

MATH1061
Discrete Mathematics I

Michael Kasumagic, s4430266

Semester 2, 2024

Contents

Chapter 1	Week 1	Page 3
1.1	Lecture 1	3
1.2	Lecture 2	5
1.3	Lecture 3	8
Chapter 2	Week 2	Page 10
2.1	Lecture 4	10
2.2	Lecture 5	13
2.3	Lecture 6	15
Chapter 3	Week 3	Page 19
3.1	Lecture 7	19
3.2	Lecture 8	20
3.3	Lecture 9	21
Chapter 4	Week 4	Page 25
4.1	Lecture 10	25
4.2	Lecture 11	26
4.3	Lecture 12	27
Chapter 5	Week 5	Page 29
5.1	Lecture 13	29
5.2	Lecture 14	31
5.3	Lecture 15	32
Chapter 6	Week 6	Page 34
6.1	Lecture 16	34
6.2	Lecture 17	35
6.3	Lecture 18	39

Chapter 7	Week 7	Page 43
7.1	Lecture 19	43
7.2	Lecture 20	44
7.3	Lecture 21	45
Chapter 8	Week 8	Page 47
8.1	Lecture 22	47
8.2	Lecture 23	49
Chapter 9	Week 9	Page 52
9.1	Lecture 24	52
9.2	Lecture 25	53
9.3	Lecture 26	55
Chapter 10	Week 10	Page 57
10.1	Lecture 27	57
10.2	Lecture 28	58
10.3	Lecture 29	59
Chapter 11	Week 11	Page 60
11.1	Lecture 30	60
11.2	Lecture 31	61
Chapter 12	Week 12	Page 65
12.1	Lecture 32	65
12.2	Lecture 33	69
12.3	Lecture 34	70
Chapter 13	Week 13	Page 72
13.1	Lecture 35	72
13.2	Lecture 36	77

Chapter 1

Week 1

1.1 Lecture 1

This course will run a little differently. Prior to every lecture, we must work through a set of pre-lecture problems. The goal of timetabled lectures is to discuss and learn from solving problems.

What is in this course?

Logic and set theory, methods of proof

Modern mathematics uses the language of set theory and the notation of logic.

$$((P \wedge \sim Q) \vee (P \wedge Q)) \wedge Q \equiv P \wedge Q$$

We will learn to read and analyse this. Historical, there was a big shift in recent history, there was a big effort to define and axiomatise everything, such that math itself is defined rigorously. Symbolic logic is the basis for many areas of computer science. It helps us formulate mathematical ideas and proofs effectively and correctly!

Definition 1.1.1: Gödel's Incompleteness Theorem (1931)

There exists true statements which we can not prove!

Number Theory

Example 1.1.1 ($1 + \dots + 100$)

A young Gauss had to add up all the numbers from 1 to 100 in primary school. What did he do?

$$\begin{array}{cccccccccccc} & & 1 & + & 2 & + & \dots & + & 98 & + & 99 & + & 100 \\ 100 & + & 99 & + & 98 & + & \dots & + & 2 & + & 1 & & \\ \hline 100 & + & 100 & + & 100 & + & \dots & + & 100 & + & 100 & + & 100 \end{array}$$

So...

$$1 + \dots + 100 = \frac{101 \cdot 100}{2} = 5050$$

This generalises to $\forall n \in \mathbb{N}$. Two leaps of faith are needed though!

- The dots: We introduce the notation to deal with them.
- The equality of two equations involving dots. We will use induction to deal with this!

Graph Theory

Example 1.1.2 (The Königsberg Bridge Problem)

Find a route through the city which crosses each of seven bridges exactly once, and returns you to your start location.

This is provably impossible! But how can we rigorously prove this? Euler solve this problem in 1935 and in doing so invented graph theory. We'll learn how eventually... :p

Counting and Probability

Both fundamental and beautifully applicable. We introduce the pigeonhole principle as an introduction to “counting.”

Example 1.1.3 (The pigeonhole principle)

If you have n pigeons sitting in k pigeonholes, if $n > k$, then at least of the pigeonholes contains at least 2 pigeons.

Question 1

If you have socks of three different colours in your drawer, what is the minimum number of socks you need to pull out to guarantee a matching pair?

Solution: $\# \text{socks} \equiv \# \text{pigeons}$ and $\# \text{colours} \equiv \# \text{holes}$. If $\# \text{socks} > \# \text{colors}$, a double must occur. Therefore, we need a minimum of 4 socks to guarantee a match.

Question 2: True or False?

In every group of five people, there are two people who have the same number of friends within the group.

Solution: True! $\# \text{people} \equiv \# \text{pigeons}$ and $\# \text{friends} \equiv \# \text{holes}$. There are 5 possible values for the amount of friends one could have, $\{0, 1, 2, 3, 4\}$, but you can never have an individual with 0 friends, and 4 friends in the same group. So there are 5 people, and 4 possible $\# \text{friend}$ values (think “holes.”) Therefore, by pigeonhole principle, the statement is true!

Question 3: True or False?

A plane is coloured blue and red. Is it possible to find exactly two points the same colour exactly one unit apart?

Note:-

We will answer this on Wednesday!

Recursion

Example 1.1.4 (The Tower of Hanoi)

Given: a tower of 8 discs in decreasing size on one of three pegs.

Problem: transfer the entire tower to one of the other pegs.

Rule 1: Move only one disc at a time.

Rule 2: Never move a larger disc onto a smaller disk.

1. Is there a solution?
2. What's the minimal number of moves necessary and sufficient for the task?

A key idea is to generalise! What if there are n discs? Let T_n be the minimal number of moves, then trivially $T_0 = 0$, $T_1 = 1$, $T_2 = 3$, so what is $T_3 = ?$. Is there a pattern? The winning strategy is

1. Move the $n - 1$ smallest discs from peg A to B .
2. Move the big disc from A to C .
3. Move $n - 1$ smallest discs from B to C

By induction we show that

$$T_n = 2T_{n-1} + 1.$$

So $T_3 = 7$, $T_4 = 15$, $T_5 = 31$, $T_6 = 63$. Remarkably, this is one less than the square numbers! We will prove this fact by induction later in the course.

1.2 Lecture 2

Definition 1.2.1: Statement or Proposition

A sentence that is either true or false but not both.

Example 1.2.1

Statements:

- The number 6 is a number.
- $\pi > 3$
- Euler was born in 1707.

Not statements:

- How are you? (This is a question.)
- Stop! (This is a command.)
- She likes math. ("She" is not well defined.)
- $x^2 = 2x - 1$ (x is not well defined.)

Definition 1.2.2: Negation

Let p be a statement. The negation of p is denoted $\sim p$ or $\neg p$ and is read "not p ." It is defined as in the following truth table:

p	$\sim p$
T	F
F	T

Definition 1.2.3: Conjunction

Let p and q be statements. The conjunction of p and q is denoted $p \wedge q$ and is read " p and q ." It is defined as in the following truth table:

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Definition 1.2.4: Disjunction

Let p and q be statements. The disjunction of p and q is denoted $p \vee q$ and is read “ p or q .” It is defined as in the following truth table:

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Definition 1.2.5: Logical Equivalence

Two statements, p and q are said to be logically equivalent if have identical truth values for every possible combination of truth values for their statement variables. This is denoted $p \equiv q$.

Example 1.2.2

$$\sim(\sim p) \equiv p.$$

p	$\sim p$	$\sim(\sim p)$
T	F	T
F	T	F

Consider $P = \sim(p \wedge q)$, $Q = \sim p \wedge \sim q$ and $R = \sim p \vee \sim q$.

p	q	$\sim p$	$\sim q$	P	Q	R
T	T	F	F	F	F	F
T	F	F	T	T	F	T
F	T	T	F	T	F	T
F	F	T	T	T	T	T

$$\therefore P \equiv R \not\equiv Q.$$

Definition 1.2.6: Contradictions and Tautologies

A contradiction has truth values of false for every possible combination of its statement's truth values, and is denoted c or \perp . A tautology has truth values of true for every possible combination of its statement's truth values, and is denoted t or \top .

Example 1.2.3

p	$\sim p$	$p \wedge \sim p$
T	F	F
F	T	F

$$\therefore p \wedge \sim p \equiv \perp$$

p	$\sim p$	$p \vee \sim p$
T	F	T
F	T	T

$$\therefore p \vee \sim p \equiv \top$$

Important Laws of Logical Equivalence!

De Morgan's Law

$$\sim(p \wedge q) \equiv \sim p \vee \sim q$$

$$\sim(p \vee q) \equiv \sim p \wedge \sim q$$

Absorbtion

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

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

Commutativity

$$p \wedge q \equiv q \wedge p$$

$$p \vee q \equiv q \vee p$$

Identity Laws

$$p \wedge \top \equiv p$$

$$p \vee \perp \equiv p$$

Associativity

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

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

Domination

$$p \vee \top \equiv \top$$

$$p \wedge \perp \equiv \perp$$

Distributivity

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

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

Negation Laws

$$p \vee \sim p \equiv \top$$

$$p \wedge \sim p \equiv \perp$$

Double Negative

$$\sim(\sim p) \equiv p$$

Negations

$$\sim \top \equiv \perp$$

$$\sim \perp \equiv \top$$

Idempotent

$$p \wedge p \equiv p$$

$$p \vee p \equiv p$$

Example 1.2.4

Prove that $((p \wedge \sim q) \vee (p \wedge q)) \wedge q \equiv p \wedge q$.

$$((p \wedge \sim q) \vee (p \wedge q)) \wedge q \equiv (p \wedge (\sim q \vee q)) \wedge q$$

(Distributivity)

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

(Negation Law)

$$\equiv p \wedge q$$

(Identity)

□

1.3 Lecture 3

Definition 1.3.1: Conditional Statement

Let p and q be statement variables. The conditional form p to q is denoted $p \rightarrow q$, and read as “if p , then q ,” or “ p implies q .” It is defined by the following truth table

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

p is called the hypothesis.

q is called the conclusion.

Example 1.3.1

Suppose I make you the following promise:

“If you do your homework then you get a chocolate.”

- (a) You do not do your homework and you get a chocolate.
- (b) You do your homework and you get a chocolate.
- (c) You do your homework and you do not get a chocolate.
- (d) You do not do your homework and you do not get a chocolate.

I only lied in scenario (c), which corresponds with $(p, q) = (F, T)$.

Note:-

$$p \rightarrow q \equiv \sim p \vee q$$

p	q	$\sim p$	$\sim p \vee q$	$p \rightarrow q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Definition 1.3.2: Contrapositive

The contrapositive of $p \rightarrow q$ is $\sim q \rightarrow \sim p$.

p	q	$\sim p$	$\sim q$	$p \rightarrow q$	$\sim q \rightarrow \sim p$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

$$p \rightarrow q \equiv \sim q \rightarrow \sim p$$

Example 1.3.2

The contrapositive of

“If you do your homework then you get a chocolate.”

Is the equivalent

“If you did not get a chocolate then you did not finish your homework.”

Negation of the Conditional Statement

The negation of $p \rightarrow q$ is given by $p \wedge \sim q$ and can be proved logically.

$$\begin{aligned} p \rightarrow q &\equiv \sim p \vee q \\ \sim(p \rightarrow q) &\equiv \sim(\sim p \vee q) \\ &\equiv \sim(\sim p) \wedge \sim q \\ &\equiv p \wedge \sim q \end{aligned}$$

Example 1.3.3

The negation of

“If today is Monday, then tomorrow is my birthday”

Is

“Today is Monday but tomorrow is not my birthday.”

Definition 1.3.3: Biconditional Statement

Let p and q be statement variables. The biconditional statement of p and q , denoted $p \leftrightarrow q$, and read “ p if and only if q ” is defined by the following truth table

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

$$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$$

Chapter 2

Week 2

2.1 Lecture 4

Definition 2.1.1: Argument

Given a collection of statements, p_1, p_2, \dots, p_n (called premises), and another statement q (called the conclusion), an argument is the assertion that the conjunction of the premises implies the conclusion. This is often represented

$$\begin{array}{ll} p_1 & \dots \\ p_2 & \dots \\ \vdots & \\ p_n & \dots \\ \hline \therefore & q \end{array}$$

An argument is **valid** if whenever all the premises are true, the conclusion is true. Mathematically,

$$\bigwedge_{i=1}^n (p_i) \rightarrow q \equiv \top$$

An argument is **invalid** if there exists a configuration, such that all the premises are true, but the conclusion is false.

$$\bigwedge_{i=1}^n (p_i) \rightarrow q \not\equiv \top$$

Example 2.1.1

$$\begin{array}{ll} p_1 & \text{If it is raining, then there are clouds.} \\ p_2 & \text{It is raining.} \\ \hline \therefore & \text{There are clouds.} \end{array}$$

$$\text{Which is an argument of form: } \begin{array}{l} p \rightarrow q \\ p \\ \hline \therefore q \end{array}$$

This is a valid argument! As long as p_1 and p_2 are true, q is necessarily true.

$$\begin{array}{ll} p_1 & \text{If it is raining then there are clouds.} \\ p_2 & \text{There are clouds.} \\ \hline \therefore & \text{It is raining.} \end{array}$$

Which is an argument of form:
$$\frac{p \rightarrow q \quad q}{\therefore p}$$

This is an invalid argument! Because the conclusion doesn't follow from the premises. For example, if p_1 and p_2 were true, q still may be false.

Rules of Inference

These are common argument forms.

Modus Ponens

$$\frac{p \rightarrow q \quad p}{\therefore q}$$

p	q	Premise 1: $p \rightarrow q$	Premise 2: p	Conclusion: q
T	T	T	T	T
T	F	F	T	F
F	T	T	F	T
F	F	T	F	T

Pay special attention to row 1. This is the only row in which every premise is true. When every premise is true, the conclusion is always true. Therefore this is a valid argument form. Every argument form can be proven with a truth table in this manner.

Modus Tollens

$$\frac{p \rightarrow q \quad \sim q}{\therefore \sim p}$$

Generalisation

$$\frac{p}{\therefore p \vee q}$$

$$\frac{q}{\therefore q \vee p}$$

Specialisation

$$\frac{p \wedge q}{\therefore p}$$

$$\frac{p \wedge q}{\therefore q}$$

Conjunction

$$\frac{p \quad q}{\therefore p \wedge q}$$

Elimination

$$\frac{p \vee q \quad \sim q}{\therefore p}$$

$$\frac{p \vee q \quad \sim p}{\therefore q}$$

Transitivity

$$\frac{p \rightarrow q \quad q \rightarrow r}{\therefore p \rightarrow r}$$

Proof by Division into Cases

$$\frac{p \vee q \quad p \rightarrow r \quad q \rightarrow r}{\therefore r}$$

Contradiction

$$\frac{\sim p \rightarrow \perp}{\therefore p}$$

Example 2.1.2 (Valid or invalid)

Is the following argument valid?

$$\begin{array}{l} 1. \quad p \rightarrow \sim r \\ 2. \quad r \vee \sim q \\ 3. \quad q \\ \hline \therefore \quad \sim p \end{array}$$

We might be tempted to use a truth table, but it'll have an unreasonable, (2^3), amount of rows! We can use our rules of inference to figure this out.

$$\begin{array}{ll} 1. & p \rightarrow \sim r \\ 2. & r \vee \sim q \\ 3. & q \\ 4. & \sim q \vee r \quad (2. \text{ by Commutativity}) \\ 5. & p \rightarrow r \quad (4. \text{ by Logical Equivalence}) \\ 6. & r \quad (3. \text{ and } 5. \text{ by Modus Ponens}) \\ 7. & \sim(\sim r) \quad (6. \text{ by Double Negative}) \\ \therefore & \sim p \quad (1. \text{ and } 7. \text{ by Modus Tollens}) \end{array}$$

Therefore the argument is valid!

Searching for Invalidity

Another method for checking validity may be to look for truth values which make the premises true, but the conclusion false. If we can find such an example, we can prove that the argument is invalid. If it is impossible to do this, then the argument is valid.

Example 2.1.3

Consider the argument

$$\begin{array}{l} p \rightarrow q \\ q \\ \hline \therefore \quad p \end{array}$$

Since p is the conclusion, take it to be false.

Since q is a premise, take it to be true.

The premise $p \rightarrow q$ is therefore $\text{False} \rightarrow \text{True} \equiv \text{True}$.

Therefore all our premises are true.

But wait! Our conclusion was set to false!

Therefore, there and is called the existential quantifier.

Let $Q(x)$ be a preda configuration of truth values, namely $(p, q) = (\text{False}, \text{True})$, such that all the premises are true, but the conclusion is false.

Therefore, the argument is invalid.

Example 2.1.4

Consider the argument

$$\begin{array}{l} p \rightarrow \sim r \\ r \vee \sim q \\ q \\ \hline \therefore \quad \sim p \end{array}$$

Let's suppose the argument is invalid.

Then, our conclusion $\sim p$, is false.

Then p is true.

Since q is a premise, take it to be true.

Consider the premise $p \rightarrow \sim r$. Since p is true, $\sim r$ must also be true, such that the premise is true.

Then, r is false.

Consider the premise $r \vee \sim q$. Substituting, we see $\text{False} \vee \text{False} \equiv \text{False}$.

Therefore, it is impossible for us to configure (p, q, r) such that all the premises are true, and the conclusion is false.

Therefore the argument is not invalid.

Therefore the argument is valid.

2.2 Lecture 5

Definition 2.2.1: Predicate

A predicate is a sentence which contains finitely many variables, and which becomes a statement if the variables are given specific values.

The **domain** of each variable in a predicate is the set of all possible values that may be assigned to it. Predicates are commonly denoted with an upper case letter followed by a list of finitely many variables within brackets, $P(x)$, $Q(x)$, $R(x)$.

Example 2.2.1

Given some variables $x, y, a, b, c \in \mathbb{Z}$, here are some example predicates:

- x is even.
- $x \leq y$.
- a divides b and b divides c .

The following are not predicates:

- Divide by 2.
- Is x an integer?

Definition 2.2.2: Truth Set

The truth set of a predicate is the set of all values in the variables' domains, such that when a value from those domains are assigned to those variables, the predicate is evaluated as true.

Example 2.2.2

Let $P(x)$ be the predicate $x|5$, and $\text{dom } x = \mathbb{N}$.

The truth set of $P(x)$ is $\{-5, -1, 1, 5\}$, because these are all the numbers in the domain which divide 5.

Common Domains

- The integers: $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$
- The positive integers: $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$
- The nonnegative integers: $\mathbb{Z}^{\geq 0} = \{0, 1, 2, 3, \dots\}$
- The natural numbers: $\mathbb{N} = \{1, 2, 3, \dots\}$
- The rational numbers: $\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z} \wedge b \neq 0 \right\}$
- The real numbers: The entire number line.

Note:-

The real numbers have a rigorous definition, but it is outside the scope of this introductory course.

The Universal Quantifier

The symbol \forall denotes “for all” and is called the universal quantifier.

