2 Review of Logic and Proofs

This chapter will review mathematical logic and basic techniques for formally proving mathematical claims. These proof techniques will be essential for proving the correctness and runtime of the algorithms we will develop and analyze in this course. Hopefully much of this content is familiar to you from CSCE 222, but it's important to establish a common foundation to ensure that everyone is set up for success when we begin applying these proof techniques to new topics.

2.1 Predicate Logic

A **predicate** is some statement which is true or false. For example $10 < 25$, $19^2 = 400$, and "The string 'strawberry' contains 2 r's" are all predicates (the first one is true, the other two are false). On the other hand an expression like $2 + 2$ is not a predicate, since it does not express a claim and therefore does not have a truth value. Similarly, $x > -2$ is not a predicate, because x is not defined, meaning that the statement does not have a well-defined truth value.

If we want to include variables in our predicate, we need to **quantify** them, meaning we need to describe what values the variable can take on. There are two main logical quantifiers.

- The universal quantifier "for all" is used to say that some expression is true for every element of a given set. We could convert our expression $x > -2$ into the (false) predicate "For all integers x, $x > -2$" by adding a universal quantifier. Note that the choice of which set to quantify over is very important. We could convert the same expression into the true predicate "For all positive integers x, $x > -2$" by choosing to quantify over $\mathbb{Z}^+$ instead of $\mathbb{Z}$.

  We represent the universal quantifier symbolically using the symbol $\forall$. So the predicate we just described could be written as $\forall\, x \in \mathbb{Z}^+, x > -2$.

  Note that any "for all" statement is true if the set that we are quantifying over is the empty set. For example

  $$\forall\, x \in \emptyset,\ 2 + 2 = 5$$

  is a true predicate! We say that a predicate universally quantifying over the empty set is **vacuously true**.

- The existential quantifier "there exists" is used to say that some expression is true for at least one element of a given set. We could convert our expression $x > -2$ into the (true) predicate "There exists an integer x such that $x > -2$" by adding an existential quantifier. Once again, the choice of set to quantify over is important. We could make a false predicate based on the same expression if we chose to quantify over the set $\{-3, -4, -5\}$.

  We represent the existential quantifier symbolically using the symbol $\exists$. For example: $\exists\, x \in \mathbb{Z}, x > -2$.

  Just as every "for all" statement about the empty set is true, every "there exists" statement about the empty set is false. For example

  $$\exists\, x \in \emptyset,\ 2 + 2 = 4$$

  is a false predicate. There is no x in the empty set for which $2 + 2 = 4$, because there is no x in the empty set at all!

We can modify and combine predicates with the logical operators "and" (denoted symbolically as $\wedge$), "or" (denoted symbolically as $\vee$), and "not" (denoted symbolically as $\neg$). So if A and B are two predicates then:

- $A \wedge B$ is true if A and B are both true and false otherwise.
- $A \vee B$ is true if either A or B is true, and false if A and B are both false. Note that in mathematics/computer science "or" almost always means "inclusive or", so $A \vee B$ is true if A and B are both true.

- $\neg A$ is true if A is false, and false if A is true.

The logical operators in the previous paragraph all correspond to common operators in many programming languages. There is another important logical operator which is not common in programming: implication. "A implies B" is a predicate which is true if A and B are both true, or if A is false. This predicate can also be written as "If A, then B" or denoted symbolically as $A \Rightarrow B$. Many of the predicates we are interested in proving are implications.

Implications can be confusing, because the way they are used in mathematics and computer science is different from the way that "if" is used in regular English. It's important to remember that $A \Rightarrow B$ is always true when A is false. For example "If I am on Mars, then $2 + 2 = 5$" is a true predicate. Since I am not on Mars, the truth value of $2 + 2 = 5$ does not affect the truth value of the whole expression (If you are reading this from a Martian colony in the distant future, replace Mars with a planet you are not on).

