

# Discrete Maths Notes

November 19, 2023

## Contents

<b>1</b>	<b>Logic</b>	<b>4</b>
1.1	Propositional Logic . . . . .	4
1.1.1	Basics . . . . .	4
1.1.2	Terminology . . . . .	4
1.1.3	Examples . . . . .	5
1.1.4	Satisfiability, Tautology, Contradiction . . . . .	5
1.2	Truth Tables . . . . .	6
1.2.1	Basics . . . . .	6
1.2.2	Connective Outputs . . . . .	6
1.2.3	Examples . . . . .	7
1.2.4	Taut/Sati/Contra Exercises . . . . .	7
1.3	Equivalence . . . . .	9
1.3.1	Introduction to Equivalence . . . . .	9
1.3.2	Equivalence Laws . . . . .	11
1.4	Arguments . . . . .	13
1.4.1	Valid Arguments / Inference Rules . . . . .	14
1.4.2	Proving a Valid Argument . . . . .	16
1.4.3	The Deduction Method . . . . .	18
1.5	Predicate Logic . . . . .	19
1.5.1	Predicate representation . . . . .	20
1.5.2	Translating to Logical Expressions . . . . .	22
1.5.3	Translation Examples . . . . .	25
1.5.4	Negating Nested Quantifiers . . . . .	27
1.5.5	Arguments In Predicate Logic . . . . .	28
1.6	Chapter 1 Cheatsheet . . . . .	35
<b>2</b>	<b>Proofs</b>	<b>37</b>
2.1	Proof Basics . . . . .	37
2.2	Proof Methods . . . . .	38
2.2.1	Direct Proof . . . . .	38
2.2.2	Proof by Contraposition . . . . .	39
2.2.3	Proof by Contradiction . . . . .	40

2.2.4	Proof By Cases	42
2.3	Disproving a Statement & Proof Strategies	43
2.4	Proof by Induction	45
2.4.1	Examples	46
2.5	Strong Induction	47
2.5.1	Examples	47
<b>3</b>	<b>Sets</b>	<b>49</b>
3.1	Set Basics	49
3.1.1	Examples	51
3.2	Relationships Between Sets	52
3.3	Proving the relationships	53
3.3.1	Examples	53
3.4	Cartesian Product	55
3.5	Set Operations	56
3.5.1	Proving Relations Involving Set Operations	58
3.6	Set Identities	60
3.6.1	Proving Identities	61
<b>4</b>	<b>Recursion</b>	<b>62</b>
4.1	Sequences	63
4.2	Closed Form Solution	65
<b>5</b>	<b>Counting</b>	<b>68</b>
5.1	Basics	68
5.1.1	Multiplication Principle	69
5.1.2	Addition Principle	70
5.1.3	Principle of Inclusion and Exclusion (2-way)	71
5.1.4	Principle of Inclusion and Exclusion (n-way)	73
5.1.5	Pigeonhole Principle	75
5.2	Permutation and Combination	77
5.2.1	Permutation	78
5.2.2	Combinations	80
5.3	More Counting	81
5.3.1	Selecting Different Types Of Identical Objects	81
5.3.2	Arranging Different Types of Identical Objects	82
5.3.3	Arranging Objects in a Circle	83
5.3.4	Arranging Objects with Constraints (examples)	84
<b>6</b>	<b>Probability</b>	<b>85</b>
6.1	Basics	85
6.2	Conditional Probability	92
6.2.1	Corollary of Conditional Probability	93
6.2.2	Independence	93
6.2.3	Bayes Theorem	95
<b>7</b>	<b>Relations</b>	<b>97</b>
7.1	Basics	97

7.1.1	Binary Relation . . . . .	97
7.1.2	Graph Representation . . . . .	98
7.1.3	Table Representation . . . . .	98
7.1.4	Relation on One Set . . . . .	99
7.2	Relation Properties . . . . .	100
7.3	Types of Relations . . . . .	102

# 1 Logic

## 1.1 Propositional Logic

### 1.1.1 Basics

A **proposition** is a statement that is either true or false.

Prepositions will be represented mathematically with capital letters A, B, C...

These prepositions are then are connected into more complex compound prepositions using *connectives*. Connectives are statements like "and, implies, if-then" and are represented mathematically with the symbols below.

❗ It's not always easy to determine if they're true/false.

Connectives			
Symbol	Name	English Term(s)	Reading
$\wedge$	AND	And, But, Also	A and B
$\vee$	OR	-	A or B
$\implies$	IMPLICATION	If A, Then B If A, then B A implies B A, therefore B A only if B B follows from A A is a sufficient condition for B B is a necessary condition for A	A implies B
$\iff$	BICONDITIONAL	If & only if A is necessary and sufficient for B	A if and only if B
$\neg$	NEGATION	Not...	Not A

❗ A Biconditional can also be thought of  $(A \implies B) \wedge (B \implies A)$

Negation may sometimes be represented as  $A'$  or  $\overline{A}$

### 1.1.2 Terminology

$A \wedge B$  - conjunction of conjuncts A and B

$A \vee B$  - disjunction of disjuncts A and B

$A \implies B$  - A is the hypothesis/antecedent and B is the conclusion/consequence

### 1.1.3 Examples

#### 1 Compound Proposition

If all humans are mortal<sub>prp A</sub> and all Greeks are human<sub>prp B</sub>  
then all Greeks are mortal<sub>prp C</sub> can be represented as  $A \wedge B \implies C$

#### 2 Negation

Chocolate is sweet  $\rightarrow$  Chocolate is not sweet

Peter is tall and thin  $\rightarrow$  Peter is short or fat

The river is shallow or polluted  $\rightarrow$  The river is deep and polluted.

❗ Short and  
fat would be  
incorrect!

❗ Not shallow  
or not pol-  
luted would  
be incorrect!

#### 3 Implication: hypothesis and conclusion

If the rain continues then the river will flood

A sufficient condition for a network failure is that the central switch goes down

The avocados are ripe only if they are dark and soft

A good diet is a necessary condition for a healthy cat

### 1.1.4 Satisfiability, Tautology, Contradiction

A proposition is satisfiable if it is true for *at least one* combination of boolean values.

A Boolean Satisfiability Problem (SAT) is checking for satisfiability in a propositional logic formula.

❗ You don't  
need a whole  
truth table for  
this, just look  
for one!

A Tautology is a proposition that is always true

ex  $A \vee \neg A$

A Contradiction is a proposition that is always false.

ex  $A \wedge \neg A$

## 1.2 Truth Tables

### 1.2.1 Basics

Truth Tables are used for determining all the possible outputs of a complex compound proposition.

The Columns Are for the prepositions, intermediate compound prepositions and the whole compound proposition.

The Rows Are to contain the different sets of possible truth values for each proposition. You will have  $2^p$  rows where  $p$  is the number of propositions (then +1 for the header).

ⓘ The intrmt<sup>3</sup> prepositions are optional steps to make solving easier, use as needed.

▲ The connectives in a compound propositional logic problem follow an order of precedence (the PEMDAS of logic) in the following order;

$\neg$  ,  $\wedge$  ,  $\vee$  ,  $\implies$  ,  $\iff$

### 1.2.2 Connective Outputs

Negation	
$A$	$\neg A$
T	F
F	T

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

Or		
$A$	$B$	$A \vee B$
T	T	T
T	F	T
F	T	T
F	F	F

Implication		
$A$	$B$	$A \implies B$
T	T	T
T	F	F
F	T	T
F	F	T

Biconditional		
$A$	$B$	$A \iff B$
T	T	T
T	F	F
F	T	F
F	F	T

An implication is true when the hypothesis is false or the conclusion is true.

A Biconditional is true when the two propositions have the same value.

Out of all these outputs, the most unintuitive is the 3rd implication output ( $F, T \implies T$ ). The easiest way to understand this output is with the proposition “If it is raining, then the ground is wet”; now say you step outside and it is not raining, but the ground is wet. The entire statement isn’t false or incorrect, but the first part of it still has a false value. The only way to make an implication false is when the hypothesis is true but the conclusion is false.

### 1.2.3 Examples

$$A \implies B \iff B \implies A$$

$A$	$B$	$A \implies B$	$B \implies A$	—
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

$$A \wedge \neg B \implies \neg C$$

$A$	$B$	$C$	$A \wedge \neg B$	—
T	T	T	F	T
T	T	F	F	T
T	F	T	T	F
T	F	F	T	T
F	T	T	F	T
F	T	F	F	T
F	F	T	F	T
F	F	F	F	T

**i** Remember, columns like  $A \implies B$  are optional in-between steps to help solve each problem.

### 1.2.4 Exercise: Finding Tautologies, Satisfiable & Contradicting Props'

Indicate whether each of the following is a tautology, satisfiable but not a tautology or a contradiction;

$$A \implies B$$

$$A \implies A$$

$$A \implies \neg B \vee \neg C$$

$$A \vee B \implies B$$

$$(A \wedge B) \implies (A \vee B)$$

$$A \vee \neg A \implies B \wedge \neg B$$

(Answers and explanations on the next page...)

❶ Notice how none of these rely on drawing out a whole truth table! Focus on trying to find a way to get each proposition to output true and a way to get it to output false!

$$A \implies B$$

*Satisfiable but not a tautology*

Just knowing the properties of an implication you should know there's way to get true outputs and a false output.

$$A \implies A$$

*Tautology*

Only would be  $T \implies T$  or  $F \implies F$ , both of which result in true.

$$A \implies \neg B \vee \neg C$$

*Satisfiable but not a tautology*

Instead of making a long unpleasant truth table, it's easiest to start by simply looking for one true and one false possible output.

We can make the left side true simply by making A false, since all that remains is an or statement we now have a true output.

We can just as easily find a false output for this proposition with  $A = T$ ,  $B = T$  ( $\neg B = F$ ) to make the implication false, then we can just make  $\neg C$  false to make the or output false.

$$A \vee B \implies B$$

*Satisfiable but not a tautology*

If we make B true then the biconditional will always be true regardless of A.

There is only one way to make an implication false, so if we can set up A and B to result in that false output, it won't be a tautology. If we make A true and B false it will make the implication false!

$$(A \wedge B) \implies (A \vee B)$$

*Tautology*

Remember the only way to make an implication false is if the hypothesis is true and the conclusion is false. There is absolutely no way to do this because of the and/or setup!

$$A \vee \neg A \implies B \wedge \neg B$$

*Contradiction*


The left side is always true and the right side is always false. So the result of the implication is always false!



## 1.3 Equivalence

### 1.3.1 Introduction to Equivalence

---

 Two (compound) propositions  $P$  and  $Q$  are **logically equivalent** when their truth values always match (Meaning they'll have the same truth table!). Equivalence is denoted by  $P \equiv Q$ .

---

Equivalence relates heavily to the concept of Tautologies;

$P$  and  $Q$  are equivalent when  $P \iff Q$  is a tautology.

A proposition  $P$  is a tautology iff (if and only if) it is equivalent to  $T$  (true), i.e  $P \equiv T$

#### Examples

<sup>1</sup>

Given the implication  $A \implies B$ , are the following equivalent?

The contrapositive:  $\neg B \implies \neg A$

The converse:  $B \implies A$


$A$	$B$	$A \implies B$	$\neg B \implies \neg A$	$B \implies A$
T	T	T	T	T
T	F	F	F	T
F	T	T	T	F
F	F	T	T	T

Looking at the table we can see that  $A \implies B$  and  $\neg B \implies \neg A$  are equivalent.

Now, what about  $\neg A \vee B$ ?

$A$	$B$	$A \implies B$	$\neg A \vee B$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

Yep!  $\neg A \vee B \equiv A \implies B$ .

