Proofs Portfolio

MAT 3100W: Intro to Proofs

Sam Ly

December 5, 2025

1 Introduction

In this paper, we will explore various fundamental mathematical ideas and concepts, as well as their proofs. Proofs of high-level mathematical concepts are difficult, so various **proof techniques** will also be explored. We begin with the logical **axioms**, providing us with a way to form **statements**. Armed with just the our axioms, we find that new statements can be constructed. This is as the **direct proof**, where we manipulate logical statements to find new insights. Venturing further, we find **conditional statements**, and their accompanied proof technique, the **transformation of conditionals**. We then explore **sets**, orderless groupings of arbitrary objects. Making statements about objects within sets requires the use of **quantifiers**. Proofs of a countably infinite number of related statements are possible via a technique known as **induction**. We also explore methods of defining infinities via **functions** and **bijections**. We also see that our numbers are actually members of special sets. Through this lense, we derive the basics of **number theory** and **modular arithmetic**. Lastly, when all hope seems lost in proving a statement, we may turn to the **proof by contradiction** as our last resort. This technique can only tell us *if* a statement is true, but not *why* or *how*.

2 Mathematical concepts

In this section, we will discuss *concepts* that are foundational for constructing and understanding mathematical proofs. Many of the concepts here build up to later concepts, so reading in order is recommended, but not necessarily required. Most concepts here will be proven later in section 3. These ideas form the basis of higher level math.

2.1 Logic, truth tables, and DeMorgan's laws

The foundations of mathematical reasoning is formal logic. We can form **logical statements** that give us insights whatever we are reasoning about.

2.1.1 Logical Statements

Definition 1. A logical statement is a statement that can either be **true** or **false**. Logical statements must be unambiguous, meaning all ratioal agents with access to the same information will come to the same conclusion.

Example 1. "The sun rose today." is a **true** logical statement.

Proof. We begin by observing that the we can currently see the sun in the sky and that we could not see the sun in the sky last night. If we can not see the sun in the sky, it must be below the horizon. Because the sun follows a continuous path, and it had been below the horizon last night, it must have crossed the horizon at some point between last night and now. Thus the sun must have risen today. □

We can then form larger statements by joining multiple statements with **logical connectives**. The give us the ability to express and reason about more complex statements.

Definition 2. Logical Connectives:

Disjunction: the disjunction of two statements P and Q denoted $P \vee Q$ is true when either P or Q or both P and Q are true.

Conjunction: the conjunction of two statements P and Q denoted $P \wedge Q$ is true when both P and Q are true.

Negation: the negation of a statement P denoted $\neg P$ is true when P is false.

Implication: statement P (the **antecedent**) implies statement Q (the **conclusion**) if Q is always true when P is true. This is denoted $P \rightarrow Q$. Note that if P is false, the entire statement is always $vacuouslytrue$.

2.1.2 Truth Tables

To visualize the truth of large and complex statements, we find it useful to draw tables. Since the truth of large statements depends purely on its component statements, a table can be drawn to visualize how the component statements effect the overall statement.

Definition 3. Certain logical statements' **truth value** depends on the truth of other statements. For example, "the sun rose today **and** it rained today" requires both statements to be true in order for the overall statements to be true. If the sun rose but it didn't rain, or if the sun hasn't risen but it is raining, the overall statement is false. Thus, to visualize this relationship, it is useful to have a table to lay out the possibilities.

Example 2. $P \rightarrow Q$.

P	Q	$A \rightarrow B$
T	T	T
T	F	F
F	T	T
F	F	T

2.1.3 DeMorgan's Laws

With logical statements, we can actually find algebraic rules that allow us to find equivalent statements that may be more useful. One of the foundational algebraic rules of formal logic are known as the **DeMorgan's Laws**.

Definition 4. Logical statements and their combinations have their own form of algebra. One of the fundamental rules are DeMorgan's Laws, which state how to find the complements of conjunctions and disjunctions.

Theorem 1. *DeMorgan's Laws:*

1. $\neg(A \wedge B) = \neg A \vee \neg B$
2. $\neg(A \vee B) = \neg A \wedge \neg B$

2.2 Sets

Another foundation of mathematics is the **set**, which gives us the ability to reason about collections of objects. In many ways, mathematical concepts can be reasoned about through sets.

Definition 5. Set: An unordered collection of unique elements.

2.2.1 Unions, intersections, complements, and set differences

Sets on their own are useful, however we can perform operations on sets to create new sets. These operations form a kind of “set algebra”.

Definition 6. Set operations:

Union: the union of two sets A, B is the set that contain elements that are in A, or in B, or both.

$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$

Intersection: the intersection of two sets A, B is the set that contains elements that are in both A and B at the same time.

$$A \cap B = \{x \mid x \in A \wedge x \in B\}.$$

Difference: the set difference of two sets A, B is the set that contains all elements of A that are not in B. This operation is not commutative.‘’

$$A \setminus B = \{x \mid x \in A \wedge x \notin B\}.$$

Complement: the complement of a set A is the set of all elements that are not in A. For the complements of a set to be defined, it must be a subset of the unversal set $\mathcal{U}$. In other words, it is the set difference between $\mathcal{U}$ and A.

$$A^c = \mathcal{U} \setminus A.$$

We can actually find that “DeMorgan’s Laws” can be applied to sets, just as they were applied to logical statements.