Let $Q(x)$ be a predicate and $\text{dom } x = D$.

The statement

$$\forall x \in D, Q(x)$$

is true if and only if $Q(x)$ is true for every single element in D .

It is false if and only if $Q(x)$ is false for at least one element in D .

Example 2.2.3

Let $Q(x)$ be the predicate $x \leq x^2$, and $\text{dom } x = \mathbb{Z}$. The statement $\forall x \in \mathbb{Z}, Q(x)$ can be expressed in the following equivalent ways:

- $\forall x \in \mathbb{Z}, x \leq x^2$
- For all $x \in \mathbb{Z}, x \leq x^2$
- Every integer is less than or equal to its square.

Are the following statements true or false?

$$\forall x \in \mathbb{Z}, x \in \mathbb{R}$$

True. $\because \mathbb{Z} \subseteq \mathbb{R}$.

$$\forall y \in \mathbb{Q}, y^2 \geq 1$$

False. Counterexample, let $y = \frac{1}{2}$. Then $\left(\frac{1}{2}\right)^2 = \frac{1}{4} < 1$. Take any $y < 1$. Its square is less than 1.

The Existential Quantifier

The symbol \exists denotes “there exists” and is called the existential quantifier.

Let $Q(x)$ be a predicate and $\text{dom } x = D$.

The statement

$$\exists x \in D : Q(x)$$

is true if and only if $Q(x)$ is true for at least a single element in D .

It is false if and only if $Q(x)$ is false for every single element in D .

Example 2.2.4

Let $Q(x)$ be the predicate $x^2 = 4$, and $\text{dom } x = \mathbb{Z}$. The statement $\exists x \in D : Q(x)$ can be expressed in the following equivalent ways:

- $\exists x \in \mathbb{Z}$ such that $x^2 = 4$
- There exists an integer x such that $x^2 = 4$
- There is some integer whose square is 4.

Are the following true or false?

$$\exists x \in \mathbb{R} : x^2 = 1 \wedge x < 0$$

Note that $P(x)$ is the conjunction of two other predicates.

This is true. Take $x = -1 \in \mathbb{R}$.
Then $-1^2 = 1$ and $-1 < 0$.

$$\exists x \in \{2, 4, 6\} : x^2 = 9.$$

False. We can prove this by exhaustion.
 $2^2 = 4 \neq 9$ $4^2 = 16 \neq 9$ $6^2 = 36 \neq 9$.
Therefore, there is no x in the domain such that the predicate is satisfied.

Universal Conditional Statements

One of the most important statement forms in mathematics:

$$\forall x \in D, P(x) \rightarrow Q(x)$$

Example 2.2.5

The universal conditional statement

$$\forall x \in \mathbb{R}, x > 3 \rightarrow x^2 > 9$$

Can be equivalently expressed

- For every real number, x , if $x > 3$, then $x^2 > 9$.
- Whenever a real number is greater than 3, its square is greater than 9.
- The squares of real numbers greater than 3, are greater than 9.

2.3 Lecture 6

Negations of Quantified Statements

Negating the Universal Quantifier

Consider the universally quantified statement

$$\forall x \in D, Q(x).$$

The negation of this statement is logically equivalent to

$$\exists x \in D : \sim Q(x).$$

\forall negates to \exists , and the predicate $Q(x)$ negates to $\sim Q(x)$.

Example 2.3.1

Consider the statement

$$\forall x \in \mathbb{Z}, x \text{ is prime.}$$

The negation of this statement is

$$\exists x \in \mathbb{Z} : x \text{ is not prime.}$$

Naturally, and to maintain logical equivalence, the original statement, in this case, evaluates to False, while its negation evaluates to True.

Now, Consider the statement

$$\text{All integers are odd or even.}$$

This can be written mathematically as

$$\forall x \in \mathbb{Z}, x \equiv 0 \pmod{2} \vee x \equiv 1 \pmod{2}.$$

And it's negation is

$$\exists x \in \mathbb{Z} : x \not\equiv 0 \pmod{2} \wedge x \not\equiv 1 \pmod{2}.$$

Which when brought back into the English language, is read

There is an integer which is not even and not odd.

Clearly, the original statement evaluates to True, and its negation to False.

Negating the Existential Quantifier

Now let's consider the existentially quantified statement

$$\exists x \in D : P(x).$$

The negation of this statement is

$$\forall x \in D : \sim P(x).$$

\exists negates to \forall , and the predicate $P(x)$ negates to $\sim P(x)$.

Example 2.3.2

Consider the statement

There is a pink elephant.

Its negation is

Every elephant is not pink.

Consider the statement

$$\exists x \in \mathbb{Q} : x \in \mathbb{Z}$$

Its negation is

$$\forall x \in \mathbb{Q}, x \notin \mathbb{Z}$$

Again, we can tell that the original statement is true, and its negation is false.

A couple more examples... Let's consider the statement

Some rabbit has white fur.

Note that this is existentially quantified, so its negation will be universally quantified,

No rabbit has white fur.

Finally, consider the statement

Every UQ student is happy.

This time, note that this statement is universally quantified, so its negation will be existentially quantified,

There is a UQ student who is not happy.

We're getting the hang of this!

Negating the Universal Conditional Quantifier

Finally, we consider the statement

$$\forall x \in D, P(x) \rightarrow Q(x).$$

Using laws of logical equivalence, and what we've just learned, we can easily conclude that the negation of this statement is

$$\exists x \in D : \sim(P(x) \rightarrow Q(x)) \equiv \exists x \in D : P(x) \wedge \sim Q(x)$$

ultimately, the \forall still negates to \exists , and if you consider the composite statement $R(x) = P(x) \rightarrow Q(x)$, then $\sim R(x) \equiv \sim(P(x) \rightarrow Q(x)) \equiv \sim(\sim P(x) \vee Q(x)) \equiv P(x) \wedge \sim Q(x)$.

Example 2.3.3

Let's negate some more statements!

$A = \forall x \in \mathbb{Z}, x \geq 1 \rightarrow x \in \mathbb{N}$	(True)
$\therefore \sim A = \exists x \in \mathbb{Z} : x \geq 1 \wedge x \notin \mathbb{N}$	(False)
$B = \forall x \in \mathbb{Z}, (3 \mid x) \rightarrow (6 \mid x)$	(False)
$\therefore \sim B = \exists x \in \mathbb{Z} : (3 \mid x) \wedge (6 \nmid x)$	(True)
$C = \text{"If a rabbit has white fur, then it has long ears"}$	(False)
$\therefore \sim C = \text{"There is a rabbit with white fur and short ears"}$	(True)
$D = \text{"All parks that have grass, have playgrounds."}$	(False)
$\therefore \sim D = \text{"Some park has grass and not playground."}$	(True)

Statements with Multiple Quantifiers

Some predicates, for instance $x \leq y$, involve more than one variable. In such a case, we use the notation $P(x, y)$ to denote such a predicate. Such predicates often appear with more than one quantifier. For example, consider the statement

$$\exists x \in \mathbb{N} : \forall y \in \mathbb{N}, x \leq y.$$

We would read this as "There exists a natural number which is smaller than all natural numbers." or "There is a smallest natural number."

Note:-

"Such that", \therefore , always pairs with the existential quantifier!

It's negation would be

$$\forall y \in \mathbb{N}, \exists x \in \mathbb{N} : x \leq y$$

which is read, "Every natural numbers has some other number which is less then or equal to it."

Establishing the Truth, when given Multiple Quantifiers

Suppose we want to prove the given the statement

$$\forall x \in D, \exists y \in E : P(x, y).$$

To prove this, we must allow someone to pick any element in D they want, and we must any element in E which makes $P(x, y)$ true.

Example 2.3.4

Let's prove the statement

$$\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z} : x + y = 0.$$

$$\forall x \in \mathbb{Z},$$

$$\text{Choose } y = -x,$$

$$\text{Then } x + y = x - x = 0.$$

□

No matter what value for x is chosen, I choose $y = -x$, and the predicate $P(x, y)$ always evaluates to true. Because we can do this for all integers x , we know that this statement is true.

Now let's suppose we have the statement

$$\exists x \in D : \forall y \in E, P(x, y).$$

To prove this statement, we need to find one particular $x \in D$ which makes $P(x, y)$ true, no matter what selection is made for $y \in E$.

Example 2.3.5

Let's prove the statement

$$\exists x \in \mathbb{N} : \forall y \in \mathbb{N}, x \leq y.$$

Take $x = 1$.

$$\text{Now, } \forall y \in \mathbb{Z}, 1 \leq y.$$

□

Negations of Statements with Multiple Quantifiers

Consider the statement

$$\forall x \in D, \exists y \in E : P(x, y).$$

This statement will negate to

$$\exists x \in D : \forall y \in E, \sim P(x, y).$$

Similarly, consider the statement

$$\exists x \in D : \forall y \in E, P(x, y).$$

This statement will negate to

$$\forall x \in D, \exists y \in E : \neg P(x, y).$$

Again, note, that the such that always pairs with the existential quantifier. Let's look at some examples now...

Example 2.3.6

$$\begin{aligned} A &= \forall x \in \mathbb{Z}, \exists y \in \mathbb{Z} : x + y = 0 && \text{(True)} \\ \therefore \sim A &= \exists x \in \mathbb{Z} : \forall y \in \mathbb{Z}, x + y \neq 0 && \text{(False)} \\ B &= \exists x \in \mathbb{R} : \forall y \in \mathbb{R}, |x| \leq |y| && \text{(False)} \\ \therefore \sim B &= \forall x \in \mathbb{R}, \exists y \in \mathbb{R} : |y| < |x| && \text{(True)} \end{aligned}$$

Chapter 3

Week 3

3.1 Lecture 7

Let's consider

Definition 3.1.1: Even and Odd

An integer n is even $\iff \exists k \in \mathbb{Z} : n = 2k$

An integer n is odd $\iff \exists k \in \mathbb{Z} : n = 2k + 1$

Definition 3.1.2: Prime and Composite

An integer n is prime $\iff n > 1, \forall r, s \in \mathbb{Z}, n = rs \implies r = 1 \vee s = 1$.

An integer n is composite $\iff n > 1, \exists r, s \in \mathbb{Z} : n = rs, r \neq 1, s \neq 1$.

Direct Proof of Existential Statements

To show $\exists x : P(x)$ is true (for some value x and some predicate $P(x)$), it is enough to find a single example of an element $x \in D$ for which $P(x)$ is true.

Example 3.1.1

Prove that $\exists x \in \mathbb{N} : x > 30, x$ is composite.

Proof. Suppose $x = 32$. Then $x > 30$ and $x = 2 \cdot 16$ which makes it composite. \square

Direct Proof of Universal Statements

One way to prove that $\forall x \in D, P(x)$ is true is by direct proof:

1. Suppose $x \in D$.
2. Show that $P(x)$ is true.

To prove statements like $\forall x \in D, P(x) \rightarrow Q(x)$ is true directly:

- Suppose $x \in D$ and $P(x)$.
- Show that the conclusion, $Q(x)$ is true, using definitions, previously established results, and rules of logical inference.

Example 3.1.2

Lemma. For all $n \in \mathbb{Z}$, n is odd $\implies n^2$ is odd.

Proof. Suppose $n \in \mathbb{Z}$ is odd.

Then $n = 2k + 1$.

$$(2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2l + 1.$$

Therefore, the square of an odd integer, is odd. □

Disproof by Counterexample

To show that $\forall x \in D, P(x) \rightarrow Q(x)$ is false, we only need to find a single example of $x \in D$ for $P(x)$ is true and $Q(x)$ is false. This is called a counterexample.

Example 3.1.3

Lemma. For all $n \in \mathbb{Z}$, n is even $\implies n/2$ is even

Proof. We will disprove this lemma with a counterexample.

Take $n = 6$.

Then n is even, since $6 = 2 \cdot 3$.

But $n/2$ is odd, since $6/2 = 3 = 2 \cdot 1 + 1$.

Therefore, the statement that all even integers divided by 2 are even, is false. □

Tips for writing proofs

1. Write the theorem to be proved.
2. Clearly mark the beginning of the proof, with *Proof*.
3. Use precise definitions for any mathematical terms.
4. Write the proof using complete sentences.
5. Give reasons for each assertion.
6. Keep the proof self contained.
7. Display equations and inequalities clearly.
8. Conclude by stating what you've proved.

3.2 Lecture 8

Proof by Contradiction of Statements $\forall x \in D, P(x)$

1. Assume the statement to be proved is false.
2. Show that this assumption logically leads to a contradiction.
3. Conclude the statement to be proved is true.

Example 3.2.1

Lemma. There is no greatest integer.

Proof. Suppose the lemma is false.

Then there is a greatest integer, N .

Hence, $\forall n \in \mathbb{Z}, N \geq n$.

Let $M = N + 1$.

Since $N \in \mathbb{Z}$ and $1 \in \mathbb{Z}$, then $M \in \mathbb{Z}$. But $M > N$
 Thus, M is an integer that is greater than N .
 So N is not the greatest integer.
 Therefore, there is no greatest integer.

✖

□

Example 3.2.2

Lemma. $\forall n \in \mathbb{Z}, n$ is not simultaneously even and odd.

Proof. Suppose the lemma is false.
 Then there is some $n \in \mathbb{Z}$ that is both odd and even.
 Thus, $n = 2k$ for some $k \in \mathbb{Z}$.
 And, $n = 2l + 1$ for some $l \in \mathbb{Z}$.
 Hence, $2k = 2l + 1 \iff 1 = 2(k - l)$.
 Therefore, $k - l = 1/2$, which is impossible, since $1/2 \notin \mathbb{Z}$.
 Therefore, there is no integer which is both even and odd simultaneously.

✖
□

Proof by Contradiction of Statements $\forall x \in D, P(x) \rightarrow Q(x)$

1. Assume the statement is false. Therefore the negation of the statement $\exists x \in D : P(x) \wedge \sim Q(x)$.
2. Show that this assumption logically leads to a contradiction.
3. Conclude the statement to be proved is true.

Example 3.2.3

Lemma. For all integers n , if n^2 is odd, then n is odd.

Proof. Suppose that the lemma is false.
 Then $\exists n \in \mathbb{Z}, n^2$ is odd and n is even.
 Since n is even, $n = 2k$, for some $k \in \mathbb{Z}$
 Since n^2 is odd, $n^2 = 2l + 1$, for some $l \in \mathbb{Z}$.
 So $n^2 = (2k)^2 = 4k^2 = 2(k^2) = 2l + 1$.
 n^2 is simultaneously odd and even, this is a contradiction.
 Therefore, the assumption that the lemma is false, is false.
 Therefore, the lemma is true.

✖

□

3.3 Lecture 9

Proof by Contraposition

Relying on the fact that a statement is logically equivalent to its contrapositive, sometimes it can be easier to prove that contrapositive. Since they are logically equivalent, proving the contrapositive, proves the target statement.

1. Express the target statement in the form $\forall x \in D, P(x) \rightarrow Q(x)$
2. Rewrite the statement in its contrapositive form $\forall x \in D, \sim Q(x) \rightarrow \sim P(x)$
3. Prove the contrapositive directly:
 - Suppose $x \in D$ and $Q(x)$ is false.
 - Show that $P(x)$ is false.

Example 3.3.1

Lemma. For all integers n , if n^2 is even, then n is even.

Remark. The lemma is written using notation,

$$\forall n \in \mathbb{Z}, n^2 \text{ is even} \implies n \text{ is even},$$

and is logically equivalent to its contrapositive

$$\forall n \in \mathbb{Z}, n \text{ is odd} \implies n^2 \text{ is odd}.$$

Proof. Suppose $n \in \mathbb{Z}$ and n is odd

n is odd, therefore $n = 2k + 1$, $k \in \mathbb{Z}$

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2l + 1, \quad l \in \mathbb{Z}$$

Therefore, n^2 is odd

So, the contrapositive is true.

Then, the lemma is true.

We conclude that, given an even square integer, its root is even. □

Example 3.3.2

Definition (Parity). Two integers have the same parity if they are both even, or both odd. Two integers have opposite parity if one is odd, and the other is even.

Lemma. $\forall m, n \in \mathbb{Z}, m + n \text{ is even} \implies m \text{ and } n \text{ have the same parity}.$

Remark. The contrapositive of the lemma is $\forall m, n \in \mathbb{Z}, m \text{ and } n \text{ have the opposite parity} \implies m + n \text{ is odd}.$

Proof. Suppose $m, n \in \mathbb{Z}$ and have opposite parity.

Then one is odd, and the other is even.

Without loss of generality, suppose that m is odd, and n is even.

Then $m = 2k + 1$, $k \in \mathbb{Z}$ and $n = 2l$, $l \in \mathbb{Z}$.

$$\text{Hence, } m + n = 2k + 1 + 2l = 2k + 2l + 1 = 2(k + l) + 1$$

Therefore, $m + n$ is odd.

So, the contrapositive is true.

Therefore, the lemma is true. □

Example 3.3.3

Lemma. $x, y \in \{z \in \mathbb{R} \mid z > 0\} = D, xy > 25 \implies x > 5 \vee y > 5.$

Remark. The contrapositive of the lemma is $x, y \in \{z \in \mathbb{R} \mid z > 0\}, x \leq 5, y \leq 5 \implies xy \leq 25.$

Proof. Suppose $x, y \in D, x \leq 5, y \leq 5.$

Therefore, $x \cdot y \leq 5 \cdot 5.$

In other words, $xy \leq 25.$

Thus, the contrapositive is true.

Therefore, the lemma is true. □

The Rational Numbers

Definition 3.3.1: The Rational Numbers

A real number is rational if and only if it can be expressed as a quotient of two integers with a nonzero denominator.

$$\forall x \in \mathbb{R}, x \text{ is rational} \iff \exists a, b \in \mathbb{Z} : x = \frac{a}{b}, b \neq 0$$

We denote the set of all rationals \mathbb{Q}

$$\mathbb{Q} = \left\{ x \in \mathbb{R} \mid \exists a, b \in \mathbb{Z} : x = \frac{a}{b}, b \neq 0 \right\}$$

We can denote the set of all irrational numbers, using \mathbb{Q} , namely

$$\mathbb{Q}' = \{x \in \mathbb{R} \mid x \notin \mathbb{Q}\}$$

Claim. The decimal expansion of a rational number either repeats or terminates.

$$\frac{1}{4} = 0.25, \quad \frac{1}{3} = 0.3333 \dots = 0.\bar{3}$$

Claim. The decimal expansion of an irrational number does not repeat or terminate.

$$\pi = 3.1415 \dots$$

Lemma 3.3.1. $a, b \in \mathbb{Q}, a + b \in \mathbb{Q}$

Proof. Suppose $a, b \in \mathbb{Q}$.

