Discrete Mathematics–Honors

Neo Wang
Lecturer: Isil Dilig

Last Updated: September 29, 2022

Contents

1 Logic and Sets 4
- 1.1 Lecture –August 23, 2022 . . . 4
  - 1.1.1 Predicate Logic . . . 4
- 1.2 Lecture–August 25, 2022 . . . 4
  - 1.2.1 Validity and Satisfiability . . . 5
- 1.3 Lecture–August 30, 2022 . . . 6
  - 1.3.1 Discussion 1 . . . 6
  - 1.3.2 Important equivalences . . . 7
  - 1.3.3 First Order Logic . . . 7
- 1.4 Lecture–September 1, 2022 . . . 8
  - 1.4.1 Quantifiers . . . 8
  - 1.4.2 DeMorgan's Laws for Propositional Logic . . . 9
  - 1.4.3 Nested Quantifiers . . . 9
- 1.5 Lecture–September 6, 2022 . . . 10
  - 1.5.1 Satisfiability and validity in FOL . . . 10
  - 1.5.2 Equivalence . . . 10
  - 1.5.3 Rules of Inference . . . 10
- 1.6 Lecture–September 8, 2022 . . . 12
  - 1.6.1 Universal Instantiation . . . 12
  - 1.6.2 Universal Generalization . . . 12
  - 1.6.3 Existential Instantiation . . . 13
  - 1.6.4 Existential Generalization . . . 13
- 1.7 Lecture–September 13, 2022 . . . 13
- 1.8 Lecture–September 15, 2022 . . . 14
  - 1.8.1 If and Only If Proofs . . . 15
  - 1.8.2 Counterexamples . . . 15
  - 1.8.3 Existence and Uniqueness . . . 15

2 Basic Set Theory 17
  - 2.0.1 Set Builder Notation . . . 17
  - 2.0.2 Set Builder Notation . . . 17
  - 2.0.3 Subsets and Supersets . . . 17
  - 2.0.4 Set Operations . . . 18
- 2.1 Lecture–September 20, 2022 . . . 19
  - 2.1.1 Undecidability . . . 19
- 2.2 Lecture–September 27, 2022 . . . 20
  - 2.2.1 Proving Injectivity . . . 20

2.2.2 Floor and Ceiling Functions 21
2.3 Lecture–September 29, 2022 22
2.3.1 Cardinality of Infinite Sets 22
2.3.2 Uncountability of Real Numbers 23

3 Number Theory **24**
3.0.1 Divisibility 24
3.0.2 Modulus 24

1 Logic and Sets

1.1 Lecture –August 23, 2022

1.1.1 Predicate Logic

There are three basic logical connectives: **and**, **or**, **not** which are denoted by $\wedge$, $\vee$, and $\neg$ respectively. The negation of a proposition p, written $\neg p$, is true if p is false and false if p is true.

1 **Example**

"Less than 80 students are enrolled in CS311H" is a proposition. The negation of this is at least 80 students are in CS311H

Conjunction of two propositions p and q is written $p \wedge q$

2 **Example**

The conjunction of p = "It is Tuesday" and q = "it is morning" is $p \wedge q$ = "It is Tuesday and it is morning"

- Disjunction is written $p \vee q$ and the disjunction between $p \vee q$ for p = "It is Tuesday" and q = "it is morning" is $p \vee q$ = "It is Tuesday or it is morning"
- If your formula has n variables then your truth table has $n + 1$ columns because you have n variables and one column for the truth value of the formula.
- The number of rows is given by the formula 2^n
- Other connectives: exclusive or $\oplus$, implication $\longrightarrow$, biconditional $\leftrightarrow$

1.2 Lecture–August 25, 2022

Let p = "I major in CS", q = "I will find a good job", r = "I can program"

- "I will not find a good job unless I major in CS or I can program": $(\neg p \wedge \neg r) \longrightarrow \neg q$
- "I will not find a good job unless I major in CS and I can program": $(\neg p \vee \neg r) \longrightarrow \neg q$
- The **inverse** of an implication $p \longrightarrow q$ is $\neg p \longrightarrow \neg q$. Therefore, "If I'm a CS major then I can program" has an inverse of "If I am not a CS Major then I'm not able to program."
- The **converse** of an implication $p \longrightarrow q$ is $q \longrightarrow p$.

3 **Definition** (Contrapositive)

The contrapositive of an implication of $p \longrightarrow q$ is $\neg q \longrightarrow \neg p$

The contrapositive of "if CS major then I can program" is "if I can't program, then I'm not a CS major"

p	q	$p \to q$	$\neg q \to \neg p$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

A converse and it's inverse are always the same.

4 **Definition** (Biconditionals)

$p \leftrightarrow q = p \to q \wedge q \to p = \neg(p \oplus q)$

5 **Example** (Operator precedence)

Given a formula $p \wedge q \vee r$ do we parse this as $(p \wedge q) \vee r$ or $p \wedge (q \vee r)$?

