Lecture notes on discrete structures

Benjamin J. Clark

Fall 2024

Contents

Chapter 1

Speaking mathematically

Key chapter concepts

1. Identify and write the three major types of mathematical statements.
2. Recognize and use basic set notation.
3. Understand what a relation and function are.
4. Know the definition of a graph and some of the associated jargon.

1.1 Variables

This section covers the basics of translating statements into mathematical statements with the use of variables. Next, it covers the three basics types of mathematical statements; universal, existential, and conditional.

- A universal statement covers conditions or properties that all elements in some space contain.
- A existential statement says that at least one element from some set contains a certain property or condition.
- A conditional statement says that if some elements satisfy a condition, then they also have another property or condition.

Note that these statements are often mixed. For example, you could have a universal statement that is also conditional.

Example 1.1.1. Below are some example sentences, try and convert them to using variables, then state what type of mathematical statement they are. Note, none is an option.

1. Are there two numbers such that doubling their product and adding two is equal to their sum of the second one squared?

   Are there numbers x, y such that $2xy + 2 = y + x^2$?

   Given x, y, can $2xy + 2 = x + y^2$?

   Does there exist numbers x, y such that $2xy + 2 = x + y^2$?

   The first sentence, is a question, which means it does not fall under one of the mathematical statements.

2. For every nonnegative number greater than 3 squaring it is greater than 9.

   For every $x > 3$, $x^2 > 9$.

   The second, is a universal and conditional statement. It contains the for every phrase, making it universal, but then it also has the conditional of the number chosen being larger than 3.

3. If a number is negative, then the cube of it is still negative.

   If $x < 0$, then $x^3 < 0$.

   The third, is a conditional statement. It follows the common if-then structure.

4. There exists a number such that it is equal to its square.

   There exists a number, x, such that $x = x^2$.

   The fourth, is an existential statement. It contains a there exists phrase.

△

1.2 The Language of sets

Definition 1.2.1. A set is defined as a collection of elements. These elements can be (almost) anything, including other sets. There is no implicit order to the elements of a set, and duplicates are ignored.

If you are curious about the almost in the definition, look in to Zermelo–Fraenkel set theory and Russell's paradoxes.

Sets have several important notational pieces to them. The $\in$ symbol is used to denote an element being an element in a set. For example, $x \in S$ which is read "x is an element of the set S" or "x is in S". The notational other piece, is the use of curly brackets, $\{\}$ which is how sets are defined and built.

Definition 1.2.2. One way to build sets is with **set-roster notation**, which is where we list all elements of the set or list the first few once the pattern is clear to the reader. For example, $\{1, 2, 3\}$ and $\{1, 2, 3, \dots\}$.

Another way to build sets is with **set-builder notation**, which is written as $\{x \in S \mid P(x)\}$ this is read as "x in S such that $P(x)$ is true" where $P(x)$ is some

property of the statement that x must satisfy. For example, $\{x \in \mathbb{R} \mid x \geq 3\}$ which is the set of all real numbers that are greater than or equal to 3. Note that instead of the $\mid$ it is also common to use, : this can be especially helpful in situations involving absolute values like $\{x \in \mathbb{R} : |x| < 1\}$.

The most common sets when working with numbers are $\mathbb{N}$ the natural numbers, $\mathbb{Z}$ the integers, $\mathbb{Q}$ the rational numbers, and $\mathbb{R}$ the real numbers. The book will exclude using $\mathbb{N}$ because it has two definitions that are used about the same, which are the nonnegative integers and the positive integers. The integers are the whole numbers, including negatives. We will use $\mathbb{Z}^+$ for the positive integers and $\mathbb{Z}^{\geq 0}$ for the nonnegative integers.

When working with sets, we often care about the idea of a **subset**, which is defined as a set that contained in another set and is denoted $A \subseteq B$. If this containment is strict, that is B contains more elements then A, we write $A \subset B$ and this is called a **proper subset**.

Two sets are called equal if and only if they contain all the same elements.

Definition 1.2.3. Given elements a, b, the symbol (a, b) denotes the **ordered pair** made from a and b with the added information that a is first and b is second.

Two ordered pairs are equal if and only if their first and second components are the same. That is, for $(a, b) = (c, d)$ we need $a = c$ and $b = d$.

The above definition can be extended to arbitrary dimension.

Definition 1.2.4. Let n be a positive integer and let $x_1, \ldots, x_n$ be elements. The **ordered n-tuple**, $(x_1, \ldots, x_n)$, consists of the above elements with the ordering that x_1 comes before x_2 and so on.

We can apply this idea of ordered pairs to construct a multiplication like operation for sets.

Definition 1.2.5. Given sets $A_1, A_2, \ldots, A_n$ the Cartesian product of $A_1, \ldots, A_n$ denoted $A_1 \times A_2 \times \cdots \times A_n$, is the set of all ordered tuples $(a_1, \ldots, a_n)$ where $a_1 \in A_1$ and so on. Symbolically, we can write this as

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

A final object about sets that is important to both mathematics and computer science are Strings.

Definition 1.2.6. Let n be a positive integer, then given a set A, a **string** is an ordered tuple of elements of A written without parentheses or commas. The elements in the string are called **characters** of the string. The **null string** is the string of no characters.

The length of a string is the number of characters in that string, the null string is defined to have length 0.

Exercises

1. Use variables to rewrite the sentence:

   Given any two distinct real numbers, there is a real number between them.

2. Rewrite the following sentence less formally, without variables. Determine if the sentence is true or false:

   There is a real number x such that $x^2 < x$.

3. Answer each of the following questions. Give reasons for your answers.

   (a) Is $3 \in \{1, 2, 3\}$?
   (b) Is $\{3\} \in \{1, 2, 3\}$?
   (c) Is $1 \subseteq \{1\}$?
   (d) Is $1 \in \{\{1\}, 2\}$?
   (e) Is $\{1\} \subseteq \{1\}$?

4. Which of the following sets are equal?

   (a) $A = \{0, 1, 2\}$
   (b) $B = \{x \in \mathbb{R} \mid -1 \leq x < 3\}$
   (c) $C = \{x \in \mathbb{R} \mid -1 < x < 3\}$
   (d) $D = \{x \in \mathbb{Z} \mid -1 < x < 3\}$
   (e) $E = \{x \in \mathbb{Z}^+ \mid -1 < x < 3\}$

Solutions

1. Use variables to rewrite the sentence:

   Given any two distinct real numbers, there is a real number between them.

   Given $x, y \in \mathbb{R}$, there exists $z \in \mathbb{R}$ such that $x < z < y$ or $x > z > y$.

2. Rewrite the following sentence less formally, without variables. Determine if the sentence is true or false:

   There is a real number x such that $x^2 < x$.

   There is a real number whose square is less than itself.

3. Answer each of the following questions. Give reasons for your answers.

(a) Is $3 \in \{1, 2, 3\}$? Yes, 3 is an element of the set.

(b) Is $\{3\} \in \{1, 2, 3\}$? No, the set containing 3 is not an element of the set.

(c) Is $1 \subseteq \{1\}$? No, 1 is not a set, so can't be a subset.

(d) Is $1 \in \{\{1\}, 2\}$? No, 1 is not an element of the set. The element $\{1\}$ is.

(e) Is $\{1\} \subseteq \{1\}$? Yes, a set is always a subset of itself.

4. Which of the following sets are equal?

(a) $A = \{0, 1, 2\}$

(b) $B = \{x \in \mathbb{R} \mid -1 \leq x < 3\}$

(c) $C = \{x \in \mathbb{R} \mid -1 < x < 3\}$

(d) $D = \{x \in \mathbb{Z} \mid -1 < x < 3\}$

(e) $E = \{x \in \mathbb{Z}^+ \mid -1 < x < 3\}$

The sets A, and D are equal. The sets B, C, and E are distinct from each other and the rest.

1.3 The Language of relations and functions

Definition 1.3.1. Let A and B be sets. A **relation** R **from** A **to** B is a subset of $A \times B$. Given an ordered pair (x, y) in $A \times B$, x **is related to** y **by** R, written xRy, if and only if $(x, y) \in R$. The set A is called the **domain** of R and the set B is called the **co-domain** of R.

The notation for a relation may be written as xRy or $(x, y) \in R$. The notation for two elements not being related is $x \not R y$ or $(x, y) \notin R$.

Definition 1.3.2. A **function** F **from a set** A **to a set** B is a relation with domain A and co-domain B that satisfies the following two properties:

1. For every element $x \in A$, there is an element $y \in B$ such that $(x, y) \in F$.
2. For all elements $x \in A$ and $y \in B$, if $(x, y) \in F$ and $(x, z) \in F$ then $y = z$.

For functions, we frequently use the notation $F(x)$ where $x \in A$ and $F(x) \in B$.

Example 1.3.3. Define a relation C from $\mathbb{R}$ to $\mathbb{R}$ as follows: For any $(x, y) \in \mathbb{R} \times \mathbb{R}$, $(x, y) \in C$ means that $x^2 + y^2 = 1$.

1. Is $(1, 0) \in C$? Yes, $1^2 + 0^2 = 1$
2. Is $(0, 0) \in C$? No, $0^2 + 0^2 \neq 1$
3. What are the domain and co-domain of C?

   The domain and co-domain are both $\mathbb{R}$.

4. Does C satisfy the requirements of being a function?

   No, consider $x = 0$, then y could be either 1 or -1. This breaks property two of being a function.

△

1.4 The Language of graphs

Definition 1.4.1. A **graph** G consists of two finite sets: a nonempty set V of **vertices** and a set E of **edges**. An edge is a set containing one or two vertices called **endpoints**.

An edge with just one endpoint is called a **loop**, and two or more distinct edges with the same set of endpoints are said to be **parallel**. Two vertices connected by an edge are called **adjacent**.

An edge is said to be **incident** on its endpoints. Similar to vertices, two edges sharing a vertex are called adjacent. A vertex with no edges is called **isolated**.

Definition 1.4.2. A **directed graph**, or digraph, consists of two finite sets: a nonempty set V of vertices and a set D of directed edges, where each edge is associated with an ordered pair of vertices.

Definition 1.4.3. Let G be a graph and v a vertex of G. The **degree of** v, denoted $\deg(v)$, equals the number of edges that are incident on v, with an edge that is a loop counted twice.

Exercises

1. Let $A = \{2, 3, 4\}$ and $B = \{6, 8, 10\}$ and define a relation R from A to B as follows: For every $(x, y) \in A \times B$, $(x, y) \in R$ means that y/x is an integer. Symbolically, we can write this as

$$R = \left\{(x, y) \in A \times B \mid \frac{y}{x} \in \mathbb{Z}\right\}.$$

   (a) Is $4R6$? Is $4R8$? Is $(3, 8) \in R$?

   (b) Write R as a set of ordered pairs.

   (c) Write the domain and co-domain of R.

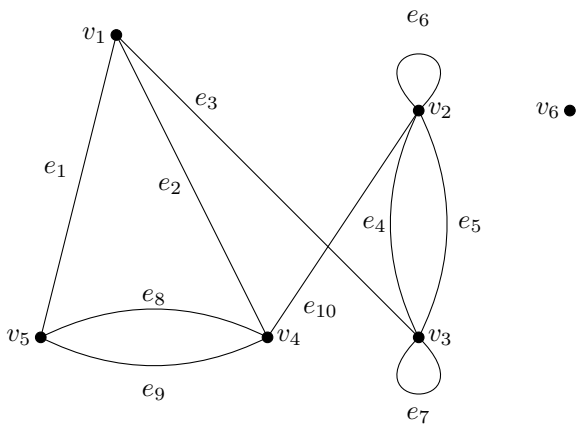
   (d) Draw an arrow diagram for R.

2. For the following graph

   (a) Find all edges that are incident on v_1.

   (b) Find all vertices that are adjacent to v_3.

   (c) Find all loops.



(d) Find all parallel edges.

(e) Find all isolated vertices.

(f) Find the degree of v_3.

3. Draw the graph, G, which has a vertex set $\{v_1, v_2, v_3, v_4, v_5\}$ and an edge set $\{e_1, e_2, e_3, e_4, e_5, e_6\}$ where the edge-endpoint functions are

$$\begin{aligned} e_1 &= \{v_1, v_2\} \\ e_2 &= \{v_1, v_2\} \\ e_3 &= \{v_3\} \\ e_4 &= \{v_1, v_4\} \\ e_5 &= \{v_4, v_5\} \\ e_6 &= \{v_2, v_4\} \end{aligned}$$

Solutions

1. Let $A = \{2, 3, 4\}$ and $B = \{6, 8, 10\}$ and define a relation R from A to B as follows: For every $(x, y) \in A \times B$, $(x, y) \in R$ means that y/x is an integer. Symbolically, we can write this as

$$R = \left\{(x, y) \in A \times B \mid \frac{y}{x} \in \mathbb{Z}\right\}.$$

(a) Is $4R6$? Is $4R8$? Is $(3, 8) \in R$?

No, $(4, 6) \notin R$ since $3/2$ is not an integer. Yes, $(4, 8) \in R$ since $8/4 = 2$ is an integer. No, $(3, 8) \notin R$ since $8/3$ is not an integer.

(b) Write R as a set of ordered pairs.

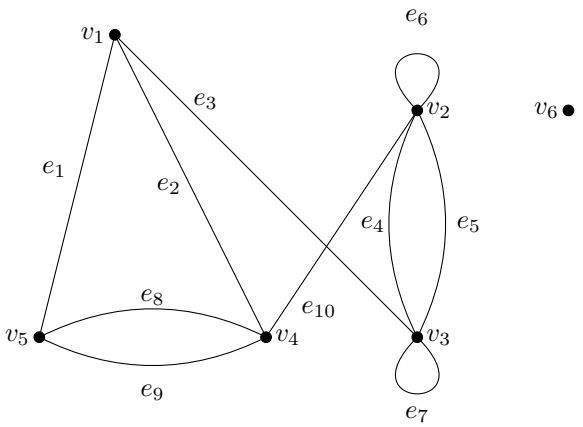
$$R = \{(2, 6), (2, 8), (2, 10), (3, 6), (4, 8)\}$$

(c) Write the domain and co-domain of R.

The domain is, A while the co-domain is B.

(d) Draw an arrow diagram for R.

2. For the following graph



(a) Find all edges that are incident on v_1.

Incident edges to v_1 are all edges connected to v_1, which are e_1, e_2, e_3.

(b) Find all vertices that are adjacent to v_3.

Adjacent vertices are vertices connected by an edge. For v_3 the adjacent vertices are v_1, v_2, v_3.

(c) Find all loops.

Loops are edges that connect a vertex to itself. Here edges e_6 and e_7 do that.

(d) Find all parallel edges.

Parallel edges are edges that share the same endpoints. In this case, e_8 and e_9 are parallel and e_4 and e_5 are parallel.

(e) Find all isolated vertices.

An isolated vertex is a vertex which is not connected to any other vertex. In this case v_6 is isolated.

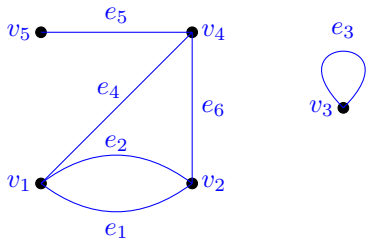
(f) Find the degree of v_3.

The degree of a vertex is the number of edges connecting to it, note that loops count double. The degree of v_3 is 5.

3. Draw the graph, G, which has a vertex set $\{v_1, v_2, v_3, v_4, v_5\}$ and an edge

set $\{e_1, e_2, e_3, e_4, e_5, e_6\}$ where the edge-endpoint functions are

$$\begin{aligned} e_1 &= \{v_1, v_2\} \\ e_2 &= \{v_1, v_2\} \\ e_3 &= \{v_3\} \\ e_4 &= \{v_1, v_4\} \\ e_5 &= \{v_4, v_5\} \\ e_6 &= \{v_2, v_4\} \end{aligned}$$



Chapter 2

Logic of statements

2.1 Logical form and logical equivalence

Definition 2.1.1. A **statement** (or **proposition**) is a sentence that is true or false, but not both.

As examples, "The sky is red right now" and "The sky is blue right now" are both statements. Given clear definitions about how to test the sky for color, we could determine the truth values of those statements. Whereas "$x - 2 \leq 0$" is not a statement since it depends on the value of x.

Notation 2.1.2. Define the logical operator $\vee$ for a logical or, $\wedge$ for a logical and, and $\sim$ for a logical not.

Given logical statements p and q we could say $p \vee q$ to represent p or q.

Definition 2.1.3. If p is a statement variable, the **negation** of p is "not p". The negation of p is denoted $\sim p$ and has the opposite truth value.

Definition 2.1.4. If p and q are statement variables, the **conjunction** of p and q is "p and q", denoted $p \wedge q$. It is true when p and q are both true and false otherwise.

Definition 2.1.5. If p and q are statement variables, the **disjunction** of p and q is "p or q", denoted $p \vee q$. It is true when either p is true, q is true, or both p and q are true. It is false only when both p and q are false.

Too common additional logical phrases are "p but q" and "neither p nor q". The first is equivalent to "p and q" and the second equivalent to "$\sim p$ and $\sim q$"

Definition 2.1.6. A **statement form** is an expression made up of statement variables and logical connectives that become a statement when actual statements are substituted for the component statement variables. The **truth table** for a given statement form displays the truth values that correspond to all possible combinations of true values for its component statement variables.

p	$\sim p$
T	F
F	T

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

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

The truth tables for the three main logical connectives are given below.

Definition 2.1.7. Two statements forms are called **logically equivalent** if and only if they have identical truth values for each possible substitution of statements for their statement variables. For statement forms P and Q this is denoted $P \equiv Q$.

To check whether two statement forms are logically equivalent, one way is to use their truth tables. If the two statement forms have the same outputted truth table they are logically equivalent.

Definition 2.1.8. De Morgan's laws of logic are

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

Definition 2.1.9. A **tautology** is a statement form that is always true. A **contradiction** is a statement form that is always false.

See list of Logical equivalences from book Theorem 2.1.1

Exercises

1. Write the following statements in symbolic form using $h =$ "Alex is healthy", $w =$ "Alex is wealthy", and $s =$ "Alex is wise."
   (a) Alex is healthy and wealthy, but not wise.
   (b) Alex is neither wealthy nor wise, but they are healthy.
   (c) Alex is wealthy, but they are not both healthy and wise.
2. Use De Morgan's laws to write negations for the statement

   Sam is an orange belt and Kate is a red belt.
3. Determine if the following statements are tautologies or contradictions.
   (a) $(p \wedge q) \vee (\sim p \vee (p \wedge \sim q))$.
   (b) $(\sim p \vee q) \vee (p \wedge \sim q)$.
4. Use Theorem 2.1.1 to verify the following logical equivalence.

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

Solutions

1. Write the following statements in symbolic form using $h =$ "Alex is healthy", $w =$ "Alex is wealthy", and $s =$ "Alex is wise."

   (a) Alex is healthy and wealthy, but not wise.
   $h \wedge w \wedge \sim s$

   (b) Alex is neither wealthy nor wise, but they are healthy.
   $\sim w \wedge \sim s \wedge h$

   (c) Alex is wealthy, but they are not both healthy and wise.
   $w \wedge \sim (h \wedge s) \equiv w \wedge (\sim h \vee \sim s)$

2. Use De Morgan's laws to write negations for the statement

   Sam is an orange belt and Kate is a red belt.

   Sam is not an orange belt or Kate is not a red belt.

3. Determine if the following statements are tautologies or contradictions.

   (a) $(p \wedge q) \vee (\sim p \vee (p \wedge \sim q))$.

$$
\begin{aligned}
(p \wedge q) \vee (\sim p \vee (p \wedge \sim q)) &\equiv (p \wedge q) \vee ((\sim p \vee p) \wedge (\sim p \vee \sim q)) && \text{(Distributive law)} \\
&\equiv (p \wedge q) \vee (\mathbf{t} \wedge (\sim p \vee \sim q)) && \text{(Negation law)} \\
&\equiv (p \wedge q) \vee \sim p \vee \sim q && \text{(Identity law)} \\
&\equiv ((p \vee \sim p) \wedge (q \vee \sim p)) \vee \sim q && \text{(Distributive law)} \\
&\equiv (\mathbf{t} \wedge (q \vee \sim p)) \vee \sim q && \text{(Negation law)} \\
&\equiv q \vee \sim p \vee \sim q && \text{(Identity law)} \\
&\equiv \mathbf{t} \vee \sim p && \text{(Negation law)} \\
&\equiv \mathbf{t}. && \text{(Identity law)}
\end{aligned}
$$

   (b) $(\sim p \vee q) \vee (p \wedge \sim q)$.

p	q	$(\sim p \vee q) \vee (p \wedge \sim q)$
T	T	T
T	F	T
F	T	T
F	F	T

   This is a tautology.

4. Use Theorem 2.1.1 to verify the following logical equivalence.

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

$$\begin{aligned}
(p \wedge (\sim (\sim p \vee q))) \vee (p \wedge q) &\equiv (p \wedge p \wedge \sim q) \vee (p \wedge q) && \text{(De Morgan's law)} \\
&\equiv (p \wedge \sim q) \vee (p \wedge q) && \text{(Idempotent law)} \\
&\equiv p \vee (\sim q \wedge q) && \text{(Distributive law)} \\
&\equiv p \vee \mathbf{c} && \text{(Negation law)} \\
&\equiv p. && \text{(Identity law)}
\end{aligned}$$

2.2 Conditional statements

Definition 2.2.1. If p and q are statement variables, the **conditional** of q by p is "If p then q" or "p implies q" and is denoted $p \to q$. It is false when p is true and q is false; otherwise it is true. We call p the **hypothesis** of the conditional and q the **conclusion**.

For order of operations $\to$ is last.

A statement which is true because the hypothesis is false is called **vacuously true**.

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

The statement $p \to q \equiv \sim p \vee q$. This means that the negation of $p \to q$ is $p \wedge \sim q$.

Definition 2.2.2. The **contrapositive** of a conditional statement of the form "If p then q" is

If $\sim q$ then $\sim p$.

A conditional statement is logically equivalent to its contrapositive, this can be seen in the following truth table.

Definition 2.2.3. For a conditional statement $p \to q$, the **converse** is $q \to p$ and the **inverse** is $\sim p \to \sim q$.

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

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

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

As we can see in the above truth tables, the converse and inverse are equivalent. Also note that the negation of a conditional statement is not equal to the converse or inverse.

Definition 2.2.4. Given statement variables p and q, the **biconditional** of p and q is "p if and only if q", it is denoted $p \leftrightarrow q$ or p iff q. This statement is true if p and q have matching truth values and false otherwise.

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

Definition 2.2.5. If p and q are statements then

- p is a **sufficient condition** for q means that $p \rightarrow q$.
- p is a **necessary condition** for q means that $q \rightarrow p$.

Saying that two statements, p and q, are necessary and sufficient is the same as saying that p if and only if q.

Exercises

1. Construct truth tables for the following statements
   (a) $\sim p \vee q \rightarrow \sim q$
   (b) $(p \rightarrow (q \rightarrow r)) \leftrightarrow ((p \wedge q) \rightarrow r)$
2. Show that $p \rightarrow q \vee r$ and $p \wedge \sim q \rightarrow r$ are equivalent.
3. Suppose that p and q are statements such that $p \rightarrow q$ is false. Find the truth value of $\sim p \rightarrow q$ and $p \vee q$.

Solutions

1. Construct truth tables for the following statements

   (a) $\sim p \vee q \rightarrow \sim q$

   (b) $(p \rightarrow (q \rightarrow r)) \leftrightarrow ((p \wedge q) \rightarrow r)$

2. Show that $p \rightarrow q \vee r$ and $p \wedge \sim q \rightarrow r$ are equivalent.

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

3. Suppose that p and q are statements such that $p \rightarrow q$ is false. Find the truth value of $\sim p \rightarrow q$ and $p \vee q$.