Then, $a = \frac{c}{d}$, and $b = \frac{e}{f}$, $c, d, e, f \in \mathbb{Z}, d \neq 0, f \neq 0$.

$$\text{So, } a + b = \frac{c}{d} + \frac{e}{f} = \frac{cf}{df} + \frac{de}{df} = \frac{cf + de}{df}.$$

$$cf + de \in \mathbb{Z}, df \in \mathbb{Z}, \text{ and } df \neq 0$$

$$\therefore a + b \in \mathbb{Q}$$

Therefore, the sum of any two rational numbers, is rational □

Lemma 3.3.2. For any rational number r , and any nonzero rational s , $\frac{r}{s}$ is rational, or,

$$\forall r, s \in \mathbb{Q}, s \neq 0 \implies \frac{r}{s} \in \mathbb{Q}$$

Proof. Suppose $r, s \in \mathbb{Q}$ and $s \neq 0$

Then, $r = \frac{a}{b}$, and $s = \frac{c}{d}$, $a, b, c, d \in \mathbb{Z}, b \neq 0, c \neq 0, d \neq 0$

$$\text{So, } r \div s = \frac{a}{b} \div \frac{c}{d} = \frac{a}{b} \cdot \frac{d}{c} = \frac{ad}{cb}$$

$$ad \in \mathbb{Z}, cb \in \mathbb{Z}, \text{ and } cb \neq 0$$

$$\therefore \frac{r}{s} \in \mathbb{Q}$$

Therefore, the quotient of any rational and any nonzero rational is a rational. □

Theorem. For all rational numbers, r, s where $r < s$, there exists another rational q such that $r < q < s$, or symbolically,

$$\forall r, s \in \mathbb{Q}, r < s, \exists q \in \mathbb{Q} : r < q < s$$

Proof. Suppose $r, s \in \mathbb{Q}$ and $r < s$

$$\text{Then, } r = \frac{a}{b}, s = \frac{c}{d}, \quad a, b, c, d \in \mathbb{Z}, \quad b \neq 0, d \neq 0$$

$$\text{Take } q = \frac{1}{2}(r + s)$$

Since, r and s are rational numbers,

$$r + s \in \mathbb{Q}. \quad (\text{Lemma 3.3.1})$$

Since, $r + s \in \mathbb{Q}$ and $2 \in \mathbb{Q}$ and $2 \neq 0$, then

$$q = \frac{r + s}{2} \in \mathbb{Q}. \quad (\text{Lemma 3.3.2})$$

Since $r < s$,

$$q = \frac{1}{2}(r + s) < \frac{1}{2}2s + s = \frac{1}{2}(2s) = s,$$

and

$$q = \frac{1}{2}(r + s) > \frac{1}{2}(r + r) = \frac{1}{2}(2r) = r,$$

$$\therefore q \in \mathbb{Q} \text{ and } r < q < s. \quad \square$$

Lemma. For every nonzero number r , there exists a nonzero rational s such that $rs = 1$, or symbolically,

$$\forall r \in \mathbb{Q}, r \neq 0, \exists s \in \mathbb{Q} : rs = 1$$

Proof. Suppose $r \in \mathbb{Q}$.

Then,

$$r = \frac{a}{b}, \quad a, b \in \mathbb{Z}, \quad a \neq 0, b \neq 0$$

$$\text{Take } s = \frac{b}{a}$$

Since $r \neq 0$ so $a \neq 0$. Therefore, $q \in \mathbb{Q}$

$$\begin{aligned} r \cdot s &= \frac{a}{b} \cdot \frac{b}{a} \\ &= \frac{ab}{ab} \\ &= 1 \end{aligned}$$

Therefore, $s \in \mathbb{Q}$ and $rs = 1$. \square

Lemma. The sum of any rational number and any irrational number is irrational, $\forall q \in \mathbb{Q}, x \in \mathbb{Q}' \implies q + x \in \mathbb{Q}'$.

Proof. Suppose the lemma is false.

Then, there exists a rational number q and an irrational number x such that $q + x \in \mathbb{Q}$.

So, by definition, $q = \frac{a}{b}$ and $x + q = \frac{c}{d}$, $a, b, c, d \in \mathbb{Z}$ and $b \neq 0, d \neq 0$.

Let's consider $x + q = \frac{c}{d}$. $x + \frac{a}{b} = \frac{c}{d}$, which implies that $x = \frac{c}{d} - \frac{a}{b} = \frac{bc}{bd} - \frac{ad}{bd} = \frac{bc-ad}{bd}$.

Since a, b, c, d are all integers, then bc , ad , and bd are all integers.

And since $b \neq 0$ and $d \neq 0$, then $bd \neq 0$.

Therefore, by definition, x is a rational number \otimes

x can't be both a rational and an irrational number, this is a contradiction.

Thus, the sum of an irrational and a rational cannot be rational.

Therefore, the lemma is true. \square

Chapter 4

Week 4

4.1 Lecture 10

Divisibility

Definition 4.1.1: Divisibility

If $n, d \in \mathbb{Z}$, $d \neq 0$ then n is divisible by d iff there exists some $k \in \mathbb{Z}$ such that $n = kd$. In other words

$$d \mid n \iff \exists k \in \mathbb{Z} : n = kd$$

Lemma. $\forall a, b, c \in \mathbb{Z}$, $a \mid b$, $b \mid c \implies a \mid c$

Proof. Suppose $a, b, c \in \mathbb{Z}$ and $a \mid b$ and $b \mid c$

$$a \mid b \iff b = ka, k \in \mathbb{Z}$$

$$b \mid c \iff c = lb, l \in \mathbb{Z}$$

$$\therefore c = l(ka) = kl(a) \iff a \mid c$$

Therefore, the lemma is proved. □

Note:-

Special Cases:

$$d \in \mathbb{Z} \setminus \{0\}$$

$$d \mid 0$$

Since, $k = 0$, gives $0 = d \cdot 0$

$$n \in \mathbb{Z}$$

$$1 \mid n \text{ and } n \mid n, (n \neq 0)$$

Since, $k = n$ gives $n = 1 \cdot n$ and $k = 1$ gives $n = n \cdot 1$.

A new way to think about prime numbers!

$$\forall n \in \mathbb{N}, n \text{ is prime} \iff n > 1, \text{ The only positive divisors of } n \text{ are } 1 \text{ and } n$$

Theorem 4.1.1 Soft Fundamental Theorem of Arithmetic

Every integer $n > 1$ can be written as a product of primes.

Proof. Suppose the theorem is false.

Then there exists an integer $n > 1$ that is not a product of primes.

Choose the smallest such n .

n is either prime, or composite

Case 1: If n is prime, then n is trivially a product of primes.

Case 2: If n is composite, then $n = rs$ for some natural numbers r and s , where $r \neq 0$, and $s \neq 0$.

This implies $1 < r < n$ and $1 < s < n$.

Since n is the smallest number which is not a product of primes, r and s are products of primes.

So therefore, n is a product of primes

Thus, assumption that the theorem is false, is false.

Therefore, the theorem is true.

✖

□

Theorem 4.1.2 Fundamental Theorem of Arithmetic

Given any integer $n > 1$, there exists: a positive integer k , distinct primes p_1, p_2, \dots, p_k , and positive integers e_1, e_2, \dots, e_k , such that

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_k^{e_k},$$

and any other expression of n as a product of primes is identical to this (commutativity notwithstanding).

4.2 Lecture 11

Modular Arithmetic

Definition 4.2.1: Floor and Ceiling

Given $x \in \mathbb{R}$, the floor of x , denoted $\lfloor x \rfloor$, is the unique integer n , such that $n \leq x < n + 1$.

Given $x \in \mathbb{R}$, the ceiling of x , denoted $\lceil x \rceil$, is the unique integer n , such that $n - 1 < x \leq n$.

Theorem 4.2.1 The Quotient-Remainder Theorem

Given an integer n and a positive integer d , there exists unique integers q and r such that

$$n = dq + r, \quad 0 \leq r < d.$$

q is called the quotient.

r is called the remainder.

Note: $q = \lfloor \frac{n}{d} \rfloor$.

Definition 4.2.2: Modulo

For integers a and b , we say that a is congruent to b modulo d , where d is a positive integer. This is denoted

$$a \equiv b \pmod{d} \iff d \mid (a - b).$$

Further, if a and b are not congruent modulo d , we can write

$$a \not\equiv b \pmod{d}$$

Claim. $n = dq + r \implies n \equiv r \pmod{d}$

Claim. $n \equiv 0 \pmod{d} \iff d \mid n$

Lemma. $a \equiv b \pmod{d}, n \equiv m \pmod{d} \implies an \equiv bm \pmod{d}$

Proof. Suppose $a, b, n, m \in \mathbb{Z}$, $d \in \mathbb{N}$, $a \equiv b \pmod{d}$, $n \equiv m \pmod{d}$.

Then, $d \mid (a - b)$ and $d \mid (n - m)$.

So, $a - b = dk$ and $n - m = dl$, $d, k, l \in \mathbb{Z}$.

Hence, $a = dk + b$ and $n = dl + m$.

Now, $an = (dk + b)(dl + m) = d^2kl + dkm + bdl + bm = d(dkl + km + bl) + bm$.

Therefore, $d \mid (an - bm) \iff an \equiv bm \pmod{d}$. □

Lemma. $a \equiv b \pmod{d}, n \equiv m \pmod{d} \implies a + n \equiv b + m \pmod{d}$

Proof. Suppose $a, b, n, m \in \mathbb{Z}, d \in \mathbb{N}, a \equiv b \pmod{d}, n \equiv m \pmod{d}$.

Then, $d \mid (a - b)$ and $d \mid (n - m)$.

So, $a - b = dk$ and $n - m = dl, d, k, l \in \mathbb{Z}$.

Hence, $a = dk + b$ and $n = dl + m$.

Now, $a + n = (dk + b) + (dl + m) = (dk + dl) + (b + m) = d(k + l) + (b + m)$.

Therefore, $d \mid (a + n) - (b + m) \iff a + n \equiv b + m \pmod{d}$. □

4.3 Lecture 12

Greatest Common Divisor

Definition 4.3.1: Greatest Common Divisor

For nonzero integers, a, b , the greatest common divisor, denoted $\gcd(a, b)$, is the integer d which satisfies these properties:

- $d \mid a$
- $d \mid b$
- For all $c \in \mathbb{Z}, c \mid a$ and $c \mid b \implies c \leq d$.

Thus, d is the largest number which divides both a and b .

Note:-

If $\gcd(a, b) = 1$, then a and b have no common factors, bar ± 1 . We call such numbers co-prime or relatively prime.

more interesting properties:

- $\gcd(0, 0)$ is undefined, since $d \mid 0, \forall d \in \mathbb{Z}$, and there is no greatest integer.
- $\gcd(a, a) = a$ since a is trivially its own greatest divisor.
- $a > 0, \gcd(b, a) = a$, since $d \mid 0, \forall d \in \mathbb{Z}$ and $\gcd(a, a) = a$.
- If $a, b \in \mathbb{Z}, b \neq 0$, and we apply the Q-R theorem, namely $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

The Euclidean Algorithm

The Euclidean Algorithm brings all of this together to help us compute $\gcd(a, b)$ for any two integers a, b .

Algorithm 1: The Euclidean Algorithm

Input: $a, b \in \mathbb{Z}, a \geq b > 0$

Output: $d \in \mathbb{Z} : d$ is the greatest common divisor of a and b .

```

/* Apply the quotient-remainder theorem */
1  $q \leftarrow \lfloor a/b \rfloor$ ;
2  $r \leftarrow a - bq$ ;
3 if  $r = 0$  then
    | /* Terminate, we've found  $\gcd(a, b)$ . */
    | return  $b$ ;
4 else
5   |
6   | recurse with arguments  $(b, r)$ ;
7 end

```

Example 4.3.1

Lets's do an example, to get a feel for the algorithm.

$$\gcd(192, 132) \rightarrow 132 \cdot 1 + 60$$

$$\gcd(132, 60) \rightarrow 60 \cdot 2 + 12$$

$$\gcd(60, 12) \rightarrow 12 \cdot 5 + 0$$

$$\gcd(12, 0) = 12$$

$$\therefore \gcd(192, 132) = 12.$$

Note:-

This algorithm will always terminate, because, by the quotient-remainder theorem, $0 \leq r < b$. Therefore, the arguments being recursed are always strictly smaller.

Example 4.3.2

Find $\gcd(18, 14)$ and $\gcd(175, 63)$.

$$\gcd(18, 14) \rightarrow 18 = 14 \cdot 1 + 4$$

$$\gcd(14, 4) \rightarrow 14 = 4 \cdot 3 + 2$$

$$\gcd(4, 2) \rightarrow 4 = 2 \cdot 2 + 0$$

$$\gcd(2, 0) = 2$$

$$\gcd(175, 63) \rightarrow 175 = 63 \cdot 2 + 49$$

$$\gcd(175, 49) \rightarrow 175 = 49 \cdot 3 + 28$$

$$\gcd(49, 28) \rightarrow 49 = 28 \cdot 1 + 21$$

$$\gcd(28, 21) \rightarrow 28 = 21 \cdot 1 + 7$$

$$\gcd(21, 7) \rightarrow 21 = 7 \cdot 3 + 0$$

$$\gcd(7, 0) = 7$$

$$\therefore \gcd(18, 14) = 2 \text{ and } \gcd(175, 63) = 7.$$

Lowest Common Multiple

Definition 4.3.2: Lowest Common Multiple

For nonzero integers, a, b , the lowest common multiple of a and b is the smallest positive integer n such that $a \mid n$ and $b \mid n$.

$$\text{lcm}(a, b) = n \iff a, b \in \mathbb{Z} \setminus \{0\}, \exists n \in \mathbb{N} : a \mid n, b \mid n, \forall k \in \mathbb{N}, a \mid k, b \mid k, n \leq k.$$

Claim. Suppose $a, b \in \mathbb{Z}, 0 < b \leq a$. Then, $\gcd(a, b) \cdot \text{lcm}(a, b) = a \cdot b$.

Chapter 5

Week 5

5.1 Lecture 13

Sequences

A sequence is an ordered list of elements. It can be finite or infinite. Each individual element of a sequence is called a term, and is often denoted with a lowercase letter and a subscript. An explicit or general formula for a sequence is a rule which shows how the value of a_k depends on k .

Consider the infinite sequence: $1, 2, 4, 8, \dots$ We could write: $a_k = k^2$.

This same sequence could be denoted in any of the following ways:

$$\{2^k\}_{k \geq 0} \quad \{2^k\}_{k=0}^{\infty} \quad (2^k)_{k \geq 0} \quad (2^k)_{k=0}^{\infty}$$

Example 5.1.1

Given the infinite sequence $a = \{(-1)^n \frac{1}{n}\}_{n \geq 1}$, write the first 5 terms.

$$a_1 = (-1)^1 \frac{1}{1} = -1$$

$$a_2 = (-1)^2 \frac{1}{2} = \frac{1}{2}$$

$$a_3 = (-1)^3 \frac{1}{3} = -\frac{1}{3}$$

$$a_4 = (-1)^4 \frac{1}{4} = \frac{1}{4}$$

$$a_5 = (-1)^5 \frac{1}{5} = -\frac{1}{5}$$

An alternating sequence is a sequence for which consecutive terms alternate between positive and negative sign. The example sequence above is an example of an alternating sequence.

Summation Notation

We use Greek capital letter Σ to indicate a sum. If $m, n \in \mathbb{Z}$, $m \leq n$, and a is some sequence, then

$$\sum_{i=m}^n a_i = a_m + a_{m+1} + a_{m+2} + \dots + a_n$$

m is called the lower limit of the summation, and n is called the upper limit of the summation.

Note that if $m = n$, then the summation will consist of a single term.

i is called a dummy variable. We could use any unused variable name or symbol here, it only exists to illustrate the behaviour of consecutive terms. The dummy variable only exists inside the sum we're taking.

Product Notation

We use Greek capital letter Π to indicate a sum. If $m, n \in \mathbb{Z}$, $m \leq n$, and a is some sequence, then

$$\prod_{i=m}^n a_i = a_m \cdot a_{m+1} \cdot a_{m+2} \cdot \dots \cdot a_n$$

m is called the lower limit of the product, and n is called the upper limit of the product.

Factorial

For all natural numbers n , we define $n!$, read “ n factorial” to be

$$\prod_{i=1}^n i = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n,$$

and $0! = 1$.

Properties of Summations and Products

Suppose we have two real numbers sequences $a = \{a_k\}_{k=m}^n$, and $b = \{b_k\}_{k=m}^n$, where $m, n \in \mathbb{Z}$, $m \leq n$, and c is some real number the following hold:

$$\begin{aligned} & \bullet \sum_{i=m}^n a_i \pm \sum_{i=m}^n b_i = \sum_{i=m}^n (a_i \pm b_i) \\ & \bullet \sum_{i=m}^n c a_i = c \sum_{i=m}^n a_i \\ & \bullet \left(\prod_{i=m}^n a_i \right) \left(\prod_{i=m}^n b_i \right) = \prod_{i=m}^n a_i b_i \end{aligned}$$

The Principle of Mathematical Induction

Let $P(n)$ be a predicate that is defined for all integers, n , greater than or equal to some fixed point integer a .

Suppose $P(a)$ is true, and for all integers $k \geq a$, $P(k) \rightarrow P(k+1)$.

Then $P(n)$ is true for all integers $n \geq a$.

Think of it as a chain of dominos. $P(1)$ implies $P(2)$ implies $P(3)$ implies ... implies $P(n)$.

Lemma. For all integers $n \geq a$, $P(n)$.

Proof. By applying the principle of mathematical induction

1. Basis Step: Prove $P(a)$
2. Inductive Step: Prove, for all integers $k \geq a$, $P(k) \implies P(k+1)$.
 - (a) Inductive Hypothesis: Suppose k is an integer, such that $k \geq a$, and $P(k)$ is true.
 - (b) Using this, show that $P(k+1)$ is true.
3. Conclude, that therefore, by the principle of mathematical induction, $P(n)$ is true, for all integers $n \geq a$. \square

Example 5.1.2

Lemma. For all integers $n \geq 1$, $1 + 2 + \dots + n = \frac{n(n+1)}{2}$.

Proof. Let $P(n)$ denote the predicate that the lemma is true for the integer n . Suppose n is an integer greater than or equal to 1.

Basis Step:

$$P(1) \implies 1 = \frac{1(1+1)}{2} = \frac{2}{2} = 1 \\ \therefore P(1) \text{ is true.}$$

Inductive Hypothesis:

Suppose $k \in \mathbb{Z} \geq 1$, $P(k)$ is true.

$$\text{Then, } k = 1 + 2 + \dots + k = \frac{k(k+1)}{2}$$

Let's now consider $k + 1$

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

Therefore, by the inductive hypothesis, the lemma is true. \square

5.2 Lecture 14

The Principle of Strong Mathematical Induction

Let $P(n)$ be a predicate that is defined for every integer $n \geq a$, where a is some fixed point integer, and let b be an integer where $b \geq a$.

Basis Step: Suppose $P(a), P(a+1), \dots, P(b)$ are true.