1. Negation $\neg$ has the highest precedence
2. Conjunction ($\wedge$) has the next highest precedence
3. Disjunction ($\vee$) has the next highest precedence
4. Implication ($\to$) has the next highest precedence
5. Biconditional ($\leftrightarrow$) has the lowest precedence
6. Make sure to explicitly use parentheses for $\oplus$

1.2.1 Validity and Satisfiability

Validity and satisfiability

- The truth value depends on truth assigments to variables
- Example: $\neg p$ evaluates to true under the assignment $p = F$ and to false under $p = T$
- Some formulas evaluate to true for all assignments–these are called **tautologies** or **valid formulas**
- Some formulas evaluate to false for all assignments–these are called **contradictions** or **unsatisfiable formulas**

6 **Definition** (Interpretation)

An interpretation I for a formula F is a mapping from each propositional value to exactly one truth value.

$$I : \{p \mapsto \text{true}, q \mapsto \text{false}, \ldots, \}$$

Each interpretation corresponds to one row in the truth table so there are 2^n interpretations for a formula with n variables.

If the formula is true under interpretation I then we write $I \models F$ and if the formula is false then we write $I \not\models F$.

Theorem: $I \models F$ if and only if $I \not\models \neg F$.

7 **Example**

Consider the formula $F : p \wedge q \to \neg p \wedge \neg q$

Let I_1 be the interpretation such that $[p \mapsto \text{true}, q \mapsto \text{true}]$

What does F evaluate to under I_1? Answer: true

8 **Example**

Let F_1 and F_2 be two propositional formulas. Suppose F_1 is true under I. Then, $F_2 \neg F_1$ evaluates to false under I (the "and" shortcuts and forces the whole equation to be false).

Satisfiability, Validy

- F is **satisfiable** iff there exists interpretation $I | I \models F$
- F is **valid** iff for all interpretations $I, I \models F$
- F is **unsatisfiable** iff for all interpretations $I, I \not\models F$
- F is **contingent** if it is satisfiable, but not valid.

9 **Example** (Are the following statements true of false?)

- If a formula is valid, then it is also satisfiable? True. All interpretations are satisfiable.
- If a formula is satisfiable, then its negation is unsatisfiable. False.
- If F_1 and F_2 are satisfiable, then $F_1 \wedge F_2$ is also satisfiable. False.
- If F_1 and F_2 are satisfiable, then $F_1 \vee F_2$ is also satisfiable. True.

10 **Theorem** (Duality Between Validity and Unsatisfiability)

F is valid iff $\neg F$ is unsatisfiable.

Proof. Definition: F is valid iff for all interpretations $I, I \models F$

Theorem: $I \models F \leftrightarrow I \not\models \neg F$

This is very easy to prove: just map all outputs of F to true. □

Question: How can we prove that a propositional formula is a tautology is true?

Answer: We can use the **truth table method** and prove that the formula is true for all possible truth assignments.

11 **Example** (Tautology)

$(p \to q) \leftrightarrow (\neg q \to \neg p)$ is a tautology.

$(p \wedge q) \vee \neg p$ is not a tautology.

1.3 Lecture–August 30, 2022

Implication: Formula F_1 implies F_2 (written $F_1 \implies F_2$) iff $\forall I, I \models F_1 \to F_2$

12 **Example** (Implication Removal)

Is $(p \wedge q) \to p$ true? False. Let $p = F, q = T$

p	q	$p \to q$	$\neg p \vee q$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

13 **Definition** (Implication Removal)

$p \to q$ is equivalent to $\neg p \vee q$

1.3.1 Discussion 1

- If p, then q: $p \to q$

- p only if q: $p \to q$
- p unless q: $\neg q \to p$
- p is necessary for q: $q \to p$
- p is sufficient for q: $p \to q$

1.3.2 Important equivalences

- Law of double negation: $\neg\neg p \equiv p$
- Identity laws: $p \wedge T \equiv p, p \vee F \equiv F$
- Domination Laws: $p \vee T \equiv T, p \wedge F \equiv p$
- Idempotent Laws: $p \wedge p \equiv p, p \vee p \equiv p$
- Negation Laws: $p \wedge \neg p \equiv F, p \vee \neg p \equiv T$

14 **Note** (Commutativity and Distributivity Laws)

- Commutative Laws: $p \vee q \equiv q \vee p, p \wedge q \equiv q \wedge p$
- Distributivity Law 1: $(p \vee (q \wedge r)) \equiv ((p \vee q) \wedge (p \vee r))$
- Distributivity Law 2: $(p \wedge (q \vee r)) \equiv ((p \wedge q) \vee (p \wedge r))$
- Associativity Laws:

$$p \vee (q \vee r) \equiv (p \vee q) \vee r$$

$$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$$

- Absorption 1: $p \wedge (p \vee q) \equiv p$
- Absorption 2: $p \vee (p \wedge q) \equiv p$

15 **Definition** (De Morgan's Laws)

Let a = "John took CS311" and b = "John took CS312". What does $\neg(a \wedge b)$ mean? It means "John did not take both CS311 and CS312". Therefore, John didn't take either CS311 or CS312.

$$\neg(a \wedge b) \equiv \neg a \vee \neg b$$

16 **Example** (Prove $\neg(p \wedge (\neg p \wedge q)) \equiv \neg p \wedge \neg q$)

p	$\neg p$	q	$p \wedge (\neg p \wedge q)$	$\neg(p \wedge (\neg p \wedge q))$
T	F	T	T	F
T	F	F	F	T
F	T	T	F	T
F	T	F	F	T

17 **Example**

If Jill carries an umbrella, it is raining. Jill is not carrying an umbrella. Therefore, it is not raining.

$$((u \to r) \wedge (\neg u)) \to \neg r$$

This can be counter-modeled with r = true, u = false.