Theorem 2. *DeMorgan’s Laws for Sets:*

1. $(A \cap B)^c = A^c \cup B^c$
2. $(A \cup B)^c = A^c \cap B^c$

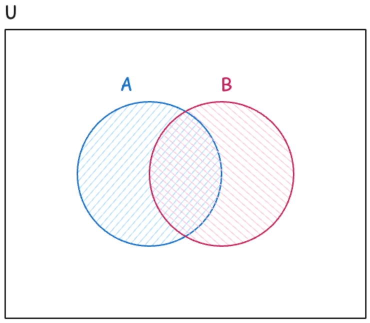
Proposition 1. *For all integers $n \geq 2$:*

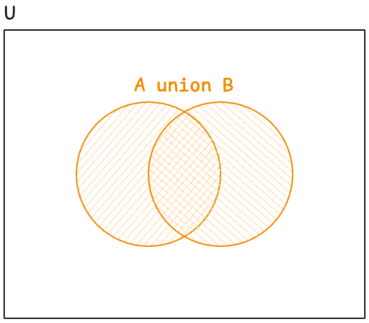
1. $(A_1 \cup A_2 \cup ... \cup A_n)^c = A_1^c \cap A_2^c \cap ... \cap A_n^c$
2. $(A_1 \cap A_2 \cap ... \cap A_n)^c = A_1^c \cup A_2^c \cup ... \cup A_n^c$

2.2.2 Venn diagrams

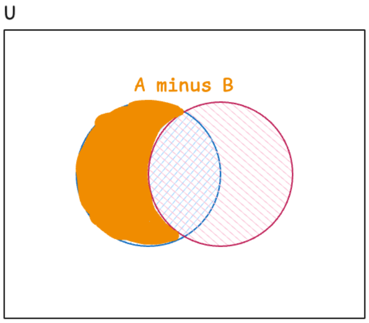
Similar to how we use truth tables to visualize the truth of logical statements, we can use **Venn diagrams** to visualize sets.

Definition 7. Venn diagrams: a visual aid for understanding sets and set operations.

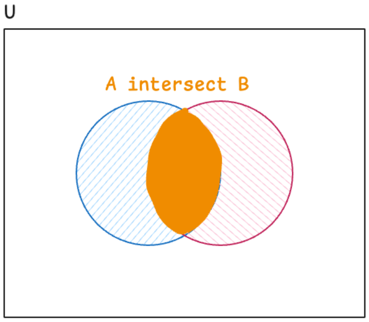




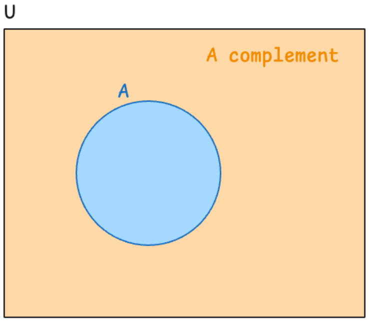
$A \cup B$



$A \setminus B$



$A \cap B$



A^c

2.3 Numbers and number systems

Now that we have defined sets, we can go on to define intuitive concepts like **numbers** formally. We can actually put numbers into sets that exhibit special properties.

Definition 8. Number: values that symbolize quantities.

Definition 9. Number system: way of representing numbers. Some are more sophisticated than others.

2.3.1 Parity, divisibility, and modular arithmetic

Within the set of natural numbers $\mathbb{N}$ and integers $\mathbb{Z}$, we can create special subsets based on how they can or can't be divided. We call this ruleset **modular arithmetic**. We have likely seen the notion of divisibility, before, however we find it useful to redefine them formally.

Definition 10. Divisibility: a number $n \in \mathbb{Z}$ is divisible by another number m if and only if $n = k \times m$ for some integer k.

Definition 11. Parity: the property of a number being even or odd. The number is even if it is divisible by two, and odd otherwise.

To generalize the idea of parity to other divisors, we must define **modular arithmetic**.

Definition 12. Modular arithmetic: a number system that groups numbers into equivalence classes based on their remainder when divided by a specific integer. More formally, for integers n, r, and m, we say n is **congruent** to r modulo m if $(n - r)$ is divisible by m.

$$n \equiv r \pmod{m} \Leftrightarrow m \mid (n - r)$$

For example, $5 \equiv 11 \pmod{3}$ since they both have a remainder 2 when divided by 3, and because $11 - 5 = 6$ is divisible by 3.

Standard arithmetic operations $+, -,$ and $\times$ are well-defined under modular arithmetic. However, $\div$ is not always well defined. These operations work the same way as they do in standard arithmetic. Notice that the parity of a number is equivalent to its divisible by 2, and a number's divisibility by $m \in \mathbb{N} > 0$ is a equivalent to it being congruent to 0 modulo m.

Proposition 2. *If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.*

Proposition 3. *If $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$, then:*

1. $a + b \equiv a' + b' \pmod{m}$
2. $a - b \equiv a' - b' \pmod{m}$
3. $a \times b \equiv a' \times b' \pmod{m}$

2.3.2 Rational and irrational numbers

Venturing past the whole numbers, we find the **rational** and **irrational** numbers. We can think of these as "decimal numbers." We find that **irrational** numbers have special properties.

Definition 13. Rational numbers $\mathbb{Q}$: the set of numbers that can be expressed as a ratio of two integers.

Definition 14. Irrational numbers: the set of numbers that can't be expressed as a ratio of two integers.

