Proofs Portfolio

MAT 3100W: Intro to Proofs

Sam Ly

November 18, 2025

1 Introduction

(Leave this blank for now. Here's an outline of course topics for your reference.)

2 Mathematical concepts

2.1 Logic, truth tables, and DeMorgan's laws

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. □

2.1.2 Truth Tables

Definition 2. 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. $A =$ the sun rose today, $B =$ it rained today.

A	B	$A \wedge B$
T	T	T
T	F	F
F	T	F
F	F	F

2.1.3 DeMorgan's Laws

Definition 3. 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

Definition 4. Set: An unordered collection of unique elements.

2.2.1 Unions, intersections, complements, and set differences

Definition 5. Union: the union of two sets A, B is the set that contain elements that are in A, or in B, or both.

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

Definition 6. 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.

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

Definition 7. 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.‘’

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

Definition 8. 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.

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

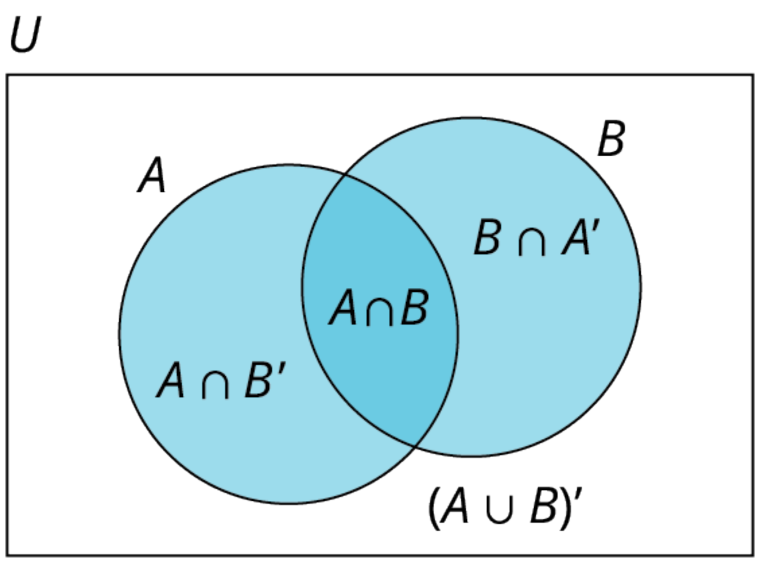
Theorem 2. *DeMorgan's Laws for Sets:*

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

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

2.2.2 Venn diagrams

Definition 9. Venn diagrams: a visual aid for understanding sets of objects and their relationships.



2.3 Numbers and number systems

Definition 10. Number: values that symbolize quantities.

Definition 11. Number system: way of representing numbers. Some are more sophisticated than others.

2.3.1 Parity, divisibility, and modular arithmetic

Definition 12. 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 13. Parity: the property of a number being even or odd. The number is even if it is divisible by two, and odd otherwise.

Definition 14. 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 divisability 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 1. *If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.*

Proposition 2. *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

Definition 15. Rational numbers $\mathbb{Q}$: the set of numbers that can be expressed as a ratio of two integers.

Definition 16. Irrational numbers: the set of numbers that can't be expressed as a ratio of two integers.

2.3.3 Real numbers, absolute value, and inequalities

Definition 17. Real number $\mathbb{R}$: the set of all numbers on our number line.

2.3.4 Combinatorics: combinations, permutations, and factorials.

Definition 18. Combinations: the cardinality of the set of all subsets of a specific cardinality.

Definition 19. Permutations: the cardinality of the set of all orderings of a specific length.

Definition 20. 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

Definition 21. Countable set: a set that is either finite, or that has a bijection to the natural numbers. A set is countably infinite if it has a bijection to the natural numbers.

2.3.6 Uncountable sets

Definition 22. Uncountable set: a set that is infinite and there does not exists a bijection from it to the natural numbers.

2.4 Relations and functions

2.4.1 Relations and equivalence relations

Definition 23. Relation R: a set of ordered pairs that represents if a two elemeent $a, b \in S$ are related. $a$and$b$ are related if and only if $(a, b) \in R$.

Definition 24. Equivalence relations: a special type of relation on a set that satisfies the properties of being symmetric, reflexive, and transitive.

2.4.2 Functions

Definition 25. Function: a mapping from a set called the domain to elemeents in a set called the codomain.

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

3 Proof techniques

3.1 Direct Proofs

Definition 26. Direct proof: using fundamental rules of logic to prove a statement.

Using the properties of modular arithmetic in definition 14, suppose $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$. Prove the following:

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 $\times$ *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.

3.2.1 Inverse statements

3.2.2 Converse statements

3.2.3 Contrapositive proofs

3.2.4 Bidirectional ("if and only if" proofs)

3.3 Quantifiers

Definition 28. Quantifier: a logical expression that denotes whether a statement is true for all cases or for specific cases.

3.3.1 Universal quantifiers

3.3.2 Existential quantifiers

3.3.3 Multiply quantified statements

3.4 Existence and uniqueness proofs

Definition 29. 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.

3.5 Proof by Induction

Definition 30. Proof by Induction: proof technique used to prove a statement is true for a countably infinite set of discrete elements.

As an example of Proof by Induction, we will prove the following.

Proposition 3. *Show that every positive integer is a sum of one or more numbers of the form 2^r3^s, where r and s are nonnegative integers and no summand divides another. (For example, $23 = 9 + 8 + 6$).*

Proof. We proceed by mathematical induction.

We start with $n = 0, 1$ as our base cases. We see that $n = 0$ is true, and $n = 1$ is true because $1 = 2^0 3^0$.

Now, we create the inductive hypothesis that all nonnegative integers strictly less than n have such summation.

If n is even, we can construct a valid summation by noticing that, from our inductive hypothesis, $\frac{n}{2}$ has a valid summation $\sum_{i=1}^{k} 2^{r_i}3^{s_i}$. Since none of these summands divide any other summand, multiplying all summands by 2 also creates a set of summands such that no summand divides another.

If n is odd, we can also construct a valid summation by picking a value 3^t that is the biggest power of 3 that is less than or equal to n. Our proposition is trivially true if $n = 3^t$. Otherwise, we must find a value $m = n - 3^t$.

Since n and 3^t are both odd, m must be even. Also notice that $m < n$. Thus, there must exist a valid summation $m = \sum_{j=1}^{k} 2^{r_j}3^{s_j}$ where all $r_j \geq 1$.

Since all summands of m are even, 3^t can not be divisible by any of the summands of m. Also, since $r_j \geq 1$, there must not be any summand where $s_j \geq t$ because if such summand existed, we would find at least a value of $n = 3^t + 2(3^t) = 3^{t+1}$. This is a contradiction, since we defined 3^t as the largest power of 3 less than or equal to n.

Thus, $n = \sum 2^r3^s$ where no summand divides another for all nonnegative integers n. □

Proposition 4. *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 $n \geq 1$. □

Proposition 5. *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 31. 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.

4 Final project

5 Conclusion and reflection

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, $\mathbb{R}$