1.3.3 First Order Logic

- The building blocks of propositional logic were propositions

- In first-ordre logic there are three kinds of basic building blocks: constants, variables, predicates.
- Constants: refer to specific objects
- Examples: George, 6, Austin, CS311, ...
- If a universe of discourse is cities in Texas, x can represent Houston, Houston, etc.
- **Predicates** describe properties of objects or relationships between objects.
- A predicate $P(c)$ is true or false depending on whether property P holds for c.
- The truth value of `even(2)` = true
- Another example: Suppose $Q(x, y)$ denotes $x = y + 3$ what is the value of $Q(3, 0)$? true

1.4 Lecture–September 1, 2022

- In propositional logic, the truth value depends on a truth assignment
- In FOL, truth depends on interpretation over some domain D
- Universe of discourse (domain) + what elements in the domain the variables map to

18 **Example** (Semantics of First-Order Logic)

Consider a FOL formula $\neg P(x)$

$$D = \{A, B\}, P(A) = \text{true}, P(B) = \text{false}, x = A$$

This is a falsifying interpretation

19 **Example**

Consider I over domain $D = \{1, 2\}$

- $P(1, 1) = P(1, 2) = \text{true}, P(2, 1) = P(2, 2) = \text{false}$
- $Q(1) = \text{false}, Q(2) = \text{true}$
- $x = 1, y = 2$
- What is $P(x, y) \wedge Q(y)$ under I? True.
- What is truth value of $P(y, x) \rightarrow Q(y)$ under I? True.
- Waht is truth value of $P(x, y) \rightarrow Q(x)$ under I? False.

1.4.1 Quantifiers

- Real power of first-order logic over propositional logic: quantifiers.
- There are two quantifiers in first-order logic:
  1. Universal quantifier (for **all** objects): $\forall x P(x)$
  2. Existential quantifier (for **some** object): $\exists x P(x)$

20 **Example**

Let $D = \{a, b\}, P(a) = \text{true}, P(b) = \text{false}$ then $\forall x.P(x)$ is false.

21 **Example**

Consider $D = \mathbb{R}$ and $P(x) = x^2 \geq x$ then $\forall x.P(x)$ is false.

- In first-order logic, domain is required to be **non-empty**.

22 **Example**
Consider the domain of reals and predicate $P(x)$ with interpretation $x < 0$. Then, $\exists x.P(x)$ is true.

- $\forall x.P(x)$ is true iff $P(o_1) \land P(o_2) \land \ldots \land P(o_n)$ is true
- $\exists x.P(x)$ is true iff $P(o_1) \lor P(o_2) \lor \ldots \lor P(o_n)$ is true

$\exists x.(\text{even}(x) \land \text{gt}(x, 100))$ is a valid formula in FOL.

23 **Example** (What is the truth value of the following formulas?)

- $\forall x.(even(x) \rightarrow div4(x))$ False. $x = 2$ is a counter-model.
- $\exists x.(\neg div4(x) \land even(x))$ True.
- $\exists x.(\neg div4(x) \rightarrow even(x))$ True.

24 **Example** (Translating English into formulas)
Assuming $\texttt{freshman}(x)$ means "x is a freshman" and $\texttt{inCS311}(x)$ to be x is taking CS311, then "someone in CS311 is a freshman" is $\exists x.(\texttt{freshman}(x) \land \texttt{inCS311}(x))$.
No one in CS311 is a freshman: $\forall x.(freshman(x) \rightarrow \neg inCS311(x))$
Everyone taking CS311 are freshmen: $\forall x.(inCS311(x) \rightarrow freshman(x))$
All freshmen take CS311: $\forall x.(freshman(x) \rightarrow inCS311(x))$

1.4.2 DeMorgan's Laws for Propositional Logic

$$\neg(p \land q) \equiv \neg p \lor \neg q$$
$$\neg(p \lor q) \equiv \neg p \land \neg q$$
$$\neg\forall x.P(x) \equiv \exists x.\neg P(x)$$
$$\neg\exists x.P(x) \equiv \forall x.\neg P(x)$$

25 **Example**
We can change $\neg\exists x.(inCS311(x) \land freshman(x))$ to $\forall x.(\neg inCS311(x) \lor \neg freshman(x))$ which is equivalent to $\forall x.(inCS311(x) \rightarrow \neg freshman(x))$.

1.4.3 Nested Quantifiers

- Sometimes may be necessary to use multiple quantifiers
- For example, can't express "EEverybody loves someone" using a single quantifier.
- Suppose predicate $L(x, y)$ means "x loves y".
- What does $\forall x.\exists y.L(x, y)$ mean? "Everybody loves someone"
- What does $\exists y.\forall x.L(x, y)$ mean? "There is someone who is loved by everybody"

26 **Example** (More Nested Quantifier Examples)

- "Someone loves everyone" $\exists x.\forall y.L(x, y)$
- "There is someone who doesn't love anyone' $\exists x.\forall y.\neg L(x, y)$
- "There is someone who is not loved by anyone" $\exists x.\forall y.\neg L(y, x)$
- "Everyone loves everyone" $\forall x.\forall y.L(x, y)$
- "Someone doesn't love themselves": $\exists x.\neg L(x, x)$