Inductive Step: Suppose for every integer $k \geq b$, if $P(1), P(2), \dots, P(k)$ are true, then $P(k+1)$ is true.

Conclusion: Then $P(n)$ is true for all integers $n \geq a$.

Claim. It can be proved that the strong PMI is equivalent to the ordinary PMI.

Strong PMI is advantageous in certain situations, like if we're proving the general form of a recursive sequence.

Example 5.2.1

Let b be a recursive sequence defined as follows:

$$b_1 = 4, \quad b_2 = 12, \quad b_n = b_{n-2} + b_{n-1}, \quad \forall n \in \mathbb{Z}, n \geq 3.$$

Lemma. $4 \mid b_k, \forall k \in \mathbb{Z}, k \geq 1$.

Let $P(n)$ be the predicate: $4 \mid b_n$.

Proof. We will utilise the principle of strong mathematical induction

Basis Case:

$$b_1 = 4, \quad 4 \mid 4, \therefore P(1). \\ b_2 = 12, \quad 4 \mid 12, \therefore P(2).$$

Inductive Step: Suppose for all integers $k \geq 3$, $P(1), P(2), \dots, P(k) \rightarrow P(k+1)$.

$$\begin{aligned} \text{Then, } P(k) \equiv 4 \mid b_k &\iff b_k = 4k, \quad k \in \mathbb{Z}, \\ \text{and } P(k-1) \equiv 4 \mid b_{k-1} &\iff b_{k-1} = 4l, \quad l \in \mathbb{Z}. \end{aligned}$$

Let's not consider $P(k+1)$, and the term b_{k+1} .

$$\begin{aligned} b_{k+1} &= b_k + b_{k-1} \\ &= 4k + 4l \\ &= 4(k+l). \\ \therefore 4 \mid b_{k+1} &\equiv P(k+1). \end{aligned}$$

Therefore, by the principle of the lemma is true. □

The Well-Ordering Principle

If S is a non-empty set of integers, all of which are greater than some fixed integer, the S has a least element.

Claim. : It can be proved that the WOP is equivalent to both the PMI and even the SPMI. All three of these principles are equivalent.

5.3 Lecture 15

Recurrence Relations

Definition 5.3.1: Recurrence Relation

A recurrence relation for a sequence $a = \{a_k\}_{k \in \mathbb{Z}}$ is a formula which relates some term a_k to some of its predecessors.

The initial conditions for such a recurrence relation specify the values of some initial terms.

Example 5.3.1

For example, the Fibonacci sequence is defined recursively:

$$\underbrace{F_0 = 1, \quad F_1 = 1}_{\text{Initial Conditions}}, \quad \underbrace{F_n = F_{n-1} + F_{n-2}, \quad \forall n \in \mathbb{Z}, n \geq 2}_{\text{Recurrence Relation}}$$

Ways to Define a Sequence

So far, we've seen sequences defined in 3 ways:

1. Informally

By listing the first few terms of a sequence, until the pattern becomes obvious.

1, 1, 2, 6, 24, 120, 720... Clearly, this sequence is the factorials of the nonnegative integers.

2. General Formula

By stating the general formula, how a_n depends on n , and stating where the sequence begins.

$a = \{n!\}_{n \geq 0}$.

3. Recursively

By stating a recurrence relation, how a term a_n depends on some combination of predecessor terms, and

specifying the initial conditions.

$$a_0 = 1, a_n = n \cdot a_{n-1}, \forall n \in \mathbb{Z}, n \geq 1.$$

Defining a Set Recursively

We have seen sequences of numbers defined recursively. Many other mathematical objects can also be defined recursively, such as: sets, sums, products, and functions.

A recursive definition of a set requires three things:

- I** Base: A statement that a certain object belongs in the set.
- II** Recursion: A collection of rules which show how to form new objects in the set, from the existing objects in the set.
- III** Restriction: A statement that no objects belong to the set, other than those arising from applications of step **I** and **II**

Example 5.3.2

Let's consider the set of all valid bracketings. Every left bracket, (is matched with a right bracket,). There are always at least as many left brackets as there are right brackets.

$(())()$ is valid.

$()()()$ is valid.

$()()()$ is invalid.

We can define this set recursively, namely

- I** Base: An empty expression, with no brackets is a valid bracketing.
- II** Recursion:
 - (a) If B is a valid bracketing, then (B) is a valid bracketing.
 - (b) If B and C are valid bracketings, then BC is a valid bracketing.
- III** Restriction: Any expression not derived from rules **I**, **IIa**, or **IIb** are invalid.

Lemma. $(())()$ is a valid bracketing

Proof.

Let $A =$ An empty expression. Then A is a valid bracketing. **(I)**

Let $B = (A) = ()$. Then B is a valid bracketing. **(IIa)**

Let $C = (B) = (())$. Then C is a valid bracketing. **(IIa)**

Let $D = CB = (())()$. Then D is a valid bracketing. **(IIb)**

Therefore, $(())()$ is a valid bracketing. □

Chapter 6

Week 6

6.1 Lecture 16

Solving Recurrence Relations

Given a sequence defined recursively, we may desire an explicit formula for the sequence. To find this formula, we use the method of iteration.

Method of Iteration

1. Use iteration to record a list of terms of the sequence and guess what the explicit formula is.
2. Use induction to prove the guess is correct.
3. If induction is successful, we've found a general form.
4. If induction is unsuccessful, make a new guess, and try again.

Note:-

It is not always possible to guess an explicit formula, and in fact, some recursively defined sequences do not have an explicit formula at all.

Example 6.1.1

Find an explicit formula for the recursive sequence

$$b_0 = 2, \quad b_n = b_{n-1} + 5, \text{ for } n \geq 1.$$

We can record some terms in a table:

n	0	1	2	3	4
b_n	2	7	13	19	24

This seems like an arithmetic sequence. The initial value is 2, and the common difference is 5. So we can guess that $b = \{2 + 5n\}_{n \geq 0}$. Let's set up our proof now:

Lemma. The sequence, b , which was previously defined recursively, is equal to the sequence $\{2 + 5n\}_{n \geq 0}$.

Proof.

Base Case: Consider b_0

$$b_0 = 2$$

$$2 + 5(0) = 2 + 0 = 2 = b_0$$

$\therefore b_0$ is equal to our guess formula.

Inductive Hypothesis: Suppose $k \in \mathbb{Z} \geq 0, P(k)$

$$\text{Then } b_k = 2 + 5k$$

Let's now consider b_{k+1}

$$b_{k+1} = b_k + 5 = 2 + 5k + 5 = 2 + 5(k + 1)$$

Thus, b_{k+1} is equal to our guess formula

Therefore, $\forall k \geq 0, b_k = 2 + 5k$.

Therefore, the lemma is true. □

Arithmetic Sequences

A sequence a_0, a_1, a_2, \dots is an arithmetic sequence if and only if there exists a constant d such that

$$a_k = a_{k-1} + d,$$

for all integers $k \geq 1$.

It follows from this that a general formula can be expressed as follows:

$$a_n = a_0 + dn, \forall n \in \mathbb{Z}, n \geq 0.$$

Geometric Sequences

A sequence a_0, a_1, a_2, \dots is a geometric sequence if and only if there exists a constant r such that

$$a_k = r a_{k-1},$$

for all integers $k \geq 1$.

It follows from this that a general formula can be expressed as follows:

$$a_n = a_0 r^n, \forall n \in \mathbb{Z}, n \geq 0.$$

6.2 Lecture 17

Defining Sets

A set, S , is a collection of objects, which are called elements of S .

If x , an object, is found in S , we write $x \in S$.

If x is not found in S , we write $x \notin S$.

We can define sets using curly braces,

$$A = \{2, 3, 4\}, 3 \in A, \pi \notin A.$$

Let E be the set of all positive even numbers,

$$E = \{0, 2, 4, 6, 8, \dots\}, 20 \in E, 21 \notin E, -2 \notin E.$$

Note that A is a finite set, and E is an infinite set. Both are fine.

Order does not matter, so $\{1, 2, 3, 4\} = \{2, 3, 1, 4\}$.

Repetitions are ignored, so $\{1, 1, 3, 4\} = \{4, 3, 1, 1, 3, 4\} = \{1, 3, 4\}$.

We can define a set by a property $P(x)$ which must be satisfied by its elements:

$$A = \{x \in S \mid P(x)\}.$$

This is read: “The set A is defined as all the elements, x in the set S , such that the property $P(x)$ is satisfied.”. The elements of A are precisely those elements of S for which the predicate $P(x)$ is true. For example,

$$\text{Even Integers} = \{n \in \mathbb{Z} \mid 2 \mid n\} = \{\dots, -4, -2, 0, 2, 4, \dots\}.$$

$$\{x \in \mathbb{Z} \mid 3 < x < 7\} = \{4, 5, 6\}.$$

It's worth noting at this point that sets are mathematical objects, and can therefore also be members of other sets.

$$\text{Let } A = \{1, 2, \{3\}, \{5, 6\}\}$$

$$2 \in A, 3 \notin A, \{2\} \notin A, \{3\} \in A, 5 \notin A, \{5\} \notin A.$$

Subsets

If A and B are sets, A is called a subset of B , written $A \subseteq B$, if and only if every element of A is also an element of B .

$$A \subseteq B \iff \forall x \in A \rightarrow x \in B.$$

Example 6.2.1

$$X = \{1, 2, 3, 4\}, \quad Y = \{1, 3, 4\}, \quad Z = \{1, 2\}$$

$$Y \subseteq X, \text{ and } Z \subseteq X, \text{ but } Z \not\subseteq Y.$$

Note:-

$$\forall \text{sets, } S, S \subseteq S.$$

If A and B are sets, A is called a *proper* subset of B , written $A \subset B$, if and only if, every element of A is also an element of B , but $A \neq B$.

$$A \subset B \iff A \neq B, \forall x \in A \rightarrow x \in B$$

This implies that there must be at least a single element of B which is not an element of A .

Properties of Sets

Two sets, A and B , are equal if and only if they contain the same elements,

$$A = B \iff \forall x, x \in A \leftrightarrow x \in B \iff A \subseteq B, B \subseteq A.$$

The empty set, denoted \emptyset , is the set which contains no elements.

$$\emptyset = \{\}$$

The empty set is a subset of all sets, so if S is any set, $\emptyset \subseteq S$.

For a finite set, A , the cardinality of A is the number of elements in the set A , which is denoted $|A|$.

$$|\{1, 2, 3, 4, 5\}| = 5, \quad |\emptyset| = 0$$

Note:-

We mentioned before that sets can contain sets. Consider the following:

$$S = \{A \mid A \text{ is a set, } A \notin A\}.$$

Is $S \in S$?

1. If $S \in S$, then (by definition), $S \notin S$ ✖
2. If $S \notin S$, then (by definition), $S \in S$ ✖

This is called Russel's Paradox. To avoid this, we can attempt to define all sets recursively, like we did in Lecture 15.

In real life, we ought to study formal set theory, the axiom of choice, the Zermelo-Fraenkel axioms, but we'll get to this in a later course.

Operations on Set

Let A and B be sets.

The union of A and B , denoted $A \cup B$, is the set of all elements in A or in B .

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

The intersection of A and B , denoted $A \cap B$, is the set of all elements in A and also in B .

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

The set difference of B and A , denoted $B \setminus A$, is the set of elements in B , but not in A .

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

If the sets we are considering are all subsets of some set U , called the universal set, then $U \setminus A$ is called the complement of A , and contains all the elements in the "universe of interest", except those in A .

$$A' = U \setminus A = \{x \in U \mid x \notin A\}.$$

Note:-

The definition of U is completely contextual. For example, if we're working in number theory, our universe may be the integers, or the natural numbers. If we're working with calculus, our universal set may be the reals. If we're working with objects in higher dimensional spaces, our universe might be \mathbb{R}^n for some n . The universe can be anything we can think of, as long as it is the totality of what we're considering.

Sequential Operations on Sets

We can do operate on sets sequentially, similar to the product and summation notation we introduced earlier. Given sets, $A_0, A_1, A_2, \dots, A_n$, and an integer $n \geq 0$,

$$\bigcup_{i=0}^n A_i = \left\{ x \mid \bigvee_{i=0}^n x \in A_i \right\}$$

This set will contain all the elements which are in at least one of the sets $A_0, A_1, A_2, \dots, A_n$. Of course, we can take this bad boy to infinity to...

$$\bigcup_{i=0}^{\infty} A_i = \left\{ x \mid \bigvee_{i=0}^{\infty} x \in A_i \right\}$$

Ultimately, we're still just taking the union of sets, so even though we're considering infinite sets, the union of them will only contain elements which are themselves elements of those sets.

Naturally, we can do the same with intersections

$$\bigcap_{i=0}^n A_i = \left\{ x \mid \bigwedge_{i=0}^n x \in A_i \right\}.$$

We can take this to infinity too,

$$\bigcap_{i=0}^{\infty} A_i = \left\{ x \mid \bigwedge_{i=0}^{\infty} x \in A_i \right\}.$$

Imagine a Venn diagram, with infinty circles, and then colour in the central area, which all the circles share.

The Power Set

The power set of a set, S , denoted $\mathcal{P}(S)$, is the set of all subsets of S .

$$\mathcal{P}(S) = \{X \mid X \subseteq S\}.$$

Example 6.2.2

$$\mathcal{P}(\{1, 2, 3\}) = \left\{ \begin{array}{l} \emptyset, \quad \{1\}, \quad \{1, 2\}, \quad \{1, 2, 3\} \\ \{2\}, \quad \{2, 3\}, \\ \{3\}, \quad \{1, 3\}, \end{array} \right\}$$

Note that $\emptyset \in \mathcal{P}(S)$ and $S \in \mathcal{P}(S)$.

Claim. If $|S| = n$, then $|\mathcal{P}(S)| = 2^n$.

Disjoint Sets

Two sets, A , and B are disjoint, if and only if $A \cap B = \emptyset$. That is, A and B share no common elements.

Sets, A_1, A_2, A_3, \dots are mutually disjoint (or pairwise disjoint, or nonoverlapping) if and only if $A_i \cap A_j = \emptyset$ whenever $i \neq j$. That is to say, given a series of sets, none share common elements.

Set Partitions

A finite or infinite set of nonempty sets, $\{A_1, A_2, A_3, \dots\}$ is a partition of the set A if and only if $A = \bigcup_{\forall i} A_i$ and A_1, A_2, A_3, \dots are mutually disjoint.

Example 6.2.3

A partition of $S = \{1, 2, 3, 4, 5, 6, 7\}$ is given by

$$\{\{1\}, \{2, 3\}, \{4, 5, 6\}, \{7\}\}.$$

Note, that there is not necessarily only one partition of S .

Consider \mathbb{Z} and division by 3. By the quotient-remainder theorem, every integer can be expressed uniquely as $n = 3q + r$.

$$\text{Let } A_0 = \{n \in \mathbb{Z} \mid n \equiv 0 \pmod{3}\}$$

$$\text{Let } A_1 = \{n \in \mathbb{Z} \mid n \equiv 1 \pmod{3}\}$$

$$\text{Let } A_2 = \{n \in \mathbb{Z} \mid n \equiv 2 \pmod{3}\}$$

Then, $\{A_0, A_1, A_2\}$ is a partition of \mathbb{Z} .

Ordered n -Tuple

Let $n \in \mathbb{N}$ and let x_1, x_2, \dots, x_n be n , not necessarily distinct elements. The ordered n -tuple, denoted (x_1, x_2, \dots, x_n) , consists of n elements with their ordering: first is x_1 , then x_2 , and so on. x_n is last.

When $n = 2$ is we call (x_1, x_2) an ordered-pair.

When $n = 3$ is we call (x_1, x_2, x_3) an ordered-triple.

$$(x_1, x_2, \dots, x_n) = (y_1, y_2, \dots, y_n) \iff x_i = y_i, \forall i, 1 \leq i \leq n.$$

Cartesian Product

The Cartesian product of two sets A and B , denoted $A \times B$,

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

Example 6.2.4

If $A = \{a, b\}$ and $B = \{1, 2\}$, then

$$A \times B = \{(a, 1), (a, 2), (b, 1), (b, 2)\}.$$

The familiar xy -plane is

$$\mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}.$$

In general,

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_i \in A_i, \forall i, 1 \leq i \leq n\}.$$

Intervals

Given $a, b \in \mathbb{R}$ with $a \leq b$,

$$(a, b) = \{x \in \mathbb{R} \mid a < x < b\} \quad (\text{Open Interval})$$

$$[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\} \quad (\text{Closed Interval})$$

$$[a, b) = \{x \in \mathbb{R} \mid a \leq x < b\}$$

$$(a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}$$

The symbols ∞ and $-\infty$ are used to denote intervals which are unbounded on either the left or right side.

$$(a, \infty) = \{x \in \mathbb{R} \mid x > a\}$$

$$[a, \infty) = \{x \in \mathbb{R} \mid x \geq a\}$$

$$(-\infty, a) = \{x \in \mathbb{R} \mid x < a\}$$

$$(-\infty, a] = \{x \in \mathbb{R} \mid x \leq a\}$$

6.3 Lecture 18

More Properties of Sets

Prove that $A \subseteq B$

1. Suppose $x \in A$
2. Show that $x \in B$

Example 6.3.1

Definition (A). Let $A = \{n \in \mathbb{Z} \mid n = 2k + 2, \text{ for some } k \in \mathbb{Z}\}$

Definition (E). Let $E = \{n \in \mathbb{Z} \mid n = 2m, \text{ for some } m \in \mathbb{Z}\}$

Lemma. $A \subseteq E$

Proof. Suppose $n \in A$.

Then $n = 4k + 2$, $k \in \mathbb{Z}$. Hence, $n = 2(2k + 1) = 2m$, $m \in \mathbb{Z}$, so $n \in E$.

Therefore $A \subseteq E$. □

Remark. Suppose $n = 4$. Then $n \in E$, but $n \notin A$. Therefore $A \subset E$.

Theorem 6.3.1 Transitive Property of Subsets

For all sets, A , B , and C , if $A \subseteq B$, and $B \subseteq C$, then $A \subseteq C$.

Proof. Suppose A , B , and C are sets, $A \subseteq B$, and $B \subseteq C$.

Consider $x \in A$.

Since $A \subseteq B$, then $x \in B$.

Since $B \subseteq C$, then $x \in C$.

Therefore, $A \subseteq C$. □

Inclusion For all sets A and B ,

$$A \cap B \subseteq A \quad A \cap B \subseteq B$$

(Inclusion of Intersection)

$$A \cup B \subseteq A \quad A \cup B \subseteq B$$

(Inclusion of Union)

Method for Proving Equality of Sets

1. Prove $A \subseteq B$ (Suppose $x \in A$, show $x \in B$)
2. Prove $B \subseteq A$ (Suppose $x \in B$, show $x \in A$)

Example 6.3.2

Definition (A). Let $A = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{6}\}$

Definition (B). Let $B = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{2}, x \equiv 1 \pmod{3}\}$

Lemma. $A = B$

Proof. Suppose $x \in A$

Then $x \equiv 1 \pmod{6} \iff 6 \mid (x - 1) \iff x = 6k + 1$, for some $k \in \mathbb{Z}$.