2.3 Valid and invalid arguments

Definition 2.3.1. An **argument** is a sequence of statements, and an **argument form** is a sequence of statement forms. The last statement is called the **conclusion**, and the other statements are called **premises**.

An argument form is called **valid** if its conclusion is true whenever its premises are all true.

An argument is valid if its form is valid.

Testing an argument form for validity

1. Identify the premises and conclusion of the argument form.

2. Construct a truth table showing the truth values of all the premises and the conclusion.

3. A row of the truth table in which all the premises are true is called a **critical row**. If there is a critical row in which the conclusion is false, then the argument is false. If every critical row has a true conclusion, then the argument is valid.

The following argument form is called **Modus ponens**

$$\begin{array}{l} \text{If } p \text{ then } q. \\ p \\ \therefore\ q \end{array}$$

The following argument form is called **Modus tollens**

$$\begin{array}{l} \text{If } p \text{ then } q. \\ \sim q \\ \therefore\ \sim p \end{array}$$

With these two forms, there are two major types of invalid arguments, which we will call fallacies. The converse error has the form

$$\begin{array}{ll} & \text{If } p \text{ then } q. \\ & q \\ \therefore & p \end{array}$$

The second type is an inverse error

$$\begin{array}{ll} & \text{If } p \text{ then } q. \\ & \sim p \\ \therefore & \sim q \end{array}$$

Definition 2.3.2. An argument is called **sound** if, and only if, it is valid and all its premises are true. An argument that is not sound is called **unsound**.

Exercises

1. Use modus ponens or modus tollens to fill in the blanks in the argument to produce valid inferences.

   If $\sqrt{2}$ is rational, then $\sqrt{2} = a/b$ for some integers a and b.
   It is not true that $\sqrt{2} = a/b$ for some integers a and b.
   $\therefore$ _____

2. Use truth tables to determine whether the following argument form is valid. Indicate which columns represent the premises and which represent the conclusion, and add a sentence explaining how the truth table supports your answer.

$$\begin{array}{ll} & p \wedge q \rightarrow \sim r \\ & p \vee \sim q \\ & \sim q \rightarrow p \\ \therefore & \sim r. \end{array}$$

3. Use symbols to write the following arguments in logical form. If the argument is valid, identify the rule of inference that gives that. Otherwise, state whether the converse or the inverse error is made.

   If this computer program is correct, then it produces the correct output when run with the test data my teacher gave me.
   This computer program produces the correct output when run with the test data my teacher gave me.
   $\therefore$ This computer program is correct.

Solutions

1. Use modus ponens or modus tollens to fill in the blanks in the argument to produce valid inferences.

   If $\sqrt{2}$ is rational, then $\sqrt{2} = a/b$ for some integers a and b.
   It is not true that $\sqrt{2} = a/b$ for some integers a and b.
   $\therefore$ _____

2. Use truth tables to determine whether the following argument form is valid. Indicate which columns represent the premises and which represent the conclusion, and add a sentence explaining how the truth table supports your answer.

$$\begin{aligned} & p \wedge q \rightarrow \sim r \\ & p \vee \sim q \\ & \sim q \rightarrow p \\ \therefore \quad & \sim r. \end{aligned}$$

3. Use symbols to write the following arguments in logical form. If the argument is valid, identify the rule of inference that gives that. Otherwise, state whether the converse or the inverse error is made.

   If this computer program is correct, then it produces the correct output when run with the test data my teacher gave me.
   This computer program produces the correct output when run with the test data my teacher gave me.
   $\therefore$ This computer program is correct.

Chapter 3

Quantified statements

3.1 Predicates and quantified statements 1

Definition 3.1.1. A **predicate** is a sentence that contains variables. When the variables are specified, a predicate becomes a statement. The **domain** of a predicate is the set of all possibles variable values.

Definition 3.1.2. If $P(x)$ is a predicate and x has domain D, the **truth set** of $P(x)$ is the set of all elements of D that make $P(x)$ true when they are substituted for x. The truth set of $P(x)$ is denoted

$$\{x \in D \mid P(x)\}.$$

The symbol $\forall$ means for all and is called the **universal quantifier**. The symbol $\exists$ means there exists and is called the **existential quantifier**. With these two quantifiers along with predicates, we can revisit the definition of a universal and existential statement.

Let $P(x)$ be a predicate with domain D. A **universal statement** is of the form

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

Which is read "for all x in D, $P(x)$ is true". Any x value in D which causes $P(x)$ to be false, is called a **counterexample**.

An **existential statement** is then of the form

$$\exists x \in D \text{ such that } P(x).$$

Which is read "there exists an x in D such that $P(x)$ is true".

We can always expand a universal or existential statement to include a conditional, for example $\forall x \in D, P(x)$ can be expanded as $\forall x$, if $x \in D$ then $P(x)$.

Let $P(x)$ and $Q(x)$ be predicates, and suppose they have a common domain of D. The notation

- $P(x) \implies Q(x)$ means $\forall x \in D, P(x) \to Q(x)$.
- $P(x) \iff Q(x)$ means $\forall x \in D, P(x) \leftrightarrow Q(x)$.

These double lined arrows give us a convenient shorthand notation for conditional universal statements.

3.2 Predicates and quantified statements 2

This section is focused on negations of quantified statements. The ideas can be summarized in the following theorem.

Theorem 3.2.1. *Let $P(x)$ be a predicate with a domain D, then*

$$\sim (\forall x \in D, P(x)) \equiv \exists x \in D \text{ such that } \sim P(x)$$

and

$$\sim (\exists x \in D \text{ such that } P(x)) \equiv \forall x \in D, \sim P(x).$$

Some things to notice with the above theorem. The negation of a quantifier changes it to the opposite quantifier, i.e. $\sim \forall$ is $\exists$. Also note that the negation of the comma becomes such that. This negation should seem very similar to De Morgan's laws. In a certain view for all is a generalization of "and" while there exists is a generalization of "or".

Exercises

1. Find a counterexample to show that the following statement is false

   $$\forall \text{ positive integers } m \text{ and } n,\ mn \geq m + n.$$

2. Let $\mathbb{R}$ be the domain of the predicate variables a, b, c, d. Which of the following are true and which are false?

   (a) $ab = 0 \Rightarrow a = 0$ or $b = 0$

   (b) $a < b$ and $c < d \Rightarrow ac < bd$.

3. Write the negation to the following statements

   (a) $\forall$ real number x, if $x > 3$ then $x^2 > 9$.

   (b) $\forall$ computer program P, if P compiles without error messages, then P is correct.

4. Write the contrapositive, converse, and inverse of the following statement and indicate if the statement is true or false.

   $\forall$ real number x, if $x^2 \geq 1$ then $x > 0$.

Solutions

1. Find a counterexample to show that the following statement is false

$$\forall \text{ positive integers } m \text{ and } n,\ mn \geq m+n.$$

Solution: Let m and n be 1, then we have $1(1) = 1$ which is not greater than $1 + 1 = 2$.

2. Let $\mathbb{R}$ be the domain of the predicate variables a, b, c, d. Which of the following are true and which are false?

   (a) $ab = 0 \Rightarrow a = 0$ or $b = 0$

   (b) $a < b$ and $c < d \Rightarrow ac < bd$.

Solution: (a) is true. The only way for the product of two real numbers to be zero is one or the other numbers being real.

(b) is false. Let $a, c = -2$ and $b, d = 1$, then we have that $-2 < 1$, but $(-2)(-2) = 4 > (1)(1) = 1$.

3. Write the negation to the following statements

   (a) $\forall$ real number x, if $x > 3$ then $x^2 > 9$.

   (b) $\forall$ computer program P, if P compiles without error messages, then P is correct.

Solution: (a) $\exists$ real number x such that $x \leq 3$ and $x^2 > 9$.

(b) $\exists$ computer program P such that P compiles with error messages and P is correct.

4. Write the contrapositive, converse, and inverse of the following statement and indicate if the statement is true or false.

   $\forall$ real number x, if $x^2 \geq 1$ then $x > 0$.

Solution:

3.3 Statements with multiple quantifiers

Statements can contain multiple quantifiers for example

$$\forall x \in D, \exists y \in E \text{ such that } P(x, y).$$

For this statement to hold we need to allow x to be picked arbitrarily in D, then we need to find a specific y such that $P(x, y)$ is true. So we apply the quantifiers left to right.

Similarly the statement

$$\exists x \in D \text{ such that } \forall y \in E, P(x, y)$$

we need to find a single x such that $P(x, y)$ holds for all y.

If the quantifiers are of the same type, then the order does not matter. If the quantifiers are of different types, then the order matters.

Theorem 3.3.1. *Let P, Q be predicates with domains D, E, then*

$$\sim (\forall x \in D, \exists y \in E \text{ such that } P(x, y)) \equiv \exists x \in D \text{ such that } \forall y \in E, \sim P(x, y)$$

and

$$\sim (\exists x \in D \text{ such that } \forall y \in E, P(x, y)) \equiv \forall x \in D, \exists y \in E \text{ such that } \sim P(x, y).$$

This negation is the same idea as with single quantifiers, but we know apply the negation left to right flipping quantifiers and negating the final predicate.

3.4 Arguments with quantified statements

Universal instantiation: If a property is true of everything in a set, then it is true of any particular thing in the set. For example

$$\begin{aligned} &\text{All men are mortal.} \\ &\text{Socrates is a man.} \\ \therefore\ &\text{Socrates is mortal.} \end{aligned}$$

Universal instantiation forms the basis for deductive reasoning.

We can now revisit modus ponens and modus tollens with the use of a universal quantifier.

Theorem 3.4.1. *Universal Modus Ponens:*

$$\begin{aligned} &\forall x, P(x) \to Q(x) \\ &P(a) \text{ for some } a \\ \therefore\ &Q(a). \end{aligned}$$

Theorem 3.4.2. *Universal Modus Tollens:*

$$\begin{aligned} &\forall x, P(x) \to Q(x) \\ &\sim Q(a) \text{ for some } a \\ \therefore\ &\sim P(a). \end{aligned}$$

As with in chapter 2 the two most common logical errors are converse errors and inverse error which are given below in their now quantified form.

Theorem 3.4.3. *Converse Error:*

$$\begin{aligned} &\forall x, P(x) \to Q(x) \\ &Q(a) \text{ for some } a \\ \therefore\ &P(a). \end{aligned}$$

Theorem 3.4.4. *Inverse Error:*

$$\begin{aligned} &\forall x, P(x) \to Q(x) \\ &\sim P(a) \text{ for some } a \\ \therefore\ &\sim Q(a). \end{aligned}$$

The names of the previous four statements are not important, the idea is what logical deductions can be made with information about a particular element of the set.

Try and think of some examples of converse errors and inverse errors and what non-valid logical conclusions you can reach. Something to notice is that the closer you are to a biconditional statement, the more likely that a converse error or inverse error will still end up being true.

Exercises

1. Let $D = \{-2, -1, 0, 1, 2\}$. Are the following statements true or false. Explain why.

   (a) $\forall x \in D,\ \exists y \in D$ such that $x + y = 0$.

   (b) $\exists x \in D$ such that $\forall y \in D, x + y = y$.

2. Rewrite the following statements without the use of symbols and find the negation of the statement.

   (a) $\forall$ odd integer n, $\exists$ an integer k such that $n = 2k + 1$.

   (b) $\exists x \in \mathbb{R}$ such that $\forall y \in \mathbb{R}$, $x + y = 0$.

3. State whether the following arguments are either valid or invalid. Justify your answer.

   (a)

   If a number is even, then twice that number is even.
   The number $2n$ is even, for a particular number n.
   $\therefore$ The particular number n is even.

   (b)

   For every student x, if x studies discrete math, then x is good at logic.
   Tarik studies discrete math.
   $\therefore$ Tarik is good at logic.

Solutions

1. Let $D = \{-2, -1, 0, 1, 2\}$. Are the following statements true or false. Explain why.

   (a) $\forall x \in D,\ \exists y \in D$ such that $x + y = 0$.

   (b) $\exists x \in D$ such that $\forall y \in D, x + y = y$.

   Solution: (a) is true. For any x we can pick y to be $-x$.

   (b) is true. Let x be picked to be 0, then for any y we have $x+y = 0+y = y$.

2. Rewrite the following statements without the use of symbols and find the negation of the statement.

   (a) $\forall$ odd integer n, $\exists$ an integer k such that $n = 2k + 1$.

   (b) $\exists x \in \mathbb{R}$ such that $\forall y \in \mathbb{R}$, $x + y = 0$.

   Solution: (a) Without symbols the statement is

   > For all odd integers n, there exists an integer k such that n is equal to twice k plus 1.

   The negation would be

   > There exists an odd integer n such that for all integers k, n is not equal to twice k plus 1.

   (b) Without symbols the statement is

   > There exists a real number x such that for all real numbers y, x plus y is equal to 0.

   The negation of the above statement is

   > For all real numbers x, there exists a real number y such that x plus y is not equal to 0.

3. State whether the following arguments are either valid or invalid. Justify your answer.

   (a)

   > If a number is even, then twice that number is even.
   > The number $2n$ is even, for a particular number n.
   > $\therefore$ The particular number n is even.

(b)

For every student x, if x studies discrete math, then x is good at logic.
Tarik studies discrete math.
$\therefore$ Tarik is good at logic.

Solution:

Chapter 4

Introduction to proofs through elementary number theory

In this chapter, we are going to approach the process of learning to write proofs through number theory. Number theory at its essence is the study of the integers. This is one of the oldest fields of mathematics and contains some of the most fundamental questions about numbers.

When learning to write proofs it is important to focus on the formal logic that you are using more than the results you are trying to prove. Lots of the examples and exercises will likely seem obvious to you, but the goal of this chapter is to show that these statements are always true.

For the motivation of this chapter, think about how you might prove the following claim: There are infinitely many prime numbers.

For more tips and ideas on writing proofs, see appendix section 1.

4.1 Direct proof and counterexample.

Definition 4.1.1. An integer n is **even** if, and only if, n equals twice some integer. An integer n is **odd** if, and only if, n equals twice some integer plus 1. Symbolically this gives:

$$\begin{aligned} n \text{ is even} &\iff n = 2k \text{ for some integer } k. \\ n \text{ is odd} &\iff n = 2k+1 \text{ for some integer } k. \end{aligned}$$

Definition 4.1.2. An integer n is **prime** if, and only if, $n > 1$ and for all positive integers r and s, if $n = rs$, then either r or s equals n. An integer n is **composite** if, and only if, $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

Note that these two definitions give us ways to break up the integers. An integer can only be even or odd, but not both. Similarly, a positive integer can be either prime or composite, but not both.

Procedure 4.1.3 (Proving existential and disproving universal statements)**.** If you need to prove an existential statement of the form,

$$\exists x \in D \text{ such that } Q(x)$$

then all it takes is finding one $x \in D$ that makes $Q(x)$ true. Similarly if you need to disprove a universal statement of the form

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

then that is the same as proving the negation which is

$$\exists x \in D \text{ such that } \sim P(x).$$

△

So to disprove the universal statement we need to find one $x \in D$ such that $P(x)$ is false. When dealing with integers I would recommend $-1, 0, 1$ as easy options to start with.

Procedure 4.1.4 (Proving universal or disproving existential statements)**.** If we want to prove a statement of the form,

$$\forall x \in D, \text{ if } P(x) \text{ then } Q(x).$$

then below are a couple of the main type of proof strategies that can be used.

1. **Method of exhaustion**: If the domain D is finite or if you can split it into a finite number of cases, then the method of exhaustion can be used by checking each case.

   For example, when dealing with integers using that they are either even or odd is a common strategy.

2. **Direct proof**: Here we start with our if $P(x)$ as an assumption and use definitions, previous theorems, and other results to directly get to our conclusion. This is the most standard proof method and is often used with other strategies.

   The general form of this proof will start with

   > Let $x \in D$ such that $P(x)$ is true, then ...

   To show that a result is true for all elements in a set we need to use a variable to represent an arbitrary element and work only off the properties that all elements in the set have.

3. **Proof by contradiction**: Another common proof strategy is proof by contradiction. Here we are going to assume $\sim Q(x)$ and $P(x)$ then try to reach a logical contradiction. This strategy can be helpful since we get the extra information on x that $\sim Q(x)$ is true.

△

Theorem 4.1.5. *The sum of any two even integers is even.*

Proof. Suppose $m, n \in \mathbb{Z}$ such that m, n are even, then by the definition of being even $m = 2r$ and $n = 2s$ for some integers $r, s \in \mathbb{Z}$. With this we have

$$m + n = 2r + 2s = 2(r + s).$$

Let $t = r + s$ and note that t is an integer since it is the sum of integers. Hence, $m + n = 2t$ which is the definition of being even. □

While a lot of problems involving concepts from even/odd and primes seem easy to prove, they can be deceptively hard. A well known open problem in math is as follows

Conjecture 4.1.6 (Goldbach conjecture)**.** *Let $n \in \mathbb{Z}$ such that $n > 2$, then n is the sum of two prime numbers.*

Exercises

Prove the following:

1. There are distinct integers m and n such that

$$\frac{1}{m} + \frac{1}{n}$$

   is an integer.

2. There is an integer $n > 5$ such that $2^n - 1$ is prime.

3. For every integer n, if $(n - 1)/2$ is an integer, then n is odd.

4. For each integer n with $1 \leq n \leq 10$, $n^2 - n + 11$ is a prime number.

5. The difference between the squares of any two consecutive integers is odd.

Solutions

Prove the following:

1. There are distinct integers m and n such that

$$\frac{1}{m} + \frac{1}{n}$$

is an integer.

Consider $m = 1$ and $n = -1$, then $1/m + 1/n = 0$.

2. There is an integer $n > 5$ such that $2^n - 1$ is prime.

Choose $n = 7$, then $2^7 - 1 = 127$ which is prime.

3. For every integer n, if $(n-1)/2$ is an integer, then n is odd.

Proof. Let n be an integer such that $(n-1)/2$ is also an integer, then $(n-1)/2 = k$ for some integer k. Now,

$$(n-1)/2 = k \implies n - 1 = 2k \implies n = 2k + 1.$$

Following the definition of odd numbers, n is odd. □

4. For each integer n with $1 \leq n \leq 10$, $n^2 - n + 11$ is a prime number.

Proof. We will apply a proof by exhaustion, this gives

$$\begin{aligned}
n = 1 &\implies n^2 - n + 11 = 11 \\
n = 2 &\implies n^2 - n + 11 = 13 \\
n = 3 &\implies n^2 - n + 11 = 17 \\
n = 4 &\implies n^2 - n + 11 = 23 \\
n = 5 &\implies n^2 - n + 11 = 31 \\
n = 6 &\implies n^2 - n + 11 = 41 \\
n = 7 &\implies n^2 - n + 11 = 53 \\
n = 8 &\implies n^2 - n + 11 = 67 \\
n = 9 &\implies n^2 - n + 11 = 83 \\
n = 10 &\implies n^2 - n + 11 = 101
\end{aligned}$$

□

5. The difference between the squares of any two consecutive integers is odd.

Proof. Let $n \in \mathbb{Z}$, then

$$(n+1)^2 - n^2 = n^2 + 2n + 1 - n^2 = 2n + 1.$$

By definition of odd numbers $2n + 1$ is odd giving that $(n+1)^2 - n^2$ is odd. □

4.2 Rational numbers

Definition 4.2.1. A real number r is rational if, and only if, it can be expressed as a quotient of two integers with a nonzero denominator. A real number that is not rational is irrational. More formally, if r is a real number, then

$$r \text{ is rational. } \iff \exists a, b \in \mathbb{Z} \text{ such that } r = \frac{a}{b} \text{ and } b \neq 0.$$

Example 4.2.2. The following are all rational numbers

$$\frac{1}{2}, \quad \frac{2}{4}, \quad \frac{1}{1}, \quad \frac{2}{3}.$$

Note that rational numbers are not just fractions. The following are not rational numbers

$$\frac{\pi}{2}, \quad \frac{\sqrt{2}}{1}, \quad \frac{1}{0}, \quad \frac{e}{3}.$$

△

Theorem 4.2.3. *Every integer is a rational number.*

Theorem 4.2.4. $\sqrt{2}$ *is irrational.*

Proof. Assume for contradiction that $\sqrt{2}$ is rational, then $\sqrt{2} = \frac{p}{q}$ for $p, q \in \mathbb{Z}$ where $q \neq 0$ and $\gcd\{p, q\} = 1$. This gives,

$$\sqrt{2} = \frac{p}{q} \implies 2 = \frac{p^2}{q^2} \implies 2q^2 = p^2$$

which implies p^2 is even. Because p^2 is even p must be even. Following p is even, $p = 2k$ for some $k \in \mathbb{Z}$. Now

$$\begin{aligned} 2q^2 = p^2 &\implies 2q^2 = (2k)^2 \\ &\implies 2q^2 = 4k^2 \\ &\implies q^2 = 2k^2. \end{aligned}$$

Therefore q is also even. However, this is a contradiction since we assumed $\gcd\{p, q\} = 1$. Thus $\sqrt{2}$ is irrational. □

4.3 Divisibility

Definition 4.3.1. If $n, d \in \mathbb{Z}$, then n is **divisible** by d if and only if n equals d times some integer and $d \neq 0$.

There are several ways to say the statement above which are

1. n is a multiple of d,

2. d is a factor of n,

3. d is a divisor of n,

4. d divides n.

We use the notation

$$d|n \iff \exists k \in \mathbb{Z} \text{ such that } n = dk \text{ where } d \neq 0.$$

If d does not divide n, then we use $d \not| n$.

Theorem 4.3.2 (Fundamental Theorem of algebra)**.** *Given any integer $n > 1$, there exist a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers $q_1, q_2, \ldots, q_k$ such that*

$$n = p_1^{q_1} p_2^{q_2} \ldots p_k^{q_k},$$

This expression for n as a product of prime numbers is unique except, perhaps, for the order in which the factors are written.

Exercises

1. Prove or give a counter example. If m is any even integer and n is any odd integer, then $m^2 + 3n$ is odd.

2. Prove that if a real number c satisfies a polynomial equation of the form

$$r_3c^3 + r_2c^2 + r_1c + r_0 = 0,$$

where r_0, r_1, r_2, r_3 are rational numbers, then c satisfies a polynomial of the form

$$n_3c^3 + n_2c^2 + n_1c + n_0 = 0,$$

where n_0, n_1, n_2, n_3 are integers.

3. Does $7|56$? Does $5|0$?

4. If $n = 4k + 1$, does 8 divide $n^2 - 1$?

5. Prove the following statement. For all integers a, b, c, if $a|b$ and $a|c$ then $a|(b + c)$.

Solutions

1. Prove or give a counter example. If m is any even integer and n is any odd integer, then $m^2 + 3n$ is odd.

Proof. Let $m, n \in \mathbb{Z}$ such that m is even and n is odd, then $m = 2k$ and $n = 2r + 1$ for some $k, r \in \mathbb{Z}$. Now

$$m^2 + 3n = (2k)^2 + 3(2r + 1) = 4k^2 + 6r + 3 = 2(2k^2 + 3r + 1) + 1.$$

Let $x = 2k^2 + 3r + 1$ and note that $x \in \mathbb{Z}$. Thus $m^2 + 3n = 2x + 1$ giving that it is odd. □

2. Prove that if a real number c satisfies a polynomial equation of the form

$$r_3c^3 + r_2c^2 + r_1c + r_0 = 0,$$

where r_0, r_1, r_2, r_3 are rational numbers, then c satisfies a polynomial of the form

$$n_3c^3 + n_2c^2 + n_1c + n_0 = 0,$$

where n_0, n_1, n_2, n_3 are integers.