Proposition 4. *$\sqrt{2}$ is irrational.*

2.3.3 Real numbers, absolute value, and inequalities

The **real numbers** are the "main" type of number we encounter in math. They encompass the natural, rational, and irrational numbers.

Definition 15. Real numbers $\mathbb{R}$: the set of all numbers on our number line.

2.3.4 Combinatorics: combinations, permutations, and factorials.

When dealing with collections of objects, we may want to calculate the number of possible "arrangements." These arrangements are called **combinations** and **permutations**. They are calculated through the mathematical operation known as the **factorial**.

Definition 16. Combinations $C(n, r)$: the cardinality of the set of all subsets of a specific cardinality.

Definition 17. Permutations $P(n, r)$: the cardinality of the set of all orderings of a specific length.

Definition 18. Factorial: the product of natural numbers before it down to zero.

$$5! = 5 \times 4 \times 3 \times 2 \times 1.$$

2.3.5 Countable sets

When discussing the notion of infinity, it is often useful to reason about them by viewing them as the size of an infinitely large set. The "smallest" of these infinities is known as the **Countability infinite**.

Definition 19. Countable set: a set that is either finite, or that has the same cardinality as natural numbers $\mathbb{N}$. The second case is called **countably infinite**.

Lemma 1. *Let A and B be countably infinite sets. The Cartesian product $A \times B$ is also countably infinite.*

Proposition 5. *$\mathbb{Q}$ is countably infinite.*

2.3.6 Uncountable sets

We find that some infinities may be larger than other infinities. Notably, any infinity larger than a countable infinity is known as **uncountably infinite**. A fun fact is that we actually can't even ask the question of 'how many infinities are there?' because the answer is "axiomatically independent."

Definition 20. Uncountable set: a set that is infinite and there does not exists a bijection from it to the natural numbers.

Proposition 6. *$\mathbb{R}$ is not countably infinite.*

2.4 Relations and functions

We have discussed collections of objects, but not necessarily the relationships between the objects themselves, and how they can be expressed and reasoned about. This leads us to explore the notion of **relations**. Relations tell us about how objects within a set are related. Then, **functions** give us a sense of how to relate objects across sets. The existence of a special type of function known as a **bijection** necessarily means the sets have equal size.

2.4.1 Relations and equivalence relations

First, we explore how to relate objects in the same set by constructing a relation.

Definition 21. Relation R: a set of ordered pairs that represents if a two element $a, b \in S$ are related. $a$and$b$ are related if and only if $(a, b) \in R$.

Definition 22. Properties of Relations:

Reflexive: a relation R on set S is reflexive if and only if for every element $s \in S$, sRs.

Symmetric: a relation R on set S is symmetric if and only if for every pair of elements $s_1, s_2 \in S$, s_1Rs_2 implies s_2Rs_1.

Transitive: a relation R on set S is transitive if and only if for every trio of elements $s_1, s_2, s_3 \in S$, s_1Rs_2 and s_2R_s3 implies s_1Rs_3.

Some relations are special, and exhibit the same properties as equality, thus we call them equivalence relations.

Definition 23. Equivalence relations: a special type of relation on a set that satisfies the properties of being symmetric, reflexive, and transitive.

Theorem 3. *Congruence under modular arithmetic is an equivalence relation.*

2.4.2 Functions

To map objects to and from two arbitrary sets, we need the function.

Definition 24. Function: a mapping from a set called the domain to elements in a set called the codomain.

2.4.3 Injections (one-to-one), surjections (onto), and bijections

Some functions exhibit special properties. These properties are as follows:

Definition 25. Types of mappings:

Injection: a function $f : A \to B$ is injective if and only if every distinct element $a \in A$ maps to a distinct element $f(a) \in B$. In other words, there does not exist a pair of elements $a, a' \in A$ where $a \neq a'$ such that $f(a) = f(a')$.

Surjection: a function $f : A \to B$ is surjective if and only if for every element $b \in B$, there exists $a \in A$ such that $f(a) = b$.

Bijection: a function $f : A \to B$ is a bijection if and only if it is both injective and surjective.

Lemma 2. *If a bijection $f : A \to B$ exists, then $|A| = |B|$.*

Lemma 3. *If $|A| = |B|$, then a bijection $f : A \to B$ exists.*

Theorem 4. *A bijection $f : A \to B$ exists if and only if $|A| = |B|$.*

3 Proof techniques

Now that we have a solid understanding of some concepts in math, we may begin to prove some propositions we stated.

3.1 Direct Proofs

The most intuitive proof technique is the **direct proof**, which makes use of the standard rules of logic.

Definition 26. Direct proof: using fundamental rules of logic to prove a statement. The fundamental rules of logic are taken for granted as **axioms**.

Example 3. Proposition 2 can be proven directly from definitions.

Proof. Assume that $a \equiv b \pmod{m}$. This means that $m \mid (a-b)$. Thus, $a - b = km$ for some $k \in \mathbb{Z}$.
If we multiply both sides by -1, we get $b - a = -km$.
Thus, by definition, $m \mid (b-a)$ and $b \equiv a \pmod{m}$. □

Using the properties of modular arithmetic in definition 12, prove proposition 3
Given $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$:

1. $a + b \equiv a' + b' \pmod{m}$.

   Proof. We begin with by defining $a \equiv a' \pmod{m}$ as $m \mid (a - a')$. Similarly, $m \mid (b - b')$.