Closely related to implication is **bi-implication**, also known as "if and only if". "A bi-implies B" or "A if and only if B" or "A iff B" all mean that A and B are either both true or both false. Bi-implication is written symbolically as $A \Leftrightarrow B$. $A \Leftrightarrow B$ is logically equivalent to $(A \Rightarrow B) \wedge (B \Rightarrow A)$.

2.2 What is a Proof?

A **proof** is a rigorous argument designed to convince other people that a given claim is true. A correct proof could be written fully in predicate logic, relying only on basic axioms of set theory. Such proofs are very tedious to write and to read, however, so typical proofs are written mostly in English. This means that what constitutes a "correct" proof is to some degree a social convention. A correct proof will never claim a false statement, but a proof which makes only true statements can still be considered incorrect if it skips too many steps and it's not clear how the lines of the proof connect to each other.

For example, let's say that I want to prove the following uninteresting theorem:

Theorem 4. $((19 \cdot 15) + 7)^2 - 9 > 10000$

Proof. We first calculate that

$$19 \cdot 15 = 285.$$

Therefore

$$(19 \cdot 15) + 7 = 285 + 7 = 292.$$

Thus,

$$((19 \cdot 15) + 7)^2 = 292^2 = 292 \cdot 292 = 85264.$$

Finally,

$$((19 \cdot 15) + 7)^2 - 9 = 85264 - 9 = 85255 > 10000.$$

□

Alternatively, we could give the following shorter proof of the same theorem:

Proof. We note that

$$((19 \cdot 15) + 7)^2 - 9 = 85255 > 10000.$$

□

For the purposes of this course, the second proof would be entirely sufficient. You may assume that the reader of your proof is capable of performing basic arithmetic and do not need to show every step of the calculation. On the other hand, you should not assume that your reader is comfortable manipulating complicated summations, and if you need to do this, you should carefully show the steps.

How much detail your proof should go into depends on the audience that you are writing for. A proof written for CS PhD's may skip many steps as "obvious" that should be fully justified if the proof is targeted at CS undergraduates. You should view the audience of the proofs you write in

this class as a fellow student in this course who is not quite as clever as you. You may assume basic results from prerequisite courses like Calculus and CSCE 222 without proving them, and you may use any theorem proven in these notes. The original parts of your proof, however, should be carefully justified. You want to make an airtight case which would convince a reader who is skeptical of the claim you are proving.

One good test for deciding whether you need to justify something in your proof is to think about what you would say if someone asked you why a particular line of the proof follows from the previous one. If you can think of a short obvious answer, the connection is probably clear enough. If you realize that *you* couldn't explain the connection, then that's a sign that your proof is missing something there.

When in doubt, err on the side of providing more detail. We will not penalize you for providing an overly rigorous proof, but we will penalize you for leaving out important details. You are also welcome to ask in office hours if you have justified a particular part of your proof sufficiently.

2.3 Proving Predicates

In the previous section we saw an example of how to prove the simplest kind of predicate, a formula with no variables or quantifiers. Most predicates we are interested in proving, however, will involve a universal or existential quantifier (or both).

To prove a universal statement of the form $\forall\, x \in S,\ P(x)$, we need to choose an *arbitrary* $x \in S$ and show that $P(x)$ holds. Here "arbitrary" means that our proof should work for any choice of x from S, we can't assume that the x we chose has any special property. Sometimes it's helpful to imagine here that x is being chosen for you by an enemy who wants your proof to fail.

