Chapter 1

Sets and Notation

1.1 Defining sets

Definition. A *set* is an unordered collection of distinct objects. The objects in a set are called the *elements,* or *members,* of the set. A set is said to *contain* its elements.

A set can be defined by simply listing its members inside curly braces. For example, the set $\{2, 4, 17, 23\}$ is the same as the set $\{17, 4, 23, 2\}$. To denote membership we use the $\in$ symbol, as in $4 \in \{2, 4, 17, 23\}$. On the other hand, non-membership is denoted as in $5 \notin \{2, 4, 17, 23\}$.

If we want to specify a long sequence that follows a pattern, we can use the ellipsis notation, meaning "fill in, using the same pattern". The ellipsis is often used after two or more members of the sequence, and before the last one, as follows: $\{1, 2, \ldots, n\}$. The pattern denoted by the ellipsis should be apparent at first sight! For instance, $\{1, \ldots, n\}$ is generally regarded as underspecified (that is, too ambiguous). Of course, even $\{1, 2, \ldots, n\}$ is still ambiguous—did we mean all integers between 1 and n, all powers of two up to n, or perhaps the set $\{1, 2, 25, n\}$?—but is generally sufficient, unless you really do mean all powers of two up to n, in which case $\{2^0, 2^1, 2^2, \ldots, 2^k\}$ for an appropriate k is a better choice. The ellipsis can also be used to define an infinite set, as in the following.

Definition. The set of *natural numbers* or *nonnegative integers*, denoted by $\mathbb{N}$, is defined as $\{0, 1, 2, \ldots\}$.

To avoid ambiguities it is often useful to use the *set builder* notation, which lists on the right side of the colon the property that any set element, specified on the left side of the colon, has to satisfy. Let's define the positive integers using the set builder notation:

$$\mathbb{N}^+ = \{x : x \in \mathbb{N} \text{ and } x > 0\}.$$

We can also write

$$\mathbb{N}^+ = \{x \in \mathbb{N} : x > 0\}.$$

This is a matter of taste. In general, use the form that will be easiest for the reader of your work to understand. Often it is the least "cluttered" one.

Ok, now onto the integers:

$$\mathbb{Z} = \{x : x \in \mathbb{N} \text{ or } -x \in \mathbb{N}\}.$$

Hmm, perhaps in this case it is actually better to write

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

Remember, when you write mathematics, you should keep your readers' perspective in mind. For now, we—the staff of this course—are your readers. In the future it might be your colleagues, supervisors, or the readers of your published work. In addition to being reasonably formal and unambiguous, your mathematical writing should be as clear and understandable to your intended readership as possible.

Here are the *rational numbers*:

$$\mathbb{Q} = \left\{ \frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{Z}, b \neq 0 \right\}.$$

Instead of $a \in \mathbb{Z}, b \in \mathbb{Z}$, you can write $a, b \in \mathbb{Z}$, which is more concise and generally more readable. Don't go overboard, though, with writing something like $a, b \neq 0 \in \mathbb{Z}$, this is way too confusing and does not say what you want it to.

Finally, the set of *real numbers* is denoted by $\mathbb{R}$. All the reals that are not rational are called *irrational*. These include the familiar $\pi = 3.1415926...$, $e = 2.7182818...$, $\sqrt{2}$, and infinitely many others. (How do we know that these numbers are irrational, do you ask? Actually, we will see a proof of this for $\sqrt{2}$ shortly. The proofs for π and e require mathematical analysis and are outside our scope.)

On being formal. Were the above definitions formal enough? The answer is: it depends. For example, defining the natural numbers is an important and non-trivial accomplishment of mathematics. After all, what do these symbols "1", "2", "3", actually *mean*? These numbers can be formally defined in terms of sets. Even more involved is the formal definition of the reals, usually covered in a first mathematical analysis course.

Here we cannot afford to cover everything in complete detail, which would have to include, among other things, basic algebra and trigonometry. Furthermore, the vast majority of mathematical works, while considered to be "formal", gloss over details all the time. For example, you'll be hard-pressed to find a mathematical paper that goes through the trouble of justifying the equation $a^2 - b^2 = (a - b)(a + b)$. In effect, every mathematical paper or lecture assumes a shared knowledge base with its readers or listeners. It is extremely important for an author of mathematics, such as yourself during this course, to estimate this shared knowledge base correctly!