   Following from these definitions, we write:

   $$a - a' = m \times k_1 \tag{1}$$

   $$b - b' = m \times k_2 \tag{2}$$

   We can add equations eq. (1) and eq. (2) together to get $a + b - a' - b' = m \times k_1 + m \times k_2$.

   With some factoring, we get $(a + b) - (a' + b') = m(k_1 + k_2)$.

   By definition, we find that $m \mid (a + b) - (a' + b')$, and thus $a + b \equiv a' + b' \pmod{m}$. □

2. $a - b \equiv a' - b' \pmod{m}$.

   Proof. Following from Proof 1, we can instead subtract equation eq. (1) and eq. (2) to get $a - b - a' + b' = m \times k_1 - m \times k_2$.

   With some factoring, we get $(a - b) - (a' - b') = m(k_1 - k_2)$.

   By definition, we find that $m \mid (a - b) - (a' - b')$, and thus $a - b \equiv a' - b' \pmod{m}$. □

3. $a \times b \equiv a' \times b' \pmod{m}$.

   Proof. Following from equation eq. (1), we get

   $$a = a' + m \times k_1. \tag{3}$$

   Similarly, from equation eq. (2), we get

   $$b = b' + m \times k_2. \tag{4}$$

   By multiplying equations eq. (3) and eq. (4), we get $a \times b = (a' + m \times k_1)(b' + m \times k_2)$.

   From now on, I will omit the × *symbol.*

   By distributing, we get

   $$ab = a'b' + a'mk_2 + b'mk_1 + m^2k_1k_2.$$

We can factor out m to find

$$ab = a'b' + m(a'k_2 + b'k_1 + mk_1k_2).$$

We can subtract $a'b'$ from both sides to find

$$ab - a'b' = m(a'k_2 + b'k_1 + mk_1k_2).$$

By definition, we see that $m \mid (ab - a'b')$, and, by extension, $ab \equiv a'b' \pmod{m}$.

□

3.2 Transformation of conditionals

Definition 27. Transformation of conditionals: using rules of conditional logic to prove conditional statements.

For the following proofs, I will prove similar/related statements as it makes it easier to see the relationships between the transformations. We first perform a direct proof.

Example 4. Lemma 3 can be proven directly.

Proof. Suppose you have two sets A and B such that $|A| = |B| = n$. Thus, the elements of A can be enumerated by a_i for $0 < i \leq n$. Similarly, the elements of B can be enumerated by b_i for $0 < i \leq n$.

So, we can construct the function $f : A \to B$ as $f(a_i) = b_i$. f is injective because there does not exist a pair a_i, a_i' such that $f(a_i) = f(a_i')$. f is also surjective becuase for every $b_i \in B$, there exists $a_i \in A$ such that $f(a_i) = b_i$. Therefore, by definition, f is a bijection. □

3.2.1 Contrapositive proofs

Definition 28. Contrapositive: given a statement $P \Rightarrow Q$, the converse is $\neg Q \Rightarrow \neg P$ The truth value of a statement is equivalent to its contrapositive. By proving the contrapositive, you also prove the original statement.

Example 5. Lemma 3 can also be proven using its contrapositive. We find that this proof is slightly simplier.

Proof. We proceed by contrapositive by saying if no bijection $f : A \to B$ exists, then $|A| \neq |B|$.

Suppose two sets A and B such that there can not exist a bijection f. Thus, for any $f : A \to B$, f is either not injective or it is not surjective.

If f is not injective, then there exists $a, a' \in A$ such that $f(a) = f(a')$. Thus, $|A| > |B|$. However, if f is not surjective, then there exists $b \in B$ such that there does not exist $a \in A$ where $f(a) = b$. Thus, $|B| > |A|$. Therefore, in either case, $|A| \neq |B|$. □

3.2.2 Converse statements

Definition 29. Converse: given a statement $P \Rightarrow Q$, the converse is $Q \Rightarrow P$ The truth value of a statement's converse is equivalent to its **inverse**.

Example 6. Lemma 2 is the converse of lemma 3, and can be proven directly.

Proof. Since f is injective, distinct elements $a_i \in A$ will always map to different elements $b \in B$. In other words, $f(a_1) \neq f(a_2)$. Also, since f is surjective, for all elements $b \in B$, there exists an element $a \in A$ such that $f(a) = b$. Therefore, $|A| = |B|$.

□

3.2.3 Inverse statements

Definition 30. Inverse: given a statement $P \Rightarrow Q$, the inverse is $\neg P \Rightarrow \neg Q$. The truth value of a statement's inverse is equivalent to its **converse**.

Example 7. We can prove lemma 2 by proving the inverse of lemma 3. We will see that this is slightly simplier than the direct proof.

Proof. Suppose we have two sets A and B such that $|A| \neq |B|$. Thus, we have two cases:

$|A| > |B|$: Since there are more elements $a \in A$ than there are $b \in B$, there must be a pair of elements $a, a' \in A$ such that $f(a) = f(a')$.

Thus, f is not injective.

$|A| < |B|$: Since there are more elements $b \in B$ than there are $a \in A$, there must exist an element $b \in B$ such that $f(a) \neq b$ for all $a \in A$.

Thus, f is not surjective.