1.5 Lecture–September 6, 2022

27 **Example**

- Every UT student has a friend: $\forall x.(atUT(x) \land student(x) \rightarrow \exists y.friends(x, y))$
- $\exists x.(atUT(x) \land student(x)) \land \forall y.\neg friends(x, y)$
- $\forall x \forall y(atUT(x) \land student(x) \land atUT(y) \land student(y)) \rightarrow friends(x, y))$

1.5.1 Satisfiability and validity in FOL

- The concepts of satisfiability validty also important in FOL
- FOL F is satisfiable if there exists some domain and some interpretation such that F is true.
- Example: Prove that $\forall x.(P(x) \rightarrow Q(x))$ is satisfiable. Solution: Let $P(x)$ be false. Let the domain $D = \{x\}$
- Example: Prove that $\forall x.(P(x) \rightarrow Q(x))$ is satisfiable. Solution: Let $P(x)$ be true, let $Q(x)$ be false. Let the domain $D = \{x\}$

1.5.2 Equivalence

- Two formulas F_1 and F_2 are equivalent iff $F_1 \leftrightarrow F_2$ is valid.
- We could prove equivalence using truth tables but not possible in FOL.
- However, we can still use known equivalences to rewrite one as the other.

28 **Example**

Prove that

$$\neg(\forall x.(P(x) \rightarrow Q(x))) \equiv \exists x.(P(x) \land \neg Q(x))$$

1.5.3 Rules of Inference

- We can prove validity in FOL by using **proof rules**
- Proof rules are written as **rules of inference**
- An example inference rule:

$$\begin{array}{c} F_1 \\ F_2 \\ \hline \therefore F_1 \land F_2 \end{array}$$

Modus Ponens

The most basic inference rule is modus ponens:

$$\frac{\begin{array}{c} F_1 \\ F_1 \rightarrow F_2 \end{array}}{\therefore F_2}$$

- Modus ponens applicable to both propositional logic and first-order logic.

Modus Tollens

- Second important inference rule is **modus tollens**:

$$\frac{\begin{array}{c} F_1 \rightarrow F_2 \\ \neg F_2 \end{array}}{\therefore \neg F_1}$$

Hypothetical Syllogism

Implication is transitive.

$$\frac{\begin{array}{c} F_1 \rightarrow F_2 \\ F_2 \rightarrow F_3 \end{array}}{\therefore F_1 \rightarrow F_3}$$

Or Introduction

$$\frac{F_1}{\therefore F_1 \vee F_2}$$

Or Elimination

$$\frac{\begin{array}{c} F_1 \vee F_2 \\ \neg F_2 \end{array}}{\therefore F_1}$$

And Introduction

$$\frac{\begin{array}{c} F_1 \\ F_2 \end{array}}{\therefore F_1 \wedge F_2}$$

Resolution

$$\frac{\begin{array}{c} F_1 \vee F_2 \\ \neg F_1 \vee \neg F_3 \end{array}}{\therefore F_2 \vee F_3}$$

Proof: ϕ_1 must be either true or false. If ϕ_1 is true, then ϕ_3 must be true. If ϕ_1 is false then ϕ_2 must be true. Therefore either ϕ_2 or ϕ_3 must be true.

29 **Example**

Assume the following:

S, C, L, H

$$\neg S \wedge C$$
$$L \rightarrow S$$
$$\neg L \rightarrow H$$
$$H \rightarrow back$$

We know that $\neg S$ is true, so S is false. Therefore, for $L \rightarrow S$ to be true, L must be false. In order for $\neg L \rightarrow H$ to be true, H must be true. Since H is true we know we must be back by sunset because that's the only way to make the last expression true.

1.6 Lecture–September 8, 2022

- Generalization and the other one is called instantiation

1.6.1 Universal Instantiation

- If we know that something is true for all members of a group we can conclude is also true for a specific member of this group.
- This idea is called **universal instantiation**

$$\frac{\forall x.(F(x))}{F(a)}$$

30 **Example**

Consider predicates $man(X)$ and $mortal(x)$ and the hypotheses:

- All men are mortal: $\forall x.(man(x \rightarrow mortal(x)))$
- Socrates is a man: $man(socrates)$
- Prove mortal(Socrates)
- $$man(socrates) \rightarrow mortal(socrates)$$
  $$mortal(socrates)(2, 3, modus\ ponens)$$

1.6.2 Universal Generalization

- Prove a claim for an **arbitrary** element in the domain.
- Since we've made no assupmtions proof should apply to all elements in the domain.
- The correct reasoning is captured by **universal generalization**
- "arbitrary" means an objects introduced through universal instantiation.

$$\frac{P(c)\text{for arbitrary c}}{\forall x.P(x)}$$

31 **Example**

Prove $\forall x.Q(x)$ from the hypothesis:

1. $\forall x.(P(x) \rightarrow Q(x))$
2. $\forall x.P(x)$
3. $P(a)$ (2, U-inst)
4. $P(a) \rightarrow Q(a)$ (1, U-inst)

5. $Q(a)$ (3, 4, MP)
6. $\forall x.Q(x)$ (5, U-gen)

Caveats about universal generalization

- When using universal generalization need to ensure that c is truly arbitrary
- If you prove something about a specific person Mary, you cannot make generalizations about all people.