 This is actually one of the equivalence laws you'll see in the next section!

Understanding equivalent boolean expressions is very important in computer science (for code) and chip design (for logic gates). Consider the code below;

```
if (x > 0 || (x <= 0 && y > 100))
```

Lets see if we can change this expression to something equivalent but simplified.

Let  $A$  be  $x > 0$  and let  $B$  be  $y > 100$

Now we can compare the truth values of  $A \vee (\neg A \wedge B)$  and  $A \vee B$ .

$A$	$B$	$A \vee (\neg A \wedge B)$	$A \vee B$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	F

They're equivalent! We can reduce the if statement's expression to simply;

```
if (x > 0 || y > 100)
```

### 1.3.2 Equivalence Laws

For more complex propositions it is impractical to create a set of massive truth tables to check for equivalence. So instead we utilize equivalence laws to directly prove equivalence.

#### Nine Equivalence Laws;

*Many of these are pretty self-explanatory*

Double Negation Law:  $\neg(\neg A) \equiv A$

Identity Laws:  $A \wedge T \equiv A$        $A \vee F \equiv A$

Domination Laws:  $A \vee T \equiv T$        $A \wedge F \equiv F$

Commutative Laws:  $A \wedge B \equiv B \wedge A$        $A \vee B \equiv B \vee A$

Associative Laws:  $(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$        $(A \vee B) \vee C \equiv A \vee (B \vee C)$

Idempotent Laws:  $A \wedge A \equiv A$        $A \vee A \equiv A$

Distributive Laws:  $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$        $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$

DeMorgan's Laws:  $\neg(A \wedge B) \equiv \neg A \vee \neg B$        $\neg(A \vee B) \equiv \neg A \wedge \neg B$

Implication Laws:  $A \implies B \equiv \neg B \implies \neg A \equiv \neg A \vee B$

ⓘ Very similar to the algebraic distributive law

## Examples

<sub>1</sub> Prove  $A \vee (\neg A \wedge B) \equiv A \vee B$

$$\begin{aligned} A \vee (\neg A \wedge B) &\equiv (A \vee \neg A) \wedge (A \vee B) && \text{(Distributive)} \\ &\equiv T \wedge (A \vee B) \\ &\equiv A \vee B && \text{(Identity)} \end{aligned}$$

**i** In solving these, the goal should be to reduce the # of letters in the propositions. Focus on the side of an equivalence with more going on and try to reduce it down since the more complex proposition will have more opportunities to utilize the different equivalence laws.

<sub>2</sub> Simplify  $A \wedge \neg(A \wedge B)$

$$\begin{aligned} A \wedge \neg(A \wedge B) &\equiv A \wedge (\neg A \vee \neg B) && \text{(DeMorgan's)} \\ &\equiv (A \wedge \neg A) \vee (A \wedge \neg B) && \text{(Distributive)} \\ &\equiv F \vee (A \wedge \neg B) \\ &\equiv A \wedge \neg B && \text{(Identity)} \end{aligned}$$

**i** You don't have to name the laws you're using in the homework, the simple  $\equiv$  down the middle format for each step is fine.

<sub>3</sub> Show that  $(A \wedge B) \implies (A \vee B)$  is a tautology.

$$\begin{aligned} (A \wedge B) \implies (A \vee B) &\equiv \neg(A \wedge B) \vee (A \vee B) && \text{(Implication)} \\ &\equiv (\neg A \vee \neg B) \vee (A \vee B) && \text{(DeMorgan's)} \\ &\equiv \neg A \vee \neg B \vee A \vee B && \text{(Associative)} \\ &\equiv \neg A \vee A \vee \neg B \vee B && \text{(Commutative)} \\ &\equiv (\neg A \vee A) \vee (\neg B \vee B) && \text{(Associative)} \\ &\equiv T \vee T \\ &\equiv T && \text{(Idempotent)} \end{aligned}$$

## 1.4 Arguments

---

 An **argument** is a sequence of propositions in which the conjunction of the initial propositions implies the final proposition

An argument can be represented as;

$$P_1 \wedge P_2 \wedge P_3 \dots \wedge P_n \implies Q$$

---

### Examples

If George Washington was the first president of the United States, then John Adams was the first vice president. George Washington was the first president of the United States. Therefore John Adams was the first vice president.

- › Let A be “George Washington was the first president of the United States.”
- › Let B be "John Adams was the first vice president.”
- ›  $(A \implies B) \wedge A \implies B$

If Martina is the author of the book, then the book is fiction. But the book is nonfiction. Therefore Martina is not the author.

- › Let A be “Martina is the author of the book.”
- › Let B be “The book is fiction.”
- ›  $(A \implies B) \wedge \neg B \implies \neg A$

The dog has a shiny coat and loves to bark. Consequently, the dog loves to bark.

- › Let A be “The dog has a shiny coat.”
- › Let B be “The dog loves to bark.”
- ›  $A \wedge B \implies B$

### 1.4.1 Valid Arguments / Inference Rules

---

 An argument is **valid** if and only if **its conclusion is never false while its premises are true**.

---

We can't use a truth table to validate an argument since it only shows the truth values for the statement as a whole, instead we need to use new **Inference Rules**

#### Inference Rules

$$\begin{array}{cc} \frac{P}{P \Rightarrow Q} & \frac{P \Rightarrow Q}{\neg Q} \\ \hline \therefore Q & \hline \therefore \neg P \end{array}$$

Ex: If George Washington...      Ex: If Martina...

$$\frac{P \wedge Q}{\therefore P} \qquad \frac{P}{\therefore P \vee Q}$$

$$\frac{\begin{array}{c} P \\ Q \end{array}}{\therefore P \wedge Q}$$

Ex: Paul is a good swimmer. Paul is a good runner.

Therefore Paul is a good swimmer and a good runner

**i** *The items above the line can be combined/transformed into a new proof step defined below the line*

### Examples (finding conclusions)

1. If the car was involved in the hit-and-run, then the paint would be chipped. But the paint is not chipped.
  - > "Car was involved in a hit-and-run"  $\rightarrow P$
  - > "Paint would be chipped"  $\rightarrow Q$
  - > "The paint is not chipped"  $\rightarrow \neg Q$
  - > Conclusion: The car was not involved in a hit-and-run. From the second rule!
2. If the bill was sent today, then you will be paid tomorrow. You will be paid tomorrow.
  - > Nothing can be concluded from this. ☺
3. If the program is efficient<sub>P</sub>, it executes quickly<sub>Q</sub>. Either the program is efficient<sub>P</sub>, or it has a bug<sub>R</sub>. However, the program does not execute quickly<sub>¬Q</sub>.
  - > "If the program is efficient"  $\rightarrow P$
  - > "it executes quickly"  $\rightarrow Q$
  - > "it has a bug"  $\rightarrow R$
  - > "the program does not execute quickly"  $\rightarrow \neg Q$
  - > We start by knowing  $P \implies Q$  and  $P \vee R$  and  $\neg Q$ ...
  - >  $(P \implies Q)$  and  $\neg Q$  can imply  $\neg P$
  - > We need to transform  $P \vee R$  to use it:  $P \vee R \equiv \neg(\neg P) \vee R \equiv \neg P \implies R$
  - >  $\neg P \implies R$  and  $\neg P$  (the first implication we isolated) now implies  $R$  by the first inference rule.

## 1.4.2 Proving a Valid Argument

Assuming the premises are true, apply a sequence of premises and derivation rules, which include the equivalence laws and inference.

### General Steps

1. Identify all the premises (might need some transformations).
2. Think backwards. Start from what you want and then seek supporting premises, current results, and necessary equivalence laws and inference rules, until you reach the given premises.
3. Write the proof sequence, where **each step is either one premise or derived from previous step(s) using equivalence laws or inference rules.**

**i** Start with the RHS of the argument on the bottom of the list and work your way up

### Examples

1 Prove  $(A \implies B) \wedge (\neg C \vee A) \wedge C \implies B$

**i** This one is already in its standard form - so we just need to identify each part of the standard  $P_1 \wedge P_2 \wedge P_3 \dots \wedge P_n \implies Q$  form. At the end of this we want to prove that  $B$  is true.

$$\begin{array}{ccccccc}
 (A \implies B) & \wedge & (\neg C \vee A) & \wedge & C & \implies & B \\
 & \downarrow & \text{Implication Law} & & & & \\
 & \downarrow & \wedge & C \implies A & \wedge & C & \downarrow \\
 (A \implies B) & \wedge & \text{first inference rule law} & A & & & \downarrow \\
 & & \text{also by first inf rule} & B & & \implies & B
 \end{array}$$

**i** This is not usually how you would format these proofs, this table was to give you an idea of the actual process. The actual proof would look like the following;

1.  $A \implies B$
2.  $\neg C \vee A$
3.  $C$
4.  $C \implies A$  (2, Implication)
5.  $A$  (3,4)
6.  $B$  (1,5)

You need to put every step in a separate (numbered) line, starting with each component of the argument and then the transformations you do with the reason given. You don't need to name the law used but you need to mention the steps you combined to achieve the next part.



<sub>2</sub> Prove  $A \wedge (B \implies C) \wedge ((A \wedge B) \implies (D \vee \neg C)) \wedge B \implies D$

**i** For this one focus on step 3 ( $D \vee \neg C$ ) as your point to figure out this argument since its the only portion that has  $D$  in it.

1.  $A$
2.  $B \implies C$
3.  $(A \wedge B) \implies (D \vee \neg C)$
4.  $B$
5.  $A \wedge B$  (1,4)
6.  $D \vee \neg C$  (3,5)
7.  $C \implies D$  (6, Commutative, Implication) - Commutative used to swap  $C, D$
8.  $C$  (2,4)
9.  $D$  (7,8)

<sub>3</sub> Prove  $(A \implies B) \wedge (\neg C \vee A) \wedge C \implies A \wedge B$

**i** For this one notice that the right-hand side isn't a single letter anymore. We now need to focus on proving the whole  $A \wedge B$  statement. So this problem is actually solved a bit backwards, start by writing the last steps ( $A, B, A \wedge B$ ) and then go up and figure out how you can prove  $A$ .

1.  $A \implies B$
2.  $\neg C \vee A$
3.  $C$
4.  $C \implies A$  (2, Implication)
5.  $A$  (3,4)
6.  $B$  (1,5)
7.  $A \wedge B$  (5,6)

**i** If instead this problem was looking for  $A \vee B$ , you could just prove either  $A$  or  $B$  to make the entire statement valid.

### 1.4.3 The Deduction Method

Now, what if the conclusion is in implication form?

There are two ways of solving for this form, the main one being **The Deduction Method...**

Suppose the argument has the form:

$$P_1 \wedge P_2 \wedge P_3 \dots \wedge P_n \implies (R \implies S)$$

where the conclusion itself is an implication. We can add R as an additional premise and then imply S.  
In other words, we can have the argument:

$$P_1 \wedge P_2 \wedge P_3 \dots \wedge P_n \wedge R \implies S$$

#### Examples

<sub>1</sub> Prove  $(A \implies B) \wedge (B \implies C) \implies (A \implies C)$

**❶** *Start with C at the bottom. Now the only way to validate C is if B is true, so make B step 4 and find the proper relations to make B true.*

Deduction:  $(A \implies B) \wedge (B \implies C) \wedge A \implies C$

1.  $A \implies B$
2.  $B \implies C$
3.  $A$
4.  $B$  (1,3)
5.  $C$  (2,4)

<sub>2</sub> Prove  $\neg(A \wedge \neg B) \wedge (B \implies C) \implies (A \implies C)$

Deduction:  $\neg(A \wedge \neg B) \wedge (B \implies C) \wedge A \implies C$

1.  $\neg(A \wedge \neg B)$
2.  $B \implies C$
3.  $A$
4.  $\neg A \vee B$  (1, DeMorgan's)
5.  $A \implies B$  (4, Implication)
6.  $B$  (3,5)
7.  $C$  (2,6)

## 1.5 Predicate Logic

---

 A **predicate** represents the properties of/reasons among objects.