Proof. Let $c \in \mathbb{R}$ and $r_0, r_1, r_2, r_3 \in \mathbb{Q}$ such that

$$r_3c^3 + r_2c^2 + r_1c + r_0 = 0.$$

By the definition of rational numbers we can write $r_j = a_j/b_j$ where $a_j, b_j \in \mathbb{Z}$, $b_j \neq 0$ and for some $j \in \{0, 1, 2, 3\}$. Now

$$\begin{aligned} r_3c^3 + r_2c^2 + r_1c + r_0 = 0 &\implies \frac{a_3}{b_3}c^3 + \frac{a_2}{b_2}c^2 + \frac{a_1}{b_1}c + \frac{a_0}{b_0} = 0 \\ &\implies a_3b_0b_1b_2c^3 + a_2b_0b_1b_3c^2 + a_1b_0b_2b_3c + a_0b_1b_2b_3 = 0. \end{aligned}$$

Let $n_0 = a_0b_1b_2b_3$, $n_1 = a_1b_0b_2b_3$, $n_2 = a_2b_0b_1b_3$, and $n_3 = a_3b_0b_1b_2$, then from above we have

$$n_3c^3 + n_2c^2 + n_1c + n_0 = 0.$$

Note that $n_0, \ldots, n_3$ are integers since they are defined as the product of integers, this gives the desired result. □

3. Does $7|56$? Does $5|0$?

   Yes to both. We can write $7(8) = 56$ and $5(0) = 0$.

4. If $n = 4k + 1$, does 8 divide $n^2 - 1$?

   Yes. Let $n \in \mathbb{Z}$ such that $n = 4k + 1$ for some $k \in \mathbb{Z}$, then

$$n^2 - 1 = (4k + 1)^2 - 1 = 16k^2 + 8k + 1 - 1 = 8(2k^2 + k).$$

   From above we can see that 8 is a multiple of $n^2 - 1$.

5. Prove the following statement. For all integers a, b, c, if $a|b$ and $a|c$ then $a|(b + c)$.

Proof. Let $a, b, c \in \mathbb{Z}$ such that $a|b$ and $a|c$, then by the definition of divisibility $am = b$ and $an = c$ for $m, n \in \mathbb{Z}$. This gives

$$b + c = am + an = a(m + n).$$

Thus $a|(b + c)$ by the multiple of $m + n$. □

4.4 Quotient remainder theorem

Theorem 4.4.1 (The quotient remainder theorem)**.** *Given any integer n and positive integer d, there exists unique integers q and r with $0 \leq r < d$ such that*

$$n = dq + r.$$

Definition 4.4.2. Given an integer n and a positive integer d, if $n = dq + r$ for q r integers such that $0 \leq r < d$ then

$$n \text{ div } d = q$$
$$n \bmod d = r.$$

We can use the quotient remainder theorem to take proofs involving an integer and break them into a finite number of cases based on the divisor d.

Definition 4.4.3. For any real number x, the **absolute value of** x, denoted $|x|$, is defined as follows:

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0. \end{cases}$$

With this definition we have the following common properties for all real numbers x, y:

1. $-|x| \leq x \leq |x|$.
2. $|-x| = |x|$.
3. $|x + y| \leq |x| + |y|$.

Exercises

1. Prove or give a counter example to the following

   (a) The sum of any three consecutive integers is divisible by 3.

   Proof. Let $n \in \mathbb{Z}$, then

   $$n + n + 1 + n + 2 = 3n + 3 = 3(n + 1).$$

   Thus $3|3(n + 1)$ giving the desired result. □

(b) For all integers a and b, if $a|b$ then $a^2|b^2$.

Proof. Let $a, b \in \mathbb{Z}$ such that $a|b$, then by the definition of divisibility there exists a $k \in \mathbb{Z}$ such that $ak = b$. Now $b^2 = a^2k^2$. Following k^2 is an integer, we have that $a^2|b^2$. □

(c) For all integers a and n, if $a|n^2$ and $a \leq n$ then $a|n$

This statement is false. Consider $a = 4$ and $n = 6$, then $4|36$ but $4 \nmid 6$.

2. (Hard): If n is a nonnegative integer such that the sum of the digits of n is divisible by 9, then prove that $9|n$.

   Hint: consider n as a string with the digits as its characters, then $n = d_1d_2 \ldots d_m$. We can also consider n as a number as a product sum of its digits, which gives $n = d_1 + 10d_2 + 100d_3 + \cdots + 10^{m-1}d_m$. Now we are assuming that $d_1 + d_2 + \cdots + d_m = 9k$ and we want to show that $9|n$.

3. Evaluate 20 mod 2, 28 mod 5, $(10^{30} + 2)$ mod 3, 50 div 7, 2^{100} div 2.

4. If today is Friday, what day of the week will it be 1000 days from today.

5. Prove that, for every integer n, $n^2 - n + 3$ is odd.

6. Prove that the product of any three consecutive integers is a multiple of 3.

7. Use the quotient-remainder theorem with divisor equal to 3 to prove that the square of any integer has the form $3k$ or $3k + 1$ for some integer k.

8. Given any integer n, if $n > 3$, could n, $n + 2$, and $n + 4$ all be prime? Prove or give a counter example.

Solutions

1. Prove or give a counter example to the following

   (a) The sum of any three consecutive integers is divisible by 3.

   Proof. Let $n \in \mathbb{Z}$, then

   $$n + n + 1 + n + 2 = 3n + 3 = 3(n + 1).$$

   Thus $3|3(n + 1)$ giving the desired result. □

   (b) For all integers a and b, if $a|b$ then $a^2|b^2$.

   Proof. Let $a, b \in \mathbb{Z}$ such that $a|b$, then by the definition of divisibility there exists a $k \in \mathbb{Z}$ such that $ak = b$. Now $b^2 = a^2k^2$. Following k^2 is an integer, we have that $a^2|b^2$. □

(c) For all integers a and n, if $a|n^2$ and $a \leq n$ then $a|n$

This statement is false. Consider $a = 4$ and $n = 6$, then $4|36$ but $4 \nmid 6$.

2. (Hard): If n is a nonnegative integer such that the sum of the digits of n is divisible by 9, then prove that $9|n$.

   Hint: consider n as a string with the digits as its characters, then $n = d_1 d_2 \dots d_m$. We can also consider n as a number as a product sum of its digits, which gives $n = d_1 + 10d_2 + 100d_3 + \cdots + 10^{m-1}d_m$. Now we are assuming that $d_1 + d_2 + \cdots + d_m = 9k$ and we want to show that $9|n$.

   Proof. Let $n \in \mathbb{Z}$ with digits $d_1, \dots, d_m$ such that $d_1 + \cdots + d_m = 9k$ for some $k \in \mathbb{Z}$. Now

$$\begin{aligned} n &= \sum_{k=0}^{m} 10^k d_{k+1} \\ &= \sum_{k=0}^{m} \underbrace{9 \cdots 9}_{k} d_{k+1} + d_{k+1} \\ &= 9k + \sum_{k=0}^{m} \underbrace{9 \cdots 9}_{k} d_{k+1} \\ &= 9\left(k + \sum_{k=0}^{m} \underbrace{1 \cdots 1}_{k} d_{k+1}\right). \end{aligned}$$

   Thus n can be written as 9 times some integer, so it is divisible by 9. □

3. Evaluate $20 \bmod 2$, $28 \bmod 5$, $(10^{30} + 2) \bmod 3$, $50 \operatorname{div} 7$, $2^{100} \operatorname{div} 2$.

$$\begin{aligned} 20 \bmod 2 &= 0 \\ 28 \bmod 5 &= 3 \\ (10^{30} + 2) \bmod 3 &= 0 \\ 50 \operatorname{div} 7 &= 7 \\ 2^{100} \operatorname{div} 2 &= 2^{99}. \end{aligned}$$

4. If today is Friday, what day of the week will it be 1000 days from today.

   There are 7 days in a week. To calculate this problem, we only care about the remainder of 1000 days divided by 7. So the problem becomes $1000 \bmod 7 = 6$ (To calculate that, I would recommend a calculator. To do it by hand, note $1000 = 700 + 4(70) + 2(7) + 6$, so the remainder is 6). Thus, the answer is 6 days after Friday, giving Thursday.

5. Prove that, for every integer n, $n^2 - n + 3$ is odd.

   Let $n \in \mathbb{Z}$, then we will proceed by cases on n being even or odd. If n is even, then $n = 2k$ for some $k \in \mathbb{Z}$. This gives

   $$n^2 - n + 3 = 4k^2 - 2k + 3 = 2(k^2 - k + 1) + 1.$$

   Let $x = k^2 - k + 1$, then we have $n^2 - n + 3 = 2x + 1$ giving that it is odd.

   If n is odd, then $n = 2k + 1$ for some $k \in \mathbb{Z}$. Now

   $$n^2 - n + 3 = 4k^2 + 4k + 1 - (2k + 1) + 1 = 4k^2 + 2k + 1 = 2(2k^2 + k) + 1.$$

   Let $x = 2k^2 + k$, then $n^2 - n + 3 = 2k + 1$ giving that it is odd.

6. Prove that the product of any three consecutive integers is a multiple of 3.

   Proof. Let $n \in \mathbb{Z}$, then by the quotient remainder theorem $n = 3q + r$ where r is either $0, 1, 2$. Proceed by cases on r this gives

   $$\begin{aligned}
   r = 0 &\implies n(n+1)(n+2) = 3q(3q+1)(3q+2) = 3(q(3q+1)(3q+2)) \\
   r = 1 &\implies n(n+1)(n+2) = (3q+1)(3q+2)(3q+3) = 3((3q+1)(3q+2)(q+1)) \\
   r = 2 &\implies n(n+1)(n+2) = (3q+2)(3q+3)(3q+4) = 3((3q+2)(q+1)(3q+4)).
   \end{aligned}$$

   In all of the above cases the product is a multiple of 3. □

7. Use the quotient-remainder theorem with divisor equal to 3 to prove that the square of any integer has the form $3k$ or $3k + 1$ for some integer k.

   Proof. By the quotient remainder theorem with divisor equal to 3 every integer can be written as $3k, 3k + 1, 3k + 2$ for some $k \in \mathbb{Z}$. Now we have

   $$\begin{aligned}
   (3k)^2 &= 9k^2 = 3(3k^2) \\
   (3k+1)^2 &= 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1 \\
   (3k+2)^2 &= 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1.
   \end{aligned}$$

   Following that none of these squares can be written as $3k + 2$ we can conclude that the square of any integer is of the form $3k$ or $3k + 1$. □

8. Given any integer n, if $n > 3$, could n, $n + 2$, and $n + 4$ all be prime? Prove or give a counter example.

   Proof. Let $n \in \mathbb{Z}$ such that $n > 3$, then by the quotient remainder theorem $n = 3q + r$ where $r \in \{0, 1, 2\}$. If we look at the cases we have

   $$\begin{aligned}
   r = 0 &\implies 3q, 3q + 2, 3q + 4 \\
   r = 1 &\implies 3q + 1, 3q + 3, 3q + 5 \\
   r = 2 &\implies 3q + 2, 3q + 4, 3q + 6.
   \end{aligned}$$

In the case $r = 0$, then $3q$ is not prime. If $r = 1$, then $3q + 3 = 3(q + 1)$ is not prime. If $r = 2$, then $3q + 6 = 3(q + 2)$ is not prime. So in each of the above cases, at least one of the numbers is not prime. □

4.5 Contradiction, contraposition, and some open problems

We mentioned proof by contradiction in section 4.2, but here is the strategy again

Procedure 4.5.1 (Method of proof by contradiction)**.**

1. Suppose the statement to be proved is false. That is, suppose that the negation of the statement is true.
2. Show that this assumption leads to a logical contradiction.
3. Conclude that the statement to be proved is true.

△

Theorem 4.5.2. *There is no greatest integer*

Proof. Assume for contradiction that $M \in \mathbb{Z}$ is the greatest integer, that is $M \geq n$ for all $n \in \mathbb{Z}$. Now define $N = M + 1$ which is an integer. This gives that $M \geq N$ by assumption. However, we have a contradiction, since $M < M + 1 = N$ and $M \geq N$. Thus, there is no greatest integer. □

Procedure 4.5.3 (Method of proof by contraposition)**.**

1. Express the statement to be proved in the form
$$\forall x \in D, P(x) \implies Q(x).$$
2. Rewrite the statement as its contrapositive
$$\forall x \in D, \sim Q(x) \implies \sim P(x)$$
3. Prove the contrapositive by another proof strategy.
4. Conclude the original statement is true.

△

Theorem 4.5.4. *For every integer n, if n^2 is even then n is even.*

Proof. Proceed by contrapositive, let $n \in \mathbb{Z}$ such that $n = 2k + 1$ for some integer $k \in \mathbb{Z}$. Now

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

Thus n^2 is odd. □

Theorem 4.5.5. *There are infinitely many primes.*

Proof. Assume for contradiction that there are a finite number of primes, call them $p_1, \ldots, p_m$. Construct a new number $a = p_1 p_2 \cdots p_m + 1$ that is a is a product of all the primes. We know a is some finite number, since it is a product of a finite number of finite numbers. Now a can't be a multiple of p_1, p_2, $\ldots$, p_m since it is shifted 1 past a multiple of those. By the fundamental theorem of arithmetic, a is a product of primes, but a is not divisible by any of the primes. Thus, we have a contradiction, giving that there are an infinite number of primes. □

More "fun" open problems.

Conjecture 4.5.6 (Twin prime conjecture)**.** *There are an infinite number of prime pairs of the form p and $p+2$.*

The current bound is that there are an infinite number of primes whose gap is less than 246 apart.

Conjecture 4.5.7. *There are an infinite number of Mersenne primes. Where a Mersenne prime is of the form $2^p - 1$ for some $p \in \mathbb{Z}$.*

Exercises

1. Prove that there exists a unique prime number of the form $n^2 + 2n - 3$ where n is a positive integer. (Hint: Factor)
2. Prove that $\sqrt{5}$ is irrational.
3. Prove that, for any integer a, 9 does not divide $a^2 - 3$.
4. Let $N = 2(3)(5)(7) + 1$. What remainder is obtained when N is divided by 2, 3, 5, or 7? Can you generalize this?
5. Prove that for every integer n, if $n > 2$ then there is a prime number p such that $n < p < n!$ where $n! = n(n-1)(n-2)\ldots(3)(2)(1)$.

Solutions

1. Prove that there exists a unique prime number of the form $n^2 + 2n - 3$ where n is a positive integer. (Hint: Factor)

   Proof. Note that when $n = 2$ we have $2^2 + 2(2) - 3 = 5$ which is prime. So we have at least one. Now we want to show it is unique.

   For $n \in \mathbb{Z}$ we can factor $n^2 + 2n - 3$ as $(n-1)(n+3)$. Thus if $n > 2$, then $n - 1$ and $n + 3$ will both be greater than 1 giving that $(n-1)(n+3)$ is composite. This gives that $n = 2$ is the unique prime number. □

2. Prove that $\sqrt{5}$ is irrational.

   We have done a very similar proof for $\sqrt{2}$ being irrational.

   Proof. Assume for contradiction that $\sqrt{5}$ is rational, then $\sqrt{5} = \frac{p}{q}$ for $p, q \in \mathbb{Z}$ where $q \neq 0$ and $\gcd\{p, q\} = 1$. This gives,

   $$\sqrt{5} = \frac{p}{q} \implies 5 = \frac{p^2}{q^2} \implies 5q^2 = p^2$$

   which implies p^2 is divisible by 5. Because p^2 is divisible by 5, p must be divisible by 5. Following p is divisible by 5, $p = 5k$ for some $k \in \mathbb{Z}$. Now

   $$\begin{aligned} 5q^2 = p^2 &\implies 5q^2 = (5k)^2 \\ &\implies 5q^2 = 25k^2 \\ &\implies q^2 = 5k^2. \end{aligned}$$

   Therefore q is also even. However, this is a contradiction since we assumed $\gcd\{p, q\} = 1$. Thus $\sqrt{5}$ is irrational. □

3. Prove that, for any integer a, 9 does not divide $a^2 - 3$.

   Proof. Assume for contradiction that 9 divides $a^2 - 3$, then we can write $a^2 - 3 = 9k$ which implies $a^2 = 3(3k + 1)$. So a^2 is a multiple of 3, but not a multiple of 9 since $3k + 1$ is not a multiple of 3. However, this is a contradiction since if a^2 is a multiple of 3, then a is a multiple of 3, but if a is a multiple of 3, then a^2 is a multiple of 9. □

4. Let $N = 2(3)(5)(7) + 1$. What remainder is obtained when N is divided by 2, 3, 5, or 7? Can you generalize this?

   The remainder for 2, 3, 5, and 7 are all 1. To see this we can use the quotient remainder theorem with the 2, 3, 5, 7 as potential divisors.

   To generalize, if I construct $N = p_1 p_2 \dots p_n + 1$ where p_j are primes, then the remainder of N with divisors of p_1, p_2, $\dots$, p_n will be 1.

5. Prove that for every integer n, if $n > 2$ then there is a prime number p such that $n < p < n!$ where $n! = n(n-1)(n-2)\dots(3)(2)(1)$.

   Proof. Consider $n! - 1$ and proceed by cases on whether it is prime. If $n! - 1$ is prime, then we are done since $n < n! - 1 < n!$. If $n! - 1$ is not prime, then it can't divide 1, 2, $\dots$, n by similar logic as from problem 4. However, following $n! - 1$ is not prime it must have prime divisors and from the above logic those divisors are between $n + 1$ and $n! - 2$. Thus, we have a prime in the range of n to $n!$ as desired. □

   Note that this bound is very poor. It turns out that given $n > 2$ we have that there is a prime between n and $2n$. This is known as Bertrand's postulate.

4.6 The handshake theorem

Definition 4.6.1. The total degree of a graph is the sum of the degrees of all vertices of the graph.

Theorem 4.6.2. *The total degree of a graph is equal to twice the number of edges of a graph.*

Corollary 4.6.3. *The total degree of a graph is even.*

Theorem 4.6.4. *In any graph there is an even number of vertices of odd degree.*

Definition 4.6.5. A **simple graph** is a graph that does not have any loops or parallel edges.

Definition 4.6.6. Let $n \in \mathbb{Z}^+$, then a **complete graph on n vertices**, denoted K_n, is a simple graph where every pair of distinct edges are connected with an edge.

Definition 4.6.7. Let $m, n \in \mathbb{Z}^+$. A **complete bipartite graph on (m, n) vertices**, denoted $K_{m,n}$ is a simple graph whose vertices are divided into two subsets V, W where no vertices within the sets are connected by edges and every combinations of vertices across V and W are connected.

These tools can be used to solve questions about graphs without knowing what the graphs look like.

4.7 Algorithms

Definition 4.7.1. Let $a, b \in \mathbb{Z}$ such that both a and b are not 0. The **greatest common divisor** of a and b, denoted $\gcd(a, b)$, is that integer d with the following properties:

1. d is a common divisor of both a and b. In other words,
$$d|a \text{ and } d|b.$$
2. For every integer c, if c is a common divisor of both a and b, then c is less than or equal to d. In other words, for every integer c, if $c|a$ and $c|b$ then $c \leq d$.

Lemma 4.7.2. *If r is a positive integer, then* $\gcd(r, 0) = r$.

Lemma 4.7.3. *If a and b are any integers not both zero, and if q and r are any integers such that*
$$a = bq + r,$$
then
$$\gcd(a, b) = \gcd(b, r).$$

This section also covers the Euclidean algorithm and the Division algorithm. I would recommend reading these over. They are used to calculate the quotient remainder theorem terms and the greatest common divisor between two integers.

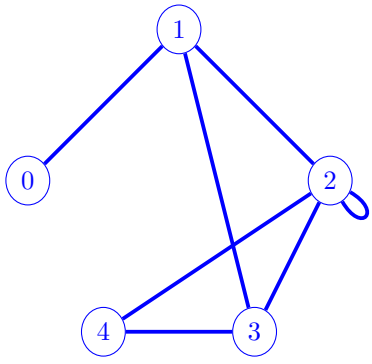
Exercises

1. Draw the following graphs or explain why they can't exist.
   (a) Graph of five vertices of degrees 1, 2, 3, 3, and 5.
   (b) Graph of four vertices of degrees 1, 2, 3, and 4.
   (c) Simple graph with five vertices of degrees 1, 1, 1, 2, and 3.
2. At a party attended by a group of people,
   - 2 people knew 1 other person
   - 5 people knew 2 other people
   - The rest of the people knew 3 other people
   - A total of 15 pairs of people knew each other before the party.

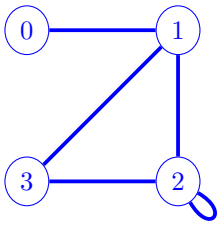
   (a) How many people attending the party knew 3 other people before the party?
   (b) How many people attended the party?
3. In a group of two or more people, must there always be at least two people who are acquainted with the same number of people within the group?
   (Hint: This is a simple graph)

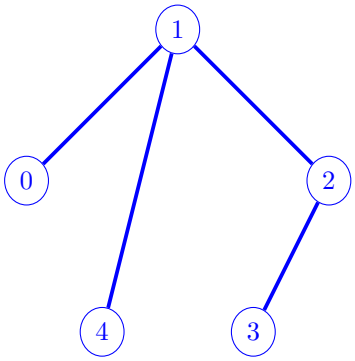
Solutions

1. Draw the following graphs or explain why they can't exist.
   (a) Graph of five vertices of degrees 1, 2, 3, 3, and 5.



   (b) Graph of four vertices of degrees 1, 2, 3, and 4.
   (c) Simple graph with five vertices of degrees 1, 1, 1, 2, and 3.





2. At a party attended by a group of people,

   - 2 people knew 1 other person
   - 5 people knew 2 other people
   - The rest of the people knew 3 other people
   - A total of 15 pairs of people knew each other before the party.

   (a) How many people attending the party knew 3 other people before the party?

   (b) How many people attended the party?

   We can think of this problem as a graph, where people are the vertices and knowing someone is the edge. With this, our information becomes,

   - 2 vertices of degree 1.
   - 5 vertices of degree 2.
   - x vertices of degree 3.
   - 15 total edges.

   To solve for x we need an equation that relates edges to vertex degrees. We have that the two times the number of edges equals the total degree of a graph. This gives,

   $$1(2) + 2(5) + 3x = 2(15) \implies 3x = 18 \implies x = 6.$$

So the answer for part (a) is 6. Now the total number of people is 6 + 5 + 2 = 13.

3. In a group of two or more people, must there always be at least two people who are acquainted with the same number of people within the group?

   (Hint: This is a simple graph)

   Proof. For a simple graph on n vertices, we have the options $0, 1, \ldots, n-1$ for possible degrees of the vertices. Notice that if I have a degree $n-1$ node, then it must be connected to every other node in the graph. This gives that the options 0 and $n-1$ are mutually exclusive for vertex degrees. So we have n nodes to pick choices for and $n-1$ options for them to pick. This gives that two vertices must share the same degree. □

Chapter 5

Sequences and mathematical induction

5.1 Sequences

Definition 5.1.1. A **sequence** is a function whose domain is either all the integers between two given numbers or all the integers greater than or equal to a given integer.

Typically, sequence are denoted as,

$$a_m, a_{m+1}, a_{m+2}, \ldots, a_n$$

where each element a_k (read as "a sub k") is called a **term**. The k in a_k is called the **index**. a_m is called the **initial term** and a_n is called the **final term**.

Example 5.1.2. The positive even integers form a sequence

$$2, 4, 6, \ldots$$

where $a_k = 2k$ and the initial term is $a_1 = 2$. △

Definition 5.1.3. Let $m, n \in \mathbb{Z}$ such that $m \leq n$, then

$$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + \cdots + a_n$$

is the summation from k equals m to n of a_k.