For example, suppose that we want to prove the following theorem:

Theorem 5. *Let* $S := \{n^2 \mid n \in \mathbb{Z}^+\}$. *Then* $\forall\, x \in S,\ x > 1 \Rightarrow x^2 > x + 10$

Proof. Let $x \in S$ be arbitrary. If $x \leq 1$ the implication is automatically true, so assume $x > 1$. Since $x \in S$, x is the square of a positive integer. Since the next smallest square number after 1 is 4, $x > 1 \Rightarrow x \geq 4$. Therefore:

$$x^2 \geq 4x = x + 3x \geq x + 12 > x + 10.$$

□

We can view this kind of proof as providing a template for creating infinitely many proofs, one for each element of S. We can pick any element of S to be x, plug it into this proof, and the proof will show us why $x > 1 \Rightarrow x^2 > x + 10$ for that value of x. Note that in this proof we explicitly considered the case where our arbitrary x was less than or equal to 1. While it is important to understand that we are proving a claim about all x, including values of x which are less than or equal to 1, this step is typically omitted in proofs of "for all" statements including implications, because it would be the same every time (every implication is true whenever its left side is false). Therefore we can shorten the proof slightly by starting "Let $x \in S$ be an arbitrary integer with $x > 1$".

Proving a "there exists" statement is usually easier. To prove $\exists\, x \in S,\ P(x)$, we simply need to find a single specific $x \in S$ for which $P(x)$ is true. For example:

Theorem 6. *Let* $S := \{n^2 \mid n \in \mathbb{Z}^+\}$. *Then* $\exists\, x \in S,\ x^2 < \log_2(x) + 10$

Proof. Choose $x = 1$. $x \in S$, since $1 \in \mathbb{Z}^+$ and $1^2 = 1$. For this choice of x, we have:

$$x^2 = 1^2 = 1 < 10 = 10 + 0 = 10 + \log_2(1).$$

□

Sometimes we will want to prove statements involving *nested quantifiers*, i.e. statements that have both "for all" and "there exists" statements. When parsing these statements it is important to pay attention to the order of the quantifiers. To prove a statement of the form $\forall\, x \in S,\ \exists\, y \in T,\ P(x, y)$, we need to show that for any arbitrary x in S, we can pick some y in T such that $P(x, y)$ is true (the choice of y will probably depend on the value of x).

For example,

Theorem 7. $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}^+, y > x$.

Proof. Let $x \in \mathbb{Z}$ be arbitrary. If $x < 0$, choose $y = 1$, and then $y \in \mathbb{Z}^+$ and $y > x$. Otherwise, $x \geq 0$, so choose $y = x + 1$. Since $x \geq 0$, $y \in \mathbb{Z}^+$, and $y = x + 1 > x$. □

Notice that we had to pay attention to the sets that x and y were quantified over here. It would be easy to simply say "choose $y = x + 1$" without considering a special case for negative x, but since the theorem says that y must be positive, that proof would be incorrect.

If we switch the order of the quantifiers in Theorem 7, we get a different predicate

$$\exists y \in \mathbb{Z}^+, \forall x \in \mathbb{Z}, y > x.$$

This predicate claims that there exists a single y, such that for every integer x, y is larger than that x. Since the existential quantifier comes first now, we have to choose y before x, meaning that our choice of y cannot depend on x like it did in the proof of Theorem 7. There is no integer which is larger than all other integers, so this predicate is false.

2.4 Disproving Predicates

Sometimes we want to disprove a predicate (i.e. to show that it is false). This is equivalent to proving the negation of the predicate. Therefore, it's important to understand how to negate universal and existential quantifiers.

The negation of the statement $\forall x \in S, P(x)$ is $\exists x \in S, \neg P(x)$. This means that to disprove a "for all" statement, it's enough to find a single counterexample. Finding one $x \in S$ for which $P(x)$ is false, proves that $P(x)$ can't be true for every single $x \in S$.

The negation of the statement $\exists x \in S, P(x)$ is $\forall x \in S, \neg P(x)$. That is, to show that a "there exists" statement is false, we need to prove that $P(x)$ is false for every single x in S. We can prove this using any of our usual techniques for proving a "for all" statement, like the "choose an arbitrary element and show the claim holds for it" method that we saw in the previous section or induction which we will talk about in Section 3.1.