Examples:

*n is a perfect square*

*x is greater than y*

---

### Often propositional logic is not enough!

There are several cases where propositional logic won't help us reach needed conclusions or information;

Suppose we know that "All CS students must take CSCI 358". We cannot conclude that "Alice must take CSCI 358 where Alice is a CS student" using our current propositional logic knowledge.

Statements that hold many objects must be enumerated;

› Example:

- \* If Alice is a CS student, then Alice must take CSCI358.
- \* If Bob is a CS student, then Bob must take CSCI358.
- \* If Chris is a CS student, then Chris must take CSCI358.
- \* ...

› Solution: make statements with variables

- \* If  $x$  is a CS student, then  $x$  must take CSCI358.

Statements that define the property of a group of objects;

› Example:

- \* All new cars must be registered.
- \* Some of the new CS students graduate with honor.

› Solution: Make statements with quantifiers:

- \* Universal Quantifier - the property is satisfied by all members of the group.
- \* Existential Quantifier - at least one member of the group satisfies the property.

### 1.5.1 Predicate representation

Predicates are represented like functions in other branches of maths;

e.g  $P(x)$  represents some predicate such as "x is a perfect square".

Note that predicates can involve multiple variables, e.g  $Q(x,y)$  is "x is greater than y."

❗ Once we plug in a value for x, the predicate becomes a proposition

The two main quantifiers are represented with  $\forall$  and  $\exists$

- Universal Quantifier:  $\forall$ 
  - Read as "for all," "for every," "for each," or "for any."
  - Ex:  $\forall x, x > 0$  is read as "for any number x, x is greater than 0."
- Existential Quantifier:  $\exists$ 
  - Read as "there exists one," "there is," "for at least one," or "for some."
  - Example:  $\exists x, x > 0$  is read as "there exists a number x such that x is greater than zero."

❗ When  $\forall xP(x)$  or  $\exists xP(x)$  is used, the domain must be specified.

### Truth Values of Predicates

Predicate	True When...	False When...	Examples
$\forall xP(x)$	If P(x) is true for <b>every</b> x in the domain	If there is <b>any</b> x in the domain such that P(x) is false	$P(x)$ is $x + 1 > x$ , $\forall P(x)$ is true for the domain consisting of all real numbers. <hr/> $Q(x)$ is $x < 2$ . $\forall xQ(x)$ is false for the domain consisting of all real numbers because $Q(3)$ is false. $x = 3$ is a counterexample of $\forall xQ(x)$
$\exists xP(x)$	There's is an x <b>any-where</b> such that P(x) is true.	P(x) is false for <b>every</b> x	$P(x)$ is $x > 3$ . $\exists xP(x)$ is true for the domain consisting of all real numbers. Because when $x=4$ , P(4) is true. <hr/> $Q(x)$ is $X = x + 1$ . $\exists xQ(x)$ is false for the domain consisting of all real numbers. Because $Q(x)$ is false for every real number x

The quantifiers  $\forall$  and  $\exists$  have higher precedence than all logical connectives from propositional logic.

For Example:

$\forall xP(x) \wedge Q(x)$  means  $(\forall xP(x)) \wedge Q(x)$  rather than  $\forall x(P(x) \wedge Q(x))$

## Negating Quantified Expressions

$$\neg \forall x P(x) \equiv \exists x \neg P(x)$$

Example:

- › Every CS Student Must take CSCI385.
- › Negation: There is a CS student who doesn't have to take CSCI358

$$\neg \exists x P(x) \equiv \forall x \neg P(x)$$

Example:

- › There is s student in this class who has taken CSCI 262.
- › Negation: Every student in this class has **not** taken CS262

## 1.5.2 Translating to Logical Expressions

### *Converting statements to expressions*

#### English to Logical Expressions

<sub>1</sub> Every parrot is beautiful

Translation:

- › Assume that the domain consists of all parrots.
  - \* Let  $B(x)$  denote "x is beautiful"
  - \* Then  $\forall x B(x)$
- › Assume that the domain consists of all animals.
  - \* Let  $P(x)$  denote "x is a parrot".
  - \* Let  $B(x)$  denote "x is beautiful"
  - \* Then  $\forall x (P(x) \implies B(x))$

**i**  
 $\forall x (P(x) \wedge B(x))$   
would be incor-  
rect

<sub>2</sub> There exists a beautiful parrot

Translation:

- › Assume that the domain consists of all parrots.
  - \* Let  $B(x)$  denote "x is beautiful"
  - \* Then  $\exists x B(x)$
- › Assume that the domain consists of all animals.
  - \* Let  $P(x)$  denote "x is a parrot"
  - \* Let  $B(x)$  denote "x is beautiful"
  - \* Then  $\exists x (P(x) \wedge B(x))$

**i**  $\exists x (P(x) \implies B(x))$  is an incorrect solution. If  $x$  is not a parrot then  $P(x)$  is false, since  $P(x)$  is attached to the start of the implication it would make the entire expression true (when it should be false)

<sub>3</sub> Let  $P(x)$  denote "x speaks Russian"  
 and let  $Q(x)$  denote "x knows the computer language C++"  
 Let the domain consist of all students at Mines.  
 Translate the following into logical expressions;

There is a student at Mines who speaks Russian and knows C++

$$> \exists x (P(x) \wedge Q(x))$$

There is a student at Mines who speaks Russian but doesn't know C++

$$> \exists (P(x) \wedge \neg Q(x))$$

Every student at Mines either speaks Russian or knows C++

$$> \forall x (P(x) \vee Q(x))$$

No student at Mines speaks Russian or knows C++

$$> \forall x (\neg P(x) \wedge \neg Q(x))$$

$$> \text{or } \neg \exists x (P(x) \vee Q(x))$$

## Nested quantifiers

*More than one quantifier may be needed to represent the meaning of a statement in predicate logic.*

<sub>1</sub> Every real number has its corresponding negative

Assume that the domain consists of all real numbers

Let  $P(x, y)$  denote " $x + y = 0$ "

Then we can write  $\forall x \exists y P(x, y)$

<sub>2</sub> There is a person who loves everybody.

Assume that the domain consists of all people

Let  $L(x, y)$  denote " $x$  loves  $y$ ".

Then we can write  $\exists x \forall y L(x, y)$

## Order of quantifiers

When quantifiers are of the **same** type, the order doesn't matter.

Example:

- › Assume that the domain consists of all real numbers.
- › Let  $P(x, y)$  denote " $x + y = y + x$ "
- ›  $\forall x \forall y P(x, y)$  represents "For every real number  $x$ , for every real number  $y$ ,  $x + y = y + x$ ."
- ›  $\forall y \forall x P(x, y)$  represents "For every real number  $y$ , for every real number  $x$ ,  $x + y = y + x$ ."
- ›  $\forall x \forall y P(x, y)$  and  $\forall y \forall x P(x, y)$  have the same meaning!

When quantifiers are of **different** types, the order does matter!

Example:

- › Assume that the domain consists of all real numbers.
- › Let  $Q(x, y)$  denote " $x + y = 0$ "
- ›  $\forall x \exists y Q(x, y)$  represents "For every real number  $x$ , there is a real number  $y$ , such that  $x + y = 0$ ."
- ›  $\exists y \text{ for all } x Q(x, y)$  represents "There is a real number  $y$ , such that for every real number  $x$ ,  $x + y = 0$ ."
- ›  $\forall x \exists y Q(x, y)$  and  $\exists y \text{ for all } x Q(x, y)$  have different meanings!

Ex: Let  $Q(x, y, z)$  be " $x + y = z$ " and assume that the domain consists of all real numbers.

$$\forall x \forall y \exists z Q(x, y, z) \not\equiv \exists z \forall x \forall y Q(x, y, z)$$



### 1.5.3 Translation Examples

#### English to Logical Expression Examples

<sub>1</sub> Given the two unique statements;

1. John loves only Mary (If John loves any person, then that person is Mary.)
2. Only John loves Mary (If any person loves Mary, then that person is John.)

Let  $J(x)$  be "x is John". let  $M(x)$  be "x is Mary". Let  $L(x,y)$  be "x loves y". The domain consists of all people.

1. John loves only Mary.

- › For any person x, if x is John, then if it loves any person y, then y is Mary.
- ›  $\forall x (J(x) \implies \forall y (L(x,y) \implies M(y)))$   
Or  $\forall x \forall y (J(x) \wedge L(x,y) \implies M(y))$

2. Only John loves Mary.

- › For any person x, if x is Mary, then if any person y loves x, then y is John.
- ›  $\forall x (M(x) \implies \forall y (L(y,x) \implies J(y)))$   
Or  $\forall x \forall y (M(x) \wedge L(y,x) \implies J(y))$

<sub>2</sub> Given that;  $D(x)$  is "x is a dog".  $R(x)$  is "x is a rabbit".  $C(x,y)$  is "x chases y". The domain consists of all animals.

Translate the following;

1. All dogs chase rabbits.

- › For any animal, if it is a dog, then for any other animal, if that animal is a rabbit, then the dog chases it.
- ›  $\forall x (D(x) \implies \forall y (R(y) \implies C(x,y)))$

2. Some dogs chase all rabbits.

- › There is some animal that is a dog and, for any other thing, if that animal is a rabbit, then the dog chases it.
- ›  $\exists x \forall y (D(x) \wedge (R(y) \implies C(x,y)))$

3. Only dogs chase rabbits.

- › For any animals, if it is a rabbit then, if any animal chases it, that animal is a dog.
- ›  $\forall y (R(y) \implies \forall x (C(x,y) \implies D(x)))$
- › or: For any two animals, if one is a rabbit and the other chases it, then the other is a dog.
- ›  $\forall y \forall x (R(y) \wedge C(x,y) \implies D(x))$

## Mathematical Statements to Logical Expression Examples

<sub>1</sub> Translate "The sum of two positive integers is always positive."

Assume that the domain consists of all integers.

› For every two integers, if they are both positive, then the sum of them is positive.

›  $\forall x \forall y (x > 0 \wedge y > 0 \implies (x + y > 0))$

Assume that the domain consists of all positive integers.

› For every two positive integers, the sum of them is positive.

›  $\forall x \forall y (x + y > 0)$

<sub>2</sub> Translate "The difference of two positive integers is not necessarily positive."

Assume that the domain consists of all integers.

› It is not the case that, for every two integers, if they are both positive, then the difference of them is positive.

›  $\neg \forall x \forall y (x > 0 \wedge y > 0 \implies (x - y > 0))$

Or:  $\exists x \exists y ((x > 0 \wedge y > 0) \wedge (x - y \leq 0))$

---

## Logical Expressions to English Examples

<sub>1</sub> Translate:  $\forall x (C(x) \vee \exists y (C(y) \wedge F(x, y)))$ , where  $C(x)$  denotes "x has a computer,"  $F(x, y)$  denotes "x and y are friends," and the domain consists of all Mines students.

For every student x at Mines, x has a computer or there is a student y such that y has a computer and x and y are friends.

Simplifies to: Every student at Mines has a computer or a friend that has a computer.