Definition 5.1.4. Let $m, n \in \mathbb{Z}$ such that $m \leq n$, then

$$\prod_{k=m}^{n} a_k = (a_m)(a_{m+1}) \ldots (a_n)$$

is the product from k equals m to n of a_k.

Theorem 5.1.5. *If $a_m, a_{m+1}, \ldots$ and $b_m, b_{m+1}, \ldots$ are sequences of real numbers and c is any real number, then*

1. $\sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k = \sum_{k=m}^{n} (a_k + b_k)$.
2. $c \sum_{k=m}^{n} a_k = \sum_{k=m}^{n} c(a_k)$.
3. $\left(\prod_{k=m}^{n} a_k \right) \left(\prod_{k=m}^{n} b_k \right) = \prod_{k=m}^{n} a_k b_k$.

Definition 5.1.6. Let $n \in \mathbb{Z}^+$, then n factorial, denoted $n!$, is defined as

$$n! := \prod_{k=1}^{n} k = n(n-1)(n-2)\ldots(2)(1).$$

Zero factorial, 0!, is defined to be 1.

Definition 5.1.7. Let n and r be integers with $0 \leq r \leq n$, then

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

is read "n choose r" and represents the number of subsets of size r that can be chosen from a set with n elements.

5.2 Mathematical Induction

Definition 5.2.1 (Principal of mathematical induction)**.** Let $P(n)$ be a property that is defined for integers n, and let a be a fixed integer. Suppose the following two statements are true:

1. $P(a)$ is true.
2. For every integer $k \geq a$, if $P(k)$ is true, then $P(k+1)$ is true.

Then the statement

$$\text{for every integer } n \geq a, P(n)$$

is true.

Procedure 5.2.2 (Method of proof by mathematical induction)**.** To prove a statement of the form

For every integer $n \geq a$, a property $P(a)$ is true

we can use mathematical induction. To do this, first we prove the base case. Which is show $P(a)$ is true, where a is the initial value the statement should hold on.

Then we need to prove the inductive step. Assume the result holds for some $k \geq a$, then we want to show that the result holds for $k+1$.

Once you have shown these two things, the original statement is proven. △

Example 5.2.3. Prove that for $n \geq 1$ we have

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

△

Proof. For the base case, $n = 1$, we have

$$\sum_{k=1}^{1} k = 1 = \frac{1(2)}{2}.$$

Now for the inductive step we assume that the result holds for some $m \geq 1$, then

$$\begin{aligned}\sum_{k=1}^{m+1} k &= (m+1) + \sum_{k=1}^{m} k \\ &= (m+1) + \frac{m(m+1)}{2} \\ &= \frac{(m+1)(m+2)}{2}.\end{aligned}$$

□

Exercises

1. Write the first 4 terms in the sequence defined by

$$a_k = \frac{k}{10+k} \text{ for } k \geq 1$$

2. Find explicit formulas for the following sequences
   (a) -1, 1, -1, 1, ...
   (b) 0, 1, -2, 3, -4, 5, ...
3. Write the following in summation or product notation.
   (a) $1^2 - 2^2 + 3^2 - 4^2 + 5^2 - 6^2 + 7^2$.
   (b) $2/(3(4)) - 3/(4(5)) + 4/(5(6)) - 5/(6(7)) + 6/(7(8))$
4. Compute the following

(a) 4!/3!

(b) 6!/8!

(c) $n!/(n-2)!$

5. Prove the following by induction

(a) $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$ for all $n \geq 1$.

(b) $\sum_{k=1}^{n+1} k2^k = n2^{n+2} + 2$.

(c) $\sum_{k=1}^{n} k(k!) = (n+1)! - 1$ for all $n \geq 1$.

Solutions

1. Write the first 4 terms in the sequence defined by

$$a_k = \frac{k}{10+k} \text{ for } k \geq 1$$

The sequence is defined for $k \geq 1$, so the first 4 terms will be 1,2,3,4. This gives

$$\begin{aligned} a_1 &= \frac{1}{10+1} = \frac{1}{11} \\ a_2 &= \frac{2}{10+2} = \frac{1}{6} \\ a_3 &= \frac{3}{10+3} = \frac{3}{13} \\ a_4 &= \frac{4}{10+4} = \frac{2}{7}. \end{aligned}$$

2. Find explicit formulas for the following sequences

(a) -1, 1, -1, 1, ...

(b) 0, 1, -2, 3, -4, 5, ...

The first sequence is oscillating between negative and positive, so we need a $(-1)^k$ term. Since it is not growing or shrinking, all we need is that term. We can start the sequence at $k = 1$ to capture that the first term is negative 1. This gives $a_k = (-1)^k$ for all $k \geq 1$.

The second sequence again will need a $(-1)^k$ following it is oscillating. However, it is growing 1 per step. This says we need a k term. The first try would be $(-1)^k k$, but when $k = 1$ we see that, we get -1 instead of 1. To fix this change $(-1)^k$ into $(-1)^{k+1}$ this shift flips which terms are negative. Putting this all together gives $a_k = (-1)^{k+1}k$.

3. Write the following in summation or product notation.

(a) $1^2 - 2^2 + 3^2 - 4^2 + 5^2 - 6^2 + 7^2$.

(b) $2/(3(4)) - 3/(4(5)) + 4/(5(6)) - 5/(6(7)) + 6/(7(8))$

For part (a), we see addition and subtraction here, so we want summation notation. The sequence inside the sum matches the previous problem, but instead of k we have k^2. To get the bounds of the sum, we just need to look at the first and last terms. In this case 1 is our first term and 7 is our last. This gives

$$\sum_{k=1}^{7}(-1)^{k+1}k^2 = 1^2 - 2^2 + 3^2 - 4^2 + 5^2 - 6^2 + 7^2.$$

For part (b), again addition and subtraction for summation notation. Here we have a fraction where the top piece increments by 1 each time and the bottom is the product of two terms also each incrementing by 1. The bottom terms are shifted forward by 1 and 2 increments respectively, this points towards a block $k/((k+1)(k+2))$. Now we also have the oscillating behavior which gives a $(-1)^k$ term. The bounds are from the first and last terms, so 2 for the first and 6 for the last. Putting this together gives

$$\sum_{k=2}^{6}\frac{(-1)^k k}{(k+1)(k+2)} = \frac{2}{3(4)} - \frac{3}{4(5)} + \frac{4}{5(6)} - \frac{5}{6(7)} + \frac{6}{7(8)}.$$

4. Compute the following

   (a) $4!/3!$ $4! = 4(3!)$, with cancellation, gives the answer of 4.

   (b) $6!/8!$ $8! = 8(7)(6!)$, so we can cancel to get $1/56$.

   (c) $n!/(n-2)!$ $n! = n(n-1)(n-2)!$, so we again cancel to get $n(n-1)$.

5. Prove the following by induction

   (a) $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$ for all $n \geq 1$.

   Proof. Proceed by induction, for the base case of $n = 1$ we have

   $$1^2 = 1 = \frac{1(2)(3)}{6}.$$

   For the inductive step, assume the result holds for some $n \geq 1$, then

   $$\begin{aligned} 1^2 + 2^2 + \cdots + n^2 + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \frac{2n^3 + 3n^2 + n}{6} + \frac{6n^2 + 12n + 6}{6} \\ &= \frac{2n^3 + 9n^2 + 13n + 6}{6} \\ &= \frac{(n+1)(n+2)(2n+3)}{6}. \end{aligned}$$

   □

(b) $\sum_{k=1}^{n+1} k2^k = n2^{n+2} + 2$.

Proof. Proceed by induction, for the base case of $n = 1$ we have

$$\sum_{k=1}^{2} k2^k = 1(2^1) + 2(2^2) = 10 = 1(2^{1+2}) + 2.$$

For the inductive step assume the result holds for some $n \geq 1$, then

$$\begin{aligned}\sum_{k=1}^{n+2} k2^k &= (n+2)2^{n+2} + \sum_{k=1}^{n+1} k2^k \\ &= (n+2)2^{n+2} + n2^{n+2} + 2 \\ &= (2n+2)2^{n+2} + 2 \\ &= (n+1)2^{n+3} + 2.\end{aligned}$$

□

(c) $\sum_{k=1}^{n} k(k!) = (n+1)! - 1$ for all $n \geq 1$.

Proof. Proceed by induction, for the base case of $n = 1$ we have

$$\sum_{k=1}^{1} k(k!) = 1(1!) = 1 = 2! - 1.$$

For the inductive step assume the result holds for some $n \geq 1$, then

$$\begin{aligned}\sum_{k=1}^{n+1} k(k!) &= (n+1)(n+1)! + \sum_{k=1}^{n} k(k!) \\ &= (n+1)(n+1)! + (n+1)! - 1 \\ &= (n+2)(n+1)! - 1 \\ &= (n+2)! - 1.\end{aligned}$$

□

5.3 Strong mathematical induction

Definition 5.3.1 (Principal of strong mathematical induction)**.** Let $P(n)$ be a property that is defined for integers n, and let a and b be fixed integers with $a \leq b$. Suppose the following two statements are true.

1. $P(a), P(a+1), \ldots, P(b)$ are all true
2. For every integer $k \geq b$, if $P(i)$ is true for each integer i from a to k, then $P(k+1)$ is true.

Then the statement

for every integer $n \geq a$, $P(n)$.

is true.

The main difference between standard induction and strong induction is the use of multiple base cases. Sometimes strong induction will also require cases in the inductive step.

Theorem 5.3.2. *Suppose that* $f_0,\ f_1,\ f_2, \ldots$ *is a sequence defined as follows:*

$$\begin{aligned} &f_0 = 5, f_1 = 16, \\ &f_k = 7f_{k-1} - 10f_{k-2} \quad \textit{for every integer } k \geq 2. \end{aligned}$$

Prove that $f_n = 3(2^n) + 2(5^n)$ *for each integer* $n \geq 0$.

Proof. Starting with the base cases, when $n = 0$ we have $f_0 = 5 = 3(2^0)+2(5^0)$. When $n = 1$ we have $f_1 = 16 = 3(2^1) + 2(5^1)$. For the inductive step, assume the result holds for some $k \geq 1$, then

$$\begin{aligned} f_{k+1} &= 7f_k - 10f_{k-1} \\ &= 7(3(2^k) + 2(5^k)) - 10(3(2^{k-1}) + 2(5^{k-1})) \\ &= (21 - 15)(2^k) + (14 - 4)(5^k) \\ &= 6(2^k) + 10(5^k) \\ &= 3(2^{k+1}) + 2(5^{k+1}) \end{aligned}$$

□

Exercises

1. Prove that, for every integer $n \geq 0$, $2^{2n} - 1$ is divisible by 3.

2. Prove that for every integer $n \geq 3$, $2n + 1 \leq 2^n$.

3. Suppose that $g_1, g_2, g_3, \ldots$ is a sequence defined as follows:

$$\begin{aligned} &g_1 = 3, \quad g_2 = 5 \\ &g_k = 3g_{k-1} - 2g_{k-2} \quad \text{for each integer } k \geq 3 \end{aligned}$$

   Prove that $g_n = 2^n + 1$ for every integer $k \geq 1$.

4. Suppose that $h_1, h_2, h_3, \ldots$ is a sequence defined as follows:

$$\begin{aligned} &h_0 = 1,\ h_1 = 2,\ h_2 = 3 \\ &h_k = h_{k-1} + h_{k-2} + h_{k-3} \quad \text{for each integer } k \geq 3 \end{aligned}$$

   Prove that $h_n \leq 3^n$ for every integer $n \geq 0$.

Solutions

1. Prove that, for every integer $n \geq 0$, $2^{2n} - 1$ is divisible by 3.

   Proof. Proceed by induction, for the base case $n = 0$ we have $2^0 - 1 = 0$ and 0 is divisible by 3. For the inductive step, we assume the result holds for $n \geq 0$, then following $2^{2n} - 1$ is divisible by 3 we will let $2^{2n} - 1 = 3k$ where $k \in \mathbb{Z}$. Now,

   $$\begin{aligned} 2^{2n+2} - 1 &= 4(2^{2n}) - 1 \\ &= 3(2^{2n}) + 2^{2n} - 1 \\ &= 3(2^{2n}) + 3k \\ &= 3(2^{2n} + k). \end{aligned}$$

   □

   Thus $2^{2n+2} - 1$ is divisible by 3.

2. Prove that for every integer $n \geq 3$, $2n + 1 \leq 2^n$.

   Proof. Proceed by induction, for the base case of $n = 3$ we have

   $$2(3) + 1 = 7 \leq 8 = 2^3.$$

   Now assume the result holds for some $n \geq 3$, then

   $$\begin{aligned} 2(n+1) + 1 &= 2n + 1 + 2 \\ &\leq 2^n + 2 \\ &\leq 2^n + 2^n \\ &= 2^{n+1}. \end{aligned}$$

   □

3. Suppose that $g_1, g_2, g_3, \ldots$ is a sequence defined as follows:

   $$\begin{aligned} &g_1 = 3, \quad g_2 = 5 \\ &g_k = 3g_{k-1} - 2g_{k-2} \qquad \text{for each integer } k \geq 3 \end{aligned}$$

   Prove that $g_n = 2^n + 1$ for every integer $k \geq 1$.

   Proof. Proceed by induction, we have two base cases here. For $k = 1$ we have

   $$g_1 = 3 = 2^1 + 1.$$

   For $k = 2$ we have

   $$g_2 = 5 = 2^2 + 1.$$

Now assume the result holds for $k \geq 2$, then

$$\begin{aligned} g_{k+1} &= 3g_k - 2g_{k-1} \\ &= 3(2^k + 1) - 2(2^{k-1} + 1) \\ &= 3(2^k) + 3 - 2^k - 2 \\ &= 2(2^k) + 1 \\ &= 2^{k+1} + 1. \end{aligned}$$

□

4. Suppose that $h_1, h_2, h_3, \ldots$ is a sequence defined as follows:

$$\begin{aligned} &h_0 = 1,\ h_1 = 2,\ h_2 = 3 \\ &h_k = h_{k-1} + h_{k-2} + h_{k-3} \quad \text{for each integer } k \geq 3 \end{aligned}$$

Prove that $h_n \leq 3^n$ for every integer $n \geq 0$.

Proof. Proceed by induction, we have three base cases here, $n = 0, 1, 2$. Checking these base cases gives

$$\begin{aligned} n = 0 &\implies 1 \leq 3^0 \\ n = 1 &\implies 2 \leq 3^1 \\ n = 2 &\implies 3 \leq 3^2. \end{aligned}$$

Assume the result holds for $n \geq 2$, then

$$\begin{aligned} h_{n+1} &= h_n + h_{n-1} + h_{n-2} \\ &\leq 3^n + 3^{n-1} + 3^{n-2} \\ &\leq 3^n + 3^n + 3^n \\ &= 3^{n+1}. \end{aligned}$$

□

5.4 Solving recurrence relations by iteration

A recurrence relation is a sequence that is defined recursively.

Example 5.4.1. Let $a_0, a_1, \ldots$ be a sequence defined recursively as follows,

$$\begin{aligned} a_0 &= 1 \\ a_k &= a_{k-1} + 2. \end{aligned}$$

We can write out some terms of this relation which are

$$\begin{aligned} a_0 &= 1 \\ a_1 &= a_0 + 2 = 3 \\ a_2 &= a_1 + 2 = a_0 + 2 + 2 = 5. \end{aligned}$$

△

One common thing we want to do with a recurrence relation is solving it for an explicit formula. In the example above, we get that $a_n = 1 + 2n$. With an explicit formula, it is much easier to compute distant terms in the sequence.

Definition 5.4.2. A sequence $a_0, a_1, a_2, \ldots$ is called an **arithmetic sequence** if and only if there is a constant d such that

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

Then

$$a_n = a_0 + dn.$$

Definition 5.4.3. A sequence $a_0, a_1, a_2, \ldots$ is called a **geometric sequence** if and only if there is a constant r such that

$$a_k = ra_{k-1}.$$

Then it follows that

$$a_n = a_0 r^n.$$

In this section, to solve a recurrence relation, we are going to use the method of iteration. To do this, we will write out the first few values of the sequence, then guess what the formula should be. Once you have your guess, use induction to try and prove that it is correct.

Exercises

1. The following sequences are defined recursively. Use iteration to guess a formula, then use induction (or strong induction) to prove the guess.
   (a) $p_k = p_{k-1} + 2(3^k)$, for each integer $k \geq 2$, and $p_1 = 2$.
   (b) $d_k = 2d_{k-1} + 3$, for each integer $k \geq 2$, and $d_1 = 2$.
   (c) $s_k = 2s_{k-2}$, for each integer $k \geq 2$, $s_0 = 1$, and $s_1 = 2$.
   (d) $w_k = w_{k-2} + k$, for each integer $k \geq 3$, $w_1 = 1$, and $w_2 = 2$.

Solutions

1. The following sequences are defined recursively. Use iteration to guess a formula, then use induction (or strong induction) to prove the guess.
   (a) $p_k = p_{k-1} + 2(3^k)$, for each integer $k \geq 2$, and $p_1 = 2$.
   Let's start by checking some cases:

$$p_1 = 2$$
$$p_2 = p_1 + 2(3^2) = 2 + 2(3^2) = 20$$
$$p_3 = p_2 + 2(3^3) = 2 + 2(3^2) + 2(3^3) = 74$$
$$p_4 = p_3 + 2(3^4) = 2 + 2(3^2) + 2(3^3) + 2(3^4) = 236.$$

From this it seems that

$$p_n = -6 + 2\sum_{k=0}^{n} 3^k.$$

Notice that the -6 comes from adding $2(3^1)$ into the sum. As is a good exercise to show

$$\sum_{k=0}^{n} 3^k = 3^{n+1} - 1.$$

This gives that the claimed solution to the sequence is

$$p_n = 3^{n+1} - 7.$$

Next, we need to prove our guess

Proof. Proceed by induction, for the base case of $n = 1$ we have

$$p_1 = 2 = 3^2 - 7.$$

For the inductive step assume the result holds for some $n \geq 1$, then

$$\begin{aligned} p_{n+1} &= p_n + 2(3^{n+1}) \\ &= 3^{n+1} - 7 + 2(3^{n+1}) \\ &= 3(3^{n+1}) - 7 \\ &= 3^{n+2} - 7. \end{aligned}$$

□

(b) $d_k = 2d_{k-1} + 3$, for each integer $k \geq 2$, and $d_1 = 2$.
Start by checking some cases:

$$\begin{aligned} d_1 &= 2 \\ d_2 &= 2d_1 + 3 = 2^2 + 3 = 7 \\ d_3 &= 2d_2 + 3 = 2^3 + 2(3) + 3 = 17 \\ d_4 &= 2d_3 + 3 = 2^4 + 2^2(3) + 2(3) + 3 \\ d_5 &= 2d_4 + 3 = 2^5 + 2^3(3) + 2^2(3) + 2(3) + 3. \end{aligned}$$

From this it seems that

$$d_n = 2^n + 3\sum_{k=1}^{n} 2^k = 2^n + 3(2^{n-1}) - 3 = 5(2^{n-1}) - 3.$$

Now to prove the guess.

Proof. Proceed by induction, for the base case of $n = 1$, we have that

$$d_1 = 2 = 5(2^0) - 3.$$

For the inductive step assume the result holds for some $n \geq 1$, then

$$\begin{aligned} d_{n+1} &= 2d_n + 3 \\ &= 2(5(2^{n-1}) - 3) + 3 \\ &= 5(2^n) - 6 + 3 \\ &= 5(2^n) - 3. \end{aligned}$$

□

(c) $s_k = 2s_{k-2}$, for each integer $k \geq 2$, $s_0 = 1$, and $s_1 = 2$.
Start by checking some cases:

$$\begin{aligned} s_0 &= 0 \\ s_1 &= 2 \\ s_2 &= 2s_0 = 2 \\ s_3 &= 2s_1 = 2^2 = 4 \\ s_4 &= 2s_2 = 2^2 = 4. \end{aligned}$$

From this it seems our sequence is multiplying by two every other step. We can use the floor function to represent this behavior. This gives the guess of

$$s_n = 2^{\lfloor (n+1)/2 \rfloor}.$$

Now to prove this we need strong induction.

Proof. Proceed by induction, for the base cases of $n = 0$ and $n = 1$ we have that

$$\begin{aligned} s_0 &= 0 = 2^{\lfloor 1/2 \rfloor} \\ s_1 &= 2 = 2^{\lfloor 2/2 \rfloor}. \end{aligned}$$

For the inductive step assume the result holds for some $n \geq 1$, then we have

$$\begin{aligned} s_{n+1} &= 2s_{n-1} \\ &= 2\left(2^{\lfloor n/2 \rfloor}\right) \\ &= 2^{\lfloor (n+2)/2 \rfloor}. \end{aligned}$$

□

(d) $w_k = w_{k-2} + k$, for each integer $k \geq 3$, $w_1 = 1$, and $w_2 = 2$.

Start by checking some cases:

$$\begin{aligned}
w_1 &= 1 \\
w_2 &= 2 \\
w_3 &= w_1 + 3 = 4 \\
w_4 &= w_2 + 4 = 6 \\
w_5 &= w_3 + 5 = w_1 + 3 + 5 = 1 + 3 + 5 = 9 \\
w_6 &= w_4 + 6 = w_2 + 4 + 6 = 2 + 4 + 6 = 12.
\end{aligned}$$

From this it seems that w_k is the sum of the first $k-1$ even numbers if k is even or the sum of the first $k-1$ odd numbers if k is odd. There is a nice formula for both of these, which is

$$w_n = \begin{cases} (k+1)^2 & \text{if } n = 2k+1 \\ k(k+1) & \text{if } n = 2k \end{cases}.$$

Proof. Starting with the base case $n = 1$ implies $n = 2(0) + 1$ so k is 0 and we have $w_1 = 1 = 1^2$. For the other base case of $n = 2$ we have $n = 2(1)$ giving that $k = 1$. Putting that into the formula gives $w_2 = 2 = (1)(2)$.
Moving to the inductive step, assume the result holds for some $n \geq 1$, then we will proceed by cases. If $n - 1 = 2k$ for some $k \in \mathbb{Z}$, then

$$\begin{aligned}
w_{n+1} &= w_{n-1} + n + 1 \\
&= k(k+1) + 2k + 2 \\
&= k^2 + 3k + 2 \\
&= (k+1)(k+2).
\end{aligned}$$

If $n - 1 = 2k + 1$ for some $k \in \mathbb{Z}$, then

$$\begin{aligned}
w_{n+1} &= w_{n-1} + n + 1 \\
&= (k+1)^2 + 2k + 3 \\
&= k^2 + 4k + 4 \\
&= (k+2)^2.
\end{aligned}$$

□

Chapter 6

Set theory

6.1 Definitions of sets

Recall the following from section 1.2.

Definition 6.1.1. A set is defined as a collection of elements. These elements can be (almost) anything, including other sets. There is no implicit order to the elements of a set, and duplicates are ignored.

Definition 6.1.2. One way to build sets is with **set-roster notation**, which is where we list all elements of the set or list the first few once the pattern is clear to the reader. For example, $\{1, 2, 3\}$ and $\{1, 2, 3, \dots\}$.

Another way to build sets is with **set-builder notation**, which is written as $\{x \in S \mid P(x)\}$ this is read as "x in S such that $P(x)$ is true" where $P(x)$ is some property of the statement that x must satisfy. For example, $\{x \in \mathbb{R} \mid x \geq 3\}$ which is the set of all real numbers that are greater than or equal to 3. Note that instead of the $\mid$ it is also common to use, $:$ this can be especially helpful in situations involving absolute values like $\{x \in \mathbb{R} : |x| < 1\}$.