$x = 3(2k) + 1 \iff 3 \mid (x - 1) \iff x \equiv 1 \pmod{3}$

$x = 2(3k) + 1 \iff 2 \mid (x - 1) \iff x \equiv 1 \pmod{2}$

$\therefore x \in B$.

$\therefore A \subseteq B$.

Now let's suppose $x \in B$

Then $x \equiv 1 \pmod{2} \iff 2 \mid (x - 1) \iff x = 2m + 1$, for some $k \in \mathbb{Z}$

And $x \equiv 1 \pmod{3} \iff 3 \mid (x - 1) \iff x = 3n + 1$, for some $k \in \mathbb{Z}$ Note that $x = 3n + 1$ is odd, because $x = 2m + 1$, is the definition of odd.

If n is odd, then for some integer l , $x = 3(2l + 1) + 1 = 6l + 4 = 2(3l + 2)$ is even ✗.

Therefore n is even. $n = 2l$

Hence, $x = 3(2l) + 1 = 6l + 1 \iff 6 \mid (x - 1) \iff x \equiv 1 \pmod{6}$.

$\therefore B \subseteq A$.

\therefore The lemma is true, $A = B$. □

Example 6.3.3

Let A and B be subsets of the universal set U . Prove that

$$(A \cap B)' = A' \cup B'$$

Proof. Let $x \in U$

$$x \in (A \cap B)' \iff x \notin A \cap B$$

$$\iff \sim(x \in A \cap B)$$

$$\iff \sim(x \in A \wedge x \in B)$$

$$\iff \sim(x \in A) \vee \sim(x \in B)$$

$$\iff x \notin A \vee x \notin B$$

$$\Longleftrightarrow x \in A' \vee x \in B'$$

$$\Longleftrightarrow x \in A' \cup B'$$

Therefore, $(A \cap B)' = A' \cup B'$. □

Set Identities

Let A, B, C be any sets. Let U be the universal set.

Commutative Laws

$$A \cup B = B \cup A$$

$$A \cap B = B \cap A$$

Associative Laws

$$(A \cup B) \cup C = A \cup (B \cup C)$$

$$(A \cap B) \cap C = A \cap (B \cap C)$$

Distributive Laws

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Absorption Laws

$$A \cup (A \cap B) = A$$

$$A \cap (A \cup B) = A$$

Idempotent Laws

$$A \cup A = A$$

$$A \cap A = A$$

De Morgan's Laws

$$(A \cup B)' = A' \cap B'$$

$$(A \cap B)' = A' \cup B'$$

Set Difference Law

$$B \setminus A = A \cap B'$$

Double Complement Law

$$(A')' = A$$

Complements of \emptyset and U

$$U' = \emptyset$$

$$\emptyset' = U$$

Complement Laws

$$A \cup A' = U$$

$$A \cap A' = \emptyset$$

Identity Laws

$$A \cup \emptyset = A$$

$$A \cap U = A$$

Universal Bound Laws

$$A \cup U = U$$

$$A \cap \emptyset = \emptyset$$

Functions

Definition 6.3.1: Functions

A function maps, from a set X , to a set Y . Denoted $f : X \rightarrow Y$, it is a subset of the Cartesian product, $X \times Y$, such that for all elements $x \in X$, there exists a unique element $y \in Y$, for which $(x, y) \in f$.

We call X the domain of f , $\text{dom } f = X$.

We call Y the co-domain of f .

If $f : X \rightarrow Y$ is a function and $(x, y) \in f$, then we write:

$$f(x) = y \quad \text{or} \quad f : x \mapsto y.$$

We can call $f(x)$ the value of f at x , or the image of x under f .

For any particular mapping to be a function, every element in the domain, $x \in X$, must map to a single element in the co-domain, $y \in Y$. If an element in X is unmapped, the proposed map is not a function. If an element in X maps to two values in the co-domain, then the proposed map is not a function.

Image and Range

Given a function, $f : X \rightarrow Y$, and an element $x \in X$, we call $f(x)$ the image of x . If $A \subseteq X$, then the image of A is

$$f(A) = \{f(x) \mid x \in A\} = \{y \mid f(x) = y \text{ for some } x \in A\}.$$

Note that $f(A) \subseteq Y$.

The set $f(X)$ is called the range of f , $\text{ran } f$.

$$f(X) = \{y \in Y \mid y = f(x) \text{ for some } x \in X\}.$$

Note that $f(X) \subseteq Y$.

Note:-

I honestly had some trouble understanding this, but it's a lot clearer once you take a look at some diagrams which illustrate how these things work. I'm not going to recreate those diagrams here right now.

Inverse Image

Given a function $f : X \rightarrow Y$, if $B \subseteq Y$, the inverse image, or preimage of B is

$$f^{-1}(B) = \{x \in X \mid f(x) \in B\}.$$

Equality of Functions

Suppose $f : X \rightarrow Y$ and $g : X \rightarrow Y$ are functions. Then

$$f = g \iff f(x) = g(x), \forall x \in X.$$

Example 6.3.4

Consider $f : \mathbb{Z} \rightarrow \mathbb{Z}$, $f(x) = x$ and $g : \mathbb{Z} \rightarrow \mathbb{Z}$, $g(x) = \sqrt{x^2}$.

Here $f \neq g$ because $f : -1 \mapsto -1$ but $g : -1 \mapsto 1$.

Note that $\text{ran } f = \mathbb{Z}$, but $\text{ran } g = \mathbb{Z}^{\geq 0}$.

Identity Functions

Given a set X , the identity function on X , denoted $\iota_X : X \rightarrow X$ is defined by

$$\iota_X : X \rightarrow X, \iota_X(x) = x, \forall x \in X.$$

This function is kind of cute! Given a set, the identity function is a mapping of every element in that set, to itself.

Sequences

An infinite sequence, $a = \{a_n\}_{n \geq k}$ is a function defined on the set of integers greater than some fixed point $k \in \mathbb{Z}$.

$$a = \{a_n\}_{n \geq k} = f : \mathbb{Z}^{\geq k} \rightarrow Y, f(n) = a_n.$$

Note that $\text{dom } f = \mathbb{Z}^{\geq k}$, where k is the integer fixed point of the sequence.

Chapter 7

Week 7

7.1 Lecture 19

One-to-One (Injective) Functions

Let f be a function mapping the set X , to the set Y . The function is injective if and only if for all elements $x_1, x_2 \in X$, $f(x_1) = f(x_2) \implies x_1 = x_2$. Or equivalently, if $x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$.

Think “Every element in the domain has a different image,” or every unique element in the domain maps to a unique element in the co-domain.

A function is not injective if and only if there exists some $x_1, x_2 \in X$, $x_1 \neq x_2$, such that $f(x_1) = f(x_2)$.

To prove injectivity, we use a direct proof:

1. Suppose $x_1, x_2 \in X$ and $f(x_1) = f(x_2)$.
2. Show that $x_1 = x_2$.

To prove that a function is not injective, we only need to present a counterexample of $x_1, x_2 \in X$, $f(x_1) = f(x_2)$, but $x_1 \neq x_2$.

Onto (Surjective) Functions

Let $f : X \rightarrow Y$ be a function, mapping from the set X to the set Y . The function is surjective if and only if, given any element $y \in Y$, it is possible to find an element $x \in X$ with the property $y = f(x)$. Equivalently,

$$f : X \rightarrow Y \text{ is surjective} \iff \forall y \in Y, \exists x \in X : f(x) = y.$$

A function is not surjective if and only if there exists some element $y \in Y$, the co-domain, that is not mapped onto by f .

To prove surjectivity, we usually use a direct proof:

1. Suppose that $y \in Y$.
2. Construct an element x of X with $f(x) = y$.

To prove that a function is not surjective, find and present a counterexample of $y \in Y$ such that $\forall x \in X$, $f(x) \neq y$. This is usually done with a proof by contradiction.

One-to-One Correspondance (Bijective) Functions

A function, $f : X \rightarrow Y$, is bijective if and only if f is injective and surjective.

This, effectively means that, every element in the co-domain is an image of an element in the domain, and every unique element in the domain maps to a unique element in the co-domain.

Theorem 7.1.1 Inverse Function

Suppose that a function $f : X \rightarrow Y$ is bijective. Then, there exists a function $f^{-1} : Y \rightarrow X$ that is defined:

$$\forall y \in Y, f^{-1}(y) = x \in X : f(x) = y.$$

The function f^{-1} is called the inverse function of f .

7.2 Lecture 20

Composition of Functions

Definition 7.2.1: Function Composition

Let $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ be functions. The composition of those functions is defined As

$$(g \circ f)(x) = g(f(x)), \forall x \in X.$$

Note that $\text{dom } g \circ f = X$, and its co-domain is Z .
 $\text{ran } g \circ f$ is the image (under g) of the range of f .

Theorem 7.2.1 Compositions of Identity Function

If $f : X \rightarrow Y$ is a function, and $\iota_X : X \rightarrow X$, $\iota_Y : Y \rightarrow Y$ are the identity functions on X and Y , respectively, then

$$f \circ \iota_X = f \quad \text{and} \quad \iota_Y \circ f = f.$$

Proof. Suppose $f : X \rightarrow Y$ is a function, $\iota_X : X \rightarrow X$ is the identity function under X and $\iota_Y : Y \rightarrow Y$ is the identity function under Y .

Then, by definition, $\iota_X(x) = x$, $\forall x \in X$,

and, $\iota_Y(y) = y$, $\forall y \in Y$.

Now, $\forall x \in X$, $(f \circ \iota_X)(x) = f(\iota_X(x)) = f(x)$. Hence, $f \circ \iota_X = f$.

And, $\forall y \in Y$, $(\iota_Y \circ f)(x) = \iota_Y(f(x)) = f(x)$. Hence, $\iota_Y \circ f = f$.

Therefore, the theorem is proven. □

Theorem 7.2.2 Bijective-Inverse Composition

Let $f : X \rightarrow Y$ be a bijective function, and $f^{-1} : Y \rightarrow X$ be its inverse. Then

$$f^{-1} \circ f = \iota_X \quad \text{and} \quad f \circ f^{-1} = \iota_Y$$

Theorem 7.2.3 Injective Compositions are Injective

If $f : X \rightarrow Y$ and $g : X \rightarrow Y$ are both injective then the composition $g \circ f$ is injective.

Proof. Suppose $f : X \rightarrow Y$ and $g : X \rightarrow Y$ are both injective functions.

Suppose $x_1, x_2 \in X$ and $(g \circ f)(x_1) = (g \circ f)(x_2)$.

Then, $g(f(x_1)) = g(f(x_2))$.

Since, g is injective, we have $f(x_1) = f(x_2)$.

Since, f is injective, we have $x_1 = x_2$.

Therefore, $g \circ f$ is injective. □

Theorem 7.2.4 Surjective Compositions are Surjective

If $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ are both surjective functions, then their composition $g \circ f$ is surjective.

Proof. Suppose $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ are surjective functions.

Suppose $z \in Z$.

Since g is surjective, $\exists y \in Y : g(y) = z$.

Since f is surjective, $\exists x \in X : f(x) = y$.

Hence, $\exists x \in X : (g \circ f)(x) = g(f(x)) = g(y) = z$.

Therefore $g \circ f$ is surjective. □

Theorem 7.2.5 Bijective Compositions are Bijective

It follows from Theorem 7.2.3 and Theorem 7.2.4 that if $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ are bijective (injective and surjective), then their composition $g \circ f : X \rightarrow Z$ is bijective.

7.3 Lecture 21

Cardinality

The cardinality of a set is a measure of how large it is. We say that two sets X and Y have the same cardinality, $|X| = |Y|$, if and only if there exists a bijection between them.

A finite set is either a set with no elements in it, or one for which there exists a bijection between it and a set of the form $\{1, 2, 3, \dots, n\}$, where n is some fixed integer.

An infinite set is a nonempty set for which there does not exist a bijection between it and a set of the form $\{1, 2, 3, \dots, n\}$, where n is some fixed integer.

Finite Sets

Theorem. Suppose X and Y are finite sets

1. If $|X| > |Y|$, then there is no injective $f : X \rightarrow Y$. (By pigeonhole principle, there will always be at least 2 $x \in X$ mapping to the same $y \in Y$.)
2. If $|X| < |Y|$, then there is no surjection $f : X \rightarrow Y$. ($x \in X$ will map to $|X|$ number of elements in Y , but there will be some left over.)
3. It follows from this that, unless $|X| = |Y|$, there can not exist a bijection $f : X \rightarrow Y$.

Corollary. For finite sets, X and Y , with $|X| = |Y|$, the following statements are equivalent:

- $f : X \rightarrow Y$ is injective.
- $f : X \rightarrow Y$ is surjective.
- $f : X \rightarrow Y$ is bijective.

Infinite Sets

Two sets, X and Y , have the same cardinality if and only if there exists a bijection between them.

Lemma. The cardinality of the even integers is equal to the cardinality of all the integers.

Proof. Define a function $f : \mathbb{Z} \rightarrow \{n \in \mathbb{Z} \mid n = 2k, k \in \mathbb{Z}\}$, $f(x) = 2x$, $\forall x \in \mathbb{Z}$.

First we will show that f is injective:

Suppose $x_1, x_2 \in \mathbb{Z}$ and $f(x_1) = f(x_2)$.

Then $2x_1 = 2x_2$. We divide both sides by 2 and find that $x_1 = x_2$.

Therefore, f is injective.

Next, we'll show that f is surjective:

Suppose $y \in \{n \in \mathbb{Z} \mid n = 2k, k \in \mathbb{Z}\}$.

Then $y = 2x$, for some $x \in \mathbb{Z}$.

Hence $f(x) = 2x = y$.

Thus, f is surjective.

Therefore, f is injective and surjective. Therefore, f is a bijection.

Therefore, $|\mathbb{Z}| = |\{n \in \mathbb{Z} \mid n = 2k, k \in \mathbb{Z}\}|$.

□

Chapter 8

Week 8

8.1 Lecture 22

Countable and Uncountable Sets

Definition 8.1.1: Countably Infinite

A set, S , is called countably infinite if and only if it has the same cardinality as the set of positive integers, \mathbb{N} .

$$|S| = |\mathbb{N}|$$

Definition 8.1.2: Countable

A set, is called countable if and only if it is finite or countably infinite. A set that is not countable is called uncountable.

Theorem 8.1.1

Any subset of any countable set is countable

Corollary 8.1.1

Any set with an uncountable subset, is uncountable

Note:-

The corollary is just the contrapositive of the theorem

Theorem 8.1.2 Reals are Uncountable

The set $I = \{x \in \mathbb{R} \mid 0 < x < 1\}$ is uncountable.

Proof. Suppose the theorem is false.

Then the set I is countable, so the decimal expansion of these numbers can be written in a list. Let's write every number now:

$$\begin{array}{l} 0.a_{11}a_{12}a_{13}a_{14} \dots a_{1n} \dots \\ 0.a_{21}a_{22}a_{23}a_{24} \dots a_{2n} \dots \\ 0.a_{31}a_{32}a_{33}a_{34} \dots a_{3n} \dots \\ \vdots \end{array}$$

We can construct a new number, d , whose decimal expansion is

$$d = 0.d_1d_2d_3d_4 \dots d_n \dots$$

according to the rule

$$d_i = \begin{cases} 1 & \text{if } a_{nn} \neq 1 \\ 2 & \text{if } a_{nn} = 1 \end{cases}$$

For each natural number, d differs from the n th real number in the list because it differs in the n th decimal place. Hence, we've constructed a number $d \in I$, but which we didn't write down originally, or $d \notin I$. \times

This is a contradiction.

Therefore, the theorem is true. \square

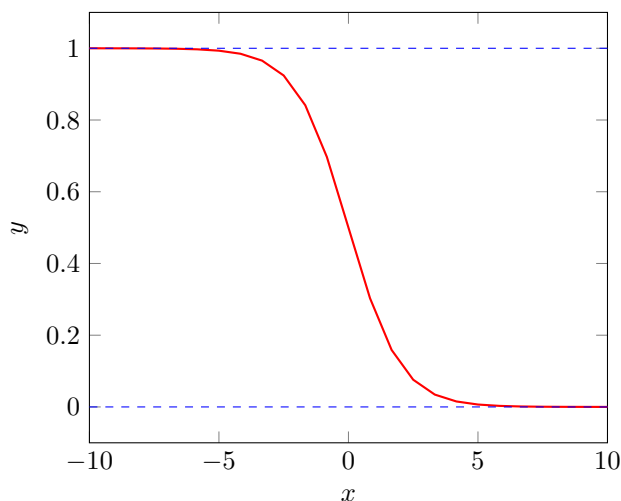
Now, since the theorem is true, the corollary is true. So it follows that, since $I \subseteq \mathbb{R}$, and I is uncountable, then \mathbb{R} is uncountable.

In fact,

$$|I| = |\mathbb{R}|$$

since there exists a bijection $f : \mathbb{R} \rightarrow I$, namely

$$f(x) = \frac{1}{1 + \exp(x)}$$



Comparing Cardinalities

For two sets, X and Y

- $|X| \leq |Y| \iff \exists$ injective $f : X \rightarrow Y$
- $|X| \geq |Y| \iff \exists$ surjective $f : X \rightarrow Y$
- $|X| < |Y| \iff \exists$ injective and not surjective $f : X \rightarrow Y$
- $|X| > |Y| \iff \exists$ surjective and not injective $f : X \rightarrow Y$
- $|\emptyset| < |X|$ and $|X| > |\emptyset| \forall X \neq \emptyset$

Theorem 8.1.3 Schröder-Bernstein Theorem

For two sets, X, Y ,

$$|X| \leq |Y|, |X| \geq |Y| \implies |X| = |Y|$$

Therefore, to show that two sets have equal cardinality, it is enough to find

1. an injective function, $f : X \rightarrow Y$ and
2. a surjective function, $f : X \rightarrow Y$

Or

1. an injective function, $f : X \rightarrow Y$ and
2. an injective function, $f : Y \rightarrow X$

Or

1. a surjective function, $f : X \rightarrow Y$ and
2. a surjective function, $f : Y \rightarrow X$

This can be easier then finding a bijection between the two sets.

8.2 Lecture 23

Relations on Sets

Definition 8.2.1: Relation

Given sets A and B , a binary relation α from A to B is a subset of the Cartesian product of A and B . If $(x, y) \in \alpha$ we can also write $x \alpha y$, and we say x is related to y .