<sub>2</sub> Translate:  $\exists x \forall y \forall z ((F(x, y) \wedge F(x, z) \wedge (y \neq z)) \implies \neg F(y, z))$ , where  $F(x, y)$  denotes "x and y are friends," and the domain consists of all students at Mines.

$\exists x \forall y \forall z ((F(x, y) \wedge F(x, z) \wedge (y \neq z)) \implies \neg F(y, z))$  means that if students x and y are friends, and students x and z are friends, and y and z are not the same student, then y and z are not friends.

There is a student x such that for every student y and every student z other than y, if x and y are friends, x and z are friends, then y and z are not friends.

There is a Mines student none of whose friends are friends.

#### 1.5.4 Negating Nested Quantifiers

**General Principle:** Moving a  $\neg$  across a quantifier changes the kind of quantifier.

What is the negation of  $\forall x \exists y (xy = 1)$ ?

Let  $P(x)$  denote  $\exists y (xy = 1)$

Then we know how to negate  $\forall x P(x)$

$$\neg \forall x P(x) \equiv \exists x \neg P(x)$$

In addition,  $\neg P(x) \equiv \neg \exists y (xy = 1) \equiv \forall y (xy \neq 1)$

Therefore, the negation of  $\forall x \exists y (xy = 1)$  is  $\exists x \forall y (xy \neq 1)$

### 1.5.5 Arguments In Predicate Logic

Just like propositional logic, we need to utilize inference rules to prove these arguments.

**Basic examples:** (Assume the domain is all Mines CS students.)

1. All the CS students must take CSCI 358. Thus some CS students must take CSCI 358.

›  $\forall x P(x) \implies \exists x P(x)$  ✓

› If every element has property P, then some element has property P

2. All the CS students must take CSCI 358. Thus Alice must take CSCI 358, where Alice is a CS student

›  $\forall x P(x) \implies P(a)$ , where  $a$  is a constant ✓

› If every element has property P, then a particular element has property P.

3. All the CS students must take CSCI 261 and CSCI 358. Thus all the CS students must take CSCI 261 and all the CS students must take CSCI 358.

›  $\forall x (P(x) \wedge Q(x)) \implies \forall x P(x) \wedge \forall x Q(x)$  ✓

› If both P and Q are true for all the elements, then P is true for all elements and Q is true for all elements (duh)

4. Some CS students graduate with honors. Thus all the CS students graduate with honors.

›  $\exists x P(x) \implies \forall x P(x)$  ✗

› If some element has property P, then all the elements have property P.

❗ The  $P(a)$  here represents a "constant" Alice whom is a particular element within the domain

❗ This one also just doesn't make intuitive sense. Try rewriting arguments like this into English and see if they make sense!

All the equivalence laws and inference rules still hold!

- Double Negation Law:  $\neg(\neg A) \equiv A$
- Identity Laws:  $A \wedge T \equiv A$        $A \vee F \equiv A$
- Domination Laws:  $A \vee T \equiv T$        $A \wedge F \equiv F$
- Commutative Laws:  $A \wedge B \equiv B \wedge A$        $A \vee B \equiv B \vee A$
- Associative Laws:  $(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$        $(A \vee B) \vee C \equiv A \vee (B \vee C)$
- Idempotent Laws:  $A \wedge A \equiv A$        $A \vee A \equiv A$
- Distributive Laws:  $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$   
 $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$
- DeMorgan's Laws:  $\neg(A \wedge B) \equiv \neg A \vee \neg B$   
 $\neg(A \vee B) \equiv \neg A \wedge \neg B$
- Implication Laws:  $A \rightarrow B \equiv \neg B \rightarrow \neg A \equiv \neg A \vee B$
- $P, P \rightarrow Q$  can imply  $Q$
- $P \rightarrow Q, \neg Q$  can imply  $\neg P$
- $P, Q$  can imply  $P \wedge Q$
- $P \wedge Q$  can imply  $P, Q$
- $P$  can imply  $P \vee Q$

However, these rules are not enough, predicates will utilize four new inference rules;

### Universal Instantiation

$\forall x P(x)$  can imply  $P(c)$ , where  $c$  is a particular element or any arbitrary element in the domain.

- › If for any  $x$  in which  $P(x)$  is true, then  $P(c)$  must also be true. More intuitively thought as the fact that if all elements in the domain have property "P", then any element (particular or arbitrary within the domain) must also have this property.

### Existential Instantiation

$\exists x P(x)$  can imply  $P(a)$ , where  $a$  is a particular element **not previously used in a proof sequence**

- ›  $\exists x P(x)$  means there must be some element in the domain that has property "P". Even though we don't know *exactly* what that element is, we can use the letter " $a$ " to represent this particular element.

### Universal Generalization

$P(c)$  can imply  $\forall x P(x)$ , where  $c$  is an arbitrary element in the domain.

- › If any/every arbitrary element in the domain has property  $P$  ( $P(c)$  always true), we can obviously say  $\forall x P(x)$

### Existential Generalization

$P(a)$  can imply  $\exists x P(x)$ , where  $a$  is a particular element.

- › If a particular element in the domain has property "P", we can obviously say  $\exists x P(x)$

**i** The first two rules can be used to remove the quantifiers in front of the predicates.  
The last two rules can be used to add quantifiers to the front of predicates

Let's look at all of these in more depth...

## Universal Instantiation (UI)

$\forall x P(x)$  can imply  $P(c)$ , where  $c$  is a particular element or any arbitrary element in the domain.

**Restrictions:** If  $c$  is a variable, it cannot be already in  $P(x)$

An **incorrect** use of UI would be saying  $\forall x \exists y P(x, y)$  implies  $\exists y P(y, y)$

For example, in the integer domain, if  $P(x, y)$  means " $y > x$ " then  $\forall x \exists y P(x, y)$  is true, but  $\exists y P(y, y)$  is false (y can't be greater than y ☺).

### Example

Prove the following argument is valid: "All CS students must take CSCI358. Alice is a CS student. Therefore Alice must take CSCI 358." The domain consists of all Mines students.

Let  $C(x)$  be " $x$  is a CS student."  $s$  is a constant symbol.  $D(x)$  is " $x$  has to take CSCI358"

The argument would be:  $\forall x (C(x) \implies D(x)) \wedge C(s) \implies D(s)$

1.  $\forall x (C(x) \implies D(x))$
2.  $C(s)$
3.  $C(s) \implies D(s)$  (1,UI)
4.  $D(s)$  (2,3)

## Existential Instantiation (EI)

$\exists x P(x)$  can imply  $P(a)$ , where  $a$  is a particular element **not previously used in a proof sequence**

In English: If  $P$  is true for some element of the domain, we can give that element a specific notation.

**Restrictions:**  $a$  must not be used before!

Incorrect Uses of EI:

›  $\exists P(x, a)$  CANNOT imply  $P(a, a)$

For example: in the integer domain, let  $P(x, y)$  denote  $x > y$  and  $a = 1$

›  $\forall x \exists y Q(x, y)$  CANNOT imply  $\forall x Q(x, a)$

For example: in the integer domain, let  $Q(x, y)$  denote that  $x > y$ .

Example:  $\forall x (P(x) \implies Q(x)) \wedge \exists y P(y) \implies Q(a)$

1.  $\forall x (P(x) \implies Q(x))$
2.  $\exists y P(y)$
3.  $P(a)$  (2,EI)
4.  $P(a) \implies Q(a)$  (1,UI)
5.  $Q(a)$  (3,4)

TODO: Update these incorrect use examples, what do these mean?

## Universal Generalization (UG)

$P(c)$  can imply  $\forall x P(x)$ , where  $c$  is an arbitrary element in the domain.

In English: If  $P(c)$  is true and  $c$  is arbitrary, then we can conclude  $\forall x P(x)$

No weird restrictions or common misuses.

Example:  $\forall x (P(x) \implies Q(x)) \wedge \forall x P(x) \implies \forall x Q(x)$

1.  $\forall x (P(x) \implies Q(x))$
2.  $\forall x P(x)$
3.  $P(c) \implies Q(c)$  (1,UI)
4.  $P(c)$  (2,UI)
5.  $Q(c)$  (3,4)
6.  $\forall x Q(x)$  (5,UG)



## Existential Generalization (EG)

$P(a)$  can imply  $\exists x P(x)$ , where  $a$  is a particular element.

In English: Something has been named as having property P, so we can say that there exists something that has property P.

**Restrictions:**  $x$  must not appear in  $P(a)$

Incorrect Uses of EG:

›  $P(z, y)$  CANNOT imply  $\exists y P(y, y)$

For example: In the positive integer domain, let  $P(x, y)$  mean that  $y > x$ , and  $a$  stands for 0, then  $y > 0$  does not mean  $y > y$

Example:  $\forall x P(x) \implies \exists x P(x)$

- |    |                  |         |
|----|------------------|---------|
| 1. | $\forall x P(x)$ |         |
| 2. | $P(a)$           | (1, UI) |
| 3. | $\exists x P(x)$ | (2, EG) |

## Proving a Valid Predicate Logic Argument (examples)

General Steps:

1. Strip off the quantifiers.
2. Work with the separate statements.
3. Insert quantifiers, as necessary.

$$_1 \forall x (P(x) \wedge Q(x)) \implies \forall x P(x) \wedge \forall x Q(x)$$

1.  $\forall x (P(x) \wedge Q(x))$
2.  $P(c) \wedge Q(c)$  (1,UI) **i** You can use the same arbitrary element  $c$  for both  $P$  and  $Q$
3.  $P(c)$  (2)
4.  $Q(c)$  (2)
5.  $\forall x P(x)$  (3,UG)
6.  $\forall x Q(x)$  (4,UG)
7.  $\forall x P(x) \wedge \forall x Q(x)$  (5,6)

$_2$  Prove the following argument is valid: “A student in this class has not attended any in-person classes. Everyone in this class passed the first exam. Therefore someone who passed the first exam has not attended any in-person classes.”

Let  $C(x)$  be “ $x$  is in this class,”  $B(x)$  be “ $x$  has attended in-person classes,” and  $P(x)$  be “ $x$  passed the first exam.” Let the domain consist of all Mines students.

$$\exists x (C(x) \wedge \neg B(x)) \wedge \forall x (C(x) \implies P(x)) \implies \exists x (P(x) \wedge \neg B(x))$$

1.  $\exists x (C(x) \wedge \neg B(x))$
2.  $\forall x (C(x) \implies P(x))$
3.  $C(a) \wedge \neg B(a)$  (1,EI)
4.  $C(a)$  (3)
5.  $C(a) \implies P(a)$  (2, UI)
6.  $P(a)$  (4,5)
7.  $\neg B(a)$  (3)
8.  $P(a) \wedge \neg B(a)$  (6,7)
9.  $\exists x (P(x) \wedge \neg B(x))$  (8,EG)

**i** Its easier to figure this one out in reverse, follow the proof from the bottom up as a process of what we need preceded by what we use to get it!

TODO: Add HW answers as examples later, HW had some weird situations that would be good to note.