The most common sets when working with numbers are $\mathbb{N}$ the natural numbers, $\mathbb{Z}$ the integers, $\mathbb{Q}$ the rational numbers, and $\mathbb{R}$ the real numbers. The book will exclude using $\mathbb{N}$ because it has two definitions that are used about the same, which are the nonnegative integers and the positive integers. The integers are the whole numbers, including negatives. We will use $\mathbb{Z}^+$ for the positive integers and $\mathbb{Z}^{\geq 0}$ for the nonnegative integers. A new set we care about is the **empty set**, which is defined to be the set of no elements, it is denoted $\emptyset$.

When working with sets, we often care about the idea of a **subset**, which is defined as a set that contained in another set and is denoted $A \subseteq B$. If this containment is strict, that is B contains more elements then A, we write $A \subset B$ and this is called a **proper subset**.

Two sets are called equal if and only if they contain all the same elements.

With our knowledge of proofs, we can now prove things about sets. The first is how to prove subsets and equality between sets.

Procedure 6.1.3. Given sets, A, B to prove that, $A \subseteq B$ we need to show for any element in A that element is in B. The standard way to do this is

1. Suppose that a is an unknown, but particular element of A.
2. Show that a is an element of B.

△

Procedure 6.1.4. Given sets A, B the standard way to prove that, $A = B$ is to prove $A \subseteq B$ and that $B \subseteq A$. △

Definition 6.1.5 (Common set operations)**.** Let A and B be subsets of a universal set U.

1. The **union** of A and B, denoted $A \cup B$, is the set of all elements that are in at least one of A or B.
2. The **intersection** of A and B, denoted $A \cap B$, is the set of all elements that are common to both A and B.
3. The **difference** of B minus A, denoted $B - A$, is the set of all elements that are in B and not in A.
4. The **complement** of A, denoted A^c, is the set of all elements in U that are not in A.

Definition 6.1.6 (Unions and intersections of an indexed collection of sets)**.** Given sets $A_0, A_1, A_2, \dots$ that are subsets of a universal set U and given a nonnegative integer n,

$$\bigcup_{i=0}^{n} A_i = \{x \in U | x \in A_i \text{ for some } i = 0, 1, \dots, n\}$$
$$\bigcap_{i=0}^{n} A_i = \{x \in U | x \in A_i \text{ for every } i = 0, 1, \dots, n\}.$$

Definition 6.1.7 (Interval notation)**.** Given real numbers a and b with $a \leq b$:

$$(a, b) = \{x \in \mathbb{R} | a < x < b\} \qquad [a, b] = \{x \in \mathbb{R} | a \leq x \leq b\}$$
$$(a, b] = \{x \in \mathbb{R} | a < x \leq b\} \qquad [a, b) = \{x \in \mathbb{R} | a \leq x < b\}.$$

Definition 6.1.8. Two sets are called **disjoint** if and only if they have no elements in common.

We can extend this definition to a list of sets $A_1, A_2, A_3, \dots$ and say that all the A_i sets are **mutually disjoint** if all pairs of the sets are disjoint.

Definition 6.1.9. A collection of nonempty sets $\{A_1, A_2, \dots\}$ is a **partition** of a set A if and only if

1. A is the union of all the A_i
2. The sets $A_1, A_2, \dots$ are mutually disjoint.

Definition 6.1.10. Given a set A, the **power set** of A, denoted $\mathcal{P}(A)$, is the set of all subsets of A.

Exercises

1. Let

$$A = \{x \in \mathbb{Z} | x = 10b - 3 \text{ for some integer } b\}$$
$$B = \{z \in \mathbb{Z} | z = 18c + 16 \text{ for some integer } c\}.$$

   Prove or give a counter example to $A \subset B$, $B \subset A$, and $A = B$.

2. Is $\{\{a, d, e\}, \{b, c\}, \{d, f\}\}$ a partition of $\{a, b, c, d, e, f\}$. If so, justify. If not how can you make it one?

3. Let $A = \{1, 2\}$ and $B = \{2, 3\}$, then find the following.

   (a) $\mathcal{P}(\emptyset)$.

   (b) $\mathcal{P}(A)$.

   (c) $\mathcal{P}(A \cap B)$.

   (d) $\mathcal{P}(A \cup B)$.

4. Given a set A has n elements, make a guess on how many elements will $\mathcal{P}(A)$ have?

Solutions

1. Let

$$A = \{x \in \mathbb{Z} | x = 10b - 3 \text{ for some integer } b\}$$
$$B = \{z \in \mathbb{Z} | z = 18c + 16 \text{ for some integer } c\}.$$

   Prove or give a counter example to $A \subseteq B$, $B \subseteq A$, and $A = B$.

   We know $-3 \in A$ since $-3 = 10(0) - 3$. For -3 to be in B we need $-3 = 18c + 16 \implies -19 = 18c$ for some integer $c \in \mathbb{Z}$. However, this is a contradiction since -19 is not divisible by 18. This gives that A is not a subset of B. Note this also shows that A is not equal to B.

   Taking a similar approach to showing that B is not a subset of A. Let $16 \in B$, then for 16 to be in A we need $16 = 10b - 3 \implies 19 = 10b$. However, this can't happen since 19 is not divisible by 10.

2. Is $\{\{a, d, e\}, \{b, c\}, \{d, f\}\}$ a partition of $\{a, b, c, d, e, f\}$. If so, justify. If not, how can you make it one?

   This is not a partition. While the sets $\{a, d, e\}, \{b, c\}, \{d, f\}$ do union to $\{a, b, c, d, e, f\}$, we have a duplicate d in sets $\{d, f\}$ and $\{a, d, e\}$.

   To fix this, we can simply remove the duplicate d. An example would be $\{\{a, d, e\}, \{b, c\}, \{f\}\}$.

3. Let $A = \{1, 2\}$ and $B = \{2, 3\}$, then find the following.

(a) $\mathcal{P}(\emptyset)$

Note that the power set is a set containing sets and that it always contains the set itself. In this case, that is the only subset giving

$$\mathcal{P}(\emptyset) = \{\emptyset\}.$$

(b) $\mathcal{P}(A)$.

$$\mathcal{P}(A) = \{\{1,2\},\{1\},\{2\},\emptyset\}.$$

(c) $\mathcal{P}(A \cap B)$.

$$\mathcal{P}(A \cap B) = \{\{2\},\emptyset\}.$$

(d) $\mathcal{P}(A \cup B)$.

$$\mathcal{P}(A) = \{\{1,2,3\},\{1,2\},\{1,3\},\{2,3\},\{1\},\{2\},\{3\},\emptyset\}.$$

4. Given a set A has n elements, make a guess on how many elements will $\mathcal{P}(A)$ have?

   From the previous example we can see that $\mathcal{P}(\emptyset)$ has 1 element; if A has 1 element, then $\mathcal{P}(A)$ has 2; if A has two elements, then $\mathcal{P}(A)$ has 4; and if A has three elements, then $\mathcal{P}(A)$ has 8.

   This would lead to the guess that if A has n elements, then the power set has 2^n elements. We will talk about a proof in a later section.

6.2 Properties of sets

Theorem 6.2.1 (Set inclusion principals)**.** *Let A, B, C be sets, then*

1. $A \cap B \subseteq A$
2. $A \subseteq A \cup B$
3. *If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.*

Theorem 6.2.2 (Set Identities)**.** *Let $A, B, C \subset U$ where U is the universal set, then*

1. *Commutative laws:*

$$A \cup B = B \cup A \text{ and } A \cap B = B \cap A.$$

2. *Associative laws:*

$$(A \cup B) \cup C = A \cup (B \cup C) \text{ and } (A \cap B) \cap C = A \cap (B \cap C).$$

3. *Distributive laws:*

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

and

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

4. *Identity laws:*

$$A \cup \emptyset = A \text{ and } A \cap U = A.$$

5. *Complement laws:*

$$A \cup A^c = U \text{ and } A \cap A^c = \emptyset.$$

6. *Double complement law:*

$$(A^c)^c = A.$$

7. *Idempotent laws:*

$$A \cup A = A \text{ and } A \cap A = A.$$

8. *Universal bound laws:*

$$A \cup U = U \text{ and } A \cap \emptyset = \emptyset.$$

9. *De Morgan's laws:*

$$(A \cup B)^c = A^c \cap B^c \text{ and } (A \cap B)^c = A^c \cup B^c.$$

10. *Absorption laws:*

$$A \cup (A \cap B) = A \text{ and } A \cap (A \cup B) = A.$$

11. *Complements of U and $\emptyset$:*

$$U^c = \emptyset \text{ and } \emptyset^c = U.$$

12. *Set difference law:*

$$A - B = A \cap B^c.$$

Theorem 6.2.3. *Let A be a set, then $\emptyset \subseteq A$.*

Theorem 6.2.4. *For all sets A, B, C, if $A \subseteq B$ and $B \subseteq C^c$, then $A \cap C = \emptyset$.*

6.3 Disproofs and algebraic proofs

One way to think of set relations is as a for all statement. That is for all sets we have this relation. So, to disprove a set relation we need to construct a counterexample.

Example 6.3.1. Disprove the following. For all sets A, B, C we have

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

To start building the counterexample think about what each side is saying. On the right we have A with everything from C removed. However on the left we have A with everything from B removed or B with everything from C removed. So if we have an element in C that is in A but not in B then it will break our equality. For example

$$\begin{aligned} A &= \{1\} \\ B &= \{2\} \\ C &= \{1\} \\ (A - B) \cup (B - C) &= \{1, 2\} \\ (A - C) &= \emptyset. \end{aligned}$$

△

Theorem 6.3.2. *Let $n \in \mathbb{Z}$ such that $n \geq 0$, if X is a set with n elements, then $\mathscr{P}(X)$ has 2^n elements.*

Proof. Let $n = 0$, then X is the set with no elements so its only subset is itself giving $\mathscr{P}(X)$ has 1 element. Now assume the result holds for some $m \geq 0$. If X has $m + 1$ elements, then it has at least one element $z \in X$. Consider $X - \{z\}$ this is a set with m elements so by our induction hypothesis $\mathscr{P}(X - \{z\})$ has 2^m subsets. Now to build $\mathscr{P}(X)$ we can either add z to each subset in $\mathscr{P}(X - \{z\})$ or not. This gives two possible choices for each element. Thus $\mathscr{P}(X)$ has $2(2^m) = 2^{m+1}$ elements. □

Exercises

1. Let $\mathbb{R}$ be the universal set and let

$$A = \{x \in \mathbb{R} \mid -3 \leq x \leq 0\},$$
$$B = \{x \in \mathbb{R} \mid -1 < x < 2\},$$
$$C = \{x \in \mathbb{R} \mid 6 < x \leq 8\}.$$

   Find the following

   (a) $A \cup B$
   (b) B^c
   (c) $A^c \cap B^c$
   (d) $(A \cap B)^c$

2. Prove the following

   (a) $(A - B) \cup (C - B) = (A \cup C) - B$
   (b) $A \cap (B - C) \subseteq (A \cap B) - (A \cap C)$
   (c) If $A \subseteq B$, then $B^c \subseteq A^c$.
   (d) $A \cap A^c = \emptyset$.

3. Find a counterexample to the following

   (a) $(A \cup B) \cap C = A \cup (B \cap C)$
   (b) If $B \cup C \subseteq A$, then $(A - B) \cap (A - C) = \emptyset$.

Solutions

1. Let $\mathbb{R}$ be the universal set and let

$$A = \{x \in \mathbb{R} \mid -3 \leq x \leq 0\},$$
$$B = \{x \in \mathbb{R} \mid -1 < x < 2\},$$
$$C = \{x \in \mathbb{R} \mid 6 < x \leq 8\}.$$

   Find the following

   (a) $A \cup B$ $[-3, 2)$ or $\{x \in \mathbb{R} \mid -3 \leq x < 2\}$.
   (b) B^c $(-\infty, -1] \cup [2, \infty)$ or $\{x \in \mathbb{R} \mid x \leq -1 \text{ or } x \geq 2\}$.
   (c) $A^c \cap B^c$ $(-\infty, -3] \cup [2, \infty)$
   (d) $(A \cap B)^c$ $(-\infty, -1] \cup (0, \infty)$

2. Prove the following

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

Proof.

$$\begin{aligned}(A - B) \cup (C - B) &= (A \cap B^c) \cup (C \cap B^c) && \text{(Set difference law)}\\ &= (A \cup C) \cap B^c && \text{(Distributive law)}\\ &= (A \cup C) - B. && \text{(Set difference law)}\end{aligned}$$

□

(b) $A \cap (B - C) \subseteq (A \cap B) - (A \cap C)$

Proof.

$$\begin{aligned}A \cap (B - C) &= A \cap (B \cap C^c)\\ &\subseteq (A \cap B) \cup C^c\\ &= \emptyset \cup ((A \cap B) \cup C^c)\\ &= ((A \cap B) \cap A^c) \cup ((A \cap B) \cup C^c)\\ &= (A \cap B) \cap (A^c \cup C^c)\\ &= (A \cap B) \cap (A \cap C)^c\\ &= (A \cap B) - (A \cap C)\end{aligned}$$

□

(c) If $A \subseteq B$, then $B^c \subseteq A^c$.

Proof. Let $x \in B^c$, then $x \notin B$ by the definition of set complement. Following $A \subseteq B$ we get that $x \notin A$. Thus by the definition of set complement $x \in A^c$. □

(d) $A \cap A^c = \emptyset$.

Proof.

$$\begin{aligned}A \cap A^c &= A - A && \text{(Set difference law)}\\ &= \emptyset.\end{aligned}$$

□

3. Find a counterexample to the following

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

$$\begin{aligned}&A = \{1\},\ B = \{2\},\ C = \{3\}\\ &(A \cup B) \cap C = \emptyset\\ &A \cup (B \cap C) = \{1\}.\end{aligned}$$

(b) If $B \cup C \subseteq A$, then $(A - B) \cap (A - C) = \emptyset$.

$$A = \{1\},\ B = \emptyset,\ C = \emptyset$$
$$B \cup C = \emptyset \subseteq A$$
$$(A - B) \cap (A - C) = \{1\}.$$

Chapter 8

Relations

8.1 Properties of relations

Definition 8.1.1. Let A and B be sets A relation R from A to B is a subset of $A \times B$. We use xRy to mean $(x, y) \in R$. The set A is called the domain and B is called the co-domain.

Definition 8.1.2. Let R be a relation from A to B. Define the inverse relation R^{-1} from B to A as

$$R^{-1} = \{(y, x) \in B \times A \mid (x, y) \in R\}.$$

Example 8.1.3. Let $A = \{2, 3, 4\}$ and $B = \{2, 6, 8\}$, then

$$A \times B = \{(2, 2), (2, 6), (2, 8), (3, 2), (3, 6), (3, 8), (4, 2), (4, 6), (4, 8)\}.$$

If we have

$$R = \{(2, 2), (2, 6), (2, 8), (3, 6), (4, 8)\},$$

then

$$R^{-1} = \{(2, 2), (6, 2), (8, 2), (6, 3), (8, 4)\}.$$

△

Definition 8.1.4. A relation on a set A is a relation from A to A.

Definition 8.1.5. Given sets $A_1, A_2, \ldots, A_n$ an n-ary relation R is a subset of $A_1 \times \cdots \times A_n$.

8.2 Reflexivity, Symmetry, and Transitivity

Definition 8.2.1. Let R be a relation on a set A.

1. R is **reflexive** if and only if for every $x \in A$, xRx.

2. R is **symmetric** if and only if for every $x, y \in A$, if xRy then yRx.

3. R is **transitive** if and only if for every $x, y, z \in A$, if xRy and yRz then xRz.

Example 8.2.2. Let $A = \{0, 1, 2, 3\}$ and define the following relations

$$R = \{(0,0), (0,1), (0,3), (1,0), (1,1), (2,2), (3,0), (3,3)\},$$
$$S = \{(0,1), (2,3)\},$$
$$T = \{(0,0)\}.$$

Are R, S, T transitive, reflexive or symmetric?

R is reflexive and is symmetric, but is not transitive since $(1,0) \in R$ and $(0,3) \in R$, but $(1,3) \notin R$.

S is not reflexive since $(0,0) \notin S$. S is not symmetric since $(0,1) \in S$, but $(1,0) \notin S$. S is transitive since there are no points such that $(x,y) \in S$ and $(y,z) \in S$.

T is transitive, is not reflexive and symmetric. △

Example 8.2.3. Let R be a relation on the real numbers where xRy if and only if $x = y$, then R is symmetric, reflexive, and transitive. △

Definition 8.2.4. Let A be a set and R a relation on A. The **transitive closure** of R is the relation R^t on A that satisfies the following three properties:

1. R^t is transitive.

2. $R \subseteq R^t$.

3. If S is any other transitive relation that contains R, then $R^t \subseteq S$.

Example 8.2.5. Let $A = \{0, 1, 2, 3\}$ and consider R defined on A as follows:

$$R = \{(0,1), (1,2)\}.$$

Then

$$R^t = \{(0,1), (1,2), (0,2)\}.$$

△

Exercises

1. Let $A = \{-1, 1, 2, 4\}$ and $B = \{1, 2\}$ and define relations R and S from A to B as follows: For every $(x, y) \in A \times B$.

$$(x, y) \in R \iff |x| = |y|$$
$$(x, y) \in S \iff x - y \text{ is even.}$$

   State which ordered pairs are in $A \times B$, R, S, $R \cup S$, and $R \cap S$.

2. Let C be the circle relation on the set of real numbers: For every $x, y \in \mathbb{R}$, $(x, y) \in C$ if and only if $x^2 + y^2 = 1$. Determine if C is reflexive, transitive, and symmetric.

3. If R and S are reflexive, then is $R \cap S$ reflexive?

4. If R and S are reflexive, then is $R \cup S$ reflexive?

5. Let R be defined on the set $A = \{0, 1, 2, 3\}$ such that

$$R = \{(0, 1), (0, 2), (1, 1), (1, 3), (2, 2), (3, 0)\}.$$

   Find the transitive closure of R.

Solutions

1. Let $A = \{-1, 1, 2, 4\}$ and $B = \{1, 2\}$ and define relations R and S from A to B as follows: For every $(x, y) \in A \times B$.

$$(x, y) \in R \iff |x| = |y|$$
$$(x, y) \in S \iff x - y \text{ is even.}$$

   State which ordered pairs are in $A \times B$, R, S, $R \cup S$, and $R \cap S$.

$$\begin{aligned} A \times B &= \{(-1, 1), (-1, 2), (1, 1), (1, 2), (2, 1), (2, 2), (4, 1), (4, 2)\} \\ R &= \{(-1, 1), (1, 1), (2, 2)\} \\ S &= \{(-1, 1), (1, 1), (2, 2), (4, 2)\} \\ R \cup S &= \{(-1, 1), (1, 1), (2, 2), (4, 2)\} \\ R \cap S &= \{(-1, 1), (1, 1), (2, 2)\}. \end{aligned}$$

2. Let C be the circle relation on the set of real numbers: For every $x, y \in \mathbb{R}$, $(x, y) \in C$ if and only if $x^2 + y^2 = 1$. Determine if C is reflexive, transitive, and symmetric.

   C is not reflexive, consider $(1, 1) \notin C$.

C is symmetric, since x and y are real numbers so we can swap any (x, y) with (y, x).

C is not transitive. Let $x = 1$, $y = 0$, and $z = 1$, then $(x, y) \in C$ and $(y, z) \in C$, but $(x, z) \notin C$.

3. If R and S are reflexive, then is $R \cap S$ reflexive?

   Yes, since R and S are reflexive, then they both must contain $(x, x) \in A \times A$ for every $x \in A$. So their intersection still contains all those pairs.

4. If R and S are reflexive, then is $R \cup S$ reflexive?

   Yes, similar reasoning to the previous question.

5. Let R be defined on the set $A = \{0, 1, 2, 3\}$ such that

$$R = \{(0, 1), (0, 2), (1, 1), (1, 3), (2, 2), (3, 0)\}.$$

   Find the transitive closure of R.

$R^t = \{(0, 1), (0, 2), (1, 1), (1, 3), (2, 2), (3, 0), (0, 3), (3, 2), (3, 1), (1, 0), (1, 2)\}$

8.3 Equivalence relations

Definition 8.3.1. Given a partition of a set A, the **relation induced by the partition**, R, is defined on A as follows: For every $x, y \in A$, $(x, y) \in R$ if x and y are contained in the same subset of the partition.

Example 8.3.2. Let $A = \{0, 1, 2, 3, 4\}$ and consider the partition

$$\{0, 3, 4\},\ \{1\},\ \{2\}.$$

The relation R induced by this partition is

$$\{(0, 0), (0, 3), (0, 4), (3, 0), (3, 3), (3, 4), (4, 0), (4, 3), (4, 4), (1, 1), (2, 2)\}$$

△

Theorem 8.3.3. *Let A be a set with a partition and let R be the relation induced by the partition. Then R is reflexive, symmetric, and transitive.*

Definition 8.3.4. Let A be a set and R a relation on A, then R is an **equivalence relation** if and only if R is reflexive, symmetric, and transitive.

Note that the above theorem and definition can be combined since they connected with if and only if statements. So we could say that R is an equivalence relation on a set A if and only if R is a relation induced by a partition of A.

Using this if you are asked to show a relation is an equivalence relation one option is to show that there exists a partition of the set such that the relation is induced on it.

Definition 8.3.5. Suppose A is a set and R is an equivalence relation on A. For each element $a \in A$, the **equivalence class of** a, denoted $[a]$ is the set of all elements $x \in A$ such that $(x, a) \in R$. The element a is called the **representative** for the equivalence class $[a]$.

Another way to think about equivalence classes is with partitions. If we have a set A and a partition, then for some $a \in A$ the equivalence class $[a]$ is the set in the partition where a is in.

Example 8.3.6. Let $A = \{0, 1, 2, 3, 4\}$ with the partition

$$\{0, 3, 4\},\ \{1\},\ \{2\},$$

then the equivalence classes of A are

$$\begin{aligned}[0] = [3] = [4] &= \{0, 3, 4\} \\ [1] &= \{1\} \\ [2] &= \{2\}.\end{aligned}$$

△

Example 8.3.7. Consider $\mathbb{Z}$ which can be partitioned into the even and odd numbers, then the equivalence classes of that partition are

$$\begin{aligned}[0] &= \{\ldots, -4, -2, 0, 2, 4, \ldots\} \\ [1] &= \{\ldots, -3, -1, 1, 3, \ldots\}.\end{aligned}$$

We can also write

$$\mathbb{Z} = [0] \cup [1].$$

△

Lemma 8.3.8. *Suppose A is a set, R is an equivalence relation on A, and $a, b \in A$. If $(a, b) \in R$, then $[a] = [b]$.*

Lemma 8.3.9. *Suppose A is a set, R is an equivalence relation on A, and $a, b \in A$. Either $[a] \cap [b] = \emptyset$ or $[a] \cap [b] = [a]$.*

Definition 8.3.10. Let $m, n \in \mathbb{Z}$ and let $d \in \mathbb{Z}^+$. We say that m is **congruent** to n modulo d and write

$$m \equiv n \bmod d$$

if and only if

$$d \mid (m - n).$$

Using the definition above we can form partitions of the integers with congruence equivalence classes. We already saw this with the even and odd integers where they are congruent modulo 2.