Therefore, f is not a bijection. □

3.2.4 Bidirectional (”if and only if” proofs)

Definition 31. Bidirectional proof: A bidirectional proof involves proving both a conditional statement and its converse to conclude that the **antecedent** and the **consequent** are logically equivalent.

Example 8. Theorem 4 can be proven bidirectionally by proving lemma 2 and lemma 3.

Proof. We have proven both lemma 3 and lemma 2 above. Thus, theorem 4 must be true. □

3.3 Quantifiers

Definition 32. Quantifier: a logical expression that denotes whether a statement is true for all cases or for specific cases.

3.3.1 Universal quantifiers

Definition 33. For a statement with a universal quantifier to be true on set S, the statement must be true for every single $s \in S$. Universal statements can be disproven by one counterexample.

Example 9. A function $f : D \to C$ is well defined on a domain D and codomain C if $f(d) \in C$ for all $d \in D$. Let $f(x) = \sqrt{x}$. Is $f : \mathbb{R} \to \mathbb{R}$ well defined?

Proof. We find that for $x < 0$, $f(x) \notin \mathbb{R}$. We have not just found one counterexample, we have found an uncountably infinite number of counterexamples.

So, f is not well defined. □

3.3.2 Existential quantifiers

Definition 34. For a statement with an existential quantifier to be true on set S, the statement must be true for at least one $s \in S$. Existential statements can be proven by one example.

Example 10. There exists a real number $r \in \mathbb{R}$, where $\sqrt{r} \in \mathbb{Q}$.

Proof. Let $r = 4$. $\sqrt{4} = 2 = \frac{2}{1}$. Thus, $\sqrt{2} \in \mathbb{Q}$. So, there exists a real number $r \in \mathbb{R}$, where $\sqrt{r} \in \mathbb{Q}$. □

3.3.3 Multiply quantified statements

Definition 35. Multiply quantified statement: statements that include more than one quantifier. Typically, they go "for all x, there exists y, such that z." They can be reasoned about by using an "adversarial" game, where player 1 picks an x that makes it hard for player 2 to pick a y to satisfies z. If player 1 can pick an x such that player 2 can't pick a valid y to satisfy z, player 1 'wins' and the statement is false.

In another case, the statement can go "there exists x, for all y, such that z. " In this case, player 1 just needs to pick one value x, such that for all values player 2 picks for y, it satisfies z. This makes the statement true.

Example 11. For all pairs of real numbers $x, y \in \mathbb{R}$ with $x < y$, there exists a rational number $r \in \mathbb{Q}$ such that $x < r < y$.

Proof. We first define a useful interpretation of constructing rational numbers by dividing two integers $r = n/d$. We are essentially taking n steps of length $1/d$.

Thus, if we have a sufficiently small step size, there must be an integer number of steps for us to land on the range $x < r < y$.

We see that if we have a step size smaller than $y - x$, we must always land within the range $x < r < y$.

We can see this by imagining a worst case scenario where $\frac{n-1}{d} = x$. Thus, because $1/d < y - x$,

$$\begin{aligned} x < \frac{n-1}{d} + \frac{1}{d} < y \\ x < \frac{n}{d} < y \end{aligned}$$

Similarly, we can see the other worst case scenario where $\frac{n+1}{d} = y$. Thus, because $1/d < y - x$,

$$\begin{aligned} x < \frac{n+1}{d} - \frac{1}{d} < y \\ x < \frac{n}{d} < y \end{aligned}$$

In order to achieve a step size smaller than $y - x$, we must satisfy the condition $1/d < y - x$. In other words, $d > \frac{1}{y-x}$. Furthermore, increasing d will only decrease the step size.

Thus, for all pairs of real numbers $x, y \in \mathbb{R}$ with $x < y$, we can find $d \in \mathbb{Z}$ with $d > \frac{1}{y-x}$. Then, there must exist an integer n where $x < n/d < y$. □

3.4 Existence and uniqueness proofs

Definition 36. Existence and uniqueness proof: a proof that results in us being sure that an element exists with a given property, and that it is the only element that exhibits such property. In many ways, existence and uniqueness proofs are equivalent to constructing a bijection.

Example 12. Lemma 1 can be proven using an existence and uniqueness proof.

Proof. Suppose sets A and B are countably infinite. By definition, there exists bijections $f_A : \mathbb{N} \to A$ and $f_B : \mathbb{N} \to B$. Thus, there must exist a bijection $f_{A\times B} : \mathbb{N}^2 \to A \times B$.

Now, if we can prove a bijection $f_{\mathbb{N}^2} : \mathbb{N} \to \mathbb{N}^2$, we also prove there exists a bijection $f : \mathbb{N} \to A \times B$ because of the transitivity of bijections.

We proceed by arranging $\mathbb{N} \times \mathbb{N}$ in a grid with rows indexed by i and columns indexed by j:

	$j = 1$	$j = 2$	$j = 3$	$j = 4$
$i = 1$	$(1, 1)$	$(1, 2)$	$(1, 3)$	$(1, 4)$
$i = 2$	$(2, 1)$	$(2, 2)$	$(2, 3)$	$(2, 4)$
$i = 3$	$(3, 1)$	$(3, 2)$	$(3, 3)$	$(3, 4)$
$i = 4$	$(4, 1)$	$(4, 2)$	$(4, 3)$	$(4, 4)$

$$(1, 1); \quad (1, 2), (2, 1); \quad (1, 3), (2, 2), (3, 1); \quad (1, 4), (2, 3), (3, 2), (4, 1); \ \dots$$

This traversal enumerates all pairs (i, j), and thus proves that there exists a bijection $f : \mathbb{N} \to \mathbb{N}^2$. In other words, **for any pair (i, j) there exists a unique $n \in \mathbb{N}$ such that the n^{th} element in this traversal is the pair**. Therefore, for any two countably infinite sets A and B, their Cartesian product is also countably infinite. □

Example 13. Proposition 5 is a natural extension of lemma 1.