## 1.6 Chapter 1 Cheatsheet

Connectives				
$\wedge$ AND	$\vee$ OR	$\implies$ IMPLIES	$\iff$ BICONDITIONAL	$\neg$ NEGATION
A and B	A or B	If A then B	A if and only if B	Not A
Both True	Either's True	$\star$	$A = B$	-

$\leftarrow$  true when

$\star$  - An implication is only false when A is true and B is false. *ref truth tables (1.2.2)*

Equivalence Laws	
Double Negation Laws	$\neg(\neg A) \equiv A$
Identity Laws	$A \wedge T \equiv A$ $A \vee F \equiv A$
Domination Laws	$A \vee T \equiv T$ $A \wedge F \equiv F$
Communicative Laws	$A \wedge B \equiv B \wedge A$ $A \vee B \equiv B \vee A$
Associative Laws	$(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$ $(A \vee B) \vee C \equiv A \vee (B \vee C)$
Idempotent Laws	$A \wedge A \equiv A$ $A \vee A \equiv A$
Distributive Laws	$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$ $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$
DeMorgans Laws	$\neg(A \wedge B) \equiv \neg A \vee \neg B$ $\neg(A \vee B) \equiv \neg A \wedge \neg B$
Implication Laws	$A \implies B \equiv \neg B \implies \neg A$ $A \implies B \equiv \neg A \vee B$
Not a law, but helpful biconditional equivalence...	$A \iff B \equiv (A \implies B) \wedge (B \implies A)$

Inference Rules	
$\frac{P \quad P \Rightarrow Q}{\therefore Q}$	Modus Ponens
$\frac{P \Rightarrow Q \quad \neg Q}{\therefore \neg P}$	Modus Tollens
$\frac{P \Rightarrow Q \quad Q \Rightarrow R}{\therefore P \Rightarrow R}$	Hypothetical Syllogism
$\frac{P \vee Q \quad \neg P}{\therefore Q}$	Disjunctive Syllogism
$\frac{P \quad Q}{\therefore P \wedge Q}$	Conjunction
$\frac{P \vee Q \quad \neg P \vee R}{\therefore Q \vee R}$	Resolution
$\frac{P}{\therefore P \vee Q}$	Addition
$\frac{P \wedge Q}{\therefore P}$	Simplification <i>• you're basically "pulling" p out to its own line</i>

### Quantified Inference Rules

**i** *These names don't really matter for this class*

TODO: Quantified Statement Inf Rules (ref saved screenshot) + other misc helpful stuff like negations of quantifiers. Just look up and copy-paste important details ☺

## 2 Proofs

### 2.1 Proof Basics

#### Some New Terminology

- › A **theorem** is a proposition that can be shown to be true.
- › A **lemma** is a preliminary proposition useful for proving later propositions.
- › A **corollary** is a proposition that can be established directly from a theorem.
- › A **conjecture** is a proposition that is being proposed to be a true statement.
- › Propositions that are simply accepted as true are called **axioms**.

ex: For all real numbers  $x$  and  $y$ ,  $x + y = y + x$

ex: There is a straight-line segment between every pair of points.

- › A **proof** is a valid argument that establishes the truth of a statement.  
Can use axioms, premises (if any) and previously proved theorems.

#### Common Theorem Forms

T

ex: " $\sqrt{2}$  is not a rational number."

$\exists x T(x)$

ex: "There exists one integer  $n$  such that  $n^2 + n + 41$  is composite"

- \* You would have to find an element  $a$  in the domain such that  $T(a)$  is true and then apply Existential Generalization
- \* To disprove, prove that  $T(x)$  is false for all elements in the domain

$\forall x (P(x) \implies Q(x))$

ex: "For every integer  $n$ , if  $3n + 2$  is odd, then  $n$  is odd."

- \* You would have to show that  $P(c) \implies Q(c)$ , where  $c$  is an arbitrary element of the domain, and then apply Universal Generalization
- \* Show that  $Q$  is true if  $P$  is true.
- \* To disprove, find a element  $e$  such that  $P(e)$  is true, but  $Q(e)$  is false.

$\forall x (P \iff Q)$

❶ Proving  $(P \iff Q)$  is equivalent to proving  $(P \implies Q) \wedge (Q \implies P)$

## 2.2 Proof Methods

There are four main proof methods;

Direct Proof   Proof by Contraposition   Proof by Contradiction   Proof by Cases

---

### 2.2.1 Direct Proof

Directly show that if P is true, then Q must be true, using axioms, definitions, and previously proven theorems, together with inference rules.

#### Examples

<sub>1</sub> Prove that "If  $n$  is odd, then  $n^2$  is odd."

Proof:

Assume that  $n$  is odd, then  $n = 2k + 1$ , where  $k$  is some integer.

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

Therefore,  $n^2$  is an odd integer.

<sub>2</sub> Prove that "If  $m$  and  $n$  are both perfect squares, then  $mn$  is also a perfect square."

Proof:

Assume that  $m$  and  $n$  are both perfect squares, then  $m = s^2$  and  $n = t^2$ , where  $s$  and  $t$  are some integers.

We have  $mn = s^2 t^2 = (st)^2$

Therefore,  $mn$  is a perfect square.

**i**  $n$  is odd when  $n = 2(\dots) + 1$ . We have to figure out how to transform  $n^2$  into this form.

### 2.2.2 Proof by Contraposition

Instead of proving  $P \implies Q$ , prove  $\neg Q \implies \neg P$ .

We do this because we can then utilize the implication law:

$$P \implies Q \equiv \neg Q \implies \neg P$$

#### Examples

<sub>1</sub> Prove that "For any integer  $n$ , if  $n^2$  is even, then  $n$  is even."

Proof:

Contraposition: "If  $n$  is odd, then  $n^2$  is odd."

(Reference example 1 of the direct proof)

We have now proven this theorem.

<sub>2</sub> Prove that "If  $3n + 2$  is odd for an integer  $n$ , then  $n$  is odd."

Proof:

Contraposition: "If  $n$  is even, then  $3n + 2$  is even"

Assume that  $n$  is even, then  $n = 2k$ , where  $k$  is some integer.

We have  $3n + 2 = 6k + 2 = 2(3k + 1)$

Therefore  $3n + 2$  is even.

We have proved the theorem "If  $3n + 2$  is odd then  $n$  is odd."

<sub>3</sub> Prove that "If  $r$  is irrational, then  $\sqrt{r}$  is also irrational"

Proof:

Contraposition: "if  $\sqrt{r}$  is rational, then  $r$  is rational."

Assume that  $\sqrt{r}$  is rational.

There exists integers  $p$  and  $q$  (no common factors), such that  $\sqrt{r} = \frac{p}{q}$

Squaring both sides gives  $r = \frac{p^2}{q^2}$

Since  $p^2$  and  $q^2$  are integers,  $r$  is also rational.

This proves the theorem.

### 2.2.3 Proof by Contradiction

Assume we want to prove  $S$  is true.

Now, suppose we can find a contradiction  $C$  such that  $\neg S \implies C$  is true.

Since  $C$  is false, but  $\neg S \implies C$  is true, then  $S$  must be true.

#### Examples

1 Prove that ' $\sqrt{2}$  is not a rational number.'

Proof:

Assume that  $\sqrt{2}$  is a rational number.

Then  $\sqrt{2} = \frac{p}{q}$  where  $p$  and  $q$  have no common factors and  $2 = \frac{p^2}{q^2}$  or  $2q^2 = p^2$

Since  $p^2$  is even,  $p$  is even (See example 1 of Proof by Contraposition). This means that 2 is a factor of  $p$ : hence 4 is a factor of  $p^2$ , and the equation  $2q^2 = p^2$  can be written as  $2q^2 = 4x$  for some integer  $x$ .

We have  $q^2$  is even and thus  $q$  is even (Same Proof by Contraposition Example)

Now 2 is a factor of  $q$  and a factor of  $p$ , which contradicts that statement that  $p$  and  $q$  have no common factors.

Hence,  $\sqrt{2}$  is not rational.



### Proof by Contradiction (cont.)

For prepositions of the implication form  $(P \implies Q)$ ...

We instead prove  $\neg(P \implies Q) \implies \text{T}$  or  $(P \wedge \neg Q) \implies \text{F}$

So, how do you find a contradiction?

- › Imply  $Q$ . Then assert  $Q \wedge \neg Q$  as a contradiction.
- › Imply  $\neg P$ . Then assert  $P \wedge \neg P$  as a contradiction.
- › Imply  $R \wedge \neg R$  during the proof for some proposition  $R$ .

### Examples

<sub>1</sub> Prove that "If  $3n + 2$  is odd for an integer  $n$ , then  $n$  is odd."

Proof:

Assume to the contrary that  $3n + 2$  is odd, and  $n$  is even.

Since  $n$  is even,  $n = 2k$ , where  $k$  is some integer.

We now have  $3n + 2 = 6k + 2 = 2(3k + 1)$

Thus  $3n + 2$  is even, which contradicts the assumption  $3n + 2$  is odd.

Therefore, we have proved the theorem "If  $3n + 2$  is odd, then  $n$  is odd."

<sub>2</sub> Prove that "If a number added to itself gives itself, then the number is 0"

Proof:

Assume to the contrary that  $x + x = x$  and  $x \neq 0$

Then  $2x = x$  and  $x \neq 0$

Because  $x \neq 0$ , we can divide both sides of the equation by  $x$  and arrive at  $2 = 1$ , which is a contradiction.

Hence,  $x + x = x \implies x = 0$

### 2.2.4 Proof By Cases

Assume that  $P \equiv P_1 \vee P_2 \vee \dots \vee P_n$ .

Instead of proving  $P \implies Q$ , prove  $(P_1 \implies Q) \wedge (P_2 \implies Q) \wedge \dots \wedge (P_n \implies Q)$ . We can do this because...

$$\begin{aligned} P_1 \vee P_2 \vee \dots \vee P_n \implies Q &\equiv \neg(P_1 \vee P_2 \vee \dots \vee P_n) \vee Q \\ &\equiv (\neg P_1 \wedge \neg P_2 \wedge \dots \wedge \neg P_n) \vee Q \\ &\equiv (\neg P_1 \vee Q) \wedge (\neg P_2 \vee Q) \wedge \dots \wedge (\neg P_n \vee Q) \\ &\equiv (P_1 \implies Q) \wedge (P_2 \implies Q) \wedge \dots \wedge (P_n \implies Q) \end{aligned}$$

#### Examples

<sub>1</sub> Prove that "If  $n$  is an even integer,  $4 \leq n \leq 12$  then  $n$  is the sum of two prime numbers."  
Proof:

We prove this for each value of  $n$  within the domain:

- >  $n = 4 = 2 + 2$
- >  $n = 6 = 3 + 3$
- >  $n = 8 = 3 + 5$
- >  $n = 10 = 5 + 5$
- >  $n = 12 = 5 + 7$

This completes the proof

<sub>2</sub> Prove that "For any two numbers  $x$  and  $y$ ,  $\|x\||y| = |xy|$ ."  
Proof:

There are 4 cases:

1.  $x \geq 0, y \geq 0$ 
  - >  $xy \geq 0$  and  $|xy| = xy = |x||y|$
2.  $x \geq 0, y < 0$ 
  - >  $xy \leq 0$  and  $|xy| = -xy = x(-y) = |x||y|$
3.  $x < 0, y \geq 0$ 
  - >  $xy \leq 0$  and  $|xy| = -xy = (-x)y = |x||y|$
4.  $x < 0, y < 0$ 
  - >  $xy > 0$  and  $|xy| = (-x)(-y) = |x||y|$

Therefore,  $|x||y| = |xy|$

## 2.3 Disproving a Statement & Proof Strategies

### Disproving a Statement

Find a counterexample of the statement! For example, "Every positive integer is the sum of the squares of two positive integers"

Proof:

3 cannot be written as the sum of squares of two integers.

To show this, note that the only possible integers are 0 and 1. And it is not possible to write 3 by summing the squares of 0 and 1 (or just 1 twice).

### What Makes a Good Proof?

- State your game plan.
- Keep a linear flow.\*
- A proof is an essay, not a calculation!
- Avoid excessive symbolism.
- Revise and simplify.
- Introduce notation thoughtfully.
- Structure long proofs.
- Be wary of the "obvious"

❗ One of the examples was showing  $2k$  was even!