Example 8.3.11. Let $d \in \mathbb{Z}^+$ and let R be the relation defined by

$$(x, y) \in R \iff x \equiv y \bmod d,$$

then R is an equivalence relation. △

Example 8.3.12. Let $A = \mathbb{Z} \times (\mathbb{Z} - \{0\})$, then define the relation

$$((a, b), (c, d)) \in R \iff \frac{a}{b} = \frac{c}{d} \iff ad = bc.$$

This relation R is an equivalence class and is a way to define the rational numbers. Consider

$$\left[\frac{1}{2}\right] = \left\{\frac{1}{2}, \frac{2}{4}, \frac{3}{6}, \dots\right\}$$

△

Exercises

1. Let $X = \{-1, 0, 1\}$, let $A = \mathscr{P}(X)$, and define R to be a relation on A such that

   $(s, t) \in R \iff$ the sum of the elements in s equals the sum of the elements in t.

   Find the distinct equivalence classes of R.

2. Let $A = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$ and define R on A to be

   $$(m, n) \in R \iff 4|(m^2 - n^2).$$

   Find the distinct equivalence classes of R.

3. Let $A = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$ and define R on A to be

   $$(m, n) \in R \iff 5|(m^2 - n^2).$$

   Find the distinct equivalence classes of R.

Solutions

1. Let $X = \{-1, 0, 1\}$, let $A = \mathscr{P}(X)$, and define R to be a relation on A such that

   $(s, t) \in R \iff$ the sum of the elements in s equals the sum of the elements in t.

   Find the distinct equivalence classes of R.

   First building $\mathscr{P}(X)$ we get

   $$\mathscr{P}(x) = \{\{-1\}, \{0\}, \{1\}, \{-1, 0\}, \{-1, 1\}, \{0, 1\}, \{-1, 0, 1\}, \emptyset\}.$$

Remember the trick to checking your work on the power set is there should be 2^n elements, so in this case 8 subsets.

Now to build the equivalence classes we could find all entrys the are related. However for this problem we can assume the relation R is an equivalence relation, so just start building the equivalence classes. So $[\{-1\}]$ is the equivalence class where the sum of the entries is -1 which gives

$$[\{-1\}] = \{\{-1\}, \{0, -1\}\}.$$

To get the next equivalence class take an element of $\mathscr{P}(X)$ that is not in $[\{-1\}]$ like $[\{0\}]$ which gives

$$[\{0\}] = \{\{0\}, \{-1, 1\}, \{-1, 0, 1\}\}.$$

The next element that is not in $[\{-1\}]$ or $[\{0\}]$ is $\{1\}$, so we can build

$$[\{1\}] = \{\{1\}, \{0, 1\}\}.$$

Finally, we are missing $\emptyset$, so we give it its own equivalence class. This gives

$$\begin{aligned} [\{-1\}] &= \{\{-1\}, \{0, -1\}\} \\ [\{0\}] &= \{\{0\}, \{-1, 1\}, \{-1, 0, 1\}\} \\ [\{1\}] &= \{\{1\}, \{0, 1\}\} \\ [\emptyset] &= \{\emptyset\}. \end{aligned}$$

as our distinct equivalence classes.

2. Let $A = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$ and define R on A to be

$$(m, n) \in R \iff 4|(m^2 - n^2).$$

Find the distinct equivalence classes of R.

Similar to last time we can assume R is an equivalence relation and just start building the classes. So take -4 and we want to find which numbers are related. This gives

$$[-4] = \{-4, -2, 0, 2, 4\}.$$

Removing those from A the next element not in $[-4]$ is

$$[-3] = \{-3, -1, 1, 3\}$$

These two equivalence classes cover all the elements.

3. Let $A = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$ and define R on A to be

$$(m, n) \in R \iff 5|(m^2 - n^2).$$

Find the distinct equivalence classes of R.

Similar to the last problem start with -4 giving

$$[-4] = \{-4, -1, 1, 4\}.$$

The next element not in $[-4]$ is

$$[-3] = \{-3, -2, 2, 3\}.$$

The last element we are missing is 0 so the distinct equivalence classes are

$$[-4] = \{-4, -1, 1, 4\}$$
$$[-3] = \{-3, -2, 2, 3\}$$
$$[0] = \{0\}.$$

8.5 Partial order relations

Definition 8.5.1. Let R be a relation on a set A. R is **antisymmetric** if and only if

$$\forall a, b \in A, \text{if } aRb \text{ and } bRa \text{ then } a = b.$$

Definition 8.5.2. Let R be a relation defined on a set A. R is a **partial order relation** if and only if R is reflexive, antisymmetric, and transitive.

Example 8.5.3. The relation defined by "less than or equal to" on any set of real numbers forms a partial order relation.

Let $x, y, z \in S \subseteq \mathbb{R}$, then

- Reflexive: $x \leq x$
- Antisymmetric: $x \leq y$ and $y \leq x$ implies $x = y$
- Transitive: $x \leq y$ and $y \leq z$ implies that $x \leq z$.

△

Definition 8.5.4. Because the idea of partial ordering is based off of $\leq$ we use $\preceq$ to denote a general partial ordering.

Theorem 8.5.5. *Let A be a set with a partial order relation R, and let S be a set of strings over A. Define a relation on S as follows:*

Let s and t be any strings in S of lengths m and n and let s_k and t_k be the characters in the kth position.

1. *If $m \leq n$ and the first m characters of s and t are the same, then $s \preceq t$.*
2. *If the first $m-1$ characters in s and t are the same, $s_m R t_m$ and $s_m \neq t_m$, then $s \preceq t$.*

3. If λ is the null string (string with no characters) then $\lambda \preceq s$.

If no strings are related by $\preceq$ other than by these three conditions, then $\preceq$ is a partial order relation on S.

*This partial order is called the **lexicographic order** for S that corresponds to the partial order R on A.*

Definition 8.5.6. Suppose $\preceq$ is a partial order relation on a set A. Elements $a, b \in A$ are said to be **comparable** if either $a \preceq b$ or $b \preceq a$. Otherwise they are called **noncomparable**.

Definition 8.5.7. If R is a partial order relation on a set A, and every element in A is comparable, then R is a **total order relation** on A.

Definition 8.5.8. A set A is called a **partially ordered set** with respect to a relation $\preceq$ if $\preceq$ is a partial order relation.

Definition 8.5.9. Let a set A be partially ordered with respect to a relation $\preceq$.

1. An element $a \in A$ is called a **maximal element** of A if for each $b \in A$, either $b \preceq a$ or b and a are not comparable.

2. An element $a \in A$ is called a **greatest element of** A if for each $b \in A$, $b \preceq a$.

3. An element $a \in A$ is called a **minimal element** of A if for each $b \in A$, either $a \preceq b$ or b and a are not comparable.

4. An element $a \in A$ is called a **least element of** A if for each $b \in A$, $a \preceq b$.

Exercises

1. Define a relation R on $\mathbb{Z}$ as follows: For every $m, n \in \mathbb{Z}$, mRn if and only if every prime factor of m is a prime factor of n.

   Is R a partial order relation? Prove or give a counter example.

2. Define a relation R on $\mathbb{Z}$ as follows: For every $m, n \in \mathbb{Z}$, mRn if and only if $m + n$ is even.

   Is R a partial order relation? Prove or give a counter example.

3. Let R and S be relations on the same set A such that R and S are antisymmetric. Must $R \cup S$ be antisymmetric?

4. Let $A = \{a, b\}$. Describe all possible partial order relations on A.

Solutions

1. Define a relation R on $\mathbb{Z}$ as follows: For every $m, n \in \mathbb{Z}$, mRn if and only if every prime factor of m is a prime factor of n.

   Is R a partial order relation? Prove or give a counter example.

   This problem is vague, for prime factorizations we only consider positive integers greater than or equal to 2. All other integers are not comparable. Given this restriction R is a partial order relation.

   Reflexive: If $m \in \mathbb{Z}$ such that $m \geq 2$, then mRm following that m has the same prime factorization as iteself.

   Antisymmetric: Let $m, n \in \mathbb{Z}$ such that $m, n \geq 2$ and such that mRn and nRm. This implies that every prime factor in m is in n and every prime factor of n is in m. Following that the prime factorization of numbers is unique this implies that $m = n$.

   Transitive: Let mRn and nRk for $m, n, k \in \mathbb{Z}$ such that $m, n, k \geq 2$. This implies that m's prime factors form a subset of n's prime factors and that n's prime factors are a subset of k's prime factors. Thus m's prime factors must be a subset of k's prime factors giving mRk.

2. Define a relation R on $\mathbb{Z}$ as follows: For every $m, n \in \mathbb{Z}$, mRn if and only if $m + n$ is even.

   Is R a partial order relation? Prove or give a counter example.

   Note that if $m + n$ is even, then their are two cases. Either both m and n are even or m and n are odd.

   R does not form a partial order relation. It does form an equivalence relation.

   Reflexive: From the cases above for any $m \in \mathbb{Z}$ we have mRm.

   Antisymmetric: This is where R breaks consider $1, 3 \in \mathbb{Z}$. We have that $1 + 3 = 4$ and that $3 + 1 = 4$ giving $1R3$ and $3R1$, but $1 \neq 3$. In this case R is actually symmetric.

   Transitive: Let $n, m, k \in \mathbb{Z}$ such that nRm and mRk, then from our cases above we have that all three numbers must either be all even or all odd. In either case nRk.

3. Let R and S be relations on the same set A such that R and S are antisymmetric. Must $R \cup S$ be antisymmetric?

   No, consider the set $A = \{1, 2\}$ with

   $$R = \{(1, 1), (1, 2), (2, 2)\},$$
   $$S = \{(1, 1), (2, 1), (2, 2)\}.$$

   Then R and S are both antisymmetric (and partial order relations), but

   $$R \cup S = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$$

is not antisymmetric. And in fact $R \cup S$ is an equivalence relation.

4. Let $A = \{a, b\}$. Describe all possible partial order relations on A.

   To start on this problem consider

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

   We know any partial order relations on A must be subsets of $A \times A$. This gives

   $$\{(a, a), (b, b)\}$$
   $$\{(a, a), (a, b), (b, b)\}$$
   $$\{(a, a), (b, a), (b, b)\}.$$

   Note that I need both (a, a) and (b, b) to be reflexive. And I can't have both (a, b) and (b, a) without the relation becoming symmetric.

Chapter 9

Counting and probability

9.1 Introduction to probability

Definition 9.1.1. A **sample space** is the set of all possible outcomes of a random process or experiment. An **event** is a subset of a sample space.

For any finite set A, $N(A)$ denotes the number of elements in A.

Definition 9.1.2 (Equally likely probability formula)**.** If S is a finite sample space in which all outcomes are equally likely and E is an event in S, then the **probability of** E denoted $P(E)$ is

$$P(E) = \frac{\text{the number of outcomes in } E}{\text{the total number of outcomes in } S} = \frac{N(E)}{N(S)}.$$

Example 9.1.3. An ordinary deck of cards contains 52 cards separated into four suits. The red suits are diamonds and hearts, and the black suits are clubs and spades. Each suit contains 13 cards; $2, 3, \ldots, 10$, Jack (J), Queen (Q), King (K), and Ace (A). The cards J, Q, K are called face cards. Compute the following assuming 1 card is drawn randomly.

1. What is the sample space of outcomes?

   The sample sapce is the 52 cards in the deck.

2. What is the event that the chosen card is a black card?

   Two of the four suits are black cards giving 26 possible black cards to pick. This gives $P(E) = 26/52 = 1/2$.

3. What is the probability that the chosen card is a red face card?

   There are 3 face cards per suit and two red suits. So the number of outcomes is 6. This gives $P(E) = 6/52 \approx 11.5\%$

4. What is the probability that the card chosen is a red card or a face card?

The probability that a chosen card is a red card is 1/2 (similar to part 2) and the probability that a card is a face card is 12/52 (3 face cards and 4 suits). Now to calculate $P(AorB)$ we need to add the two probabilities, then subtract the double counting. In this case the double counting is the probability of drawing a red face card. Which from (3) is 6/52. This gives

$$P(E) = \frac{1}{2} + \frac{12}{52} - \frac{6}{52} = \frac{32}{52} \approx 61.5\%.$$

△

Example 9.1.4 (The Monty Hall problem)**.** You are in a game show with three doors in front of you, lets call them A, B, C. Behind one of these doors is a prize and behind the other two is nothing.

The host asks you to pick a door, lets say you pick B, then the host opens one of the 2 doors you didn't pick, door C, to reveal no prize. Finally, the host asks you do you want to swap doors? If your goal is to maximize the chance of getting the prize should you swap doors? Does it make a difference?

Yes, you should swap doors. When you choose the first door you have no information, this gives a 1/3 chance of getting the prize and a 2/3 chance that the prize was behind a different door. Once the host opens a false door that 2/3 chance doesn't change since the host will always pick a door that does not have a prize. Therefore by switching you go from a 1/3 chance of winning to a 2/3 chance of winning. △

Theorem 9.1.5. *If m and n are integers and $m \leq n$, then there are $n - m + 1$ integers from m to n inclusive.*

Exercises

1. Given the sample space from the example with the cards.
   (a) What is the probability that the chosen card is red and is not a face card?
   (b) What is the probability that the chosen card is black and has an even number on it? (Assume Jack, Queen, King, and Ace are not even)
   (c) What is the probability that the denomination of the chosen card is at most 4? (Assume Jack, Queen, King, and Ace are above 4)
2. How many positive two digit integers are multiples of three?
3. What is the probability that a randomly chosen positive two digit integer is a multiple of three?
4. If the largest of 56 consecutive integers is 279, what is the smallest?

Solutions

1. Given the sample space from the example with the cards.

   (a) What is the probability that the chosen card is red and is not a face card?

   The number of red cards is 26 out of the total of 52. We have 3 face cards (J,Q,K) and two suits so there are 6 red face cards. This gives 20 cards we can pick from, giving a probability of $20/52 \approx 38.4\%$.

   (b) What is the probability that the chosen card is black and has an even number on it? (Assume Jack, Queen, King, and Ace are not even)

   There are 5 even cards in a suit (2,4,6,8,10) and there are two black suits. This gives 10 choices out of 52 which is a probability of $10/52 \approx 19.2\%$.

   (c) What is the probability that the denomination of the chosen card is at most 4? (Assume Jack, Queen, King, and Ace are above 4)

   There are 3 cards in a suit of denomination at most 4 (2,3,4) and 4 suits. This gives 12 cards to pick out of 52 or a probability of $12/52 \approx 23.1\%$.

2. How many positive two digit integers are multiples of three?

3. What is the probability that a randomly chosen positive two digit integer is a multiple of three?

   We get this from the last question, the probability is $30/90 = 1/3$.

4. If the largest of 56 consecutive integers is 279, what is the smallest?

   We can use the theorem for counting integers between two numbers here. We know $n = 279$ and $n - m + 1 = 56$. This gives $m = n - 56 + 1 = 279 - 55 = 224$. So the smallest integer is 224. Notice that if you directly subtract 279 and 56 we get 223 which misses the first integer.

9.2 The multiplication rule

Theorem 9.2.1. *If an operation consists of k steps and the ith step can be performed in n_i ways for $1 \leq i \leq k$ regardless of how the other steps were performed, then the entire operation can be performed in*

$$\prod_{i=1}^{k} n_i = n_1 n_2 \dots n_k$$

ways.

Example 9.2.2. A personal identification number (PIN) is a sequence of any four symbols chosen from the 26 uppercase letters and the ten digits.

1. How many different PINs are possible if repetition of symbols is allowed?

   We have 4 choices and each choice has $26 + 10 = 36$ options. Using the multiplication rule this gives $36^4 = 1679616$ choices

2. How many different PINs are possible if repetition of symbols is not allowed?

   We have 4 choices and the first choice has $26 + 10 = 36$ options. However, after each choice we remove one option from the pool, so for choice 2 we only have 35 options. Using the multiplication rule this gives $36(35)(34)(33) = 1413720$ choices.

3. If all PIN choices are equally likely what is the probability that a PIN does not have a repeated symbol?

   From our previous section to calculate the probability we take

$$\frac{1413720}{1679616} \approx 84\%$$

△

Example 9.2.3. Three officers – a president, a treasurer, and a secretary – are to be chosen from among four people: Ann, Bob, Cyd, and Dan. Suppose that Ann cannot be president and either Cyd or Dan must be secretary. How many ways can the officers be chosen?

To use the multiplication rule we need to be careful. First we need to pick the secretary, then the president, then the treasurer. This gives $2(2)(2) = 8$ total options. △

Definition 9.2.4. A **permutation** of a set of objects is an ordering of the objects in a row.

Example 9.2.5. Let $A = \{a, b, c\}$, then abc and acb are permutations. How many total permutations are there of A? What about a set with n elements?

For A there are 6 permutations. In general there are $n!$ permutations. △

Definition 9.2.6. An r-permutation of a set of n elements is an ordered selection of r elements taken from the set of n elements. The number of r-permutations of a set of n elements is denoted $P(n, r)$. We can calculate $P(n, r)$ using either

$$P(n, r) = n(n-1)(n-2)\dots(n-r+1)$$

or

$$P(n, r) = \frac{n!}{(n-r)!}$$

Example 9.2.7. 1. Evaluate $P(5, 2)$

$$\frac{5!}{3!} = 5(4) = 20.$$

2. How many 4-permutations in a set of 7 objects?

$$\frac{7!}{(7-4)!} = 7(6)(5)(4) = 840.$$

3. How many 5-permutations in a set of 5 objects?

$$\frac{5!}{(5-5)!} = 5! = 120.$$

△

Exercises

1. Sally wants to buy a triple scoop ice cream cone. There are five flavors to choose from, chocolate, vanilla, mint, strawberry, and pineapple.

   (a) How many ways can Sally build her ice cream cone?

   (b) If Sally does not want to repeat flavors how many ways are there to build the cone?

   (c) If Sally is equally as likely to choose any combination of flavors, what is the probability that Sally will have repeat flavors?

2. A coin is flipped 4 times with equal probability between heads (H) and tails (T).

   (a) How many distinct outcomes are possible? (order matters)

   (b) How many outcomes of a certain number of heads and certain number of tails are possible? (order does not matter)

   (c) What is the probability that exactly 1 head occurs?

Solutions

1. Sally wants to buy a triple scoop ice cream cone. There are five flavors to choose from, chocolate, vanilla, mint, strawberry, and pineapple.

   (a) How many ways can Sally build her ice cream cone?

   There are 5 options for the first scoop, 5 options for the second scoop, and 5 options for the third scoop. This gives $5^3 = 125$ total ways to build the ice cream cone.

(b) If Sally does not want to repeat flavors how many ways are there to build the cone?
There are 5 options for the first scoop. Then we remove the option taken giving 4 options for the second scoop. Removing that choice again gives 3 options for the third scoop. This gives $5(4)(3) = 60$ total ways to build the ice cream cone.

(c) If Sally is equally as likely to choose any combination of flavors, what is the probability that Sally will have repeat flavors?
There are 125 ways for Sally to build her ice cream cone and 60 of those don't contain repeats. So there are $125 - 60 = 65$ ways that she will have repeats. This gives a probability of $65/125 = 52\%$.

2. A coin is flipped 4 times with equal probability between heads (H) and tails (T).

(a) How many distinct outcomes are possible? (order matters)
If order matters, then there are $2^4 = 16$ outcomes since each coin flip can be heads or tails and we flip the coin 4 times.

(b) How many outcomes of a certain number of heads and certain number of tails are possible? (order does not matter)
If order does not matter, then we could have 4 heads and no tails, 3 heads and 1 tail, 2 heads and 2 tails, 1 head and 3 tails, and 0 heads and 4 tails. This gives 5 outcomes. Note that the probability of each of these outcomes is not the same.

(c) What is the probability that exactly 1 head occurs?
There are 4 outcomes that give 1 head HTTT, THTT, TTHT, and TTTH. This gives $4/16 = 1/4 = 25\%$

9.3 Counting elements of disjoint sets, the addition rule

Remember that, for a set A, $N(A)$ denotes the number of elements in A. Other texts will often use $|A|$ instead.

Theorem 9.3.1. *Suppose a finite set A equals the union of k distinct mutually disjoint subsets $A_1, A_2, \ldots, A_k$. Then*

$$N(A) = N(A_1) + N(A_2) + \cdots + N(A_k).$$

Theorem 9.3.2. *If A is a finite set and B is a subset of A, then*

$$N(A - B) = N(A) - N(B).$$

Theorem 9.3.3. *If S is a finite sample space and A is an event in S, then*

$$P(A^c) = 1 - P(A),$$

where $A^c = S - A$.

Example 9.3.4. A certain password consists of 3 through 5 uppercase letters, with repetitions allowed.

1. How many different passwords are allowed?

   $26^3 = 17576$ length 3, $26^4 = 456976$ length 4, and $26^5 = 11881376$ length 5 passwords. Giving a total of 12,355,928 passwords.

2. How many different passwords have no repeated letters?

   $26(25)(24) + 26(25)(24)(23) + 26(25)(24)(23)(22) = 8,268,000$

3. How many different passwords contain atleast one repeated letter?

   Using the difference rule we get $12,355,928 - 8,268,000 = 4,087,928$

4. If all passwords are equally likely, what is the probability that a randomly chosen password has at least one repeated letter?

   $4,087,928/12,355,928 \approx 33.1\%$.

△

Theorem 9.3.5. *If A, B, and C are finite sets, then*

$$N(A \cup B) = N(A) + N(B) - N(A \cap B)$$

and

$$N(A \cup B \cup C) = N(A) + N(B) + N(C) - N(A \cap B) - N(A \cap C) - N(B \cap C) + N(A \cap B \cap C).$$

The idea for these is that $N(A) + N(B)$ double counts the intersection so we need to remove it with $-N(A \cap B)$. In the 3 set case we double count all combinations of intersections, but when we remove all of them we have removed the intersection of all 3 so we need to add that back in.

9.4 The pigeonhole principle

Theorem 9.4.1 (Pigeonhole principle)**.** *A function from a finite set to a smaller finite set cannot be one-to-one: There must be at-least two elements in the domain that have the same image in the co-domain.*

Example 9.4.2. Given a group of 370 people, show there exists two or more people who share the same birthday.

There are at most 366 days in a year. So by the pigeonhole principle some of the 370 people must share a birthday. △

Theorem 9.4.3 (Generalized pigeonhole principle)**.** *For any function f from a finite set X with n elements to a finite set Y with m elements and for any positive integer k, if $km < n$, then there is some $y \in Y$ such that y is the image of at least $k + 1$ distinct elements of X.*

Example 9.4.4. Given a group of 85 people, show at least 4 must have the same last initial.

There are 26 possible last initials and we have that $3(26) = 78 < 85$, so $(3 + 1)$ people share the same last initial. △

Note: Careful when using this principle. It does not tell you anything about the minimum number. So for example, we could have 10,000 people and there may still exist someone with a unique birthday.

Theorem 9.4.5 (Generalized pigeonhole principle, contrapositive form)**.** *For any function f from a finite set X with n elements to a finite set Y with m elements and for any positive integer k, if for each $y \in Y$, $f^{-1}(y)$ has at most k elements, then X has at most km elements. Or in other words, $n \leq km$.*

Exercises

1. (a) If any seven digits could be used to form a telephone number, how many seven-digit telephone numbers would not have any repeated digits?
   (b) How many seven-digit telephone numbers would have at least one repeated digit?
   (c) What is the probability that a randomly chosen seven-digit telephone number would have at least one repeated digit?
2. In a group of 700 people, must there be 2 who have the same first and last initials? Why?
3. If $n + 1$ integers are chosen from the set $\{1, 2, 3, \ldots, 2n\}$, where n is a positive integer, must at least one of them be even? Why?
4. A group of 15 executives are to share 5 assistants. Each executive is assigned exactly 1 assistant, and no assistant is assigned to more than 4 executives. Show that at least 3 assistants are assigned to 3 or more executives.

Solutions

1. (a) If any seven digits could be used to form a telephone number, how many seven-digit telephone numbers would not have any repeated digits?

