove without induction that for a graph the sum of the degrees of the vertices is twice the number of edges. Find a proof of that fact using

(a) induction on the number of vertices;

(b) induction on the number of edges.

Exercise 2.4.5. Here's a challenge to your induction skills. The *Towers of Hanoi* is a puzzle consisting of a board with three pegs sticking up out of it and a collection of disks that fit on the pegs, each with a different diameter. The disks are placed on a single peg in order of size (smallest on top) and the goal is to move the entire stack to a different peg. A move consists of removing the top disk from any peg and placing it on another peg; a disk may never be placed on top of a smaller disk.

Determine how many moves it requires to solve the puzzle when there are n disks, and prove your answer by induction.

Recursion

To define a class *recursively* means to define it via a set of basic objects and a set of rules allowing you to extend the set of basic objects. We may give some simple examples.

Example 2.4.6. The natural numbers may be defined recursively as follows:

- $0 \in \mathbb{N}$.
- if $n \in \mathbb{N}$, then $n + 1 \in \mathbb{N}$.

Example 2.4.7. The *well-formed formulas* (wffs) in propositional logic are a recursively defined class.

- Any propositional symbol P, Q, R, etc., is a wff.
- If φ and ψ are wffs, so are the following:

  (i) $(\varphi \,\&\, \psi)$;

(ii) $(\varphi \vee \psi)$;

(iii) $(\varphi \to \psi)$;

(iv) $(\varphi \leftrightarrow \psi)$;

(v) $(\neg\varphi)$.

The important fact, which gives the strength of this method of definition, is that we may apply the building-up rules repeatedly to get more and more complicated objects.

For example, $((A\&B) \vee ((P\&Q) \to (\neg A)))$ is a wff, as we can prove by giving a construction procedure for it. A, B, P, and Q are all basic wffs. We combine them into $(A\&B)$ and $(P\&Q)$ by operation (i), obtain $(\neg A)$ from (v), $((P\&Q) \to (\neg A))$ from (iii), and finally our original formula by (ii).

Exercise 2.4.8. (i) Prove that $((A \vee (B\&C)) \leftrightarrow C)$ is a wff.

(ii) Prove that $(P \to Q(\vee$ is *not* a wff.

Exercise 2.4.9. (i) Add a building-up rule to the recursive definition of $\mathbb{N}$ to get a recursive definition of $\mathbb{Z}$.

(ii) Add a building-up rule to the recursive definition of $\mathbb{Z}$ to get a recursive definition of $\mathbb{Q}$.

Exercise 2.4.10. Write a recursive definition of the rational functions in x, those functions which can be written as a fraction of two polynomials of x. Your basic objects should be x and all real numbers. For this exercise, don't worry about the problem of division by zero.

We may also define functions recursively. For that, we say what $f(0)$ is (or whatever our basic object is) and then define $f(n+1)$ in terms of $f(n)$. For example, $(n+1)! = (n+1)n!$, with $0! = 1$, is *factorial*, a recursively defined function you've probably seen before. We could write a recursive definition for addition of natural numbers:

$$a(0,0) = 0;$$

$$a(m+1,n) = a(m,n) + 1;$$

$$a(m,n+1) = a(m,n) + 1.$$

This looks lumpy but is actually used in logic in order to minimize the number of operations that we take as fundamental: this definition of addition is all in terms of *successor*, the plus-one function.

Exercise 2.4.11. Write a recursive definition of $p(m,n) = m \cdot n$, on the natural numbers, in terms of addition.

Induction Again

Beyond simply resembling each other, induction and recursion have a strong tie in proofs. To prove something about a recursively-defined class requires induction. This use of induction is less codified than the induction on $\mathbb{N}$ we saw above. In fact, the limited version of induction we saw above is simply the induction that goes with the recursively-defined set of natural numbers, as in Example 2.4.6. Let's explore how this works in general.

The base case of the inductive argument will match the basic objects of the recursive class. The inductive step will come from the operations that build up the rest of the class. If they match exactly, you are showing the set of objects that have a certain property contains the basic objects of the class and is closed under the operations of the class, and hence must be the entire class.

Example 2.4.12. Consider the class of wffs, defined in Example 2.4.7. We may prove by induction that for any wff φ, the number of positions where binary connective symbols occur in φ (that it, $\&, \vee, \rightarrow$, and $\leftrightarrow$) is one less than the number of positions where propositional symbols occur in φ.

Proof. For any propositional symbol, the number of propositional symbols is 1 and the number of binary connectives is 0, one less than 1.