1.6.3 Existential Instantiation

- Consider formula $\exists x.P(x)$
- We know there is an element c in the domain for which $P(c)$ is true.
- This is called **existential instantiation**

$$\frac{\exists x.P(x)}{P(c)}$$

- Here c is a **fresh** name (i.e. not used in the original formula)

32 **Example**

Prove $\exists x.P(x) \land \forall x.\neg P(x)$ is unsatisfiable.

1. $\exists x.P(x)$ (and elimination)
2. $\forall x.\neg P(x)$ (and elimination)
3. $P(a)$
4. $\neg P(a)$
5. False

1.6.4 Existential Generalization

- Suppose we know $P(c)$ is true for someone constant c
- Then there exists an element for which P is true.
- Thus we canc conlude $\exists x.P(x)$
- This inference rule is called **existential generalization**

$$\frac{P(c)}{\exists x.P(x)}$$

1.7 Lecture–September 13, 2022

Some terminology

- Important mathematical statements that can be shown to be true are **theorems**
- Many famous mathematical theormes, e.g., Pythagoraean theorem, Fermat's Last Theorem
- Pythagorean theorem: $a^2 + b^2 = c^2$
- Fermat's Last Theorem: $a^n + b^n = c^n$ has no solutions for $n > 2$

Theorems, Lemmas, and propositions

- Lemma: minor auxilary result aids in the proof of a theorem.

- Corollary: a result whose proof follows immediately from a theorem or proposition

Conjectures vs. Theorems

- Conjecture is a statement that is suspected to be true by experts but not proven.
- Goldman's Conjecture: Every even integer greater than 2 can be expressed as the sum of two prime numbers
- One of the most famous unsolved problems in mathematics

General Strategies for Proving Theorems:

- Direct proof: $p \rightarrow q$ proved by directly showing that if p then q.
- Proof by contraposition: $p \rightarrow q$ proved by showing that if $\neg q$ then $\neg p$.

33 **Example**

If n is an odd integer then n^2 is also odd.

Assume n is odd.

Proof. $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2k' + 1$.

$\therefore n^2$ is odd □

34 **Example**

In proof by contraposition, you prove $p \rightarrow q$ by assuming $\neg q$ and $\neg p$ follows. For example: n is an odd integer, then n^2 is also odd. Or, you can prove if n is not odd, then n^2 is not odd.

Proof. $n = 2k$

$n^2 = 4k^2$

$2(2k^2)$ is even □

Proof by contradiction: A formula ϕ is valid iff $\neg\phi$ is unsatisfiable.

Assume $\neg(p \rightarrow q)$ is unsatisfiable. If you can prove that it is unsatisfiable then you have proved that $p \rightarrow q$ is valid.

35 **Example**

Prove by contradiction that if $3n + 2$ is odd, then n is odd.

Proof. Assume $3n + 2$ is odd and n is even. Since n is even, $3n + 2$ can be written as $6k + 2 | k \in \mathbb{Z}$ which contradicts our assumption. □

1.8 Lecture–September 15, 2022

36 **Example**

Example: Prove that every rational number can be expressed as a product of two **irrational numbers**.

Suppose r is a non-zero rational number. From lemma, we have $\frac{r}{\sqrt{2}}$ is irrational. From earlier proofs, we know that $\sqrt{2}$ is irrational. This implies r can be written as product of 2 irrationals.

Lemma: If r is a non-zero rational number, then $\frac{r}{\sqrt{2}}$ is irrational.

Proof. Proof by contradiction. Suppose r is a non-zero rational number and $\frac{r}{\sqrt{2}}$ is also rational.

From definition of rational numbers, $r = \frac{a}{b}$ and $\frac{r}{\sqrt{2}} = \frac{p}{q}$.

where $a, b, p, q \in \mathbb{Z}$ and $b, q \neq 0$.

$$\frac{r}{\sqrt{2}} = \frac{p}{q} \implies \sqrt{2} = \frac{rq}{p}$$

which would imply that $\sqrt{2}$ is irrational, which cannot be true because it would contradict. Therefore, $\frac{r}{\sqrt{2}}$ is irrational. □

1.8.1 If and Only If Proofs

- Some theorems are of the form "P if and only if Q" ($P \iff Q$).
- We can prove $P \iff Q$ by proving $P \to Q$ and $Q \to P$.

37 **Example**

Prove: "A positive integer n is odd if and only if n^2 is odd."

- $\to$ has been shown using a direct proof earlier.
- $\leftarrow$ has shown by a proof by contraposition.
- Since we have both directions the proof is complete.

1.8.2 Counterexamples

- How do we want to prove that a statement is false? Counterexample!
- The product of two irrational numbers is irrational? False. Consider $\sqrt{2}\sqrt{2} = 2$.

For all integers n, if n^3 is positive, n is also positive. We can use contraposition.

1.8.3 Existence and Uniqueness

- Common math proofs involve showing **existence** and **uniqueness** of certain objects.
- Existence proofs require showing that an object with the desired property exists.
- One way to prove existence is show that one object has the desired property.
- Example: Prove exists an integer that is sum of two perfect squares.
- Proof: $2^2 + 2^2 = 8$
- Indirect existence proofs are called non-constructive proofs.

Prove: "There exist irrational numbers x, y s.t. x^y is rational."