Example 8.2.1

Let $A = \{1, 2, 5\}$ and $B = \{5, 6\}$, define a binary relation σ by

$$\forall a \in A, b \in B, a \sigma b \iff a < b$$

Then

$$A \times B \supseteq \sigma = \{(1, 5), (1, 6), (2, 5), (2, 6), (5, 6)\}$$

We can represent this with a diagram, drawing arrows from the elements in set A to elements in set B . We draw an error if and only if the element in A is related to the element in B .

We can thereby observe that a relation is a generalisation of a function.

Definition 8.2.2: Inverse Relation

If ρ is a relation from sets A to B , then the inverse relation ρ^{-1} is defined by

$$\rho^{-1} = \{(b, a) \in B \times A \mid (a, b) \in \rho\}$$

Example 8.2.2

Let $A = \{2, 3\}$ and $B = \{2, 6, 9\}$ and $\rho \subseteq (A, B)$ such that

$$\forall a \in A, b \in B, a \rho b \iff a \mid b$$

Then

$$\rho = \{(2, 2), (2, 6), (3, 6), (3, 9)\}$$

and

$$\rho^{-1} = \{(2, 2), (6, 2), (6, 3), (9, 3)\}$$

Definition 8.2.3

A relation on a set, is a relation from a set A to itself.

Example 8.2.3

Let ρ be a relation on set $A = \{2, 3, 6\}$:

$$\forall x, y \in A, x \rho y \iff x \mid y$$

Then

$$A \times A \supseteq \rho = \{(2, 2), (3, 3), (6, 6), (2, 6), (3, 6)\}$$

Definition 8.2.4

Let ρ be a relation on a set A .

- ρ is reflexive $\iff \forall x \in A, x \rho x$
- ρ is symmetric $\iff \forall x, y \in A, x \rho y \implies y \rho x$
- ρ is transitive $\iff \forall x, y, z \in A, x \rho y, y \rho z \implies x \rho z$

On an arrow diagram, a relation is

- reflexive if and only if every element has an arrow pointing to itself.
- symmetric if and only if for every arrow from one element to another, there is a second arrow travelling in the opposite direction.
- transitive if and only if for every two consecutive arrows, there is a third arrow connecting the ultimate start element with the ultimate end location (think about how the opposite and adjacent lengths of a triangle connect points P to Q and Q to R , but the hypotenuse ultimately connects P to R .)

Example 8.2.4

Let $d \in \mathbb{N}$ be fixed. The relation ρ on \mathbb{Z} , defined by

$$\forall a, b \in \mathbb{Z}, a \rho b \iff a \equiv b \pmod{d}$$

Is reflexive

$$\begin{aligned} &\text{Suppose } a \in \mathbb{Z} \\ &\text{Then } a - a = 0 \\ &d \mid 0 \iff a \equiv a \pmod{d} \\ &\therefore a \rho a \end{aligned}$$

Is symmetric

$$\begin{aligned} &\text{Suppose } a, b \in \mathbb{Z}, a \rho b \\ &\text{Then } a \equiv b \pmod{d}, d \mid (a - b), d \mid -(b - a), d \mid (b - a) \iff b \equiv a \pmod{d} \\ &\therefore b \rho a \end{aligned}$$

Is transitive

$$\begin{aligned} &\text{Suppose } a, b, c \in \mathbb{Z}, a \rho b, b \rho c \\ &\text{Then } a \equiv b \pmod{d}, b \equiv c \pmod{d} \\ &d \mid (a - b), d \mid (b - c) \iff d \mid (a - b) + (b - c) \iff d \mid (a - c) \iff a \equiv c \pmod{d} \\ &\therefore a \rho c \end{aligned}$$

Lemma. A relation ρ on set A is symmetric if and only if $\rho = \rho^{-1}$.

Proof. Let ρ be a relation on set A .

Show that ρ is symmetric $\implies \rho = \rho^{-1}$

Suppose ρ is symmetric.

Let $(x, y) \in \rho$. Then $(y, x) \in \rho^{-1}$, because ρ is symmetric.

Hence, $(x, y) \in \rho^{-1}$.

So, $\rho \subseteq \rho^{-1}$.

Now, let $(x, y) \in \rho^{-1}$. Then $(y, x) \in \rho$ by definition.

Hence $(x, y) \in \rho$, since ρ^{-1} is symmetric.

So, $\rho^{-1} \subseteq \rho$.

Therefore, $\rho = \rho^{-1}$

Show that $\rho = \rho^{-1} \implies \rho$ is symmetric.

Suppose $\rho = \rho^{-1}$

Let $(x, y) \in \rho$. Then $(y, x) \in \rho^{-1}$.

But, $\rho = \rho^{-1}$, therefore $(y, x) \in \rho$.

Therefore, ρ is symmetric.

Therefore, ρ is symmetric $\iff \rho = \rho^{-1}$

□

Chapter 9

Week 9

9.1 Lecture 24

Equivalence Relations

Definition 9.1.1: Equivalence Relation

Let ρ be a relation on the set A . Then ρ is an equivalence relation if and only if ρ is symmetric, reflexive, and transitive.

Example 9.1.1

The relation ρ on \mathbb{Z} from example 8.2.4 is reflexive, symmetric and transitive.

Therefore, ρ is an equivalence relation.

Definition 9.1.2: Equivalence Class

Let ρ be an equivalence relation on the set A , and let $a \in A$.

The equivalence class of a is

$$[a] = \{x \in A \mid x \rho a\}$$

So, $\forall x \in A, x \in [a] \iff x \rho a$

Example 9.1.2

Let ρ be the relation on \mathbb{Z} defined by $a \rho b \iff a \equiv b \pmod{3} \iff 3 \mid (a - b)$.

Then ρ is an equivalence relation with equivalence classes

$$\begin{aligned} [0] &= \{\dots, -6, -3, 0, 3, 6, \dots\} \\ [1] &= \{\dots, -5, -2, 1, 4, 7, \dots\} \\ [2] &= \{\dots, -4, -1, 2, 5, 8, \dots\} \end{aligned}$$

Notice that $[0] = [3] = [-6]$, etc.

Also notice that every element of the set has been put into one of these classes. A partition

Lemma. Let ρ be an equivalence relation on S and $a, b \in S : a \rho b$, then $[a] = [b]$.

Proof. Let ρ be an equivalence relation on the set A , $a, b \in A$, and $a \rho b$.

Show $[a] \subseteq [b]$

Let $x \in [a]$. Then $x \rho a$, by definition.

Now, since $x \rho a$ and $a \rho b$, then $x \rho b$, by the transitive property.

Thus, $x \in [b]$

$\therefore [a] \subseteq [b]$

Show $[b] \subseteq [a]$

Let $x \in [b]$. Then $x \rho b$, by definition.

Now, since $x \rho b$ and $b \rho a$, then $x \rho a$, by the transitive property.

Thus, $x \in [a]$

$\therefore [b] \subseteq [a]$

$\therefore [a] = [b]$

□

Lemma. If ρ is an equivalence relation on the set A , and $a, b \in A$ and $[a] \cap [b] \neq \emptyset$, then $[a] = [b]$.

Or, equivalently

If ρ is an equivalence relation on the set A , and $a, b \in A$, then either $[a] \cap [b] = \emptyset$ or $[a] = [b]$.

Theorem 9.1.1

If ρ is an equivalence relation on A , then the set of equivalence classes of ρ form a partition of A .

$$\bigcup_{\forall a \in A} [a] = A$$

This can work in the opposite direction too,

Theorem. Given a partition of A , and a binary relation ρ , induced by the partition, it follows that ρ is reflexive, symmetric, and transitive.

9.2 Lecture 25

Partial Order Relations

Definition 9.2.1: Antisymmetric

A relation ρ on a set A is antisymmetric if and only if

$$\forall a, b \in A, a \rho b, b \rho a \implies a = b$$

Definition 9.2.2: Partial Order Relation

A relation ρ on the set A is a partial order relation on A if and only if ρ is reflexive, antisymmetric, and transitive.

Example 9.2.1

Consider the relation “less than or equal to” on \mathbb{R}

- Reflexive: $\forall x \in \mathbb{R}, x \leq x$.
- Antisymmetric: $\forall x, y \in \mathbb{R}, x \leq y, y \leq x \implies x = y$.
- Transitive: $\forall x, y, z \in \mathbb{R}, x \leq y, y \leq z \implies x \leq z$.

Therefore, \leq is a partial order relation on \mathbb{R}

Definition 9.2.3: Comparable Elements

Let ρ be a relation on a set A . Elements $a, b \in A$ are comparable if and only if $a \rho b$ or $b \rho a$. Otherwise, a and b are incomparable.

Definition 9.2.4: Total Order Relation

Let ρ be a relation on a set A . Then ρ is a total order relation if and only if ρ is a partial order relation such that all elements are comparable.

That is, ρ is a total order relation if and only if

- ρ is reflexive,
- ρ is antisymmetric,
- ρ is transitive,
- $\forall a, b \in A, a \rho b \vee b \rho a$.

Example 9.2.2

Show that the relation ρ be defined by $a \rho b \iff a \mid b$ on the set $A = \{1, 2, 4, 8, 16\}$. Show that this relation is a total order relation on the set A .

$\forall a \in A, a \mid a$.

Therefore ρ is reflexive on A .

Suppose $a, b \in A$ and $a \mid b$ and $b \mid a$.

Then $b = ka$ and $a = lb$, for some $k, l \in \mathbb{N}$.

Thus $b = klb \iff 1 = lb$. Therefore $a = b$.

Therefore, ρ is antisymmetric

Suppose $a, b, c \in A$ and $a \mid b$ and $b \mid c$.

Then $b = ka$ and $c = lb$, for some $k, l \in \mathbb{N}$.

Thus $c = kla$ Therefore $a \mid c$.

Therefore, ρ is transitive.

Therefore, ρ is a partial order relation.

Let $a, b \in A$.

Then, $a = 2^k, b = 2^l$, for some $k, l \in \{0, 1, 2, 3, 4\}$.

Without loss of generality, assume $k \leq l$.

Then $b = 2^l = 2^{l-k}2^k$.

Since $2^k \in \mathbb{Z}$, we have $2^k \mid b$, hence $a \mid b$.

Therefore, all the elements of A are comparable.

Therefore ρ is a total order relation on A .

9.3 Lecture 26

Groups

Definition 9.3.1: Group

Let G be a set, and let $*$ be a binary operation, $*$: $G \times G \rightarrow G$. We call $(G, *)$ group if and only if it has the following properties:

- **Closure:** $\forall g, h \in G, g * h \in G$.
- **Associative:** $\forall g, h, k \in G, (g * h) * k = g * (h * k)$.
- **Identity:** $\exists i \in G : \forall i \in G, i * g = g * i = e$.
- **Inverse:** $\forall g \in G, \exists g^{-1} \in G : g * g^{-1} = g^{-1} * g = i$.

Example 9.3.1

$(\mathbb{Z}, +)$ is a group.

$+: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, +: (a, b) \mapsto a + b, a + b \in \mathbb{Z}, \forall a, b \in \mathbb{Z}$. Hence, $(\mathbb{Z}, +)$ is closed since $(a + b) + c = a + (b + c), \forall a, b, c \in \mathbb{Z}$, hence, $(\mathbb{Z}, +)$ is associative
 $0 \in \mathbb{Z} : \forall n \in \mathbb{Z}, 0 + a = a + 0 = a$. Hence, 0 is the identity.
 $\forall a \in \mathbb{Z}, -a \in \mathbb{Z}, a + (-a) = (-a) + a = 0$. Hence, every element has an inverse.

Therefore, $(\mathbb{Z}, +)$ is a group.

Example 9.3.2

Is (\mathbb{R}, \cdot) a group?

Closure? $\forall x, y \in \mathbb{R}, x \cdot y \in \mathbb{R}$. YES

Associative? $\forall x, y, z \in \mathbb{R}, (x \cdot y) \cdot z = x \cdot (y \cdot z)$. YES

Identity? $1 \in \mathbb{R}, \forall x \in \mathbb{R}, 1 \cdot x = x \cdot 1 = x$. YES

Inverse? $\forall x \in \mathbb{R}$, take $y = \frac{1}{x} \in \mathbb{R}, x \cdot y = y \cdot x = 1$. yes..? EXCEPT $0 \in \mathbb{R}, \frac{1}{0} \notin \mathbb{R}$. NO!

Therefore (\mathbb{R}, \cdot) is not a group. However, it's interesting to note that $(\mathbb{R} \setminus \{0\}, \cdot)$ IS a group!

These are examples of an infinite groups, since the sets \mathbb{Z} and \mathbb{R} are infinite sets.

Let's consider the set \mathbb{Z}_n where \mathbb{Z}_n denotes the set of equivalence classes of the integers modulo n ,

$$\mathbb{Z}_n = \{[0], [1], [2], \dots, [n-1]\}$$

Next we'll define

$$\begin{aligned} + : \mathbb{Z}_n \times \mathbb{Z}_n &\rightarrow \mathbb{Z}_n, [a] + [b] = [a + b] \\ \cdot : \mathbb{Z}_n \times \mathbb{Z}_n &\rightarrow \mathbb{Z}_n, [a] \cdot [b] = [a \cdot b] \end{aligned}$$

Example 9.3.3

Consider $(\mathbb{Z}_3, +)$

We can make an “addition table” to represent this

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

- Closure: YES. Every element inside the table is in the set \mathbb{Z}_3
- Associative: YES.
- Identity: YES, namely [0].
- Inverse: YES, namely $[0]^{-1} = [0]$, $[1]^{-1} = [2]$, $[2]^{-1} = [1]$.

Therefore, $(\mathbb{Z}_3, +)$ is a group.

Note:-

Note that the above table is called a Cayley Table, an $n \times n$ array with rows and columns labeled by the n elements. The entry in column x , row y is $x * y$, where $*$ is the group operation.

Definition 9.3.2: Abelian

A group $(G, *)$ is called Abelian if the operation $*$ is commutative, that is

$$\forall g, h \in G, g * h = h * g$$

Otherwise, we call the group non-Abelian.

For $n \in \mathbb{N}$, the symmetric group S_n consists of all bijections

$$f : X \rightarrow X \text{ where } X = \{a \in \mathbb{N} \mid a \leq n\}$$

under the operation \circ , the composition of functions.

We should note that S_n is non-Abelian for $n \geq 3$.

Chapter 10

Week 10

10.1 Lecture 27

Elementary Properties of Groups

Theorem 10.1.1 Unique Identity Element

Suppose $(G, *)$ has two unique identity elements, e_1 and e_2 . We can now evaluate $e_1 * e_2$ in two ways.

Since e_1 is the identity, and $e_2 \in G$, $e_1 * e_2 = e_2$.

Since e_2 is the identity, and $e_1 \in G$, $e_1 * e_2 = e_1$.

Hence, $e_1 = e_2$, but this is a contradiction, since e_1 and e_2 are defined to be unique identity elements.

Hence, $(G, *)$ has only one unique identity element. \square

Theorem 10.1.2 Every Element has an Inverse

Suppose $(G, *)$ is a group and $g \in G$ has two unique inverses $h_1, h_2 \in G$. Let e be the identity of $(G, *)$.

Then, $(h_1 * g) * h_2 = e * h_2 = h_2$.

And, $h_1 * (g * h_2) = h_1 * e = h_1$.

So, $h_1 = h_2$, but this is a contradiction, since h_1 and h_2 is defined to be unique inverses of g .

Therefore, for the group $(G, *)$ every element $g \in G$ has one unique inverse. \square

Definition 10.1.1: Subgroup

Let $(G, *)$ be a group, and let $H \subseteq G$. We say that H is a subgroup of G if $(H, *)$ itself is a group.

That is, H is a subgroup of G if:

- Closure: $\forall g, h \in H$, we have $g * h \in H$.
- Identity: e is the identity of $(G, *)$, then $e \in H$.
- Inverses: $\forall h \in H$, $\exists h^{-1} : h * h^{-1} = e$.

We write $H \leq G$ to denote “ H is a subgroup of G ”, when the group context is clear.

If $H \leq G$ and $H \neq G$, then H is a proper subgroup of G .

If e is the identity element of group G , then $(\{e\}, *)$ is a trivial subgroup.

Definition 10.1.2: Element Powers

Let $(G, *)$ be a group. By associativity we have $(a * b) * c = a * (b * c)$, $\forall a, b, c \in G$. Thus, we can write $a * b * c$ without ambiguity.

Given this group, and element $g \in G$, we can define powers as follows:

- $g^k = g * g * \dots * g$ (k times), $k \in \mathbb{Z}_+$.
- $g^{-k} = g^{-1} * g^{-1} * \dots * g^{-1}$, (k times), $k \in \mathbb{Z}_+$.
- $g^0 = e$.

Definition 10.1.3: Cyclic Subgroups

Let $a \in G$ be an element of the group $(G, *)$. We let $\langle a \rangle$ denote “the set generated by a ,”

$$\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\} = \{\dots, a^{-2}, a^{-1}, a^0, a^1, a^2, \dots\}$$

For any $a \in G$ where $(G, *)$ is a group, $\langle a \rangle$ is a subgroup of G :

- Closure: $x, y \in \langle a \rangle$, $x = a^i$, $y = a^j$, $i, j \in \mathbb{Z}$. Then, $x * y = a^i * a^j = a^{i+j} \in \langle a \rangle$.
- Identity: $e = a^0 \in \langle a \rangle$.
- Inverses: $x^{-1} = \{a^i\}^{-1} = a^{-i} \in \langle a \rangle$.

$\langle a \rangle$ is called the cyclic subgroup of G generated by a .

If $G = \langle a \rangle$ for some $a \in G$, we say G is cyclic and a is a generator of G .

10.2 Lecture 28

Group Isomorphisms

Definition 10.2.1: Isomorphic Groups

Two groups, $(G, *)$ and (H, \circ) are isomorphic if and only if there exists a bijection $f : G \rightarrow H$ such that for all $x, y \in G$, $f(x * y) = f(x) \circ f(y)$. Such a bijection is called an isomorphism.

If f is an isomorphism from group G to group H and $e \in G$ and $\iota \in H$ are the identity elements of G and H , respectively, then $f(e) = \iota$.

If G and H are isomorphic, they share the same properties, like number of elements, abelian-ness, number of sub-groups, fundamental structure, etc.

Theorem 10.2.1

For any prime p , the group $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is isomorphic to $(\mathbb{Z}_{p-1}, +)$, where \mathbb{Z}_n denotes the natural numbers modulo n .

Theorem 10.2.2

Suppose $n, m \in \mathbb{Z}_+$. Then $(\mathbb{Z}_n \times \mathbb{Z}_m, +)$ is isomorphic to $(\mathbb{Z}_{nm}, +)$ if and only if $\gcd(n, m) = 1$, (i.e. n and m are coprime).

This means that modular arithmetic for large numbers,

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots p_n^{e_n}$$

can be done with as arithmetic modulo the prime powers $p_i^{e_i}$.

Group isomorphism is important, because what we know about a groups, we also know about its Isomorphic groups.