Suppose by induction that $p_1 = c_1 + 1$ and $p_2 = c_2 + 1$ for p_1, p_2 the number of propositional symbols and c_1, c_2 the number of binary connectives in the wffs φ, ψ, respectively. The number of propositional symbols in $(\varphi Q \phi)$, for Q any of $\vee, \&, \rightarrow$, and $\leftrightarrow$, is $p_1 + p_2$, and the number of connective symbols is $c_1 + c_2 + 1$. By the inductive hypothesis we see

$$p_1 + p_2 = c_1 + 1 + c_2 + 1 = (c_1 + c_2 + 1) + 1,$$

so the claim holds for $(\varphi Q \psi)$.

Finally, consider $(\neg\varphi)$. Here the number of binary connectives and propositional symbols have not changed, so the claim still holds. $\square$

Exercise 2.4.13. Suppose φ is a wff which does not contain negation (that is, it comes from the class defined as in Example 2.4.7 but without closure operation (v)). Prove by induction that the length of φ is of the form $4k + 1$ for some $k \geq 0$, and that the number of positions at which propositional symbols occur is $k + 1$ (for the same k).

Note that we can perform induction on $\mathbb{N}$ to get results about other recursively-defined classes if we are careful. For wffs, we might induct on the number of propositional symbols or the number of binary connectives, for instance.

Exercise 2.4.14. Recall from calculus that a function f is *continuous at a* if $f(a)$ is defined and equals $\lim_{x\to a} f(x)$. Recall also the *limit laws*, which may be summarized for our purposes as

$$\lim_{x\to a}(f(x)\Box g(x)) = (\lim_{x\to a} f(x))\Box(\lim_{x\to a} g(x)), \quad \Box \in \{+,-,\cdot,/\},$$

as long as both limits on the right are defined and if $\Box = /$ then $\lim_{x\to a} g(x) \neq 0$. Using those, the basic limits $\lim_{x\to a} x = a$ and $\lim_{x\to a} c = c$ for all constants c, and your recursive definition from Exercise 2.4.10, prove that every rational function is continuous on its entire domain.

Exercise 2.4.15. Using the recursive definition of addition from the previous section ($a(0,0) = 0$; $a(m+1,n) = a(m,n+1) = a(m,n)+1$), prove that addition is commutative (i.e., for all m and n, $a(m,n) = a(n,m)$).

2.5 Partial Functions

Let's go back to calculus, or possibly even algebra. When we define a function, we are supposed to give not only the rule that associates domain elements with range elements, but we are also supposed to specify what the domain *is*, or we have only incompletely defined the function. However, in calculus, we abuse this to give functions as algebraic formulas that calculate a range element from a domain element, and don't specify their domains; instead we say their domain is all elements of $\mathbb{R}$ on which they are defined. However, we treat these functions as though their domain is actually all of $\mathbb{R}$, and talk about, for example, values at which the function is discontinuous.

Here we take that mentality and make it official. In computability we discuss *partial functions* on $\mathbb{N}$. A partial function $f : \mathbb{N} \to \mathbb{N}$ is a function which takes elements of some subset of $\mathbb{N}$ as inputs, and produces elements of $\mathbb{N}$ as outputs. Generally "partial" means "partial or total": saying we are considering an arbitrary partial function does not imply there *must* be some value of $\mathbb{N}$ on which it is not defined.

The intuition here is that the function is a computational procedure which may be given any natural number as input, but might go into an infinite loop on certain inputs and never output a result. Because we want to allow all computational procedures, we have to work with this possibility.

Most basically, we want notation to represent what situation we're in. In computability we use arrows: $f(x)\downarrow$ means the function f on input x *halts*; that is, x is in the domain of f. We might specify halting when saying what the output of the function is, $f(x)\downarrow = y$, though there the $\downarrow$ is fairly superfluous. When x is not in the domain of f we say the computation *diverges* and write $f(x)\uparrow$.

For *total* functions f and g, we say $f = g$ if $(\forall x)(f(x) = g(x))$. When f and g may be partial, we require a little more: $f = g$ means

$$(\forall x)[(f(x)\downarrow \leftrightarrow g(x)\downarrow) \;\&\; (f(x)\downarrow = y \to g(x) = y)].$$

Some authors write this as $f \simeq g$ to distinguish it from equality for total functions and perhaps to highlight the fact that f and g might be partial.

One final bit of notation: for individual domain elements x, if $f(x) = y$ we might write $x \mapsto y$.