Proof. Consider $z = \sqrt{2}^{\sqrt{2}}$

Case 1: z is rational. Then since $z = \sqrt{2}^{\sqrt{2}}$ is rational and $\sqrt{2}$ is irrational, z is irrational.

Case 2: z is irrational.

- We know $\sqrt{2}$ is irrational.
- Our assumption for case 2 is $\sqrt{2}^{\sqrt{2}}$ is irrational.
- $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$ so $x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$

□

38 **Example**

Prove: There is a real unique number r such that $ar + b = 0$

Existence proof: $r = -\frac{b}{a}$

39 **Example**

Uniqueness: There exists a unique r satisfying $ar + b = 0$.

Proof.

- Suppopse there are two difference $r_1 + r_2$ that satisfy $ar + b = 0$.
- Then that would mean $ar_1 + b = ar_2 + b = 0$. Then $r_1 = r^2$ which is a contradiction which proofs uniqueness.

□

2 Basic Set Theory

2.0.1 Set Builder Notation

40 **Definition** (Common Sets)

- Many sets that play fundamental roles in mathematics are infinite.
- Set of integers $\mathbb{Z} = \ldots, -2, -1, 0, 1, 2, \ldots$.
- Set of positive integers: $\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$
- Natural numbers: $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$
- Set of real numbers: $\mathbb{R}$
- All rational numbers: $\mathbb{Q}$
- Irrational numbers: $\mathbb{I}$

2.0.2 Set Builder Notation

- Infinite sets are often written using set builder notation.

$$S = \{x \mid P(x)\}$$

- Universal set U includes all objects under consideration.
- The empty set written as $\emptyset$ is the set with no elements.
- A set containing exactly one element is called a singleton set.

2.0.3 Subsets and Supersets

- A set A is a subset of set B written $A \subseteq B$ if every element of A is also an element of B.

$$\forall x.(x \in A \rightarrow x \in B)$$

- If $A \subseteq B$ then B is called a superset of A, written $B \supseteq A$.
- A set A is a proper subset of set B written $A \subset B$ if $A \subseteq B$ and $A \neq B$.
- Sets A and B are equal, written $A = B$, if $A \subseteq B$ and $B \subseteq A$.

41 **Definition** (Power Set)

- The power set of a set S written $P(S)$ is the set of all subsets of S.
- What is the powerset of $\{a, b, c\}$?

$$\{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

- $|P(S)| = 2^{|S|}$
- $P(\emptyset) = \{\emptyset\}$
- $P(P(\emptyset)) = \{\emptyset, \{\emptyset\}\}$

42 **Definition** (Cartesian Product)

- To define the Cartesian product we need ordered tuples.
- An **ordered n-tuple** is the ordered collection with a_1 as its first element, a_2 as its second element, and a_n as its last element.
- Observe: $(1, 2)$ and $(2, 1)$ are different ordered pairs.
- The Cartesian product of two sets A and B is the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$.

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

43 **Example**

Let $A = \{1, 2\}$ and $B = \{a, b, c\}$. Find $A \times B$.

$$A \times B = \{(a, b) \mid a \in A, b \in B\} = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$$

We can also extend the Cartesian product to more than two sets.

44 **Definition** (Cartesian Product of More than Two Sets)

- The Cartesian product of more than two sets is defined recursively.
- Let $A_1, A_2, \ldots, A_n$ be sets. Then

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}$$

45 **Example**

If $A = \{1, 2\}, B = \{a, b\}, C = \{\star, \circ\}$ what is $A \times B \times C$?

$$A \times B \times C = \{(a, b) \mid a \in A, b \in B\} = \{(1, a, \star), (1, a, \circ), (1, b, \star), (1, b, \circ), (2, a, \star), (2, a, \circ), (2, b, \star), (2, b, \circ)\}$$

2.0.4 Set Operations

46 **Definition** (Set union)

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$$

47 **Definition** (Intersection)

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$

48 **Definition** (Difference)

$$A - B = \{x \mid x \in A \text{ and } x \notin B\}$$

49 **Definition** (Complement)

$$\overline{A} = \{x \mid x \notin A\}$$

2.1 Lecture–September 20, 2022

Prove De Morgan's Law for Sets: $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Proof.

$$\begin{aligned}
\overline{A \cup B} &= \{x \mid x \notin A \cup B\} && (2.1)\\
&= \{x \mid \neg(x \in A \cup B)\} && (2.2)\\
&= \{x \mid x \notin a \wedge x \notin b\} && (2.3)\\
&= \{x \mid x \in \overline{A} \wedge x \in \overline{B}\} && (2.4)\\
&= \overline{A} \cap \overline{B} && (2.5)
\end{aligned}$$

□

- Intuitive formulation for sets is called naive set theory.
- Any definable collection is a set
- In other words unrestricted comprehension says that $\{x \mid F(x)\}$ is a Set for any formula F.
- Russell showed that Cantor's set theory is inconsistent.
- This can be shown using so-called "Russell's Paradox".

50 **Definition** (Russell's Paradox)

- Let A be a set. Then A is a member of A if and only if A is not a member of A.
- This is a contradiction.

$$R = \{S \mid S \notin S\}$$

2.1.1 Undecidability

- A proof similar to Russell's paraodx can be used to show **undecidability** of the Halting Problem.
- A decision problem is a question that has a yes or no answer.
- A decision problem is **undecidable** if it is not possible to have an algorithm that always terminates and gives correct answer.