### Proof Strategies

- Understand the definitions
- Analyze the meaning of the hypothesis and the conclusion
- Prove the statement using one of the proof methods.
- Use forward and backward reasoning.

## Example: Incorrect Proofs

The examples below contain proofs with some sort of highlighted issue related to the strategies and pitfalls mentioned above.

1. "The sum of two even numbers is a multiple of 4."

• Proof:

- Let  $x$  and  $y$  be even numbers.
- Then  $x = 2k$  and  $y = 2k$ , where  $k$  is an integer.
- So  $x + y = 2k + 2k = 4k$ , which is a multiple of 4.

$x$  and  $y$  may not be equal.

2. " $1/8 > 1/4$ ."

• Proof:

- $3 > 2$
- $3 \log_{10}(1/2) > 2 \log_{10}(1/2)$
- $\log_{10}(1/2)^3 > \log_{10}(1/2)^2$
- $(1/2)^3 > (1/2)^2$

The inequality symbol should be reversed when multiplying by a negative number.

3. " $1\text{¢} = \$1$ ."

• Proof:

$$1\text{¢} = \$0.01 = (\$0.1)^2 = (10\text{¢})^2 = \$1$$

$\$ \neq \$^2$

## 2.4 Proof by Induction

If you can prove that you can get to  $P(n+1)$  from  $P(n)$  and also prove that just  $P(1)$  is true you can prove  $\forall n P(n)$  since you're starting at 1 being true and saying anything following it will also be true.

❶ if  $P(1)$  is true and  $\forall k (P(k) \implies P(k+1))$  is true. Then we just follow  $P(1) \implies P(2), P(2) \implies P(3)$  and so on...

More specifically;

Let  $P$  be a predicate on positive integers. If...

1. Basis Step:  $P(1)$  is true.
2. Inductive Step:  $\forall k (P(k) \implies P(k+1))$  is true.
  - You prove this by assuming  $P(k)$  is true for an arbitrary positive integer  $k$  and show that  $P(k+1)$  is true.

$P(n)$  is true for all positive integers.

### General Steps / Template

1. Translate into the form “For all  $n \geq b, P(n)$ ” for a fixed integer  $b$ .
2. Write out the words “Basis step.” Then show that  $P(b)$  is true.
  - This is often just a basic sub-in and proving equality.
3. Write out the words “Inductive step.”
  - (a) State and clearly identify the inductive hypothesis, in the form “Assume that  $P(k)$  is true for an arbitrary (fixed) integer  $k \geq b$ .”
  - (b) State what needs to be proved under the assumption that the inductive hypothesis is true, i.e., write out what  $P(k+1)$  says.
  - (c) Prove  $P(k+1)$  to be true using the assumption  $P(k)$  is true.
4. Finally, state the conclusion.

### 2.4.1 Examples

**Note:**  
there's a ton  
of additional  
practice prob-  
lems on the  
9/19 slides if  
needed.

1 Prove:  $1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$  for any positive integer  $n$ .

Let  $f(n)$  denote " $1 + 2 + 3 + \dots + n$ "

Basis Step ( $n = 1$ ):  $1 = 1(1 + 1)/2$  ✓

Inductive Step:

- > Assume that for any arbitrary positive integer  $k$ ,  $f(k) = \frac{k(k+1)}{2}$
- > We need to show  $f(k+1) = \frac{(k+1)(k+2)}{2}$  ← here we're plugging in  $k+1$  in for  $k$
- >  $f(k+1) = 1 + 2 + 3 + \dots + k + (k+1) = f(k) + k(k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}$
- > Thus, the statement is true for  $k+1$  as well.

2 Prove  $n^2 > 3n$  for  $n \geq 4$  for any positive integer  $n$ .

Basis step ( $n = 4$ ): we have  $4^2 > 3 * 4$  ✓

Inductive Step:

- > Assume that for any arbitrary positive integer  $k \geq 4$ ,  $k^2 > 3k$
- > We need to show that  $(k+1)^2 > 3(k+1)$
- >  $(k+1)^2 = k^2 + 2k + 1$ 
  - $> 3k + 2k + 1$  (by the inductive hypothesis)
  - $\geq 3k + 8 + 1$  ( $k \geq 4$ )
  - $> 3k + 3$
  - $= 3(3 + 1)$  ← remember this is what we were trying to reduce the RHS to prove  $(k+1)^2 > 3(k+1)$

this completes the proof

3 Prove  $7^n - 2^n$  is divisible by 5 for any positive integer  $n$

Basis Step: ( $n = 1$ ): we have  $7 - 2 = 5$ , which is divisible by 5.

We need to show that  $7^{k+1} - 2^{k+1}$  is divisible by 5

Induction Step:

- > Assume that for any arbitrary positive integer  $k$ ,  $7^k - 2^k$  is divisible by 5.
- > We need to show that  $7^{k+1} - 2^{k+1}$  is divisible by 5.
$$\begin{aligned} 7^{k+1} - 2^{k+1} &= 7 * 7^k - 2 * 2^k \\ &= 7 * 7^k - 7 * 2^k + 5 * 2^k \\ &= 7 * (7^k - 2^k) + 5 * 2^k \end{aligned}$$
By the inductive hypothesis,  $7 * (7^k - 2^k)$  is divisible by 5,  
thus  $7^{k+1} - 2^{k+1}$  is divisible by 5.

this completes the proof

## 2.5 Strong Induction

---

Let  $P$  be a predicate on positive integers. If...

1.  $P(1)$  is true.

**i** This doesn't necessarily mean integer positive 1. This is wherever the set begins.

2.  $\forall k(P(1) \wedge P(2) \wedge P(3) \wedge \dots \wedge P(k) \implies P(k+1))$

Then  $P(n)$  is true for all positive integers.

---

This method has more assumptions that can be utilized for the proof as it's assuming a bunch of elements *up to*  $P(k)$  are true.

The template is nearly identical to our proof by induction.

### Induction vs Strong Induction

- Induction applies when information about "one position back" is enough for the inductive step.
- Strong induction applies when you cannot directly prove that  $P(k+1)$  is true just because you know  $P(k)$  is true.

**i** *Technically, you could use either type for a proof (as their technically equivalent). However, each is significantly easier for different types of proofs.*

#### 2.5.1 Examples

1 Prove: every integer  $n > 1$  is prime or a product of primes.

Basis step ( $n = 2$ ): 2 is prime.

Inductive step.

- > Assume that for any integer  $k \geq 2$ , the statement is true for any integer  $r$ , where  $2 \leq r \leq k$
- > We need to show that  $k+1$  is prime or a product of primes.

**i** we can split it into two the separate conditions using proof by cases.

- \* If  $k+1$  is prime, we're done.
- \* If  $k+1$  isn't prime, then  $k+1 = ab$ , where  $1 < a < k+1$  and  $1 < b < k+1$ , or equivalently  $2 \leq a \leq k$ ,  $2 \leq b \leq k$ . Based on this assumption,  $a$  and  $b$  are either prime or the product of primes. Thus,  $k+1 = ab$  is a product of primes.

This completes the proof

**i** There's also extra exercises for this on the 9/26 slides.

<sup>2</sup> Prove any amount of postage greater than or equal to 8 cents can be built using only 3-cent and 5-cent stamps.

Basis Step ( $n = 8$ ):  $8 = 3 + 5$

Inductive Step

- › Assume that given any positive integer  $k \geq 8$ , the statement is true for any integer  $r$ , where  $8 \leq r \leq k$ .
- › Show that  $k + 1$  can be built using only 3-cent and 5-cent stamps.
  - \* Case 1: ( $k + 1 = 9$ ):  $9$
  - \* Case 2: ( $k + 1 = 10$ ):  $10 = 5 + 5$
  - \* Case 3 ( $k + 1 \geq 11$ ):  $k + 1 = k - 2 + 3$ . Since  $k - 2 \geq 8$ ,  $k - 2$  can be written as the sum of 3's and 5's. Thus  $k + 1$  can be written as a sum of 3's and 5's.

This completes the proof.

That's a lot of cases to go through in the induction steps! Let's do this example again but let's add more base cases in the basis step to avoid adding proof by cases within the inductive step.

<sup>2.1</sup> Prove any amount of postage greater than or equal to 8 cents can be built using only 3-cent and 5-cent stamps.

Basis Step: ( $n = 8, 9, 10$ ):  $8 = 3 + 5, 9 = 3 + 3 + 3, 10 = 5 + 5$

Inductive Step:

- › Assume that given any positive integer  $k \geq 10$ , the statement is true for any integer  $r$ , where  $8 \leq r \leq k$
- › Show that  $k + 1$  can be built using only 3-cent and 5-cent stamps.
- ›  $k + 1 = k - 2 + 3$ . Since  $k - 2 \geq 8$ ,  $k - 2$  can be written as the sum of 3's and 5's.
- › Thus,  $k + 1$  can be written as the sum of 3's and 5's.

ⓘ this connects our inductive step to our basis step


This completes the proof.

TODO: add the tribonacci sequence exercise (its very different than the other examples covered)



## 3 Sets

---

 A **set** is an unordered collection of objects, which are called the members or elements of the set.

---

### 3.1 Set Basics

A Set is denoted by a capital letter with it's elements contained within curly brackets (comma seperated).

>  $C = \{\text{red, green, blue}\}$

$y \in S$  means that  $y$  is a member or an element of  $S$ ,

$y \notin S$  means that  $y$  is not a member or an element of  $S$ .

>  $\text{red} \in C = \{\text{red, green, blue}\}$ , but  $\text{yellow} \notin C$ .

Sets have no order!

>  $\{x, y\}$  is the same as  $\{y, x\}$

Each element only occurs once in a set.

>  $\{x, x\} \rightarrow x$

You can have sets of sets...

>  $\{\{a, b\}, \{\{b\}\}, \{\{e\}, f\}\}$

### Standard Sets


$\mathbb{N}$  = Set of all nonnegative integers  $\mathbb{N} = \{0, 1, 2, 3, \dots\}$

$\mathbb{Z}$  = Set of all integers  $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$

$\mathbb{Q}$  = Set of all rational numbers  $\frac{1}{2}, \frac{-3}{5}, 16, \dots$

$\mathbb{R}$  = Set of all real numbers  $\pi, e, -9, \sqrt{2}, \dots$

$\emptyset$  = Empty set A set with no elements.

 Note that  $\emptyset$  is not the same as  $\{\emptyset\}$

 A superscript of "+" restricts a set to its positive elements


### Describing a Set


List all the elements.

> Set of all positive even integers:  $S = \{2, 4, 6, 8, \dots\}$

Characterize the property of the elements -  $\{x|P(x)\}$

> Set of all positive even integers:  $S = \{x|x > 0 \text{ and } x = 2k \text{ for } k \in \mathbb{N}\}$

 this essentially means all  $x$  such that  $P(x)$  is true

 you can also use  $\wedge$  instead of "and" here.

### Size of a Set

The size or cardinality of set  $S$  is the number of elements in  $S$  denoted by  $|S|$ .

- ›  $A$  is the set of odd positive integers less than 10.  $|A| = 5$ .
- ›  $S$  is the set of letters in the English alphabet.  $|S|=26$
- ›  $|\emptyset| = 0$
- ›  $|\mathbb{N}| = \text{infinity}$ .