Proof. Since rational numbers in $\mathbb{Q}$ are constructed as the ratio of two natural numbers $a, b \in \mathbb{N}$, we can think of $\mathbb{Q}$ as the cartesian product of $\mathbb{N}$ and itself. We notice that certain pairs are equivalent. For example, $2/4 = 1/2 \in \mathbb{Q}$, however they form distinct pairs in $\mathbb{N}^2$. Thus, in our diagonal traversal, we simple skip the redundant elements. In other words $\mathbb{Q} \subset \mathbb{N}^2$. Therefore, $\mathbb{Q}$ is countably infinite. □

3.5 Proof by Induction

Definition 37. Proof by Induction: proof technique used to prove a statement is true for a countably infinite set of discrete elements.

When doing proofs by induction, it is useful to enumerate the cases as $n \in \mathbb{N}$. This proof begins with a **base case** (or in some scenarios **base cases**) proving that the proposition is true for some "small" cases. Typically this means proving the proposition is true for $n = 0, 1, 2$. It is also helpful to "play" to gain intuition about our problem before proceding to the inductive step.

We then form an **inductive hypothesis** that assumes our proposition is true for cases $n \leq k$. Our **inductive step** is to prove that this assumption necessarily means that the $n = k + 1$ case must be true.

Thus, the cases n up to k implies case $n = k + 1$. So, starting at our base case, we know that $n = 0$ is true. Then we know that $n = 1$ is true. Since, cases $n = 0$ and $n = 1$ are true, case $n = 2$ is true. Then since cases $0 \leq n \leq 2$ are true, case $n = 3$ is true, and so on.

Now, it may seem that this proof is circular at first, since we are making a massive assumption in the form of our inductive hypothesis. However, our assumption is not the same as our conclusion. Our inductive hypothesis is used to prove that for any case $n = k$, its successor must be true.

Example 14. Proposition 1 can be proven with induction.

For the first case, we have

$$(A_1 \cup A_2 \cup ... \cup A_n)^c = A_1^c \cap A_2^c \cap ... \cap A_n^c.$$

Proof. First, we define some useful notation for a union and intersection for a large series of sets $A_1, A_2, ..., A_3$:

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup ... \cup A_n$$

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap ... \cap A_n.$$

First, we use theorem 2 (DeMorgan's Law for Sets) as the base case $n = 2$, $(A_1 \cup A_2)^c = A_1^c \cap A_2^c$.

Then, as our inductive hypothesis, we assume that

$$\left(\bigcup_{i=1}^{n} A_i\right)^c = \bigcap_{i=1}^{n} A_i^c, \text{ for } n \leq k.$$

Then, we see that for $n + 1$,

$$\left(\bigcup_{i=1}^{n+1} A_i\right)^c = \left(\bigcup_{i=1}^{n} A_i \cup A_{n+1}\right)^c$$

$$\left(\bigcup_{i=1}^{n+1} A_i\right)^c = \left(\bigcup_{i=1}^{n} A_i\right)^c \cap A_{n+1}^c.$$

We can use our inductive hypothesis to substitute $\left(\bigcup_{i=1}^{n} A_i\right)^c = \bigcap_{i=1}^{n} A_i^c$ to get,

$$\begin{aligned}\left(\bigcup_{i=1}^{n+1} A_i\right)^c &= \bigcap_{i=1}^{n} A_i^c \cap A_{n+1}^c. \\ &= A_1^c \cap A_2^c \cap ... \cap A_n^c \cap A_{n+1}^c.\end{aligned}$$

Therefore,

$$(A_1 \cup A_2 \cup ... \cup A_n)^c = A_1^c \cap A_2^c \cap ... \cap A_n^c$$

for any integer $n \geq 2$. □

Similarly, for the second case, we have

$$(A_1 \cap A_2 \cap ... \cap A_n)^c = A_1^c \cup A_2^c \cup ... \cup A_n^c.$$

Proof. First, we use theorem 2 (DeMorgan's Law for Sets) as the base case $n = 2$, $(A_1 \cap A_2)^c = A_1^c \cup A_2^c$.

Then, as our inductive hypothesis, we assume that

$$\left(\bigcap_{i=1}^{n} A_i\right)^c = \bigcup_{i=1}^{n} A_i^c, \text{ for } n \leq k.$$

Then, we see that for $n+1$,

$$\begin{aligned}\left(\bigcap_{i=1}^{n+1} A_i\right)^c &= \left(\bigcap_{i=1}^{n} A_i \cap A_{n+1}\right)^c \\ \left(\bigcap_{i=1}^{n+1} A_i\right)^c &= \left(\bigcap_{i=1}^{n} A_i\right)^c \cup A_{n+1}^c.\end{aligned}$$

We can use our inductive hypothesis to substitute $\left(\bigcap_{i=1}^{n} A_i\right)^c = \bigcup_{i=1}^{n} A_i^c$ to get,

$$\begin{aligned}\left(\bigcap_{i=1}^{n+1} A_i\right)^c &= \bigcup_{i=1}^{n} A_i^c \cup A_{n+1}^c. \\ &= A_1^c \cup A_2^c \cup ... \cup A_n^c \cup A_{n+1}^c.\end{aligned}$$

Therefore,

$$(A_1 \cap A_2 \cap ... \cap A_n)^c = A_1^c \cup A_2^c \cup ... \cup A_n^c$$

for any integer $n \geq 2$. □

Example 15. Let F_n be the n-th Fibonacci number, where $F_0 = F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$. Prove that $F_n \leq 1.9^n$ for all $n \geq 1$.