51 **Theorem** (Halting Problem is Undecideable)

Proof by contradiction: Let a program called Calvin take parameter p.

- Let $b = TermChecker(P, P)$.
- If b, then Calvin will infinite loop.
- Otherwise, Calvin will terminate.

Because of this self-reference, we don't know whether Calvin will terminate or not. Does Calvin terminate on itself? By Russell's Paradox, we can't know. Contradiction.

Other famous undecideable problems

- **Validity in first-order logic**. Given an arbitrary first order logic formula F, is F valid? (Hilbert's Entschiedungsproblem)
- Program verification: Given a problem P and a non-trivial property Q does P satisfy Q? (Rice's theorem)
- Hilbert's 10th problem: Does a diophantine equation $p(x_1, x_2, \ldots, x_n) = 0$ have a solution?

- Image = a group of some elements of the output set when some elements of the input set are passed to the function. When the function is passed the entire input set, this is sometimes known as the range.

- Preimage = a group of some elements of the input set which are passed to a function to obtain some elements of the output set. It is the inverse of the Image.
- Domain = all valid values of the independent variable. This makes up the input set of a function, or the set of departure. These are all elements that can go into a function.
- Codomain = all valid values of the dependent variable. This makes up the output set of a function, or the set of destination. These are all elements that may possibly come out of a function.

2.2 Lecture–September 27, 2022

2.2.1 Proving Injectivity

Consider the function

$$f(x) = \begin{cases} 3x + 1 & \text{if } x \geq 0 \\ -3x + 2 & \text{if } x < 0 \end{cases}$$

Proof. Case 1: $x \geq 0$ and $y \geq 0$.

$$\begin{aligned} f(x) &= 3x + 1 \\ f(y) &= 3y + 1 \\ 3x + 1 &= 3y + 1 \\ x &= y \end{aligned}$$

Case 2: $x < 0$ and $y < 0$.

$$\begin{aligned} -3x + 2 &= -3y + 2 \\ -3x &= -3y \\ x &= y \end{aligned}$$

Case 3: $x < 0$ and $y \geq 0$.

$$\begin{aligned} f(x) &= 3x + 1 \\ f(y) &= 3y + 1 \\ 3x + 3y &= 1 \\ x + y &= \frac{1}{3} \end{aligned}$$

It can never be the case that $x + y = \frac{1}{3}$ because x and y are integers. Therefore we have reached a contradiction and the function is not injective. □

52 **Definition** (Onto functions)

Items are onto if

$$\forall y \in B. \exists x \in A. f(x) = y$$

all elements in the codomain are images of some element in the domain.

53 **Definition** (Bijective Functions)

- Function that is both onto and one-to-one is called a **bijection**
- One-to-one correspondence or invertible function are synonymous.

54 **Example** (Identity function)

$$\forall x \in A . I(x) = x$$

Every bijection from set A to set B has an inverse function f^{-1}.
Why does inverse not exist if f is not surjective? There are elements in the new domain that would not map.
Composition: $f(x) = 2x + 3$ and $g(x) = 3x + 2$ then $f \circ g = 2(3x + 2) + 3 = 6x + 8$.
Another composition: prove that $f^{-1} \circ f$ is the identity function. You swap the domain and codomain twice.

55 **Example**
If f and g are injective, then $f \circ g$ is also injective.
Proof.

$$f(a) = f(b) \iff a = b$$
$$g(a) = g(b) \iff a = b$$
$$g(f(a)) = g(f(b)) \implies f(a) = f(b) \implies a = b$$

□

2.2.2 Floor and Ceiling Functions

56 **Definition** (Floor and Ceiling Functions)
Both floor and ceiling functions map $f : \mathbb{R} \to \mathbb{Z}$.

- **Floor function** $f(x) = \lfloor x \rfloor$ is the largest integer less than or equal to x.
- **Ceiling function** $f(x) = \lceil x \rceil$ is the smallest integer greater than or equal to x.

$x = y + \epsilon$ for some $\epsilon \in [0, 1)$.
$x = y - \epsilon$ for some $\epsilon \in [0, 1)$.

57 **Example**
Prove that $\lfloor -x \rfloor = -\lceil x \rceil$.
Proof.
RHS:

$$y = x + \epsilon$$
$$x = y - \epsilon$$
$$-y$$

LHS:

$$-(y - \epsilon)$$

$$-y + \epsilon$$
$$-y$$

□

58 **Example**

Prove that $\lfloor x + k \rfloor = \lfloor x \rfloor + k$.

RHS:

$$\lfloor x \rfloor + k = y + k$$

LHS:

$$\lfloor x + k \rfloor = \lfloor y + \epsilon + k \rfloor = y + k$$

More Examples:

Proof.

$$\begin{cases} \epsilon \geq 0.5 & \text{then } \lfloor y + \epsilon \rfloor + \lfloor y + \epsilon + \frac{1}{2} \rfloor = y + y + 1 = 2y + 1 \\ \epsilon < 0.5 & \text{then } \lfloor y + \epsilon \rfloor + \lfloor y + \epsilon + \frac{1}{2} \rfloor = y + y = 2y \end{cases}$$

□

2.3 Lecture–September 29, 2022

2.3.1 Cardinality of Infinite Sets

Sets with infinite cardinality are either countablly infinite or uncountably infinite.