2.6 Some Notes on Proofs and Abstraction

Definitions

Definitions in mathematics are somewhat different from definitions in English. In natural language, the definition of a word is determined by the usage and may evolve. For example, "broadcasting" was originally just a way of sowing seed. Someone used it by analogy to mean spreading messages widely, and then it was adopted for radio and TV. For speakers of present-day English I doubt the original planting meaning is ever the first to come to mind.

In contrast, in mathematics we begin with the definition and assign a term to it as a shorthand. That term then denotes exactly the objects which fulfill the terms of the definition. To say something is "by definition impossible" has a rigorous meaning in mathematics: if it contradicts one of the properties of the definition, it cannot hold of an object to which we apply the term.

Mathematical definitions do not have the fluidity of natural language definitions. Sometimes mathematical terms are used to mean more than one thing, but that is a re-use of the term and not an evolution of the definition. Furthermore, mathematicians dislike that because it leads to ambiguity (exactly what is being meant by this term in this context?), which defeats the purpose of mathematical terms in the first place: to serve as shorthand for specific lists of properties.

Proofs

There is no way to learn how to write proofs without actually writing them, but I hope you will refer back to this section from time to time

A proof is an object of convincing. It should be an explicit, specific, logically sound argument that walks step by step from the hypotheses to the conclusions. That is, avoid vagueness and leaps of deduction, and strip out irrelevant statements. Make your proof self-contained except for explicit reference to definitions or previous results (i.e., don't assume your reader is so familiar with the theorems that you may use them without comment; instead say "by Theorem 2.5, ...").

Our proofs will be very verbal – they will bear little to no resemblance to the two-column proofs of high school geometry. A proof which is just strings of symbols with only a few words is unlikely to be a good (or even understandable) proof. However, it can be clumsy and expand proofs out of readability to avoid symbols altogether.

It is also important for specificity to assign symbolic names to (arbitrary) numbers and other objects to which you will want to refer. Striking the symbol/word balance is a big step on the way to learning to write proofs.

Your audience is a person who is familiar with the underlying definitions used in the statement being proved, but not the statement itself. For instance, it could be yourself after you learned the definitions, but before you had begun work on the proof. You do not have to put every tiny painful step in the write-up, but be careful about what you assume of the reader's ability to fill in gaps. Your goal is to convince the reader of the truth of the statement, and that requires the reader to understand the proof. Along those lines, it is often helpful to insert small statements (I call it "foreshadowing" or "telegraphing") that let the reader know why you are doing what you are currently doing, and where you intend to go with it. In particular, when working by contradiction or induction, it is important to let the reader know at the beginning.

Cautionary notes:

* Be careful to state what you are trying to prove in such a way that it does not appear you are asserting its truth prior to proving it.

* If you have a definition before you of a particular concept and are asked to prove something about the concept, you must stick to the definition.

* Be wary of mentally adding words like *only*, *for all*, *for every*, or *for some* which are not actually there; likewise if you are asked to prove an implication it is likely the converse does not hold, so if you "prove" it you will be in error.

* If you are asked to prove something holds of all objects of some type, you cannot pick a specific example and show the property holds of *that* object – it is not a proof that it works for all. Instead give a symbolic name to an arbitrary example and prove the property holds using only facts that are true for all objects of the given type.

* There is a place for words like *would*, *could*, *should*, *might*, and *ought* in proofs, but they should be kept to a minimum. Most of the time the appropriate words are *has*, *will*, *does*, and *is*. This is especially important in proofs by contradiction. Since in such a proof you are assuming something which is not true, it may feel more natural to use the subjunctive, but that comes across as tentative. You assume some hypothesis; given that hypothesis other statements *are* or *are not* true. Be bold and let the whole contraption go up in flames when it runs into the statement it contradicts.

* And finally, though math class is indeed not English class, sentence fragments and tortured grammar have no place in mathematical proofs. If a sentence seems strained, try rearranging it, possibly involving the neighboring sentences. Do not fear to edit: the goal is a readable proof that does not require too much back-and-forth to understand.

Exercise 2.6.1. Here are some proofs you can try that don't involve induction:

(i) $\neg(\forall m)(\forall n)(3m + 5n = 12)$ (over $\mathbb{N}$)

(ii) For any integer n, the number $n^2 + n + 1$ is odd.

(iii) If every even natural number greater than 2 is the sum of two primes, then every odd natural number greater than 5 is the sum of three primes.

(iv) For nonempty sets A and B, $A \times B = B \times A$ if and only if $A = B$.