In CS103X we will assume most of high-school mathematics, including perhaps some AP math like single-variable calculus, as our shared knowledge base. Thus notions and techniques from this base will generally not be justified in lecture, and can be used freely in your homework and exams. Furthermore, once we develop certain

notation or prove some theorem in class, you can use these freely in your homework and exams, provided that you clearly cite the appropriate theorems. In writing and speaking mathematics, a delicate balance is maintained between being formal and not getting bogged down in minutia.[1] This balance usually becomes second-nature with experience. You should all get the hang of it by the end of the quarter.

1.2 Set operations

A is said to be a subset of B if and only if every element of A is also an element of B, in which case we write $A \subseteq B$. A is a *strict subset* of B if A is a subset of B and A is not equal to B, which is denoted by $A \subset B$. For example, $\{4, 23\} \subset \{2, 4, 17, 23\} \subseteq \{2, 4, 17, 23\}$.

Two sets A and B are considered equal if and only if they have the same elements. This is denoted by $A = B$. More formally, $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

For two sets A and B, the operations of union, intersection, and difference are defined as follows:

$$\begin{aligned} A \cup B &= \{x : x \in A \text{ or } x \in B\} \\ A \cap B &= \{x : x \in A \text{ and } x \in B\} \\ A \setminus B &= \{x : x \in A \text{ and } x \notin B\} \end{aligned}$$

The $\cup$ and $\cap$ notation can be extended to the union and intersection of multiple sets. Given n sets $A_1, A_2, \ldots, A_n$, we can write

$$\bigcup_{i=1}^{n} A_i$$

for their union, and

$$\bigcap_{i=1}^{n} A_i$$

for their intersection. In fact, this notation is pretty flexible and the same union can be written as

$$\bigcup_{i=1}^{n} A_i = \bigcup_{1 \le i \le n} A_i = \bigcup_{i \in \{x \,:\, 1 \le x \le n\}} A_i.$$

Here is another example:

$$\bigcap_{\substack{i \in \{x \,:\, 1 \le x \le 10\} \\ i \text{ is prime}}} A_i = A_2 \cap A_3 \cap A_5 \cap A_7.$$

Given a set A, the *cardinality* of A, also known as the *size* of A, is simply the number of elements in A. The cardinality of A is denoted by $|A|$. For example, if $A = \{2, 4, 17, 23\}$, then $|A| = 4$.

[1] Of course, what is considered minutia differs from subfield to subfield, and from classroom to classroom.

1.3 More sets

The *empty set* is denoted by $\emptyset$. It is the unique set without elements. It holds that $\emptyset \subseteq A$ for any set A. Why? By definition, this holds if every element of $\emptyset$ is also an element of A. Since $\emptyset$ has no elements, all possible statements about the elements of $\emptyset$ are true! In particular, all elements of $\emptyset$ are also elements of A. If this is confusing don't worry, we will go into such matters more rigorously when we get to logic. (For now, you can ponder the following: If we know for a fact that there are no unicorns <Gasp!>, then it is definitely true that all unicorns have soft light-blue fur.)

A set can contain sets as its elements. For example, $\{\{2,4\},\{17\},23\}$ is a perfectly valid set with three elements, two of them sets. (The second element is a *singleton*, a set with one element.) Note that $\{2,4\} \in \{\{2,4\},\{17\},23\}$, but $\{2,4\} \subseteq \{2,4,17,23\}$, and that $17 \notin \{\{2,4\},\{17\},23\}$, but $\{17\} \in \{\{2,4\},\{17\},23\}$. Also, $\{\emptyset\}$ is *not* the empty set. (Think about it.)

The *power set* of a set A is the set of all subsets of A, and is denoted by 2^A. That is,

$$2^A = \{S : S \subseteq A\}.$$

For example, for $A = \{2,4,17,23\}$, we have

$$2^A = \Big\{\emptyset, \{2\}, \{4\}, \{17\}, \{23\}, \{2,4\}, \{2,17\}, \{2,23\}, \{4,17\}, \{4,23\}, \{17,23\}, \{2,4,17\}, \{2,4,23\}, \{2,17,23\}, \{4,17,23\}, \{2,4,17,23\}\Big\}.$$

The cardinality of this set is 16, and $16 = 2^4$. This is not a coincidence: As we shall see when we get to combinatorics and counting, for a set A with n elements, the cardinality of 2^A is 2^n. This is in fact the reason for the power set notation.

Chapter 2

Induction

2.1 Introducing induction

Suppose there is an infinite line of people, numbered $1, 2, 3, \ldots$, and every person has been instructed as follows: "If something is whispered in your ear, go ahead and whisper the same thing to the person in front of you (the one with the greater number)". Now, what will happen if we whisper a secret to person 1? 1 will tell it to 2, 2 will tell it to 3, 3 will tell it to 4, and ... everybody is going to learn the secret! Similarly, suppose we align an infinite number of dominoes, such that if some domino falls, the next one in line falls as well. What happens when we knock down the first domino? That's right, they all fall. This intuition is formalized in the principle of mathematical induction:

Induction Principle: Given a set A of positive integers, suppose the following hold:

- $1 \in A$.
- If $k \in A$ then $k + 1 \in A$.