2.5 Using Cases

Often in a proof we need to divide a claim up into several cases and prove each of them separately. For example, to prove a statement of the form $A \vee B \Rightarrow C$, we may have one case where we assume A is true, and then prove C, and a second case where we assume B is true, and then prove C. Note that these cases may overlap (it's possible that A and B are both true), which is not a problem. The important thing is that our cases are comprehensive. Any situation where $A \vee B$ is true will fall into at least one of our cases.

Cases can also be helpful when proving a "for all" statement. As we've seen, the standard approach to proving a statement of the form $\forall x \in S, P(x)$ is to take an arbitrary $x \in S$ and show that $P(x)$ holds. Sometimes we need a different proof structure depending on some property of the arbitrary x we chose (for example, we might use a different proof for odd x than for even x). This is another natural place to use case work. Again it's important to justify that every $x \in S$ will fall into at least one of our cases. Here is an example of using casework to prove a "for all" statement.

Theorem 8. *Let $S := \{n^2 \mid n \in \mathbb{Z}_{\geq 0}\}$. Then $\forall x \in S$, the last digit of x is either 0, 1, 4, 5, 6, or 9.*

Proof. Let $x \in S$ be arbitrary. By the definition of S, x is a perfect square, so $\sqrt{x} \in \mathbb{Z}_{\geq 0}$. Let $n := \sqrt{x}$. We note that the last digit of n^2 depends only on the last digit of n (this follows from the grade school algorithm for multiplication). We case on the last digit of n.

- If the last digit of n is 0, then the last digit of n^2 is 0
- If the last digit of n is 1, then the last digit of n^2 is 1
- If the last digit of n is 2, then the last digit of n^2 is 4

- If the last digit of n is 3, then the last digit of n^2 is 9
- If the last digit of n is 4, then the last digit of n^2 is 6
- If the last digit of n is 5, then the last digit of n^2 is 5
- If the last digit of n is 6, then the last digit of n^2 is 6
- If the last digit of n is 7, then the last digit of n^2 is 9
- If the last digit of n is 8, then the last digit of n^2 is 4
- If the last digit of n is 9, then the last digit of n^2 is 1

These are all the possible values for the last digit of n. Thus, in every case, the last digit of n^2 (which by definition equals x) is either 0, 1, 4, 5, 6, or 9. □

2.6 Using the Contrapositive

Remember that an implication is a statement of the form "If A then B", written $A \Rightarrow B$. The standard way to prove an implication is to start by assuming A is true and then use this to show that B is true (perhaps by applying definitions or performing algebraic manipulation).

Sometimes it's easier to prove an implication if we first convert it into a different equivalent form. One of the most common ways to do this is by taking the **contrapositive**. The contrapositive of $A \Rightarrow B$ is $\neg B \Rightarrow \neg A$. Just like the original implication the contrapositive is false only when A is true and B is false, so the two forms are logically equivalent, and we can choose to prove whichever is more convenient. Here is an example of a proof by contrapositive:

Theorem 9. $\forall\, x, y \in \mathbb{Z}_{\geq 0},\ x + y > 21 \Rightarrow x > 10 \vee y > 11.$

Proof. Let x and y be arbitrary non-negative integers. We want to prove that $x + y > 21 \Rightarrow x > 10 \vee y > 11$. We will prove the contrapositive:

$$\neg(x > 10 \vee y > 11) \Rightarrow \neg(x + y > 21).$$

By De Morgan's Laws, this is equivalent to

$$x \leq 10 \wedge y \leq 11 \Rightarrow x + y \leq 21.$$

If $x \leq 10$ and $y \leq 11$, then $x + y \leq 10 + 11 = 21$, which proves the theorem. □

Here it was not quite clear how to directly prove the implication starting from the fact $x + y > 21$ and trying to prove an "or" statement, but the proof of the contrapositive is very short and simple. Note that taking the contrapositive only affected the implication, not the quantifiers, we were still proving a "for all" statement about non-negative integers.