- A set is **countable** if it can be put into one-to-one correspondence with the set of positive integers.
- Otherwise, the set is called **uncountable** or **uncountably infinite**.

59 **Example**

The set of odd positive integers is countably infinite.

Proof. Let $f(x) = 2x - 1$ which forms a bijection.

This function is injective because $f(x) = f(y) \implies x = y$ and surjective because for any odd positive integer o, $\frac{o+1}{2} \in \mathbb{Z}^+$

$$\{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, \ldots\}$$
$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \ldots\}$$

□

Another proof method is to show that members of A can be written as a sequence $(a_1, a_2, a_3, \ldots)$ since such a sequence is a bijective function from $\mathbb{Z}^+$ to A.

60 **Example**

Prove that the set of all integers is countable. You can start from zero and go in order of magnitude and then by positive and negative integers. This forms the sequences

$$0, -1, 1, -2, 2, -3, 3, \ldots$$

61 **Example**

Is Q countable? Yes.

We traverse the diagonals, which are finite.

$$
\begin{tikzcd}
\frac{1}{1} \arrow[d] & \frac{1}{2} \arrow[r] & \frac{1}{3} \arrow[dl] & \frac{1}{4} \arrow[r] & \frac{1}{5} \arrow[dl] & \frac{1}{6} \arrow[r] & \frac{1}{7} \arrow[dl] & \frac{1}{8} \arrow[r] & \cdots \\
\frac{2}{1} \arrow[ur] & \frac{2}{2} \arrow[dl] & \frac{2}{3} \arrow[ur] & \frac{2}{4} \arrow[dl] & \frac{2}{5} \arrow[ur] & \frac{2}{6} \arrow[dl] & \frac{2}{7} \arrow[ur] & \frac{2}{8} & \cdots \\
\frac{3}{1} \arrow[d] & \frac{3}{2} \arrow[ur] & \frac{3}{3} \arrow[dl] & \frac{3}{4} \arrow[ur] & \frac{3}{5} \arrow[dl] & \frac{3}{6} \arrow[ur] & \frac{3}{7} & \frac{3}{8} & \cdots \\
\frac{4}{1} \arrow[ur] & \frac{4}{2} \arrow[dl] & \frac{4}{3} \arrow[ur] & \frac{4}{4} \arrow[dl] & \frac{4}{5} \arrow[ur] & \frac{4}{6} & \frac{4}{7} & \frac{4}{8} & \cdots \\
\frac{5}{1} \arrow[d] & \frac{5}{2} \arrow[ur] & \frac{5}{3} \arrow[dl] & \frac{5}{4} \arrow[ur] & \frac{5}{5} & \frac{5}{6} & \frac{5}{7} & \frac{5}{8} & \cdots \\
\frac{6}{1} \arrow[ur] & \frac{6}{2} \arrow[dl] & \frac{6}{3} \arrow[ur] & \frac{6}{4} & \frac{6}{5} & \frac{6}{6} & \frac{6}{7} & \frac{6}{8} & \cdots \\
\frac{7}{1} \arrow[d] & \frac{7}{2} \arrow[ur] & \frac{7}{3} & \frac{7}{4} & \frac{7}{5} & \frac{7}{6} & \frac{7}{7} & \frac{7}{8} & \cdots \\
\frac{8}{1} \arrow[ur] & \frac{8}{2} & \frac{8}{3} & \frac{8}{4} & \frac{8}{5} & \frac{8}{6} & \frac{8}{7} & \frac{8}{8} & \cdots \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots
\end{tikzcd}
$$

2.3.2 Uncountability of Real Numbers

- Prime example of uncountably infinite sets is **real numbers**
- The fact that $\mathbb{R}$ is uncountable was proven by Cantor using Cantor's diagonalization argument.
- Reminiscient of Russell's paradox.

62 **Example**

Prove that $\mathbb{R}$ is uncountable.

- For contradiction assume the set of reals was countable.
- Since any subset of a countable set is also countable, this would imply that the set of reals between 0 and 1 is also countable.
- Cantor's diagonalization argument constructs R' by taking $a_1 1, a_2 2, a_3 3, \ldots$ and so on and using the rule:

$$R'_i = \begin{cases} 4 & \text{if } a_{ij} = 5 \\ 5 & \text{if } a_{ij} \neq 5 \end{cases}$$

3 Number Theory

3.0.1 Divisibility

63 **Definition**

$a|b$ or a divides b iff there exists an integer k such that $b = ka$.

64 **Example**

If n and d as positive integers, how many positive integers not exceeding n are divisible by d.

$$\lfloor n/d \rfloor$$

65 **Example**

If $a|b$ and $b|c$, then $a|c$.

Proof. Let $a|b$ and $b|c$. Then there exist integers x and y such that $b = ax$ and $c = by$. Then $c = a(x + y)$. □

66 **Example**

$a|b$ and $a|c$ implies $a|(mb + nc)$.

$b = ak$ and $c = ak'$ then

$$mb + nc = mak + nak' = a(mk + nk')$$

3.0.2 Modulus

I hope you know what this is.

67 **Example**

Prove $a \equiv b(\mod m) \iff a \bmod m = b \bmod m$

Proof. Proof by trivial. □

68 **Remark**

This article is a good read.