   There are 10 options for each digit and 7 digits. This gives 10^7 total 7 digit numbers. If we require that there are no repeated digits, then we get $10(9)(8)(7)(6)(5)(4) = 10!/3!$.

   (b) How many seven-digit telephone numbers would have at least one repeated digit?

From part (a) we found there are a total of 10^7 7 digit phone numbers of which $10!/3!$ don't have any repeated digits. This implies that the remaining $10^7 - 10!/3!$ have at least one repeated digit.

(c) What is the probability that a randomly chosen seven-digit telephone number would have at least one repeated digit?

For the probability of an event we take the number of ways the event can happen over the total number events this gives

$$\frac{10^7 - 10!/3!}{10^7} = 0.93952 = 93.952\%.$$

2. In a group of 700 people, must there be 2 who have the same first and last initials? Why?

   There are $26^2 = 676$ possible first and last initial combinations. By the pigeonhole principle, we must have at least two people who share the first and last initial.

3. If $n + 1$ integers are chosen from the set $\{1, 2, 3, \ldots, 2n\}$, where n is a positive integer, must at least one of them be even? Why?

   We have n even integers and n odd integers in the list, and we are choosing $n + 1$ options. So by the pigeonhole principle, we must pick at least 1 to be even.

4. A group of 15 executives are to share 5 assistants. Each executive is assigned exactly 1 assistant, and no assistant is assigned to more than 4 executives. Show that at least 3 assistants are assigned to 3 or more executives.

   We can define a function that maps executives to assistants, since we know each executive gets exactly one assistant. Now we can get $2(5) < 15$ so our k for the generalized pigeonhole principle is 2. This gives that at least one assistant must have at least 3 executives assigned. We know that the assistant can't be assigned to more than 4 executives, so we can remove the one assistant and 4 executives (we want to maximize here because we are trying to show that we always have 3 assistants falling into this situation).

   This leaves us with 4 assistants and 11 executives. Apply the same function $4(2) < 11$. Giving a second assistant with at least 4 executives. Remove the assistant and 4 executives, giving 3 assistants and 7 executives. Finally, we have $3(2) < 7$ forcing a third assistant to have at least 3 executives.

9.5 Counting subsets of a set: combinations

Definition 9.5.1. Let n and 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.

Reminder we use the notation

$$\binom{n}{r} = \frac{n!}{(n-r)!r!} = \frac{P(n,r)}{r!},$$

which is read "n choose r" to denote the number of r-combinations of a set of n elements.

Example 9.5.2. Given a deck of 52 cards. We have 13 cards (2-10, J, Q, K, A) and 4 suits (hearts, diamonds, spades clubs) of those 13 cards.

1. How many 5 card hands contain two pairs?

   To calculate this consider the following process, first we need two different cards of which there are $\binom{13}{2}$ ways to pick these. For step 2 we need the number of ways to pick the suits of the pairs, since there are 4 suits we get $\binom{4}{2}$ and $\binom{4}{2}$. Finally we need to choose the final card, we have 44 cards remaining giving $\binom{44}{1}$ ways to pick that card. Putting everything together gives

   $$\binom{13}{2}\binom{4}{2}\binom{4}{2}\binom{44}{1} = 123,552$$

2. If a 5 card hand is dealt at random, what is the probability that the hand contains two pairs?

   There are $\binom{52}{5} = 2,598,960$ different possible hands. Giving the probability of a hand consisting of two pairs at

   $$\frac{123,552}{2,598,960} \approx 4.75\%.$$

△

Example 9.5.3. How many ways are there to rearrange the letters of the word

MISSISSIPPI

Don't try to do this by hand. There are 4 S letters, 4 I letters, 2 P letters and 1 M letter. This gives that there are $\binom{11}{4}$ places to put the S letters, then removing those locations there are $\binom{7}{4}$ places to put the I letters. One those are placed there are $\binom{3}{2}$ places to put the P letters and finally there is $\binom{1}{1}$ place to put the M. This gives a total of

$$\binom{11}{4}\binom{7}{4}\binom{3}{2}\binom{1}{1} = 34,650.$$

△

Theorem 9.5.4. *Suppose we have a collection of n object where we can separate them into k groups where they are all indistinguishable from each other inside those groups. Let $n_1, n_2, \ldots, n_k$ denote the number of elements in each of those groups, then the number distinguishable permutations of the n objects is*

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-n_2-\cdots-n_{k-1}}{n_k} = \frac{n!}{n_1!n_2!n_3!\ldots n_k!}$$

9.6 r-combinations with repetition allowed

Definition 9.6.1. An r-combination with repetition allowed, or multiset of size r, chosen from a set X of n elements is an unordered selection of elements taken from X with repetition allowed. If $X = \{x_1, x_2, \ldots, x_n\}$, then we write an r-combination with repetition allowed as $[x_{i_1}, x_{i_2}, \ldots, x_{i_r}]$ where $x_{i_1} \in X$ and some may be equal.

The number of r-combinations with repetition that can be selected from a set of n elements is

$$\binom{r+n-1}{r}$$

Example 9.6.2. A person giving a party wants to set out 15 assorted cans of drinks. They shop at a store that sells five different types of drinks.

1. How many different selections of cans of 15 drinks can they make?

   We can think of the 15 cans as the r objects we are picking and the types of drinks as the n items from the set. This gives

   $$\binom{15+5-1}{15} = 3876.$$

2. If root beer is one of the types of drink, how many selections contain at least 6 cans of root beer?

   If we need at least 6 cans of root beer, we can choose those first since order does not matter. This leaves 9 cans and still the 5 types (since we can take more root beer). This gives

   $$\binom{9+5-1}{9} = 715.$$

3. If the store has only 5 cans of root beer, but 15 cans of everything else, how many selections can be made?

   We are going to use the difference rule here. The total number of cans from part (a) is 3876 and the number of ways to choose the drinks with at least 6 cans of root beer is 715. So the number of ways to get at most 5 cans of root beer is $3876 - 715 = 3161$.

△

The following table gives the different ways we can choose k elements from n.

	Order matters	Order does not matter
Repetition is allowed	n^k	$\binom{k+n-1}{k}$
Repetition is not allowed	$P(n,k)$	$\binom{n}{k}$

Exercises

1. Given a deck of 52 cards. We have 13 cards (2-10, J, Q, K, A) and 4 suits (hearts, diamonds, spades clubs) of those 13 cards. How many 5 card hands contain a full house (three of a kind and a pair)?

2. An instructor gives an exam with fourteen questions. Students are allowed to choose any ten to answer.

   (a) How many different choices of ten questions are there?

   (b) Suppose that six questions require a proof and eight do not.

      i. How many groups of ten questions contain four proof questions and six non-proof questions?

      ii. How many groups of ten questions contain at least one that requires proof?

      iii. How many groups of ten questions contain at most three that require proof?

   (c) Suppose the exam instructions specify that at most one of questions 1 and 2 may be included among the ten. How many different choices of ten are there?

   (d) Suppose that the exam instructions specify that either both questions 1 and 2 are to be included or neither is to be included. How many different choices of ten questions are there?

3. How many solutions are there to $x+y+z = 20$ where x, y, z are nonnegative integers.

4. How many solutions are there to $a + b + c + d + e = 500$ where a, b, c, d, e are integers at least 2.

5. How many integers from 1 through 99,999 have the sum of their digits equal to 10?

Solutions

1. Given a deck of 52 cards. We have 13 cards (2-10, J, Q, K, A) and 4 suits (hearts, diamonds, spades clubs) of those 13 cards. How many 5 card hands contain a full house (three of a kind and a pair)?

2. An instructor gives an exam with fourteen questions. Students are allowed to choose any ten to answer.

   (a) How many different choices of ten questions are there?

   (b) Suppose that six questions require a proof and eight do not.

      i. How many groups of ten questions contain four proof questions and six non-proof questions?

      ii. How many groups of ten questions contain at least one that requires proof?

      iii. How many groups of ten questions contain at most three that require proof?

   (c) Suppose the exam instructions specify that at most one of questions 1 and 2 may be included among the ten. How many different choices of ten are there?

   (d) Suppose that the exam instructions specify that either both questions 1 and 2 are to be included or neither is to be included. How many different choices of ten questions are there?

3. How many solutions are there to $x+y+z = 20$ where x, y, z are nonnegative integers.

   Think of 20 as the units that we need to divide it up between the variables x, y, z. This is then a r-combinations with repetition

$$\binom{20+3-1}{20} = \binom{22}{20} = 231.$$

4. How many solutions are there to $a+b+c+d+e = 500$ where a, b, c, d, e are integers at least 2.

   Think of 500 as the units that we need to divide it up between the variables a, b, c, d, and e. Since each variable starts at 2 we can remove those 10 units. This is then a r-combinations with repetition

$$\binom{490+5-1}{490} = \binom{494}{490} = 2,451,372,001.$$

5. How many integers from 1 through 99,999 have the sum of their digits equal to 10?

We can treat the digits as individual numbers, and we are trying to get the sum of those 5 numbers to be 10. Those numbers can be between 0 and 9. This gives

$$\binom{10+5-1}{10} = \binom{14}{10} = 1001.$$

We need to be careful about the fact that we are starting at 1 instead of 0. Because of this, we need to remove the 5 outcomes that comes from this. This gives $1001 - 5 = 996$ total outcomes.

9.7 Pascal's formula and the binomial theorem

Example 9.7.1. Show the following

1. $\binom{n}{n} = 1$

$$\binom{n}{n} = \frac{n!}{n!(n-n)!} = 1.$$

2. $\binom{n}{n-1} = n$

$$\binom{n}{n-1} = \frac{n!}{(n-1)!(n-(n-1))!} = \frac{n}{1} = n.$$

3. $\binom{n}{n-2} = \frac{n(n-1)}{2}$.

$$\binom{n}{n-2} = \frac{n!}{(n-2)!(n-(n-2))!} = \frac{n(n-1)}{2}.$$

△

Example 9.7.2. Given a set with 10 items how many ways can you pick 4 of them? How about 6 of them?

There are $\binom{10}{4} = 210$ ways to pick 4 items from a set of 10. There are $\binom{10}{6} = 210$ ways to pick 6 items from 10. △

Theorem 9.7.3. *Let n, r be positive integers with $r \leq n$, then*

$$\binom{n}{r} = \binom{n}{n-r}.$$

Theorem 9.7.4 (Pascal's formula)**.** *Let n, r be positive integers with $r \leq n$, then*

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}.$$

Example 9.7.5. Use Pascal's formula to write

$$\binom{n+2}{r}$$

in terms of

$$\binom{n}{r}, \binom{n}{r-1}, \binom{n}{r-2}.$$

$$\begin{aligned}\binom{n+2}{r} &= \binom{n+1}{r-1} + \binom{n+1}{r} \\ &= \binom{n}{r-2} + \binom{n}{r-1} + \binom{n}{r-1} + \binom{n}{r} \\ &= \binom{n}{r-2} + 2\binom{n}{r-1} + \binom{n}{r}.\end{aligned}$$

△

Definition 9.7.6. Given two numbers, a, b, we call $a+b$ a **binomial**.

Theorem 9.7.7 (Binomial theorem)**.** *Given real numbers a and b and a non-negative number, n we have*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Example 9.7.8. Prove that

$$2^n = \sum_{k=0}^{n} \binom{n}{k}$$

for every integer $n \geq 0$.

Let n be a positive integer, then consider

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k} = \sum_{k=0}^{n} \binom{n}{k}.$$

△

Exercises

1. Express the following sums in closed form (no summation symbol)

   (a) $\sum_{k=0}^{n} \binom{n}{k} 5^k$.

   (b) $\sum_{i=0}^{n} \binom{n}{i} x^i$.

   (c) $\sum_{j=0}^{2n} (-1)^j \binom{2n}{j} x^j$.

2. Use the binomial theorem to expand out $(p+q)^6$.

3. Derive the following formulas

   (a) $\binom{n+3}{n+1} = \frac{(n+3)(n+2)}{2}$ for $n \geq -1$.

   (b) $\binom{2(n+1)}{2n} = (n+1)(2n+1)$, for $n \geq 0$.

Solutions

1. Express the following sums in closed form (no summation symbol)

   (a) $\sum_{k=0}^{n} \binom{n}{k} 5^k$.

   $$\sum_{k=0}^{n} \binom{n}{k} 5^k = \sum_{k=0}^{n} \binom{n}{k} 5^k 1^{n-k} = (5+1)^n = 6^n.$$

   (b) $\sum_{i=0}^{n} \binom{n}{i} x^i$.

   $$\sum_{i=0}^{n} \binom{n}{i} x^i = \sum_{i=0}^{n} \binom{n}{i} x^i 1^{n-i} = (x+1)^n.$$

   (c) $\sum_{j=0}^{2n} (-1)^j \binom{2n}{j} x^j$.

   $$\sum_{j=0}^{2n} (-1)^j \binom{2n}{j} x^j = \sum_{j=0}^{2n} \binom{2n}{j} (-x)^j = \sum_{j=0}^{2n} \binom{2n}{j} (-x)^j 1^{2n-j} = (1-x)^{2n}.$$

2. Use the binomial theorem to expand out $(p+q)^6$.

   The 6th row (remember we need to write out 7 rows to account for row 0 where $n=0$) of Pascal's triangle is

   $$1\ 6\ 15\ 20\ 15\ 6\ 1.$$

   These will be the coefficients giving

   $$p^6q^0 + 6p^5q^1 + 15p^4q^2 + 20p^3q^3 + 15p^2q^4 + 6p^1q^5 + p^0q^6.$$

3. Derive the following formulas

   (a) $\binom{n+3}{n+1} = \frac{(n+3)(n+2)}{2}$ for $n \geq -1$.

   $$\binom{n+3}{n+1} = \frac{(n+3)!}{((n+3)-(n+1))!(n+1)!} = \frac{(n+3)(n+2)}{2!} = \frac{(n+3)(n+2)}{2}.$$

   (b) $\binom{2(n+1)}{2n} = (n+1)(2n+1)$, for $n \geq 0$.

   $$\binom{2(n+1)}{2n} = \frac{(2(n+1))!}{((2(n+1))-2n)!(2n)!} = \frac{(2n+1)(2n+2)}{2!} = (2n+1)(n+1).$$

9.8 Probability Axioms and expected value

Definition 9.8.1. Let S be a sample space. A **probability function** P from the set of all events in S to the set of real numbers satisfies the following three axioms: For all events A and B in S:

1. $0 \leq P(A) \leq 1$.
2. $P(\emptyset) = 0$ and $P(S) = 1$.
3. If A and B are disjoint ($A \cap B = \emptyset$), then

   $$P(A \cup B) = P(A) + P(B).$$

Theorem 9.8.2. *If A is any event in a sample space S, then*

$$P(A^c) = 1 - P(A).$$

Theorem 9.8.3. *If S is any sample space and A and B are any events in S, then*

$$P(A \cup B) = P(A) + P(B) - P(A \cap B).$$

Example 9.8.4. Suppose a sample space contains three outcomes: $0, 1, 2$. Let $A = \{0\}$, $B = \{1\}$, and $C = \{2\}$, and suppose $P(A) = 0.4$ and $P(B) = 0.3$. Find each of the following.

1. $P(A \cup B)$

   Since A and B are disjoint we have $P(A \cup B) = P(A) + P(B) = 0.4 + 0.3 = 0.7$.

2. $P(C)$

   Since the sum of events needs to add to 1 we have $P(C) = 1 - (P(A) + P(B)) = 0.3$

3. $P(A \cup C)$

   Same as 1 giving 0.7.

4. $P(A^c)$

   Since $P(A) = 0.4$ we have $P(A^c) = 1 - P(A) = 0.6$

5. $P(A^c \cap B^c)$

   $A^c = \{1, 2\}$ and $B^c = \{0, 2\}$ so $A^c \cap B^c = \{1\}$ which is C. This gives $P(A^c \cap B^c) = P(C) = 0.3$.

6. $P(A^c \cup B^c)$

   $A^c = \{1, 2\}$ and $B^c = \{0, 2\}$ so $A^c \cup B^c = \{0, 1, 2\} = S$. This gives $P(A^c \cup B^c) = P(S) = 1$.

△

Definition 9.8.5. Suppose the possible outcomes of an experiment, or random process, are real numbers $a_1, a_2, \ldots, a_n$, which occur with probabilities $p_1, p_2, \ldots, p_n$. The **expected value** of this process is

$$\sum_{k=1}^{n} a_k p_k = a_1 p_1 + a_2 p_2 + \cdots + a_n p_n.$$

Example 9.8.6. Suppose that there are 500,000 tickets to play a lottery. Each ticket is \$5 and there are the following prizes:

Number of tickets	Payout
1	1,000,000
10	1000
1000	500
10000	10

What is the expected value of a ticket?

Each ticket has equal probability so $p_k = 1/500000$. Let a_k be the net gains for the tickets, so $a_1 = 1,000,000 - 5 = 999,995$. This gives the following

$$\begin{aligned}\sum_{k=1}^{500,000} a_k p_k &= \frac{1}{500,000} \sum_{k=1}^{500,000} a_k \\ &= \frac{1}{500,000}(999,995 + (10)995 + (1000)495 + (10000)5 + (-5)488,989) \\ &= -1.78\end{aligned}$$

△

Exercises

1. A company offers a raffle whose grand prize is a $40,000 new car. Additional prizes are a $1000 television, and a $500 computer. Tickets cost $20 each and 3000 tickets will be sold. What is the expected gain loss of each ticket?

2. When a pair of balanced 6 sided dice are rolled, the sum of the numbers showing face up is computed. The result can be any number from 2 to 12. What is the expected value of the sum?

3. Suppose a person offers to play a game with you. In this game, when you draw a card from a standard 52-card deck, if it is a face card you win $3, and if it is anything else you lose $1. What is the expected value of this game?

Solutions

1. A company offers a raffle whose grand prize is a $40,000 new car. Additional prizes are a $1000 television, and a $500 computer. Tickets cost $20 each and 3000 tickets will be sold. What is the expected gain loss of each ticket?

2. When a pair of balanced 6 sided dice are rolled, the sum of the numbers showing face up is computed. The result can be any number from 2 to 12. What is the expected value of the sum?

3. Suppose a person offers to play a game with you. In this game, when you draw a card from a standard 52-card deck, if it is a face card you win $3, and if it is anything else you lose $1. What is the expected value of this game?

9.9 Conditional probability, Bayes' formula, and independent events

Definition 9.9.1. Let A and B be events in sample space S. If $P(A) \neq 0$, then the **conditional probability of B given A**, denoted $P(B|A)$, is

$$P(B|A) = \frac{P(A \cap B)}{P(A)}.$$

Example 9.9.2. Imagine you are flip a fair coin twice, call flip 1 F_1 and flip 2 F_2. Now suppose you know that ones of the coins is heads, what is the probability that the other coin flip is heads?

We can think of A as the events where one of the coin flips is heads that is $A = \{HH, HT, TH\}$. Now B is when the other flip is heads which means $B = \{HH\}$. So the conditional probability of B given A is

$$P(B|A) = \frac{P(A \cap B)}{P(A)} = \frac{1/4}{3/4} = \frac{1}{3}.$$

△

Theorem 9.9.3 (Bayes' theorem)**.** *Let A and B be events in sample space S such that $P(B) \neq 0$, then*

$$P(B|A) = \frac{P(A|B)P(B)}{P(A)}.$$

This can be generalized, and this is what the book gives, to be

Theorem 9.9.4. *Let S be a sample space which is partitioned into events $B_1, B_2, \ldots, B_n$ and let A and B_k be events in S with nonzero probability, then*

$$P(B_k|A) = \frac{P(A|B_k)P(B_k)}{P(A|B_1)P(B_1) + P(A|B_2)P(B_2) + \cdots + P(A|B_n)P(B_n)}.$$

Example 9.9.5. Consider a medical test that screens for a disease found in 5 people out of 1000. Suppose that the false positive rate is 3% and the false negative rate is 1%. Then 99% of the time a person who has the condition tests positive for it and 97% of the time a person who does not have the condition tests negative for it.

Let A be the event that a person tests positive for the condition, B_1 be the event that the person actually has the condition, and B_2 be the event that the person does not have the disease, then we have the following

$$P(A|B_1) = 0.99,\ P(A^c|B_1) = 0.01,\ P(A^c|B_2) = 0.97,\ P(A|B_2) = 0.03.$$

Since 5 people in 1000 have the disease we also have

$$P(B_1) = 0.005 \text{ and } P(B_2) = 0.995.$$

1. What is the probability that a randomly chosen person who tests positive for the condition actually has the condition?

   By Bayes's theorem

$$\begin{aligned} P(B_1|A) &= \frac{P(A|B_1)P(B_1)}{P(A|B_1)P(B_1) + P(A|B_2)P(B_2)} \\ &= \frac{(0.99)(0.005)}{(0.99)(0.005) + (0.03)(0.995)} \\ &\approx 0.1422 \\ &= 14.22\% \end{aligned}$$

   Thus the probability that a person with a positive test result actually has the disease is around 14%.

2. What is the probability that a randomly chosen person who tests negative for the condition does not have the condition?

   By Bayes's theorem

$$\begin{aligned} P(B_2|A^c) &= \frac{P(A^c|B_2)P(B_2)}{P(A^c|B_1)P(B_1) + P(A^c|B_2)P(B_2)} \\ &= \frac{(0.97)(0.995)}{(0.03)(0.995) + (0.97)(0.995)} \\ &\approx 0.999948 \\ &= 99.995\%. \end{aligned}$$

   The probability that a person with a negative test result does not have the disease is around 99.995%.

△

Definition 9.9.6. If A and B are events in a sample space S, then A and B are independent if and only if $P(A \cap B) = P(A)P(B)$.

Exercises

1. Suppose $P(A|B) = 1/2$ and $P(A \cap B) = 1/6$. What is $P(B)$?
2. The instructor of a discrete math class gives two tests, 25% of students get an A on the first test and 15% get an A on both tests. What percentage of the students who received an A on the first test also received an A on the second test?
3. One urn contains 10 red balls and 25 green balls, and a second urn contains 22 red balls and 15 green balls. A ball is chosen as follows: First, an urn is selected by tossing a loaded coin with probability 0.4 of landing heads up and probability 0.6 of landing tails up. If the coin lands heads up, the first urn is chosen; otherwise, the second urn is chosen. Then a ball is picked at random from the chosen urn.
   (a) What is the probability that the chosen ball is green?
   (b) If the chosen ball is green, what is the probability that it was picked from the first urn

Solutions

1. Suppose $P(A|B) = 1/2$ and $P(A \cap B) = 1/6$. What is $P(B)$?
2. The instructor of a discrete math class gives two tests, 25% of students get an A on the first test and 15% get an A on both tests. What percentage of the students who received an A on the first test also received an A on the second test?
3. One urn contains 10 red balls and 25 green balls, and a second urn contains 22 red balls and 15 green balls. A ball is chosen as follows: First, an urn is selected by tossing a loaded coin with probability 0.4 of landing heads up and probability 0.6 of landing tails up. If the coin lands heads up, the first urn is chosen; otherwise, the second urn is chosen. Then a ball is picked at random from the chosen urn.
   (a) What is the probability that the chosen ball is green?
   (b) If the chosen ball is green, what is the probability that it was picked from the first urn

Chapter 10

Graph theory and trees

10.1 Trails, Paths, and Circuits

Definition 10.1.1. Let G be a graph, and let v and w be vertices in G.

A **walk** from v to w is a finite alternating sequence of adjacent vertices and edges of G. Thus, a walk has the form

$$v_0 e_1 v_1 e_2 \dots v_{n-1} e_n v_n,$$

where the v's represent vertices and the e's represent the edges.