10.3 Lecture 29

Fields

Definition 10.3.1: Field

A field, $(F, +, \cdot)$ consists of a set F , and two binary operators:

- $+: F \times F \rightarrow F$
- $\cdot: F \times F \rightarrow F$

such that

1. $(F, +)$ is an Abelian group, with identity, e .
2. $(F \setminus \{e\}, \cdot)$ is an Abelian group.
3. $\forall f, g, h \in F, f \cdot (g + h) = (f \cdot g) + (f \cdot h)$
4. $\forall f, g, h \in F, (f + g) \cdot h = (f \cdot h) + (g \cdot h)$

Consequently, a field will have two identities, an additive identity and a multiplicative identity. We will also have two types of inverses, additive inverses and multiplicative inverses.

Fields are used when defining structures in linear algebra, for example, the components of a vector or matrices can be elements of a field $(F, +, \cdot)$.

Finite groups like $(\mathbb{Z}_p, +, \cdot)$ are important in computer science, because they can can “behave” like real numbers, but are small enough to describe precisely using finite bits.

Chapter 11

Week 11

11.1 Lecture 30

Introduction to Counting

Example 11.1.1

Suppose a restaurant has 5 types of cake and 2 types of ice cream.

How many choices for dessert are there, if we select one cake, and one ice cream?

$$5 \text{ cakes} \cdot 2 \text{ ice creams} = 10 \text{ choices}$$

How many choices for dessert are there if we select either one cake or one ice cream?

$$5 \text{ cakes} + 2 \text{ ice creams} = 7 \text{ choices}$$

In one example, we had a sequence of two separate **tasks**, and therefore, used a multiplication to find the answer. In the second, we only had one task, but were choosing from 2 types of options, and therefore addition was used to find the total.

Example 11.1.2

Consider the set of all passwords consisting of 3 letters from the set $\{A, B, C, \dots, X, Y, Z\}$.

How many passwords are possible?

There are 26 choices for the first, second, and third letters.

$$26 \cdot 26 \cdot 26 = 26^3 = 17,576 \text{ passwords}$$

How many passwords contain no repeated letters? There are 26 choices for the first letter, 25 for the second, and 24 for the third.

$$26 \cdot 25 \cdot 24 = 15,600 \text{ passwords with no repeated letters}$$

How many passwords contain only vowels or only consonants?

Here we need to consider and compute two options, then add them together.

Option 1: only vowels

$$5 \cdot 5 \cdot 5 = 5^3 = 125$$

Option 2: only consonants

$$21 \cdot 21 \cdot 21 = 21^3 = 9,261$$

Total = option 1 + option 2

$$5^3 + 21^3 = 9,386$$

Definition 11.1.1: Permutation

A permutation of a set of objects is an arrangement of the objects into an order.

Theorem. A set with cardinality n elements will have $n!$ permutations.

Example 11.1.3

Consider the permutations of the letters of the word OBJECTS.

How many start with a vowel?

Option 1: words starting with O

$$1 \text{ choice for first letter (O)} \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \text{ choices for proceeding letters} = 6! = 720$$

Option 2: words starting with E

$$1 \text{ choice for first letter (E)} \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \text{ choices for proceeding letters} = 6! = 720$$

Total = option 1 + option 2

$$6! + 6! = 720 + 720 = 1440$$

Alternatively (and more elegantly) we can calculate it in one go, by noting that we have two choices for the first letter,

$$1 \text{ choices for first letter (O/E)} \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \text{ choices for proceeding letters} = 2 \cdot 6! = 1440$$

Example 11.1.4

Consider all license plates consisting of 3 letters from the set $\{A, B, \dots, Y, Z\}$ followed by 3 digits from the set $\{0, 1, \dots, 8, 9\}$.

How many plates are possible?

$$10 \cdot 10 \cdot 10 \cdot 26 \cdot 26 \cdot 26 = 10^3 \cdot 26^3 = 17.576.000$$

How many plates have no repeated symbols (digits or letters)?

$$10 \cdot 9 \cdot 8 \cdot 26 \cdot 25 \cdot 24 = 11.232.000$$

How many plates have at least one repeated symbol?

We note that we've already calculated the total number of plates, and the number of plates with no repeated digits. Therefore the number of plates with at least one repeated digit will be the total minus the number without repeated digits

$$17.576.000 - 11.232.000 = 6.344.000$$

11.2 Lecture 31

Counting Selections

Let n and r be nonnegative integers.

Problem:

Select r elements from a set of n elements. How many ways are there to make the selections?

Considerations:

- Does order matter?
- Is repetition of element selections allowed?

Order matters, Repetitions allowed

Example 11.2.1

Suppose we need to choose a PIN number, and we may do so from the set

$$S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

Order matters, and we may choose the same digit multiple times. How many PINs are there?

In each of 4 selections, we have 10 choices, hence

$$\text{total} = 10 \cdot 10 \cdot 10 \cdot 10 = 10^4 = 10,000 \text{ possibilities}$$

Theorem. In general, the number of selections of r elements from a set containing n elements, where order matters and repetition is allowed is

$$T(n, r) = n^r$$

Order matter, Repetitions disallowed

Example 11.2.2

If there are 7 runners in race, in how many ways can First, Second, and Third place be awarded?

There are 7 runners which can possibly come first. This runner is removed from the pool, hence there are 6 possible runners who can come second. That runner is removed from the pool, and finally, there are 5 possible runners who can come third.

$$\text{total} = 7 \cdot 6 \cdot 5 = 210 \text{ possible podiums}$$

Definition (r -permutation). Let n and r be nonnegative integers, with $r \leq n$. An r -permutation of a set is an ordered selection of r elements taken from the set of n elements. The total number of possible r -permutations is denoted $P(n, r)$.

So, in the previous example, we calculated $P(7, 3)$.

Theorem 11.2.1 $P(n, r)$

If $n, r \in \mathbb{Z}$ and $1 \leq r \leq n$, then

$$P(n, r) = n(n-1)(n-2) \dots (n-r+1) = \frac{n!}{(n-r)!}$$

Order does not matter, Repetitions disallowed

Example 11.2.3

In how many ways can we select a 5 student committee from a class of 15 students?

If order mattered, we would count

$$P(15, 5) = \frac{15!}{10!} = 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 = 360,360$$

However, order does matter, and we've overcounted. Because committee $ABCDE$ is the same as committee $ECDBA$. In fact each set of 5 students has been overcounted $5! = 120$ times, one for each ordering. So

the actual number of committees we could form is

$$\frac{P(15, 5)}{5!} = \frac{15!}{5!10!} = \frac{360.360}{120} = 3.003$$

Overcounting is generally fine, as long as we keep track by how much we've overcounted, to find the true answer in the end.

Definition (r -combination). Let n, r be nonnegative integers, with $r \leq n$. An r -combination of a set of n elements is a subset of r of the n elements. The total number of r -combinations of a set can be denoted $C(n, r)$, which is consistent with the permutation's notation, however $\binom{n}{r}$ is more common and is read “ n choose r .”

Theorem 11.2.2 $\binom{n}{r}$

If $n, r \in \mathbb{Z}$ with $0 \leq r \leq n$ then

$$\binom{n}{r} = \frac{P(n, r)}{r!} = \frac{n!}{r!(n-r)!}$$

Order does not matter, Repetition is allowed

Example 11.2.4

Suppose a store has 4 large buckets of each with a different type of candy: red, yellow, blue, and pink. If you select a total of 7 candies, how many different choices are possible?

Select 7 elements from $\{r, b, y, p\}$ (repetition is allowed) and order doesn't matter, for example *rrbbyp* is the same as *rbrbpyp*.

The answer is 120

We will not give a generalised solution to this problem in this class.

I however did some research, and found that this is known in combinatorics as “combinations with repetitions” or multisets. The formula is

$$\binom{n+r-1}{r} = \binom{n+r-1}{n-1} = \frac{(n+r-1)!}{r!(n-1)!}$$

and can be read “ n multichoose r .” This type of problem typically requires a bit more background in combinatorial reasoning. A further combinatorics course will certainly cover this topic.

Permutations of Typed objects

Example 11.2.5

How many permutations of the letters “AAAFLL” are there?

Method 1: There are 7 possible positions. We can place the *A*s in 3 of the 7 positions, the *F*s in 2 of the remaining 4 positions, and the 2 *L*s in the remaining 2 positions.

$$\binom{7}{3} \cdot \binom{4}{2} \cdot \binom{2}{2} = \frac{7!}{3!4!} \cdot \frac{4!}{2!2!} \cdot \frac{2!}{2!0!} = 35 \cdot 6 \cdot 1 = 210$$

Note that, we could have also placed the *L*s then the *F*s then the *A*s, or any other order. The total comes out the same. Showing this is left as an exercise to the reader.

Method 2: We could treat the letters as distinguishable, for example, $A_1A_2A_3F_1F_2L_1L_2$. Then the total

number of orderings is simply

$$P(7, 7) = \frac{7!}{0!} = 7! = 5.040$$

However, we've now overcounted by some factor. $A_1A_2A_3F_1F_2L_1L_2$ is counted as a different solution as $A_3A_2A_1F_2F_1L_2L_1$. In fact, the A s have been overcounted by a factor of $3!$ (one for each ordering of A s). Similarly, the F s and L s have been overcounted by factors of $2!$. Therefore, we need to divide through by these overcounting factors.

$$\frac{5.040}{3!2!2!} = \frac{5.040}{6 \cdot 2 \cdot 2} = 210$$

Theorem 11.2.3 Numbr Permutations of Typed Elements

Suppose we have n objects of which n_1 is type 1, n_2 is type 2... n_k is type k . The number of distinct permutations of the n objects is

$$\binom{n}{n_1} \cdot \binom{n-n_1}{n_2} \cdot \dots \cdot \binom{n-n_1-n_2-\dots-n_k}{k} = \frac{n!}{n_1!n_2!\dots n_k!}$$

Note that, the LHS of Theorem 11.2.3 corresponds to method 1 Example 11.2.5, whereas the RHS corresponds to method 2.

Chapter 12

Week 12

12.1 Lecture 32

Probability

Example 12.1.1

Let's flip 2 fair coins.

What is the probability that both coins land heads up?

There are 4 possibilities:

$$HH \quad HT \quad TH \quad TT$$

and each outcome is equally likely. Therefore, the probability of HH occurring is 1 in 4, or 25%.

What is the probability of at least one coin landing face up?

The outcomes with at least one T are HT, TH, TT , which is 3 in 4, or 75%.

Definition (Random Process). A process is said to be random if, when it takes place, one outcome from some set of possible outcomes occurs, but it is impossible to predict with certainty which outcome it will be.

Definition (Sample Space). A sample space is the set of all possible outcomes of a random process of an experiment.

For example, in our example above, the sample space was

$$S = \{HH, HT, TH, TT\}.$$

Definition (Event). An event is a subset of the sample space.

In the above example, we examined two events,

$$E_1 = HH, \quad E_2 = HT, TH, TT.$$

Definition 12.1.1: Finite Probability with Uniform Likelihood

If S is a finite sample space in which all outcomes are equally likely to occur, and E is an event in S , then the probability of E , denoted $\mathbb{P}(E)$ is

$$\mathbb{P}(E) = \frac{|E|}{|S|}$$

Theorem 12.1.1 Value of $\mathbb{P}(E)$

For any event E in a finite sample space S , with uniform likelihood across all elements of S is

$$0 \leq \mathbb{P}(E) \leq 1$$

Example 12.1.2

A fair coin is tossed 7 times. The sample space S is the set of all sequences H/T of length 7. $\therefore |S| = 2^7$.

What is the probability that we get exactly 5 heads?

$$|E| = \binom{7}{5} \cdot \binom{2}{2} = 21 \quad \therefore \mathbb{P}(E) = \frac{|E|}{|S|} = \frac{2^7}{21} \approx 0.1641$$

What is the probability that we get at least 5 heads?

The probability of getting at least 5 heads is equal to the probability of getting exactly 7 heads, plus exactly 6 heads plus exactly 5 heads.

$$|E| = \binom{7}{5} \cdot \binom{2}{2} + \binom{7}{6} \cdot \binom{1}{1} + \binom{7}{7} \cdot \binom{0}{0} = 29 \quad \therefore \mathbb{P}(E) = \frac{29}{2^7} \approx 0.2266$$

Example 12.1.3

A standard deck of cards consists of 52 cards, divided among 4 suits (spades, hearts, clubs, diamonds), with 13 cards each (2,3,4,5,6,7,8,9,10,J,Q,K,A).

Suppose 3 cards are drawn at random from a deck. What is the probability that all 3 cards have the same suit?

The sample space is the set of all possible selections of 3 cards from the deck of 52. Order does not matter, but repetition is not allowed.

$$|S| = \binom{52}{3} = 22.100$$

Let E be the set of 3 card selections that are all the same suit. This will consist of 2 tasks: (1) select a suit, (2) select 3 cards from it.

$$|E| = \binom{4}{1} \text{ suits} \cdot \binom{13}{3} \text{ cards} = 4 \cdot 286 = 1.144$$

Therefore the probability of drawing 3 cards of the same suit is

$$\mathbb{P}(E) = \frac{|E|}{|S|} = \frac{1.144}{22.100} \approx 0.0504$$

Example 12.1.4

Suppose there are 23 people in a room. What is the probability that there are at least two people who share a birthday? (Assuming 365 days a year, ignoring leap years.)

The sample space is the set of all possible ordered lists of birthdays for the 23 people.

$$|S| = 365^{23}$$

Let E be the event that at least two people share a birthday. Let E' be the event that all 23 people have different birthdays

$$|E'| = P(365, 23) = \frac{365!}{23!}$$

$$|E| = |S| - |E'|$$

So the probability of E is

$$\mathbb{P}(E) = \frac{|S| - |E'|}{|S|} = 1 - \frac{|E'|}{|S|} \approx 0.5073$$

This is cool! The probability that two people share a birthday in only 23 people is greater than 50%.

Binomial Coefficients

Let $n, r \in \mathbb{Z}$ and $0 \leq r \leq n$. Let S be a set with $|S| = n$.

$$\binom{n}{r} = \frac{\# \text{ of subsets of } S \text{ with exactly } r \text{ elements}}{r!} = \frac{n!}{r!(n-r)!}$$

The result is called a binomial coefficient.

Claim. $\binom{n}{r} = \binom{n}{n-r}$

proof.

$$\binom{n}{n-r} = \frac{n!}{(n-r)!(n-(n-r))!} = \frac{n!}{(n-r)!(r)!} = \frac{n!}{r!(n-r)!} = \binom{n}{r}$$

□

Theorem 12.1.2 Pascal's Formula

Let $n, r \in \mathbb{Z}$ and $l \leq r \leq n$. Then

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$$

Proof. By algebra.

$$\begin{aligned} \binom{n}{r-1} + \binom{n}{r} &= \frac{n!}{(r-1)!(n-r+1)!} + \frac{n!}{r!(n-r)!} \\ &= \frac{n!}{(r-1)!(n-r+1)!} \cdot \frac{r}{r} + \frac{n!}{r!(n-r)!} \cdot \frac{n-r+1}{n-r+1} \\ &= \frac{r \cdot n!}{r!(n-r+1)!} + \frac{n!(n-r+1)}{r!(n-r+1)!} \\ &= \frac{r \cdot n! + n!(n-r+1)}{r!(n-r+1)!} \\ &= \frac{r \cdot n! + n \cdot n! - r \cdot n! + n!}{r!(n-r+1)!} \\ &= \frac{n!(n+1)}{r!(n-r+1)!} \\ &= \frac{(n+1)!}{r!(n+1-r)!} \\ &= \binom{n+1}{r} \end{aligned}$$

□

Proof. By combinatorics.

Let S be a set with cardinality $|S| = n+1$. Then $\binom{n+1}{r}$ is the number of ways of choosing $A \subseteq S$ with $|A| = r$.

Fix a particular $x \in S$. The number of r -subsets of S is the number of that contain x plus the number that do not contain x .

1. The number of subsets $A \subseteq S$ with $|A| = r$ and $x \in A$ is $\binom{n}{r-1}$.
2. The number of subsets $A \subseteq S$ with $|A| = r$ and $x \notin A$ is $\binom{n}{r}$.

Therefore,

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$$

□

Theorem 12.1.3 Binomial Theorem

Given any real numbers a, b and any nonnegative integer n ,

$$\begin{aligned} (a+b)^n &= \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k \\ &= a^n + \binom{n}{1} a^{n-1} b^1 + \binom{n}{2} a^{n-2} b^2 + \cdots + \binom{n}{n-2} a^2 b^{n-2} + \binom{n}{n-1} a^1 b^{n-1} + b^n \end{aligned}$$

Proof. If $n = 0$, we have $(a+b)^0 = 1$ and

$$\sum_{k=0}^0 \binom{0}{k} a^{0-k} b^k = \binom{0}{0} a^0 b^0 = \binom{0}{0} = \frac{0!}{0!(0-0)!} = 1.$$

So the theorem holds for $n = 0$.

For $n \geq 1$ we present a combinatorial proof. Let's consider small n s,

$$\begin{aligned} (a+b)^2 &= (a+b)(a+b) = a^2 + 2ab + b^2 \\ (a+b)^3 &= (a+b)(a+b)(a+b) = a^3 + 3a^2b + 3ab^2 + b^3 \end{aligned}$$

Expanding $(a+b)^k$ gives us the sum of all ordered combinations of n symbols, each of which is a or b . For each $k = 0, 1, 2, \dots, n$,

$$a^{n-k} b^k = \underbrace{a \cdot a \cdot a \cdot \dots \cdot a}_{n-k} \cdot \underbrace{b \cdot b \cdot b \cdot \dots \cdot b}_k$$

occurs exactly $\binom{n}{k}$ times in the expansion of $(a+b)^n$ since there are $\binom{n}{k}$ ways to choose the position of the b s and the a s fill the remaining positions.

$$\therefore (a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$$

□

Example 12.1.5

Expand $(x+y)^4$ using the binomial theorem.

$$\begin{aligned} (x+y)^4 &= \sum_{k=0}^4 \binom{4}{k} x^{4-k} y^k \\ &= \binom{4}{0} x^{4-0} y^0 + \binom{4}{1} x^{4-1} y^1 + \binom{4}{2} x^{4-2} y^2 + \binom{4}{3} x^{4-3} y^3 + \binom{4}{4} x^{4-4} y^4 \\ &= 1x^4y^0 + 4x^3y^1 + 6x^2y^2 + 4x^1y^3 + 1x^0y^4 \end{aligned}$$

$$= a^4 + 4a^3b + 6a^2b^2 + 4a^1b^3 + b^4$$

What is the coefficient of x^5 in the expanded form of $(x - 1)^8$?

$$(x - 1)^8 = \sum_{k=0}^8 \binom{8}{k} x^{n-k} (-1)^k$$

x^5 occurs when $k = 8 - 5 = 3$, so the binomial coefficient is

$$\binom{8}{3} (-1)^3 = 56 \cdot -1 = -56$$

12.2 Lecture 33

The Inclusion-Exclusion Principle

Example 12.2.1

Suppose in a fishtank there are 14 blue fish, 7 striped fish, and 4 fish which are blue *and* striped. How many fish are blue *and* striped?