Then *all* positive integers belong to A. (That is, $A = \mathbb{N}^+$.)

Here are two simple proofs that use the induction principle:

Theorem 2.1.1. *Every positive integer is either even or odd.*

Proof. By definition, we are required to prove that for every $n \in \mathbb{N}^+$, there exists some $l \in \mathbb{N}$, such that either $n = 2l$ or $n = 2l + 1$. The proof proceeds by induction. The claim holds for $n = 1$, since $1 = 2 \cdot 0 + 1$. Suppose the claim holds for $n = k$. That is, there exists $l \in \mathbb{N}$, such that $k = 2l$ or $k = 2l + 1$. We prove that the claim holds for $n = k + 1$. Indeed, if $k = 2l$ then $k + 1 = 2l + 1$, and if $k = 2l + 1$ then $k + 1 = 2(l + 1)$. Thus the claim holds for $n = k + 1$ and the proof by induction is complete. □

Theorem 2.1.2. *Every positive integer power of 3 is odd.*

Proof. By definition, we are required to prove that for every $n \in \mathbb{N}^+$, it holds that $3^n = 2l + 1$, for some $l \in \mathbb{N}$. The proof proceeds by induction. For $n = 1$, we have $3 = 2 \cdot 1 + 1$, so the claim holds. Suppose the claim holds for k, so $3^k = 2l + 1$, for some $l \in \mathbb{N}$. Then

$$3^{k+1} = 3 \cdot 3^k = 3(2l + 1) = 2(3l + 1) + 1,$$

and the claim also holds for $k + 1$. The proof by induction is complete. □

Proof tip: If you don't know how to get a proof started, look to the definitions, and state formally and precisely what it is that you need to prove. It might not be obvious how to prove that "Every positive integer power of 3 is odd", but a bit easier to proceed with proving that "for every $n \in \mathbb{N}^+$, it holds that $3^n = 2l + 1$, for some $l \in \mathbb{N}$." If you need to prove an implication (that is, a claim of the form "if ... then ..."), then formally state all the assumptions as well as what you need to prove that they imply. Comparing the two might lead to some insight.

Proof technique: Induction. The induction principle is often used when we are trying to prove that some claim holds for all positive integers. As the above two proofs illustrate, when we use induction we do not need to explicitly refer to the set A from the statement of the induction principle. Generally, this set is the set of numbers for which the claim that we are trying to prove holds. In the first proof, it was the set of numbers n that are either even or odd. In the second proof, it was the set of numbers n for which 3^n is odd. Suppose we want to show that some claim holds for all positive integers. Here is a general template for proving this by induction:

(a) State the method of proof. For example, "The proof proceeds by induction."

(b) Prove the "induction basis". That is, prove that the number 1 satisfies the claim. (This step is often easy, but is crucially important, and should never be omitted!)

(c) Assume the "induction hypothesis". That is, state the assumption that the claim holds for some positive integer k.

(d) Prove, using the induction hypothesis, that the claim holds for $k+1$. The proof should consist of a chain of clear statements, each logically following from the previous ones combined with our shared knowledge base. The final statement in the chain should state that the claim holds for $k + 1$.

(e) Conclude the proof. For example, "This completes the proof by induction."

Theorem 2.1.3. *For every positive integer n,*

$$1 + 2 + \cdots + n = \frac{n(n + 1)}{2}.$$

Proof. The proof proceeds by induction. For $n = 1$, we have $1 = \frac{1 \cdot 2}{2}$ and the claim holds. Assume $1 + 2 + \cdots + k = k(k+1)/2$. Then

$$1+2+\cdots+k+(k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{k(k+1)+2(k+1)}{2} = \frac{(k+1)(k+2)}{2},$$

which proves the claim for $k + 1$ and completes the proof by induction. □

Sigma and Pi notations. Just as the $\bigcup$ symbol can be used to compactly express the union of many sets, the $\sum$ symbol can be used to express summations. For example,

$$1 + 2 + \cdots + n = \sum_{i=1}^{n} i = \sum_{1 \le i \le n} i = \sum_{i \in \{x \,:\, 1 \le x \le n\}} i.$$

You should not assume just because $\sum$ appears that there is an actual summation, or that there are any summands at all. For example, when $n = 1$, $\sum_{i=1}^{n} i = 1$, and when $n \le 0$, $\sum_{i=1}^{n} i = 0$!