### Power Set

For a set  $S$ , the set consisting of **all** the subsets of  $S$  is called the power set of  $S$ , denoted by  $2^S$ .  $2^S = \{x \mid x \subseteq S\}$

The size of  $2^S$  is  $|2^S| = 2^{|S|}$

### Examples

<sub>1</sub> What is the power set of  $\emptyset$ ?

$$2^\emptyset = \{\emptyset\}$$

$$|2^\emptyset| = 2^0 = 1$$

<sub>2</sub> Let  $S = \{a, b, c\}$ . What is  $2^S$ ?

The subsets of  $S$ :

$$\emptyset$$

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

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

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

$$2^S = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$$

### 3.1.1 Examples

<sub>1</sub> Describe the following sets by listing their elements:

1.  $\{ x \mid x \in \mathbb{N} \text{ and } 3 < x \leq 7 \}$   
     $\triangleright \{4, 5, 6, 7\}$
2.  $\{ x \mid x \text{ is a month with exactly 30 days} \}$   
     $\triangleright \{ \text{April, June, September, November} \}$
3.  $\{ x \mid x \text{ is the capital of the United States} \}$   
     $\triangleright \{ \text{Washington DC} \}$

<sub>2</sub> Describe the following sets by giving a characterizing property.

1.  $\{ 1, 4, 9, 16 \}$   
     $\triangleright \{ x \mid 1 \leq x \leq 16 \text{ and } x = k^2 \text{ for } k \in \mathbb{N} \}$
2.  $\{ 2, 3, 5, 7, 11, 13, 17, \dots \}$   
     $\triangleright \{ x \mid x \text{ is prime} \}$

<sub>3</sub> Simplify the descriptions of the following sets:

1.  $A = \{ x \mid \exists y (y \in \{0,1,2\} \text{ and } x = y^3) \}$   
    •  $A = \{0,1,8\}$
2.  $B = \{ x \mid x \in \mathbb{N} \text{ and } \exists y (y \in \mathbb{N} \text{ and } x \leq y) \}$   
    •  $B = \mathbb{N}$
3.  $C = \{ x \mid x \in \mathbb{N} \text{ and } \forall y (y \in \mathbb{N} \implies x \leq y) \}$   
    •  $C = \{ 0 \}$   
    • (this is basically saying  $x$  is an integer that is smaller than every single integer, so our only option is 0.)

## 3.2 Relationships Between Sets

There are three main set relationships important to this class;

Subset   Equal   Proper Subset

Relationship	Definition	Details
<b>Subset</b>	A is a <u>subset</u> of B if every element of A is also in element B	<p>Denoted by: <math>A \subseteq B</math></p> <p>Logical Representation:  <math>\forall x (x \in A \implies x \in B)</math></p> <p>If <math>B = \{x   P(x)\}</math> and <math>A \subseteq B</math>, every element in A also has property <math>P(x)</math></p>
<b>Equal</b>	Two sets are <u>equal</u> if and only if they contain the same elements	<p>Denoted by <math>A = B</math></p> <p>Logical Representation:  <math>\forall x (x \in A \iff x \in B)</math>  or <math>\forall x (x \in A \implies x \in B) \wedge \forall x (x \in B \implies x \in A)</math></p> <p><math>A = B</math> if and only if <math>A \subseteq B \wedge B \subseteq A</math></p>
<b>Proper Subset</b>	If $A \subseteq B$ but $A \neq B$ , then A is a <u>proper subset</u> of B	<p>Denoted By <math>A \subset B</math></p> <p>Logical Representation:  <math>\forall x (x \in A \implies x \in B) \wedge \exists x (x \in B \wedge x \notin A)</math></p>

### Example

Let  $A = \{1, 7, 9, 15\}$ ,  $B = \{7, 9\}$ ,  $C = \{7, 9, 15, 20\}$

Then the following statements are all true;

$B \subseteq C$     $\{7,9\} \subseteq B$     $B \subset A$     $\{7\} \subset A$     $B \subseteq A$     $\emptyset \subseteq C$     $15 \in C$

" $\emptyset \subseteq C$ " is easier to understand if you look at the logical representation:

$\forall x (x \in \emptyset \implies x \in C) \rightsquigarrow \forall x (F \implies x \in C)$

Since  $\emptyset$  is an empty set, the first part of that implication is false (x cant be in nothing). Meaning the entire statement is true.

There are additional examples and exercises in the 9/28 slides if needed.

### 3.3 Proving the relationships

Prove that  $a \in A = \{x \mid P(x)\}$

- › Show that  $P(a)$  is true.

Prove that  $A \subseteq B = \{x \mid P(x)\}$

- › Pick an arbitrary  $x \in A$  and show that  $P(x)$  holds.  
(UG used to get the  $\forall$  in the subset def)

Prove that  $A \subset B = \{x \mid P(x)\}$

- › Prove that  $A \subseteq B$  but there exists  $a \in B$  such that  $a \notin A$ .

Prove that  $A = B$

- ›  $A = B$  means  $\forall x(x \in A \implies x \in B) \wedge \forall x(x \in B \implies x \in A)$
- › Equivalently,  $A = B$  if and only if  $A \subseteq B \wedge B \subseteq A$ .
- › Prove that  $A \subseteq B$  and  $B \subseteq A$ .

#### 3.3.1 Examples

<sup>1</sup> Let  $A = \{x \mid x \text{ is a multiple of } 8\}$ , and  $B = \{x \mid x \text{ is a multiple of } 4\}$ .

Prove that  $A \subseteq B$ .

Proof:

Let  $x \in$  be any arbitrary element.

We need to show that  $x$  is a multiple of 4.

Since  $x$  is a multiple of 8,  $x = 8k$  for some  $k \in \mathbb{Z}$

$x = 8k = 4 \cdot 2k = 4m$ , where  $m = 2k$ .

Thus  $x$  is a multiple of 4 and  $x \in B$ . So  $A \subseteq B$ .

(Some numbers, like 12, are multiples of 4 but not 8. So  $A \subset B$ )

• bruh

<sub>2</sub> Let  $A = \{ x \mid x \in \mathbb{R} \text{ and } x^2 - 4x + 3 = 0 \}$ , and  $B = \{ x \mid x \in \mathbb{N} \text{ and } 1 \leq x \leq 4 \}$ .

Prove that  $A \subset B$ .

Proof:

A can be written as  $A = 1, 3$  (just solving for when  $x$  satisfies that eq)

Let  $x \in A$ . We need to show that  $x \in \mathbb{N}$  and  $1 \leq x \leq 4$ . Thus  $x \in B$ .

If  $x = 3$ , then  $x \in \mathbb{N}$  and  $1 \leq x \leq 4$ . Thus  $x \in B$ .

› Same idea for 1.

So  $A \subseteq B$ .

$2 \in B$  but  $2 \notin A$ . So  $A \subset B$ .

❗ Since there's only two elements, we can just prove each directly.

<sub>3</sub> Let  $A = \{ x \mid x \in \mathbb{N}^+ \text{ and } x^2 < 15 \}$ , and  $B = \{ x \mid x \in \mathbb{N}^+ \text{ and } 2x < 7 \}$ .

Prove that  $A = B$ .

Proof:

$A \subseteq B$

› Let  $x \in A$ . Then  $x$  can be 1, 2 or 3.

›  $2x < 7$  for any of these three integers.

› Thus  $x \in B$  and  $A \subseteq B$ .

$B \subseteq A$

› Let  $x \in B$ . Then  $x$  can be 1, 2 or 3.

›  $x^2 < 15$  for any of these three integers.

› Thus  $x \in A$  and  $B \subseteq A$ .

Therefore, we proved that  $A = B$ .

❗ We're essentially just showing that the items of each of these sets are the same.

### 3.4 Cartesian Product

The Cartesian product of A and B, denoted by  $A \times B$ , is defined as  $A \times B = \{(x,y) \mid x \in A \wedge y \in B\}$ .

*This essentially means all the possible ordered pairs you can make with the items in A and B.*

$$A \times \emptyset = \emptyset, \emptyset \times A = \emptyset$$

$$A \times B = B \times A \text{ if}$$

$$> A = B \text{ or}$$

$$> A \text{ or } B \text{ is } \emptyset \text{ as this would satisfy that first bullet point idea.}$$

$$|A \times B| = |A| \times |B|$$

$$A^n = A \times A \times \dots \times A. \text{ (n times)}$$

$$> A^2 = A \times A$$

$$> A^3 = A \times A \text{ times } A.$$

Note that these multi-products creates an n-tuple set  $(\_, \_, \_, \dots)$

$$\text{In general, } (A \times B) \times C \neq A \times (B \times C) \neq A \times B \times C.$$

$$((\_, \_), \_) \quad (\_, (\_, \_)) \quad (\_, \_, \_)$$

These would only be equal when A, B, or C =  $\emptyset$

#### Examples

$$_1 A = \{1,2\}, B = \{2,4\}$$

$$A \times B = \{(1,2), (1,4), (2,2), (2,4)\}$$

$$B \times A = \{(2,1), (4,1), (2,2), (4,2)\}$$

$$_2 A = \{1,2\}$$

$$A^2 = \{(1,1), (1,2), (2,1), (2,2)\}$$

$$A^3 = \{(1,1,1), (1,1,2), (1,2,1), (1,2,2), (2,1,2), (2,2,1), (2,2,2)\}$$

## 3.5 Set Operations

Union   Intersection   Set Difference   Complement

Before each of these operations is introduced, let's look at the Venn Diagram as it is an important tool to demonstrate what these operations are "pulling" from the sets.

A set  $S$  is called the universal set if it contains all objects under consideration

A Venn diagram is used to visualize all possible relations of sets. All within this universal set  $S$  (depicted as a box around the Venn Diagram). Reference the image next to every set operations description for a quick visualization of the set relation.

**i** If we're considering all real numbers then  $S = \mathbb{R}$ . If we're considering students at Mines, then the set is all students at Mines.

**i** Note that while Venn diagrams are helpful for illustrating an operation, they should not be used for a proof

---

### Union

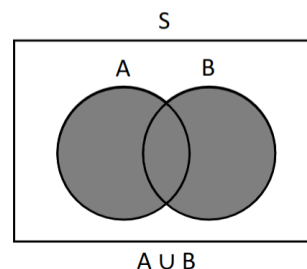
The union of  $A$  and  $B$ , denoted by  $A \cup B$  is  $\{x|x \in A \vee x \in B\}$

All the elements in  $A$  combined with all the elements in  $B$

#### Example

Let  $A = \{1, 3, 5, 7, 9\}$  and  $B = \{3, 5, 6, 10, 11\}$

Then  $A \cup B = \{1, 3, 5, 6, 7, 9, 10, 11\}$



### Intersection

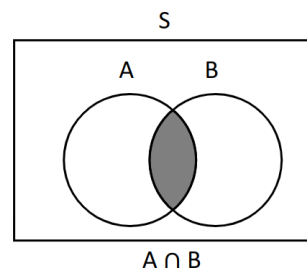
The intersection of  $A$  and  $B$ , denoted by  $A \cap B$  is  $\{x|x \in A \wedge x \in B\}$

The elements that are in both  $A$  and  $B$

#### Example

Let  $A = \{1, 3, 5, 7, 9\}$  and  $B = \{3, 5, 6, 10, 11\}$ .