If we add the blue fish and the striped fish, we get $14 + 7 = 21$. However, we've double counted the blue striped which are included in both groups. To get around this, we subtract the fish which are blue *or* striped, and the actual answer is

$$|\text{blue and striped}| = |\text{blue}| + |\text{striped}| - |\text{blue or striped}| = 14 + 7 - 4 = 17$$

Theorem 12.2.1 The Inclusion-Exclusion Principle for Two Sets

For any two sets, A and B ,

$$|A \cup B| = |A| + |B| - |A \cap B|$$

A special case of the theorem is for two **disjoint** sets A and B , so $|A \cap B| = 0$. Therefore, $|A \cup B| = |A| + |B|$.

Example 12.2.2

Suppose A, B are sets with $|A| = 9$, $|B| = 15$, $|A \cup B| = 19$. What is $|A \cap B|$?

$$|A \cup B| = |A| + |B| - |A \cap B| \iff 19 = 9 + 15 - |A \cap B| \iff |A \cap B| = 9 + 15 - 19 = 24 - 19 = 5$$

Theorem 12.2.2 The Inclusion-Exclusion Principle for Three Sets

For any three sets, A , B , C ,

$$\begin{aligned} |A \cup B \cup C| = & |A| + |B| + |C| \\ & - |A \cap B| - |A \cap C| - |B \cap C| \\ & + |A \cap B \cap C| \end{aligned}$$

Example 12.2.3

100 students are surveyed about the subjects they are taking.

50 students are taking maths
 40 students are taking chemistry
 35 students are taking physics
 18 students are taking maths and chemistry How many students are taking none of the subjects?
 15 students are taking maths and physics
 16 students are taking chemistry and physics
 10 students are taking all 3 subjects

Let M , C , P denote the sets of students only taking maths, chemistry, or physics, respectively.

$$\begin{aligned}
 |M \cup C \cup P| &= |M| + |C| + |P| - |M \cap C| - |M \cap P| - |C \cap P| + |M \cap C \cap P| \\
 &= 50 + 40 + 35 - 18 - 15 - 16 + 10 \\
 &= 86
 \end{aligned}$$

$$\therefore |(M \cup C \cup P)'| = 14$$

So 14 students take none of the subjects maths, chemistry, or physics.

12.3 Lecture 34

Definition 12.3.1: The Pigeonhole Principle

Suppose you have n pigeons sitting in k pigeonholes. If $n > k$, then at least one pigeonhole contains two pigeons.

If a function maps from a finite set to a finite set with smaller cardinality, then it cannot be injective.

The contrapositive of the pigeonhole principle is: If you have n pigeons sitting in k pigeonholes, if each pigeonhole contains at most one pigeon, then $n \leq k$.

If a function is injective, then it maps from a finite set to a set with equal or greater cardinality.

Example 12.3.1

If you have socks of 3 different colours in your drawer, what is the minimum number of socks you need to pull out in order to guarantee a matching pair?

pigeons = socks pigeonholes = colours

Since $\# \text{colors} = 3$, $\# \text{socks} = 4 > 3$.

Suppose there are 680 people in a room. Must there be at least two people with the exact same initials?

pigeons = people pigeonholes = initials

Since $\# \text{initials} = 26 \cdot 26 = 676$ and $680 > 676$, then yes, at least two people share initials.

Suppose $n \in \mathbb{Z}_+$ and $n \geq 3$. Show that in every group of n people there are at least two people who have the same number of friends within the group.

pigeons = people pigeonholes = friends

Let $f : \mathbb{Z}_{\geq 3} \rightarrow \mathbb{Z}_+$ map the i th person, p_i , to the number of friends p_i has. Let $f(p_1) = 1$, $f(p_2) = 2, \dots, f(p_{n-1}) = n - 1$. Now, $f(p_n)$ needs to map to something. All of the integers before it have been mapped to, and $p_n \not\rightarrow n$ because a person cannot be friends with themselves. Therefore, by the pigeonhole principle, at least two people must have the same number of friends.

Theorem 12.3.1 Generalised Pigeonhole Principle

Suppose you have n pigeons sitting in k pigeonholes. If $n > km$, then at least one of the pigeonholes contains at least $m + 1$ pigeons.

The contrapositive form: Suppose you have n pigeons sitting in k pigeonholes. If each pigeonhole contains at most m pigeons then $n \leq km$.

Example 12.3.2

Show that in a group of 25 people, at least 3 people share a birthmonth.

$$n = 25, \quad m = 2, \quad k = 12, \quad n = 25 > 24 = 12 \cdot 2 = k \cdot m$$

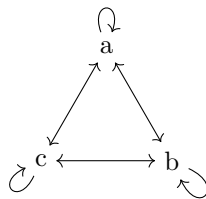
By the generalised pigeonhole principle, at least 3 people share a birthmonth.

Chapter 13

Week 13

13.1 Lecture 35

Introduction to Graph Theory

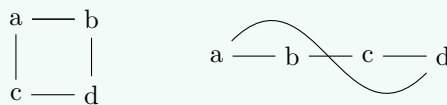


Definition 13.1.1: Graph

A graph, G , consists of two finite sets:

- a nonempty set of vertices, $V(G)$.
- a possibly empty set of edges, $E(G)$, where each edge is associated with a set $\{v, w\} \subseteq V(G)$. The vertices v and w are called the endpoints of the edge.

Example 13.1.1



This graph G has $V(G) = \{a, b, c, d\}$ and $E(G) = \{\{a, b\}, \{b, c\}, \{c, d\}, \{a, d\}\}$.

Note that both these representations are equivalent. How the graph is drawn is irrelevant, what matters is the relationships between vertices and edges.

Definition 13.1.2: Loops, Parallel Edges, Simple Graphs

$$x \begin{array}{c} \xrightarrow{e_1} \\ \xleftarrow{e_2} \end{array} y \xrightarrow{e_3} z \xrightarrow{e_4} z$$

$$V(G) = \{x, y, z\} \quad E(G) = \{e_1, e_2, e_3, e_4\}$$

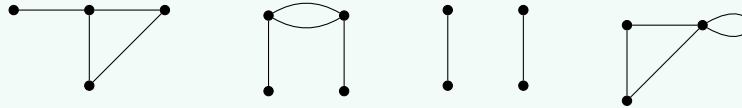
Definition (Loop). A loop is an edge whose endpoints are equal, which is denoted $\{v, v\}$ or $\{v\}$.

Definition (Parallel Edges). Edges are parallel (also called multiple edges) if there is at least one other edge with the same set of endpoints.

Definition (Simple Graph). A simple graph is a graph with no loops or parallel edges.

The example above has a loop, e_4 , has a pair of parallel edges, e_1, e_2 , and is therefore not a simple graph.

Example 13.1.2



From left to right:

1. Simple
2. Not simple (has a loop)
3. Simple
4. Not simple (has a loop)

Definition 13.1.3: Incident, Adjacent, Isolated

Definition (Incident Edges). An edge and a vertex are incident if and only if the vertex is an endpoint of the edge.

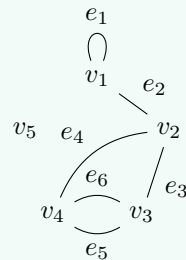
Definition (Adjacent Edges). Two edges are adjacent if and only if they are incident with the same vertex.

Definition (Adjacent Vertices). Two vertices are adjacent if and only if there exists an edge such that both vertices are incident with it (they are connected by an edge).

Definition (Isolated Vertex). An isolated vertex is a vertex which is incident with no edges.

Example 13.1.3

G :



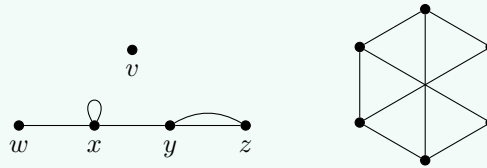
In the example above,

- e_3 is incident with v_2 and v_4 .
- v_1 is incident with e_1 and e_2 .
- e_2 is adjacent to e_3 (v_2 in common).
- v_2 and v_4 are adjacent (e_4 in common).
- v_1 and v_4 are non-adjacent (no edges in common).
- v_5 is isolated (no incident edges).

Definition 13.1.4: Vertex Degree

The degree of a vertex v is the number of edges incident with v , where we count each loop twice. We denote this $\deg(v)$.

Example 13.1.4



With the graph on the left, G ,

- $\deg(v) = 0$
- $\deg(w) = 1$
- $\deg(x) = 4$
- $\deg(y) = 3$
- $\deg(z) = 2$

The degree sum of G is 10, which we note is $2 \cdot 5$, where 5 is interestingly the number of edges.

With the graph on the right, H , each vertex has $\deg(v) = 3$. There are 6 vertices, so the degree sum for H is $3 \cdot 6$. This is also $2 \cdot 9$ and H has 9 edges.

Theorem 13.1.1 The Handshake Theorem

Let G be a graph with n vertices,

$$V(G) = \{v_1, v_2, \dots, v_n\}.$$

Then

$$\sum_{i=1}^n \deg(v_i) = \deg(v_1) + \deg(v_2) + \dots + \deg(v_n) = 2 \cdot |E(G)|.$$

proof. Let G be a graph with n vertices and $n \geq 1$ and $V(G) = \{v_1, v_2, \dots, v_n\}$.

First, the degree sum can be counted by counting the degree of each vertex individually, then summing them, $\sum_{i=1}^n \deg(v_i)$.

Second, let e be any edge of G with endpoints $\{v_i, v_j\}$. Then, e contributes 1 to the degree of v_i and 1 to the degree of v_j . If $v_i = v_j$, then it still contributes 1 to v_i and 1 to v_j (which essentially means loops contribute 2 to a vertex). Hence, the degree sum is $2|E(G)|$.

$\therefore \sum_{i=1}^n \deg(v_i) = 2|E(G)|$. □

Corollary 13.1.1

In any graph, there is an even number of vertices with odd degree.

Walks, Trails, and Circuits

Definition 13.1.5: Walk

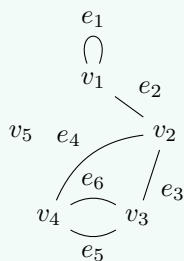
Let G be a graph, and let v, w be vertices of G . A walk from v to w is a finite alternating sequence

$$v_0 e_1 v_1 e_2 \dots v_{n-1} e_n v_n$$

where $v_0 = v$ and $v_n = w$ and e_i is an edge with endpoints $\{v_{i-1}, v_i\}$, for $i \in \{1, 2, \dots, n\}$.

Example 13.1.5

G :



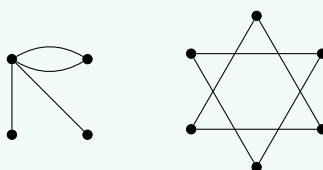
A path from v_4 to v_3 could be $v_4 e_4 v_2 e_2 v_1 e_1 v_1 e_2 v_2 e_3 v_3$.

Another path could be $v_4 e_6 v_3$.

Definition 13.1.6: Connected Graph

A graph is connected if, given any two vertices, v and w in G , there exists a walk from v to w .

Example 13.1.6



The graph on the left is connected.

The graph on the right is not connected.

Definition 13.1.7: Trail and Circuit

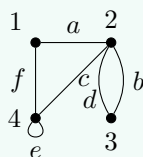
A trail is a walk whose edges are distinct.

A circuit is a trail that starts and ends at the same vertex.

Definition 13.1.8: Euler Circuit

Let G be a graph. An Euler circuit for G is a circuit which uses every edge of G exactly once.

Example 13.1.7



$3d2c4e4f1a2b3$ is an Euler circuit.

Lemma 13.1.1

If a graph G has an Euler circuit, then each of its vertices has even degree.

Proof. Let G be a graph with an Euler circuit. Let $v \in V(G)$ be any vertex. We consider cases depending on whether or not v is the start/end point of the Euler circuit.

If v is not the start/end point, then each time the Euler circuit visits v , it comes along one edge, and out along another. Each pass contributes 2 to the degree of the vertex. Hence $\deg(v) = 2k$, $k \in \mathbb{Z}_+$.

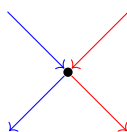
If v is the start/end point, then the Euler circuit starts by exiting the vertex, contributing 1 to its degree. Then the circuit may pass through the vertex many times, but each time it enters, it leaves, contributing 2 to the degree for each pass through. Finally, the Euler circuit concludes at v , contributing another 1 to the degree. Hence, $\deg(v) = 1 + 2k + 1 = 2 + 2k = 2(k + 1)$, $k \in \mathbb{Z}_+$.

Therefore, if G has an Euler circuit, then each of its vertices has even degree. \square

Theorem 13.1.2 Euler Circuit

Let G be a connected graph. Then, G has an Euler circuit if and only if every vertex of G has even degree.

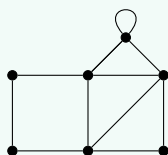
To find an Euler circuit, we can find any circuit in a graph, remove the circuit's edges, and then remove any isolated vertices. We can keep decomposing the graph in this way, until we find a trivial Euler circuit (a single vertex). Then we can “splice” together these decompositions, by

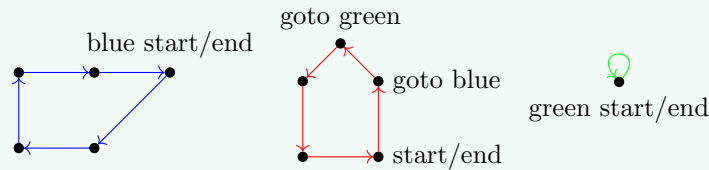


entering a vertex which the two decomposed circuits have in common and exiting using the other circuit. In the example above, the blue and red edges represent different decomposed circuits. To create an Euler circuit, we can enter with the blue, exit with the red, complete the red circuit, re-enter with the red, and exit with the blue, finally complete the blue circuit which can potentially complete an Euler circuit.

Example 13.1.8

Decompose this graph, and find an Euler circuit.





I've decomposed the graph, and used the decomposition to find an Euler circuit, as required.

Definition 13.1.9: Euler Trail

Let G be a graph and let $u, v \in V(G)$. An Euler trail is a trail from u to v that uses every edge exactly once.

Theorem 13.1.3 Euler Trail

Let G be a connected graph and let $u, v \in V(G)$.

If $u = v$, then G has an Euler trail from u to v if and only if every vertex of G has even degree.

If $u \neq v$, then G has an Euler trail from u to v if and only if u, v have odd degree and all other vertices have even degree.

13.2 Lecture 36

Matrix Representations of Graphs

Definition ($m \times n$ -matrix). An m -by- n matrix over a set S is a rectangular array of elements of S arranged into m rows and n columns.

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1j} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2j} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots & \dots & \vdots \\ a_{i1} & a_{i2} & \dots & a_{ij} & \dots & a_{in} \\ \vdots & \vdots & \ddots & \vdots & \dots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mj} & \dots & a_{mn} \end{pmatrix}$$

We write $A = [a_{ij}]$ or $A = [a_{ij}]_{m \times n}$. The symbol a_{ij} denotes the entry in row i , column j . For our purposes, $S = \mathbb{Z}_{\geq 0}$.

Definition 13.2.1: Adjacency Matrix

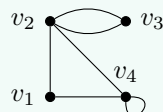
Let G be a graph with n vertices and suppose we label the vertices $V(G) = \{v_1, v_2, \dots, v_n\}$.

The adjacency matrix of G is the $n \times n$, $A = [a_{ij}]$, where a_{ij} is the number of edges with the endpoints $\{v_i, v_j\}$. ie,

$$a_{ij} = \begin{cases} r & \text{if } \exists r \text{ edges connecting } v_i \text{ and } v_j \\ 0 & \text{otherwise} \end{cases}$$

Example 13.2.1

Write the adjacency matrix for the following graph:



$$A = \begin{matrix} & \begin{matrix} v_1 & v_2 & v_3 & v_4 \end{matrix} \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{matrix} & \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 2 & 1 \\ 0 & 2 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} \end{matrix}$$

Note:-

For an adjacency matrix $A = [a_{ij}]$, $a_{ij} = a_{ji}$, $\forall i, j \in \{1, 2, \dots, n\}$.

Definition 13.2.2: Incidence Matrix

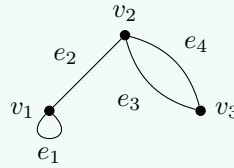
Let G be a graph with n vertices and m edges, and suppose we label the vertices $V(G) = \{v_1, v_2, \dots, v_n\}$ and label the edges $E(G) = \{e_1, e_2, \dots, e_m\}$.

The incidence matrix for the graph G is the $n \times m$ matrix $N = [n_{ij}]$ where each entry n_{ij} is the number of times vertex v_i is incident with e_j . ie,

$$n_{ij} = \begin{cases} 2 & \text{if } e_j \text{ is a loop on vertex } v_i \\ 1 & \text{if } e_j \text{ is an edge connecting } v_i \text{ to some other vertex} \\ 0 & \text{otherwise} \end{cases}$$

Example 13.2.2

Write the incidence matrix for the following graph:



$$A = \begin{matrix} & \begin{matrix} e_1 & e_2 & e_3 & e_4 \end{matrix} \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \end{matrix} & \begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \end{matrix}$$

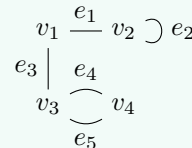
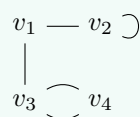
Note:-

For every adjacency matrix, every column will contain two 1s or one 2. The sum of each row is the degree of the corresponding vertex.

Example 13.2.3

Draw the graphs corresponding to the following matrices:

$$A(G) = \begin{matrix} & \begin{matrix} v_1 & v_2 & v_3 & v_4 \end{matrix} \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{matrix} & \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 2 \\ 0 & 0 & 2 & 0 \end{pmatrix} \end{matrix} \quad N(H) = \begin{matrix} & \begin{matrix} e_1 & e_2 & e_3 & e_4 & e_5 \end{matrix} \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{matrix} & \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \end{matrix}$$



Trees

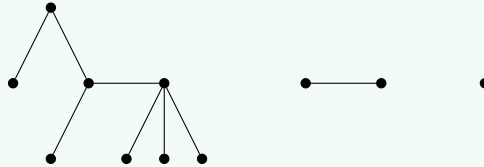
Definition 13.2.3: Tree

Definition (Circuit-Free Graph). A graph is circuit-free if and only if it has no nontrivial circuits.

A graph is a tree if and only if it is connected and circuit-free.

Since loops and multiple edges are nontrivial circuits, trees are simple graphs.

Example 13.2.4



All three of these are examples of trees.

Theorem 13.2.1 Trees are...

A graph, G with n vertices, is a tree if and only if G is simple, connected, and has $n - 1$ edges.