Proof. We proceed by induction, starting with the base cases, where $n = 1, 2$:

$$n = 1, F_1 = 1 \leq 1.9^1 = 1.9$$

$$n = 2, F_2 = 2 \leq 1.9^2 = 3.61.$$

We assume as an inductive hypothesis that $F_n \leq 1.9^n$ for $1 \leq n \leq k$.

Using our inductive hypothesis, we see that $F_k \leq 1.9^k$ and $F_{k-1} \leq 1.9^{k-1}$.

So, $F_k + F_{k-1} \leq 1.9^k + 1.9^{k-1}$.

By refactoring $1.9^k + 1.9^{k-1}$, we get:

$$1.9^k + 1.9^{k-1} = 1.9(1.9^{k-1}) + 1.9^{k-1} = 2.9(1.9^{k-1}).$$

Also, 1.9^{k+1} can be rewritten as $1.9^2(1.9^{k-1}) = 3.61(1.9^{k-1})$.
Finally, we see

$$F_{k+1} = F_k + F_{k-1} \leq 2.9(1.9^{k-1}) \leq 3.61(1.9^{k-1}) = 1.9^{k+1}$$
$$F_{k+1} \leq 1.9^{k+1}.$$

Thus, we conclude that by the principle of mathematical induction, $F_n \leq 1.9^n$ for all $n \geq 1$. □

Example 16. Look up the Tower of Hanoi puzzle. Prove that given a stack of disks, you can solve the puzzle in moves.

Proof. We begin by defining the Tower of Hanoi problem.

In this problem, we begin with a stack of n disks. The disks are ordered from largest at the bottom to smallest at the top. We are also given 3 'spots' to place our disks under one condition: that we never place a larger disk on top of a smaller disk.

Following these rules, what is the minimum number of moves required to move the entire pile to a new 'spot'?

We define the function $f : \mathbb{N} \to \mathbb{N}$ such that it maps the starting stack height n to the minimum number of moves required to move the entire pile $f(n)$.

Before immediately proving that $f(n) = 2^n - 1$, it is more intuitive to first define f as a recurrence relation, then prove that the recurrence relation is equal to $2^n - 1$.

We notice that moving the entire pile of n disks essentially requires 3 'phases':

1. Moving the top $n - 1$ disks onto a single pile.
2. Moving the nth disk to another vacant spot.
3. Moving the top $n - 1$ disks onto the new spot.

Thus, we know that $f(n) = f(n-1) + 1 + f(n-1) = 1 + 2f(n-1)$, where $f(1) = 1$. We can then prove $f(n) = 2^n - 1$ using induction.

We begin with our base cases:

n	$f(n)$
1	$1 = 2^1 - 1$
2	$3 = 2^2 - 1$
3	$7 = 2^3 - 1$

Now, we assume that $f(k) = 2^k - 1$ for all $1 \leq k \leq n$.
We see that

$$f(k+1) = 1 + 2f(k)$$
$$f(k+1) = 1 + 2(2^k - 1)$$
$$f(k+1) = 2^{k+1} - 1.$$

Thus, $f(n) = 2^n - 1$. □

3.6 Proof by Contradiction

Definition 38. Proof by contradiction: proof technique that assumes the opposite of our proposition, then showing that this leads to an absurd conclusion, ie. a contradiction. Used as a “last resort” proof technique.

This proof works because all statements in our mathematical universe can either be true or false. Thus, by assuming the opposite of our proposition, and showing that the opposite of our proposition **can not** be true, our original proposition then **must** be true. We show that the opposite of our proposition can’t be true through finding a contradiction.

This proof technique is used as a last resort since it doesn’t necessarily tell you much abou why/how our proposition is true, just that it must be true.

Example 17. Proposition 4 can be proven by contradiction.

We proceed by contradiction by assuing that $\sqrt{2} \in \mathbb{Q}$. So, we can write

$$\sqrt{2} = \frac{a}{b}$$

for $a, b \in \mathbb{N}$, and such that $\frac{a}{b}$ is in lowest form.

Then, with algebraic manipulation, we see

$$2 = \frac{a^2}{b^2}.$$

Thus, we get $a^2 = 2b^2$ and $b^2 = a^2/2$. So, a^2 is even, and by extension, a is even. Since a is even, we write $a = 2m$ for $m \in \mathbb{Z}$. Thus,

$$\begin{aligned} b^2 &= \frac{(2m)^2}{2}, \\ b^2 &= \frac{4m^2}{2}, \\ b^2 &= 2m^2, \end{aligned}$$

showing that b^2 must also be even.