2.7 Proving Subset Relationships and Set Equality

To prove that one set S is a subset of another set T we need to prove the predicate

$$\forall\, x \in S,\ x \in T.$$

Just like proving any other "for all" statement, this will typically involve taking an arbitrary element of S, and then showing that it is in T (usually by expanding the definitions of S and T and showing how they relate to each other).

Proving that two sets are equal requires a little more effort. The most common approach is a proof by **double containment**, which means showing $S \subseteq T$ and $T \subseteq S$ (if both of these are true, then we must have $S = T$). Here is an example of a set equality proof (which includes two subset proofs):

Theorem 10. *Let $S := \{25x + 15y \mid x, y \in \mathbb{Z}\}$, and let $T := \{5n \mid n \in \mathbb{Z}\}$. Prove that $S = T$.*

Proof. We prove this by double containment:

- First we show $S \subseteq T$. Let $a \in S$ be arbitrary. By the definition of S, a can be expressed as $25x + 15y$ for some integers x and y. We need to show that there exists an integer n such that $a = 5n$. Let $n := 5x + 3y$. Then we have that

  $$5n = 5(5x + 3y) = 25x + 15y = a.$$

  So by the definition of T, $a \in T$.

- Now we show $T \subseteq S$. Let $a \in T$ be arbitrary. By the definition of T, $a = 5n$ for some integer n. We need to show that there exist integers x and y such that $25x + 15y = a$. We note that $25(-1) + 15(2) = 5$. Let $x := -n$ and let $y := 2n$ (clearly these are both integers). Then we have that

  $$25x + 15y = 25(-n) + 15(2n) = -25n + 30n = 5n = a.$$

  Thus, by the definition of S, $a \in S$.

□

If you are asked to prove set equality it is important to remember to prove both directions.

2.8 Acknowledgments

Some of the topics and problems in this chapter are inspired by ones in Building Blocks for Theoretical Computer Science by Margaret Fleck, the textbook that I used to teach Discrete Structures at UIUC.