The following are special types of walks

1. A **trivial walk** is a walk that consists of a single vertex.
2. A **trail** is a walk from v to w that does not contain a repeated edge.
3. A **path** is a trail that does not contain a repeated vertex.
4. A **closed walk** is a walk that starts and ends at the same vertex.
5. A **circuit** is a closed walk that contains at least one edge and does not contain a repeated edge.
6. A **simple circuit** is a circuit that does not have any other repeated vertices except the first and last.

Sadly lots of graph notation is not standard and these terms get used interchangeably. Because of this, make sure to check your references definitions of these terms before you use them.

Definition 10.1.2. A graph H is said to be a **subgraph** of a graph G if and only if every vertex in H is also a vertex in G, every edge in H is an edge in G, and every edge in H has the same endpoints as it has in G.

Definition 10.1.3. Let G be a graph. Two vertices v and w of G are **connected** if and only if there is a walk from v to w. The graph G is connected if and only if given any two vertices v and w in G, there is a walk from v to w.

Lemma 10.1.4. *Let G be a graph.*

1. *If G is connected, then any two distinct vertices of G can be connected by a path.*
2. *If vertices v and w are part of a circuit in G and one edge is removed from the circuit, then there still exists a trail from v to w.*
3. *If G is connected and G contains a circuit, then an edge of the circuit can be removed without disconnecting G.*

Definition 10.1.5. A graph H is a **connected component** of a graph G if and only if

1. H is a subgraph of G
2. H is connected
3. no connected subgraph of G has H as a subgraph and contains vertices or edges that are not in H.

Definition 10.1.6. Let G be a graph. An **Euler circuit** for G is a circuit that contains every vertex and every edge of G. Another way to say that is an Euler circuit is a walk that starts and ends in the same vertex, which uses every vertex at least once, and uses every edge exactly once.

Theorem 10.1.7. *If a graph has an Euler circuit, then every vertex of the graph has positive even degree.*

Theorem 10.1.8. *If some vertex of a graph has odd degree, then the graph does not have an Euler circuit.*

Theorem 10.1.9. *A graph G has an Euler circuit if and only if G is connected and the degree of every vertex of G is a positive even integer.*

The algorithm to find a Euler circuit of a graph is as follows:

1. Pick any vertex v in G to start.
2. Build any circuit in G that starts and ends at v and call this circuit C.
3. If C contains every vertex and edge of G, then we are done.
4. If C does not contain every vertex and edge of G, then pick any vertex in C that has edges in G that are not in C and call it w.
5. Build a circuit in G from w that does not contain any edges or vertices from C and call it C'.
6. Patch circuits C and C' together calling this combined circuit C and go back to step 3.

Definition 10.1.10. Let G be a graph and let v and w be two distinct vertices of G. An **Euler trail** from v to w is a walk that starts in v, ends in w, passes through every vertex of G at least once, and traverses every edge of G exactly once.

Corollary 10.1.11. *Let G be a graph, and let v and w be two distinct vertices of G. These is an Euler trail from v to w if and only if G is connected, v and w have odd degree, and all other vertices of G have positive even degree.*

Definition 10.1.12. Given a graph G, a **Hamiltonian circuit** for G is a simple circuit that includes every vertex of G. Or a **Hamiltonian circuit** is a walk that starts and ends at the same vertex, contains no repeated edges, and contains every vertex of G exactly once.

While we have an easy way to check if a graph contains an Euler circuit, there is no known efficient method of checking if a graph contains a Hamilton circuit.

Proposition 10.1.13. *If a graph G has a Hamiltonian circuit, then G has a subgraph H with the following properties:*

1. *H contains every vertex of G.*
2. *H is connected.*
3. *H has the same number of edges as vertices.*
4. *Every vertex of H is degree 2.*

Definition 10.1.14. If G is a simple graph, the **complement of** G, denoted G', is obtained by keeping the vertex set the same and connecting two vertices if they are not connected in the orginal graph.

Exercises

1. Show that at a party with at least two people, there are at least two mutual acquaintances or at least two mutual strangers.

   How many people would we need such that there are at least three mutual acquaintances or at least three mutual strangers?

2. Give two examples of graphs that have Euler circuits but not Hamiltonian circuits.

3. Give two examples of graphs that have Hamiltonian circuits but not Euler circuits.

4. Let G be a simple graph with n vertices. What is the relation between the number of edges of G and the number of edges of G'?

Solutions

1. Show that at a party with at least two people, there are at least two mutual acquaintances or at least two mutual strangers.

2. Give two examples of graphs that have Euler circuits but not Hamiltonian circuits.

3. Give two examples of graphs that have Hamiltonian circuits but not Euler circuits.

4. Let G be a simple graph with n vertices. What is the relation between the number of edges of G and the number of edges of G'?

10.2 Matrix representations of graphs

Definition 10.2.1. An $m \times n$ **matrix** A over a set S is a rectangular array of elements of S arranged into m rows and n columns:

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}.$$

We can also write $A = (a_{ij})$.

For a square matrix of size n by n, the **main diagonal** of A are the entries $a_{11}, a_{22}, a_{33}, \dots, a_{nn}$.

Definition 10.2.2. Let G be a graph with ordered vertices $v_1, v_2, \dots, v_n$. The **adjacency matrix** of G is the n by n matrix $A = (a_{ij})$ over the set of nonnegative integers such that a_{ij} represents the number of arrows from v_i to v_j.

Definition 10.2.3. A n by n matrix $A = (a_{ij})$ is called **symmetric** if and only if $a_{ij} = a_{ji}$ for every $i, j = 1, 2, \dots, n$.

Definition 10.2.4. Let $A = (a_{ij})$ be a m by n matrix and $B = (b_{ij})$ be a n by p matrix, then

$$AB = (c_{ij}),$$

where

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj} = \sum_{k=1}^{n} a_{ik}b_{kj}.$$

Definition 10.2.5. The n by n **identity matrix**, denoted I_n, is the n by n matrix whose main diagonal entries are all 1's and all other entries are 0's. That

is

$$I_n = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix}.$$

Multiplying any square matrix A by the identity matrix will just leave the matrix A.

Definition 10.2.6. For any n by n matrix A, the powers of A are defined as follows:

$$A^0 = I_n$$
$$A^n = AA^{n-1} = A^{n-1}A.$$

Theorem 10.2.7. *If G is a graph with vertices $v_1, v_2, \dots, v_m$ and A is the adjacency matrix of G, then for each positive integer n and for all integers $i, j = 1, 2, \dots, m$, the ijth entry of A^n is equal to the number of walks of length n from v_i to v_j.*

Exercises

1. Find graphs that have the following adjacency matrices

   (a)
   $$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 0 \end{bmatrix}$$

   (b)
   $$\begin{bmatrix} 0 & 2 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

2. Find each of the following products

   (a)
   $$\begin{bmatrix} 2 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 3 \\ 5 & -4 \\ -2 & 2 \end{bmatrix}$$

   (b)
   $$\begin{bmatrix} -1 \\ 2 \end{bmatrix} \begin{bmatrix} 2 & 3 \end{bmatrix}$$

3. Let
   $$A = \begin{bmatrix} 1 & 1 & -1 \\ 0 & -2 & 1 \end{bmatrix}, \; B = \begin{bmatrix} -2 & 0 \\ 1 & 3 \end{bmatrix}, \; C = \begin{bmatrix} 0 & -2 \\ 3 & 1 \\ 1 & 0 \end{bmatrix}.$$
   Determine if each of the following exists, if so calculate it. If not explain why.

   (a) AB

   (b) BA

   (c) A^2

   (d) B^2

   (e) CB

Solutions

1. Find graphs that have the following adjacency matrices

   (a)
   $$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 0 \end{bmatrix}$$

(b)
$$\begin{bmatrix} 0 & 2 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

2. Find each of the following products

(a)
$$\begin{bmatrix} 2 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 3 \\ 5 & -4 \\ -2 & 2 \end{bmatrix}$$

(b)
$$\begin{bmatrix} -1 \\ 2 \end{bmatrix} \begin{bmatrix} 2 & 3 \end{bmatrix}$$

3. Let
$$A = \begin{bmatrix} 1 & 1 & -1 \\ 0 & -2 & 1 \end{bmatrix},\ B = \begin{bmatrix} -2 & 0 \\ 1 & 3 \end{bmatrix},\ C = \begin{bmatrix} 0 & -2 \\ 3 & 1 \\ 1 & 0 \end{bmatrix}.$$
Determine if each of the following exists, if so calculate it. If not explain why.

(a) AB

(b) BA

(c) A^2

(d) B^2

(e) CB

10.3 Isomorphisms of graphs

Definition 10.3.1. Let G and G' be graphs with vertex sets $V(G)$ and $V(G')$ and edge sets $E(G)$ and $E(G')$, respectively. G is **isomorphic** to G' if and only if there exists one-to-one correspondences: $g : V(G) \to V(G')$ and $h : E(G) \to E(G')$ that preserve the edge-endpoint functions of G and G'.

Theorem 10.3.2 (Graph isomorphism is an equivalence relation)**.** *Let S be a set of graphs and let R be the relation of graph isomorphism on S. Then R is an equivalence relation on S.*

Definition 10.3.3. A property P is called an **invariant for graph isomorphism** if and only if given any graphs G and G' if G has property P and G' is isomorphic to G, then G' has property P.

Theorem 10.3.4. *Each of the following properties is an invariant for graph isomorphism, where n, m, and k are all nonnegative integers:*

1. *has n vertices*
2. *has n edges*
3. *has a vertex of degree k*
4. *has m vertices of degree k*
5. *has a circuit of length k*
6. *has a simple circuit of length k*
7. *has m simple circuit of length k*
8. *is connected*
9. *has an Euler circuit*
10. *has a Hamiltonian circuit*

Definition 10.3.5. If G and G' are simple graphs, then G is **isomorphic** to G' if and only if there exists a one-to-one correspondence g from the vertex set $V(G)$ of G to the vertex set $V(G')$ of G' that preserves the edge-endpoint functions of G and G'.

Exercises

1. Draw all nonisomorphic simple graphs with 3 vertices
2. Draw all nonismorphic graphs with four vertices and 3 edges.

10.4 Trees: examples and basic properties

Definition 10.4.1. A graph is said to be **circuit-free** if and only if it has no circuits. A graph is called a **tree** if and only if it is circuit-free and connected. A **trivial tree** is a graph that consists of a single vertex. A graph is called a **forest** if and only if it is circuit-free and not connected.

Definition 10.4.2. Let T be a tree. If T has at least two vertices, then a vertex of degree 1 in T is called a **leaf** and a vertex of degree greater than 1 in T is called an **internal vertex**.

Theorem 10.4.3. *For any positive integer n, any tree with n vertices has $n-1$ edges.*

Lemma 10.4.4. *If G is any connected graph, C is any circuit in G, and any one of the edges of C is removed from G, then the graph that remains is circuit free.*

Theorem 10.4.5. *For any positive integer n, if G is a connected graph with n vertices and $n-1$ edges, then G is a tree.*

Corollary 10.4.6. *If G is any graph with n vertices and m edges, where m and n are positive integers and $m \geq n$, then G has a circuit.*

Exercises

1. A connected graph has nine vertices and eleven edges. Does it have a circuit? Why?
2. A connected graph has twelve vertices and eleven edges. Does it have a circuit? Why?
3. Find all nonisomorphic trees with four vertices.
4. Find all nonisomorphic trees with six vertices.
5. What is the total degree of a tree with n vertices?

Solutions

1. A connected graph has nine vertices and eleven edges. Does it have a circuit? Why?

2. A connected graph has twelve vertices and eleven edges. Does it have a circuit? Why?

3. Find all nonisomorphic trees with four vertices.

10.5 Rooted Trees

Definition 10.5.1. A **rooted tree** is a tree in which there is one vertex that is distinguished from the others and is called the **root**.

- The **level** of a vertex is the number of edges along the unique path between it and the root.
- The **height** of a rooted tree is the maximum level of any vertex of the tree.
- Given the root or any internal vertex v of a rooted tree, the **children** of v are all those vertices that are adjacent to v and are one level farther away from the root than v.
- If w is a child of v, then v is called the **parent** of w, and two distinct vertices that are both children of the same parent are called **siblings**.
- Given two distinct vertices v and w, if v lies on the unique path between w and the root, then v is an **ancestor** of w and w is a **descendant** of v.

Definition 10.5.2. A **binary tree** is a rooted tree in which every parent has at most two children. Each child in a binary tree is designated either a **left child** or a **right child** (but not both), and every parent has at most one left child and one right child. A **full binary tree** is a binary tree in which each parent has exactly two children.

Given any parent v in a binary tree T, if v has a left child, then the **left subtree** of v is the binary tree whose root is the left child of v, whose vertices consist of the left child of v and all its descendants, and whose edges consist of all those edges of T that connect the vertices of the left subtree. The **right subtree** of v is defined analogously.

Theorem 10.5.3. *If k is a positive integer and T is a full binary tree with k internal vertices, then*

1. *T has a total of $2k + 1$ vertices.*
2. *T has $k + 1$ leaves.*

Theorem 10.5.4. *For every integer $h \geq 0$, if T is any binary tree with height h and t leaves, then*

$$t \leq 2^h.$$

Corollary 10.5.5. *A full binary tree in which all the leaves are on the same level and has a height of h has 2^h leaves.*

Exercises

In each of the following, either draw a graph with the given specifications or explain why it cannot exist.

1. Full binary tree, 5 internal vertices.
2. Full binary tree, 5 internal vertices, 7 leaves.
3. Full binary tree 12 vertices.
4. Binary tree, height 4, 18 leaves.
5. Full binary tree, height 3, 7 leaves.

Problem for next time: How many nonisomorphic binary trees are there?

For now, try to derive the number of nonisomorphic binary trees of size up to 5.

Chapter 11

Appendix

11.1 Proof writing tips

11.1.1 General tips

Copy the statement of the theorem to be proved on your paper

This makes the theorem statement available for reference to anyone reading the proof.

Clearly mark the beginning of your proof with the word Proof

This word separates general discussion about the theorem from its actual proof.

Make your proof self-contained

Explain the meaning of each variable used in your proof. Begin proofs by introducing the initial variables to be used. This is similar to declaring variables and their data types at the beginning of a computer program.

Common words to start a proof are Assume, Let, If, Suppose.

Write your proof in complete, grammatically correct sentences

This does not mean that you should avoid using symbols and shorthand abbreviations, just that you should incorporate them into sentences.

Don't start your sentences with symbols. Try and prep the symbols with short phrases of where the sentence is going. Common words are Following, Since, This gives, We have, Now.

Keep your reader informed about the status of each statement in your proof

Your reader should never be in doubt about whether something in your proof has been assumed or established, or is still to be deduced. If something is assumed,

preface it with a word like Suppose or Assume. If it is still to be shown, preface it with words like, We must show that or In other words, we must show that. This is especially important if you introduce a variable in rephrasing what you need to show. (See Common Mistakes.)

Give a reason for each assertion in your proof

Each assertion in a proof should come directly from the hypothesis of the theorem, or follow from the definition of one of the terms in the theorem, or be a result obtained earlier in the proof, or be a mathematical result that has previously been established or is agreed to be assumed. Indicate the reason for each step of your proof using phrases such as by hypothesis, by definition of ... by theorem ... and so forth.

It is best to refer to definitions and theorems by name or number. If you need to state one in the body of your proof, avoid using a variable when you write it because otherwise your proof could end up with a variable that has two conflicting meanings.

Proofs in more advanced mathematical contexts often omit reasons for some steps because it is assumed that students either understand them or can easily figure them out for themselves. However, in a course that introduces mathematical proof, you should make sure to provide the details of your arguments because you cannot guarantee that your readers have the necessary mathematical knowledge and sophistication to supply them on their own.

Include the "little words and phrases" that make the logic of your arguments clear

When writing a mathematical argument, especially a proof, indicate how each sentence is related to the previous one. Does it follow from the previous sentence or from a combination of the previous sentence and earlier ones? If so, start the sentence with the word Because or Since and state the reason why it follows, or write Then, or Thus, or So, or Hence, or Therefore, or Consequently, or It follows that, and include the reason at the end of the sentence.

If a sentence expresses a new thought or fact that does not follow as an immediate consequence of the preceding statement but is needed for a later part of a proof, introduce it by writing Observe that, or Note that, or Recall that, or But, or Now.

Sometimes in a proof, it is desirable to define a new variable in terms of previous variables. In such a case, introduce the new variable with the word Let.

Display equations and inequalities

The convention is to display equations and inequalities on separate lines to increase readability, both for other people and for ourselves so that we can more easily check our work for accuracy.

11.1.2 Common Mistakes

Arguing from examples

Looking at examples is one of the most helpful practices a problem solver can engage in, and is encouraged by all good mathematics teachers. However, it is a mistake to think that a general statement can be proved by showing it to be true for some individual cases. A property referred to in a universal statement may be true in many instances without being true in general.

Using the same letter to mean two different things

Think of the "scope" of a mathematical variable as covering the entire proof. Make sure to not double use the same letter or symbol, unless you clearly redefine it.

Jumping to a conclusion

To jump to a conclusion means to allege the truth of something without giving an adequate reason. Especially for early proofs, always justify every step you take.

Assuming what is to be proved

To assume what is to be proved is a variation of jumping to a conclusion. This can be difficult with early proof classes, as sometimes a theorem can be used on a proof which itself relies on the validity of what is trying to be proved. This can generally be avoided by justifying every step of the proof.

Use of any when the correct word is some

Sometimes the word some acts like an any in a statement, and other times it acts like a there exists. I generally only use some when writing the phrase "[statement is true] for some [value]".

Misuse of the word if

Another common error is not serious in itself, but it reflects imprecise thinking that sometimes leads to problems later in a proof. This error involves using the word if when the word because is really meant. Using the word "if" can sometimes lead to doubt on whether the value is known. I like to use "if" in proofs when I am doing a proof with cases.

11.1.3 Example proofs:

Lemma 11.1.1. *If $p \in \mathbb{Z}$ is even, then p^2 is even.*

Proof. Let $p \in \mathbb{Z}$ be even, then by the definition of even $p = 2k$ for some $k \in \mathbb{Z}$. Now

$$p^2 = (2k)^2 = 4k^2 = 2(2k^2).$$

Letting $x = 2k^2$ we have $p^2 = 2x$ giving p^2 is even. □

Theorem 11.1.2. *$\sqrt{2}$ is irrational.*

Proof. Assume for contradiction that $\sqrt{2}$ is rational, then $\sqrt{2} = \frac{p}{q}$ for $p, q \in \mathbb{Z}$ where $q \neq 0$ and $\gcd\{p, q\} = 1$. This gives

$$\sqrt{2} = \frac{p}{q} \implies 2 = \frac{p^2}{q^2} \implies 2q^2 = p^2$$

which implies p^2 is even. Because p^2 is even p must be even. Following p is even $p = 2k$ for some $k \in \mathbb{Z}$. Now

$$\begin{aligned} 2q^2 = p^2 &\implies 2q^2 = (2k)^2 \\ &\implies 2q^2 = 4k^2 \\ &\implies q^2 = 2k^2. \end{aligned}$$

Therefore q is also even. However, this is a contradiction since we assumed $\gcd\{p, q\} = 1$. Thus $\sqrt{2}$ is irrational. □

Theorem 11.1.3. *For every integer n, $2n - 1$ is odd.*

Here are three different ways to prove this theorem.

Proof. If $n \in \mathbb{Z}$ is odd, then by the definition of odd $n = 2k + 1$ for some $k \in \mathbb{Z}$. Now

$$2n - 1 = 2(2k + 1) - 1 = 4k + 2 - 1 = 2(2k) + 1.$$

Let $x = 2k$ which is an integer. Therefore by the definition of being odd $2n - 1 = 2x + 1$ is odd.

If $n \in \mathbb{Z}$ is even, then by the definition of even $n = 2k$ for some $k \in \mathbb{Z}$. Now

$$2n - 1 = 2(2k) - 1 = 4k - 1 = 4k - 1 + 2 - 2 = 2(2k - 1) + 1.$$

Let $x = 2k - 1$ which is an integer. Therefore by the definition of being odd $2n - 1 = 2x + 1$ is odd. □

Proof. Assume for contradiction that $2n - 1$ is even for some integer $n \in \mathbb{Z}$, then $2n - 1 = 2k$ for some $k \in \mathbb{Z}$. Now

$$2n - 1 = 2k \implies 2n = 2k + 1 \implies n = k + \frac{1}{2}.$$

However this is a contradiction since we assumed n, k to be integers but $1/2$ is not an integer. Thus $2n - 1$ is odd. □

Proof. Let $n \in \mathbb{Z}$, then

$$2n - 1 = 2n + 2 - 2 - 1 = 2(n - 1) + 1.$$

Let $x = n - 1$ which is an integer. Therefore $2n - 1 = 2x + 1$ is odd. □

Theorem 11.1.4. *For every integer m, if m is even, then $3m + 5$ is odd.*

Proof. Let $m \in \mathbb{Z}$ such that m is even, then $m = 2k$ for some $k \in \mathbb{Z}$. Now

$$3m + 5 = 6k + 5 = 6k + 4 + 1 = 2(3k + 2) + 1.$$

Let $x = 3k + 2$ which is an integer. Therefore $3m + 5 = 2x + 1$ is odd. □

Theorem 11.1.5. *If k is any odd integer and m is any even integer, then $k^2 + m^2$ is odd.*

Proof. Let $k, m \in \mathbb{Z}$ such that k is odd and m is even, then $k = 2a + 1$ and $m = 2b$ for some $a, b \in \mathbb{Z}$. Now

$$k^2 + m^2 = (2a + 1)^2 + (2b)^2 = 4a^2 + 4a + 1 + 4b^2 = 2(2a^2 + 2a + 2b^2) + 1.$$

Let $x = 2a^2 + 2a + 2b^2$ which is an integer. Therefore $k^2 + m^2 = 2x + 1$ is odd. □

To show the statement "There exists an integer $m \geq 3$ such that $m^2 - 1$ is prime." is false we can take the negation and show it is true.

Theorem 11.1.6. *For all integers m, if $m \geq 3$ then $m^2 - 1$ is composite.*

Proof. Let $m \in \mathbb{Z}$ such that $m \geq 3$, then

$$m^2 - 1 = (m + 1)(m - 1).$$

Following that $m + 1$ and $m - 1$ are greater than 1 we have that $m^2 - 1$ is composite with factors of $m + 1$ and $m - 1$. □

To show the statement "There exists an integer n such that $6n^2 + 27$ is prime." is false we can take the negation and show it is true.

Theorem 11.1.7. *For all integers n, $6n^2 + 27$ is composite.*

Proof. Let $n \in \mathbb{Z}$, then

$$6n^2 + 27 = 3(2n^2 + 9).$$

Following 3 and $2n^2+9$ are integers greater than 1 we have $6n^2+27$ is composite with factors 3 and $2n^2 + 9$. □

To show the statement "There exists an integer $k \geq 4$ such that $2k^2 - 5k + 2$ is prime." is false we can take the negation and show it is true.

Theorem 11.1.8. *For all integers $k \geq 4$, $2k^2 - 5k + 2$ is composite.*

Proof. Let $k \in \mathbb{Z}$ such that $k \geq 4$, then

$$2k^2 - 5k + 2 = (2k - 1)(k - 2).$$

Following that $2k - 1$ and $k - 2$ are integers greater than 1 for $k \geq 4$ we have $2k^2 - 5k + 2$ is composite with factors $2k - 1$ and $k - 2$. □

Theorem 11.1.9. *Prove that the sum of any 3 consecutive integers is divisible by 3.*

Proof. Let $n \in \mathbb{Z}$, then 3 consecutive integers are $n - 1$, n, $n + 1$. Now

$$(n - 1) + n + n + 1 = 3n$$

which is divisible by 3. □