This is a contradiction because we assumed that a/b was in lowest terms, however, we have just found a way to factor out a common 2. This contradiction shows that our original proposition was be false. So, $\sqrt{2}$ must be irrational.

Example 18. Proposition 6 can be proven by contradiction. This is the famous Cantor’s diagonalization argument.

First we assume that $\mathbb{R}$ is countably infinite. In other words, $|\mathbb{R}| = |\mathbb{N}|$, and that there exists a bijection between $\mathbb{R}$ and $\mathbb{N}$.

Thus, we can list out all the real numbers $r_i \in \mathbb{R}$ for $i \in \mathbb{N}$ in a table as follows where the rows are distinct real numbers r_i and the columns are their decimal places:

	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	$\cdots$	
r_1	$\mathbf{a_{11}}$	a_{12}	a_{13}	a_{14}	a_{15}	$\cdots$	a_{1n}
r_2	a_{21}	$\mathbf{a_{22}}$	a_{23}	a_{24}	a_{25}	$\cdots$	a_{2n}
r_3	a_{31}	a_{32}	$\mathbf{a_{33}}$	a_{34}	a_{35}	$\cdots$	a_{3n}
r_4	a_{41}	a_{42}	a_{43}	$\mathbf{a_{44}}$	a_{45}	$\cdots$	a_{4n}
r_5	a_{51}	a_{52}	a_{53}	a_{54}	$\mathbf{a_{55}}$	$\cdots$	a_{5n}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	
r_n	a_{n1}	a_{n2}	a_{n3}	a_{n4}	a_{n5}	$\cdots$	$\mathbf{a_{nn}}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	

Then, we see the bolded diagonal. With this diagonal, for each a_{jj} for $j \in \mathbb{N}$, we can construct an **entirely new** real number just be changing a_{jj}. In the original arument, Cantor states to add 1 if $a_{jj} < 9$ and to subtract 1 if $a_{jj} = 9$. However a more general way of saying this is to just pick a new integer $0 \leq a'_{jj} \leq 9$ that is not equal to a_{jj}.

So, we have now constructed a new real number, contradicting our assumption. Thus, we see that $\mathbb{R}$ must not be countably infinite.

4 Final project

5 Conclusion and reflection

Throughout this semester, I've found myself struggling with many concepts and problems. However, the problem that I struggled with most and that was the most memoriable is Choice Exercise 10 from HW08. It was memoriable for a very precise reason: that it truly exposed my weaknesses in problem solving. In class, we discussed the concept of "over abstracting" problems before we are truly ready to, and that is exactly what happend during my attempt at this problem.

I know I shouldn't have spent so much time on this one problem, but I spent literal hours engrossed in this problem trying to come up with "clean" algorithm to calculate the number of transitive and anti-transitive relations that could run with good asymptotic performance. Now, I love a a good puzzle, so I avoided looking at hints for a while. Eventually I came to my senses and realized that this wasn't even the problem that was assigned. I've been trained to always try to find the "best" solution in terms of algorithmic performance, that I just default to throwing out the brute force solution, and that was exactly what I need! When I eventually looked up the solution, I realized that there isn't actually a good closed formula for this yet! In retrospect, it's obvious that the brute force solution should be the very first solution I test and come up with, and there was no reason for me to try to optimize the algorithmic performance before I even had a working solution. Although I've heard this before, and I myself believe it, this experience with the problem really goes to show that premature optimization is root of all evil.

Zooming out slightly, I find that this course really felt like a primer for a lot of math topics that I am curious about. It's made math topics with scary names like "Category Theory" slightly less intimidating, and has really made me more curious to learn more about them. Specifically, I would like to explore the intersection between higher level math and Computer Science in areas like Type theory and compiler optimization. This goes hand in hand with my mathematical imagination. I feel as though this course really opened my eyes to higher level math.

Appendix

(The first section, "Course objectives and student learning outcomes" is just here for your reference.)

A Course objectives and student learning outcomes

1. Students will learn to identify the logical structure of mathematical statements and apply appropriate strategies to prove those statements.
2. Students learn methods of proof including direct and indirect proofs (contrapositive, contradiction) and induction.
3. Students learn the basic structures of mathematics, including sets, functions, equivalence relations, and the basics of counting formulas.
4. Students will be able to prove multiply quantified statements.
5. Students will be exposed to well-known proofs, like the irrationality of $\sqrt{2}$ and the uncountability of the reals.

A.1 Expanded course description

- Propositional logic, truth tables, DeMorgan's Laws
- Sets, set operations, Venn diagrams, indexed collections of sets
- Conventions of writing proofs
- Proofs
  - Direct proofs
  - Contrapositive proofs
  - Proof by cases
  - Proof by contradiction
  - Existence and Uniqueness proofs
  - Proof by Induction
- Quantifiers
  - Proving universally and existentially quantified statements
  - Disproving universally and existentially quantified statements
  - Proving and disproving multiply quantified statements
- Number systems and basic mathematical concepts
  - The natural numbers and the integers, divisibility, and modular arithmetic
  - Counting: combinations and permutations, factorials
  - Rational numbers, the irrationality of $\sqrt{2}$
  - Real numbers, absolute value, and inequalities
- Relations and functions
  - Relations, equivalence relations
  - Functions
  - Injections, surjections, bijections

- Cardinality
  - Countable and uncountable sets
  - Countability of the rational numbers, $\mathbb{Q}$
  - Uncountability of the real numbers, $\mathbb{R}$