Similarly, products can be expressed using the $\prod$ symbol, as in

$$2^0 \cdot 2^1 \cdot 2^2 \cdot \ldots \cdot 2^n = \prod_{i=0}^{n} 2^i.$$

One thing to be aware of is that the empty product is defined to equal 1, so

$$\prod_{i=3}^{1} i \quad = \quad \prod_{\substack{i \,\in\, \{2,4,10,14\} \\ i \text{ is odd}}} i \quad = \quad 1.$$

A single $\sum$ or $\prod$ symbol can also be used to describe the sum or product over more than one variable. For example,

$$\sum_{1 \le i,j \le n} (i+j) = \sum_{i=1}^{n} \sum_{j=1}^{n} (i+j).$$

2.2 Strong induction

Suppose that a property P holds for $n = 1$, and the following is true: If P holds for all integers between 1 and k, then it also holds for $k + 1$. Under these assumptions, P holds for all positive integers. This is the principle of strong induction. It differs from regular induction in that we can assume something stronger to derive the same conclusion. Namely, we can assume not only that P holds for k, but that in fact P holds for all positive integers up to k. We state the strong induction principle more formally, and then demonstrate its usefulness.

Strong Induction Principle: Given a set A of positive integers, suppose the following hold:

- $1 \in A$.
- If $\{1, 2, \ldots, k\} \subseteq A$ then $k + 1 \in A$.

Then all positive integers belong to A.

Definition. An integer $p > 1$ is said to be *prime* if the only positive divisors of p are 1 and p itself.

Theorem 2.2.1. *Every positive integer greater than* 1 *can be expressed as a product of primes.*

Proof. The proof proceeds by strong induction. Since 2 is a prime, the claim holds for 2. (Note how the induction basis in this case is 2, not 1, since we are proving a claim concerning all integers equal to or greater than 2.) Now assume the claim holds for all integers between 2 and k. If $k+1$ is a prime then the claim trivially holds. Otherwise it has a positive divisor a other than 1 and $k + 1$ itself. Thus, $k + 1 = a \cdot b$, with $2 \leq a, b \leq k$. Both a and b can be expressed as products of primes by the induction hypothesis. Their product can therefore also be thus expressed. This completes the proof by strong induction. □

The versatility of induction. We have seen in the proof of Theorem 2.2.1 that if we want to prove a statement concerning all positive integers equal to or greater than 2, we can use induction (or strong induction) with 2 as the base case. This holds for any positive integer in the place of 2. In fact, induction is an extremely versatile technique. For example, if we want to prove a property of all even positive integers, we can use 2 as the base case, and then prove that if the property holds for k, it will also hold for $k + 2$. Generally we will just assume that such variations are ok, there is no need to state a separate induction principle for each of these cases.

Fairly subtle variations of induction are often used. For example, if we can prove that a statement holds for 1 and 2, and that if it holds for k it will also hold for $k + 2$, we can safely conclude that the statement holds for all the positive integers. However, don't get carried away with variations that are simply incorrect, like using 1 as a base case, proving that if a statement holds for k then it also holds for $k + 2$, and then claiming its validity for all positive integers.

2.3 Why is the induction principle true?

Some of you might be surprised by the title question. Isn't it obvious? I mean, you know, the dominoes are aligned, you knock one down, they all fall. End of story. Right? Not quite.

"Common sense" often misleads us. You probably noticed this in daily life, and you're going to notice it a whole lot if you get into mathematics. Think of optical

illusions: we see, very clearly, what isn't really there. Our mind plays tricks on us too, just like our eyes sometimes do. So in mathematics, we are after proving everything. To be mathematically correct, every statement has to logically follow from previously known ones. So how do we prove the induction principle?

The answer lies in the previous paragraph. We said that every statement has to logically follow from other statements that we have proven previously. But this cannot go on forever, do you see? We have to start from some statements that we *assume* to be true. Such statements are called axioms. For example, why is it true that for any two natural numbers a, b, c, it holds that $a+(b+c) = (a+b)+c$? Because we assume it to be so, in order to build up the rest of mathematics from this and a small number of other such axioms.

This is also what we do with the induction principle: We accept it as an axiom. And if we accept the induction principle, strong induction can be proved from it, as you'll discover in the homework.

Chapter 3

More Proof Techniques

3.1 Proofs by contradiction

The following proof proceeds by contradiction. That is, we will assume that the claim we are trying to prove is wrong and reach a contradiction. If all the derivations along the way are correct, then the only thing that can be wrong is the assumption, which was that the claim we are trying to prove does not hold. This proves that the claim does hold.