2.9 Comprehension Questions

1. Determine which of the following predicates are true and which are false:

   (a) $3 > 4 \vee 3 > 2$

   (b) $3 > 4 \wedge 3 > 2$

   (c) $3 > 4 \Rightarrow 3 > 2$

   (d) $3 > 2 \Rightarrow 3 > 4$

   (e) $\forall x \in \mathbb{Z}, x \neq 4.11$

   (f) $\exists x \in \mathbb{Z}, x \neq 4$

   (g) $\forall x \in \{-3, 3\}, x^2 = 9$

   (h) $\exists x \in \mathbb{Z}^+, x \leq 0$

   (i) $\forall x \in \emptyset, x^2 = -1$

   (j) $\exists x \in \emptyset, x = x$

   (k) $\forall x \in \mathbb{Z}, x > 4 \Rightarrow x^2 > x$

   (l) $\forall x \in \mathbb{Z}, x > 0 \Rightarrow 2 + 2 = 4$

   (m) $\forall x \in \mathbb{Z}^+, 2 + 2 = 4 \Rightarrow x > 0$

   (n) $\exists x \in \mathbb{Z}^+, 2 + 2 = 4 \Rightarrow x = 7$

   (o) $\exists x \in \mathbb{Z}^+, x > 7 \Rightarrow x = -3$

   (p) $\exists x \in \mathbb{Z}^+, x > 0 \Rightarrow x = 5$

   (q) $\exists x \in \mathbb{Z}^+, x > 0 \Rightarrow x = -3$

   (r) $\forall x \in \mathbb{Z}^+, x > 7 \Rightarrow x \neq 1$

2. Find the negation of each of the following predicates

   (a) $\forall\, x \in \mathbb{Z},\, \exists\, y \in \mathbb{Z}^+,\, x + y = 7$

   (b) $\exists\, x \in \mathbb{Z},\, \forall\, y \in \mathbb{Z}^+,\, x + y = 7$

   (c) $\exists\, x, y \in \mathbb{Z}^+, x + y = 7$

   (d) $\forall\, x \in \mathbb{Z}_{\geq 0}, x > 5 \Rightarrow x \neq 3$

3. Find the contrapositive of each of the following implications:

   (a) $x > 5 \Rightarrow x^2 > 10$

   (b) x^2 is odd $\Rightarrow x$ is odd

   (c) $x \notin A \cap B \Rightarrow x \notin A$

4. True or False? For all sets A and B, $A = B \Leftrightarrow (A \subseteq B \wedge B \subseteq A)$.

5. Fill in the blank: When we convert the implication $A \Rightarrow B$ to the equivalent implication $\neg B \Rightarrow \neg A$, we have taken the _____.

6. Suppose that we want to prove "$\forall\, x \in \mathbb{R}^+, x^2 > 0$." What is the main flaw with the following "proof"?

   Proof. Let $x \in \mathbb{R}^+$ be arbitrary. Then we have that

   $$x^2 = x \cdot x \geq x \geq 0.$$

   □

7. Suppose that we want to prove that $\{2n \mid n \in \mathbb{Z}_{\geq 0}\} = \{n \in \mathbb{Z}_{\geq 0} \mid$ the last digit of n is either $0, 2, 4, 6$ or $8\}$." What is the main flaw with the following "proof"?

   Proof. Let $S := \{2n \mid n \in \mathbb{Z}_{\geq 0}\}$ and let $T := \{n \in \mathbb{Z}_{\geq 0} \mid$ the last digit of n is either $0, 2, 4, 6$ or $8\}$. Let $x \in S$ be arbitrary. Then $x = 2n$ for some $n \in \mathbb{Z}_{\geq 0}$. We case on the last digit of n:

   - If the last digit of n is 0 or 5, the last digit of $x = 2n$ is 0, so $x \in T$.
   - If the last digit of n is 1 or 6, the last digit of $x = 2n$ is 2, so $x \in T$.
   - If the last digit of n is 2 or 7, the last digit of $x = 2n$ is 4, so $x \in T$.
   - If the last digit of n is 3 or 8, the last digit of $x = 2n$ is 6, so $x \in T$.
   - If the last digit of n is 4 or 9, the last digit of $x = 2n$ is 8, so $x \in T$.

   Since n must end with one of these digits, we conclude that in every case $x \in T$ and thus $S = T$. □

2.10 Exercises

1. Prove that $\forall\, a \in \mathbb{Z}, \exists\, b, c \in \mathbb{Z}, a \neq b \wedge a \neq c \wedge b + c = a$.

2. Prove that $\forall\, a, b \in \mathbb{Z},\ a < b \Rightarrow \exists\, q \in \mathbb{Q},\ a < q < b$.

3. Prove that $\forall\, x \in \mathbb{Q}^+, \forall\, y \in \mathbb{R}, \frac{y+1}{2} \in \mathbb{Q} \Rightarrow \frac{1}{x} + y \in \mathbb{Q}$

4. Prove that if $r \in \mathbb{R}^+ \setminus \mathbb{Q}^+$ and $q \in \mathbb{Q}^+$, then $rq \in \mathbb{R} \setminus \mathbb{Q}$ (i.e. prove that multiplying a positive irrational number with a positive rational number gives an irrational number).

5. Define a new operation $\ominus$ by $a \ominus b := 2(a + b)$. **Disprove** the following claim:
   Claim: $\forall\, x, y, z \in \mathbb{R}, x \ominus (y \ominus z) = (x \ominus y) \ominus z$

6. Let A, B, and C be sets. Prove that

$$(A \setminus B) \cup (B \setminus C) \subseteq (A \cup B) \setminus (A \cap B \cap C)$$

7. Prove that for every positive integer n, if n^2 is even, then n is even.

8. Let Σ be an alphabet. Prove that

$$\{x \cdot y \mid x, y \in \Sigma^* \text{ with } |x| = |y|\} = \{s \in \Sigma^* \mid |s| \text{ is even }\}$$