Theorem 3.1.1. *$\sqrt{2}$ is irrational.*

Proof. We have seen previously that every integer is either even or odd. That is, for every $n \in \mathbb{Z}$ there exists $k \in \mathbb{Z}$, such that either $n = 2k$ or $n = 2k+1$. Now, if $n = 2k$ then $n^2 = (2k)^2 = 4k^2 = 2 \cdot (2k^2)$, which means that if n is even then n^2 is also even. On the other hand, if $n = 2k+1$ then $n^2 = (2k+1)^2 = 4k^2+4k+1 = 2 \cdot (2k^2+2k)+1$, so if n is odd then n^2 is also odd.

We now proceed with a proof by contradiction. Assume that $\sqrt{2}$ is rational, that is, $\sqrt{2} \in \mathbb{Q}$. (This is the assumption that should lead to a contradiction.) By definition, this means that there exist two numbers $p, q \in \mathbb{Z}$, with $q \neq 0$, such that

$$\frac{p}{q} = \sqrt{2},$$

and thus

$$\left(\frac{p}{q}\right)^2 = 2.$$

We can assume that p and q have no common divisor, since all common divisors can be divided out to begin with. We have

$$p^2 = 2q^2.$$

This shows that p^2 is even, and consequently p must be even; that is, $p = 2k$ for some $k \in \mathbb{Z}$. Then

$$p^2 = 4k^2 = 2q^2,$$

so

$$2k^2 = q^2.$$

This shows that q^2 is even, and consequently that q is even. Thus both p and q are even, contradicting the fact that p and q have no common divisor. We have reached a contradiction, which completes the proof. □

Proof Technique: Proof by contradiction. Suppose we want to prove some statement A by contradiction. A common template for such proofs is as follows:

(a) State the method of proof. For example, "The proof proceeds by contradiction."

(b) State the assumption that should lead to the contradiction. For example, "Assume statement A does not hold."

(c) Proceed with a chain of clear statements, each logically following from the previous ones combined with our shared knowledge base. The final statement in the chain should be a contradiction, either of itself (as in, $0 \neq 0$), or of some previous statement in the chain, or of part of our shared knowledge base.

(d) Conclude the proof. For example, "We have reached a contradiction, which completes the proof."

Theorem 3.1.2. $\log_2 3$ *is irrational.*

Proof. The proof proceeds by contradiction. Assume that $\log_2 3$ is rational. By definition, there exist two numbers $p, q \in \mathbb{Z}$, with $q \neq 0$, such that

$$\log_2 3 = \frac{p}{q},$$

which means that

$$2^{\frac{p}{q}} = 3,$$

and thus

$$2^p = 3^q.$$

We can assume that $p, q > 0$. (Indeed, if $p/q > 0$ then we can just work with $|p|$ and $|q|$, and if $p/q \leq 0$ we reach a contradiction of the form $3 = 2^{p/q} \leq 2^0 = 1$.) Now, any positive integer power of 2 is even, because it has 2 as a divisor, so 2^p is even. On the other hand, a positive integer power of 3 is odd, as we've seen previously. We have reached a contradiction. □

3.2 Direct proofs

We should not forget perhaps the most intuitive proof technique of all: the direct one. Direct proofs start out with our shared knowledge base and, by a sequence of logical derivations, reach the conclusion that needs to be proved. Such proofs are often particularly ingenious and surprising.

Consider the following well-known puzzle question. Take the usual 8×8 chessboard and cut out two diagonally opposite corner squares. Can the remaining 62 squares be tiled by domino-shaped 2×1 tiles, each covering two adjacent squares of the board? (That is, each tile can be placed either horizontally or vertically, so as to precisely cover two squares of the board.)

Theorem 3.2.1. *A tiling as above is impossible.*

Proof. Every tile covers one white square and one black square. Thus in any tiling as above, the number of white squares covered is the same as the number of black ones. The two removed squares have the same color, hence the number of white squares left on the board is not the same as the number of black ones. So the remaining squares cannot be tiled. □

The above proof can also be phrased as a proof by contradiction, or even in terms of induction. However, even though such a phrasing might appear more formal, it is rather unnecessary, as the above proof is already logically sound (which is critical!), and better conveys the power (and dare I say, the beauty) of the argument.

Proof Technique: Direct proof. Here is a common template for direct proofs:

(a) Provide a chain of clear statements, each logically following from our shared knowledge base and the previous ones. The final statement in the chain should be the claim we need to prove.

(b) (Optional.) Conclude the proof. For example, "This completes the proof."