Then  $A \cap B = \{3, 5\}$





## Set Difference

The set difference of A and B, denoted by  $A - B$ , is  $\{x | x \in A \wedge x \notin B\}$

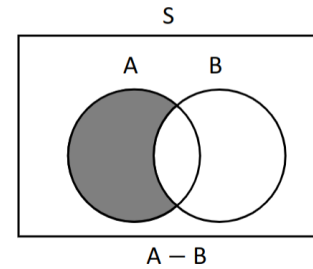
The elements that are in A but not in B

Note:  $A - B = A - (A \cap B)$

### Example

Let  $A = \{1, 3, 5, 7, 9\}$  and  $B = \{3, 5, 6, 10, 11\}$

Then  $A - B = \{1, 7, 9\}$



## Complement

Let  $A \subseteq S$ . The complement of A, denoted by  $A'$ , is  $\{x | x \in S \wedge x \notin A\}$

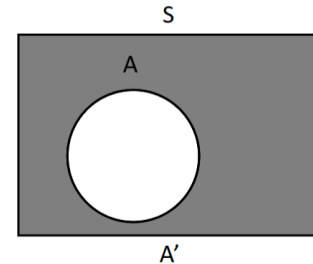
The set of everything not in A

### Example

$S = \mathbb{N}$

$A = \{x | x \in \mathbb{N} \wedge x = 2k \text{ for } k \in \mathbb{N}\}$

$A' = \{x | x \in \mathbb{N} \wedge x = 2k + 1 \text{ for } k \in \mathbb{N}\}$



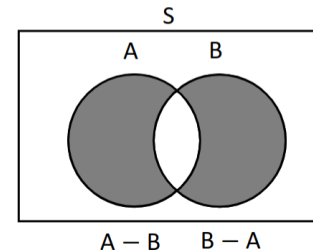
## Set Difference and Intersection

Two sets A and B are disjoint if  $A \cap B = \emptyset$ .

Meaning they have no elements in common

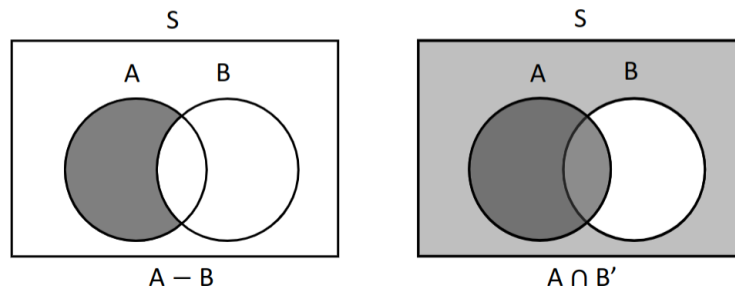
If A and B are disjoint, then  $A - B = A$  and  $B - A = B$

For any  $A \subseteq S, B \subseteq S$ ,  $A - B$  and  $B - A$  are disjoint.



## Set Difference and Complement

The set difference can be rewritten as  $\{x | x \in A \wedge x \in B'\}$ . Therefore,  $A - B = A \cap B'$



The darkest shaded part is what is actually included by the operation  $A \cap B'$ , the other shades are the "layers" of each operation

### 3.5.1 Proving Relations Involving Set Operations

(Examples)

In general, its good to start by looking at the Venn Diagram for visually understanding why a statement is true, and deriving the formal proof from there.

<sub>1</sub> Prove that  $A \cup B \subseteq A$

*We need to show that for some arbitrary element in A, that element is also in B.*

$\rightsquigarrow x \in A \implies x \in B$

Proof:

Let x be an arbitrary member of  $A \cap B$ .

$$\begin{aligned} x \in A \cap B &\implies x \in A \wedge x \in B \text{ using the definition of intersection here} \\ &\implies x \in A \text{ Treat } x \in A \wedge x \in B \text{ as } P \wedge Q \text{ and use Simplification Inf' Law} \end{aligned}$$

Therefore,  $A \cap B \subseteq A$ . *By the definition of subset relation*

*Or intuitively we've shown that any x in  $A \cap B$  is also in just A*

<sub>2</sub> Prove that  $C \subseteq A$  and  $C \subseteq B$  if and only if  $C \subseteq A \cap B$ .

*Remember we can break  $P \iff Q$  into  $(P \implies Q) \wedge (Q \implies P)$  where P is " $C \subseteq A$  and  $C \subseteq B$ " and Q is " $C \subseteq A \cap B$ "*

Proof:

First we need to prove the "only if" ( $P \implies Q$ ) part:

Let x be an arbitrary member of C.

$$\begin{aligned} x \in C &\implies x \in A \wedge x \in B \text{ Since } C \subseteq A \text{ and } C \subseteq B \\ &\implies x \in A \cap B \text{ Reference the intersection definition.} \end{aligned}$$

Now we prove the "If"  $Q \implies P$  part:

Let x be an arbitrary member of C.

$$\begin{aligned} x \in C &\implies x \in A \cap B \text{ From hypothesis } "C \subseteq A \cap B" \\ &\implies x \in A \wedge x \in B \text{ From the intersection definition again.} \end{aligned}$$

Therefore,  $C \subseteq A \wedge C \subseteq B$  *Reference the logical rep' of a subset (from the table)*

3 Prove that  $2^A \cap 2^B = 2^{A \cap B}$

*You can prove two sets to be equal by proving  $Left \subseteq Right$  and  $Right \subseteq Left$*

$\rightsquigarrow$  Prove  $2^A \cap 2^B \subseteq 2^{A \cap B}$  and  $2^{A \cap B} \subseteq 2^A \cap 2^B$

Proof:

$$2^A \cap 2^B \subseteq 2^{A \cap B}$$

Let  $x$  be an arbitrary member of  $2^A \cap 2^B$ .

$$\begin{aligned} x \in 2^A \cap 2^B &\implies x \in 2^A \wedge x \in 2^B \\ &\implies x \subseteq A \wedge x \subseteq B \quad \text{Ref Power Set Definition, If } x \text{ is a member of a power set, its also a member of the main set} \\ &\implies x \subseteq A \cap B \quad \text{Intersection Def-kinda ref examples above} \\ &\implies x \in 2^{A \cap B} \quad \text{Reverse use of the same Power Set Def, if } x \text{ is a member of this set, its also a member of the power set} \end{aligned}$$

Therefore  $2^A \cap 2^B \subseteq 2^{A \cap B}$

$$2^{A \cap B} \subseteq 2^A \cap 2^B$$

Let  $x$  be an arbitrary member of  $2^{A \cap B}$

$$\begin{aligned} x \in 2^{A \cap B} &\implies x \subseteq A \cap B \\ &\implies x \subseteq A \wedge x \subseteq B \\ &\implies x \in 2^A \wedge x \in 2^B \end{aligned}$$

Therefore,  $2^{A \cap B} \subseteq 2^A \cap 2^B$ .

4 Prove that if  $A \neq \emptyset$  and  $A \cap B = A - B$ , then  $B = \emptyset$

*Both a direct proof and proof by contraposition lead to you trying to prove a set is empty, which is very difficult. So the best option is proof by contradiction*

Proof:

Assume to the contrary that  $A \neq \emptyset$ ,  $A \cap B = A - B$  and  $B \neq \emptyset$

Case 1:  $A \cap B = \emptyset$  ( $A \cap B$  is empty)

$$A \cap B = A - B \quad (\text{from second assumption})$$

$$A - B = A \quad (\text{ref "set difference and intersection" notes.})$$

$$\text{All combining to } A \cap B = \emptyset = A - B = A \neq \emptyset$$

" $\emptyset \neq \emptyset$ ", We have a contradiction.


Case 2:  $A \cap B \neq \emptyset$

Let  $x$  be any element in  $A \cap B$ .

$$\begin{aligned} x \in A \cap B &\implies x \in A - B \quad (\text{from } A \cap B = A - B) \\ &\implies x \notin B \quad (\text{defn of a set difference}) \end{aligned}$$

This is a contradiction, since  $x \in A \cap B$  implies that  $x \in B$

## 3.6 Set Identities

 Set identities are a group of laws that can be used to prove equality between sets. They are all equalities, involving union, intersection, difference, and complementation, that are always true for all subsets of a given set S.

Set Identities	
Identity Laws	$A \cup \emptyset = A$ $A \cap S = A$
Domination Laws	$A \cup S = S$ $A \cap \emptyset = \emptyset$
Idempotent Laws	$A \cup A = A$ $A \cap A = A$
Complementation Law	$(A')' = A$
Commutative Laws	$A \cup B = B \cup A$ $A \cap B = B \cap A$
Associative Laws	$(A \cup B) \cup C = A \cup (B \cup C)$ $(A \cap B) \cap C = A \cap (B \cap C)$
Distributive Laws	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
DeMorgan's Laws	$(A \cap B)' = A' \cup B'$ $(A \cup B)' = A' \cap B'$
Absorption Laws	$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$
Complement Laws	$A \cup A' = S$ $A \cap A' = \emptyset$

TODO: Add venn diagram images (pictures including the rule is fine)

### 3.6.1 Proving Identities

(Examples)

1 Prove that  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Proof:

We need to prove:

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

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

Prove that  $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ :

Let  $x$  be an arbitrary member of  $A \cup (B \cap C)$

$$\begin{aligned} x \in A \cup (B \cap C) &\implies x \in A \vee x \in (B \cap C) \\ &\implies x \in A \vee (x \in B \wedge x \in C) \\ &\implies (x \in A \vee x \in B) \wedge (x \in A \vee x \in C) \\ &\implies (x \in A \cup B) \wedge (x \in A \cup C) \\ &\implies x \in (A \cup B) \cap (A \cup C) \end{aligned}$$

Prove that  $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$


Let  $x$  be an arbitrary member of  $(A \cup B) \cap (A \cup C)$ .

$$\begin{aligned} x \in (A \cup B) \cap (A \cup C) &\implies (x \in A \cup B) \wedge (x \in A \cup C) \\ &\implies (x \in A \vee x \in B) \wedge (x \in A \vee x \in C) \\ &\implies x \in A \vee (x \in B \wedge x \in C) \\ &\implies x \in A \vee x \in (B \cap C) \\ &\implies x \in A \cup (B \cap C) \end{aligned}$$

TODO: Add exercises if needed

## 4 Recursion

---

 A recursive definition is a definition in which the object being defined appears as part of the definition

---

There are two parts of a recursive definition:

Basis Step: some simple cases of the object being defined are explicitly given (end of the recursion).

Recursive step: New cases of the object being defined are given in terms of "previous" or "simpler" cases.

The relation in the recursive step is called the recurrence relation.

### Examples

1. Give a recursive definition for the ancestors of James.

Recursive Definition:

- Basis Step: James' parents are ancestors of James.
- Recursive Step: The parents of James' ancestors are ancestors of James.

2. Give a recursive definition of the exponentiation operation  $a^n$  on a nonzero real number  $a$ , where  $n$  is a nonnegative integer.

Recursive Definition:

- Basis Step:  $a^0 = 1$
- Recursive Step:  $a^n = (a^{n-1})a$  for  $n \geq 1$

## 4.1 Sequences

A sequence is an ordered list of elements, denoted by,

$$S_1, S_2, S_3, \dots$$

Where  $S_k$  denotes the  $k$ th element in the sequence.

Examples:

1,2,3,5,8 is a sequence of 5 elements.

1,3,9,27,81,...,  $3^n$ , ... is an infinite sequence.

### Summations

Given the sequence  $a_1, a_2, a_3, \dots, a_n$  we use the notation

$$\sum_{i=m}^n a_i$$

to denote the sum of the terms  $a_m, a_{m+1}, \dots, a_n$ . Read as "the sum from  $i = m$  to  $i = n$  of  $a_i$ "

Examples:

$$1 + 2 + \dots + n = \sum_{i=1}^n i$$

$$\sum_{j=1}^5 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2$$

### Recursively Defined Sequences

A sequence might be defined recursively by explicitly naming the first value (or the first few values) and then defining later values in terms of previous values.

#### Examples

1 Sequence  $F_n$

Basis Step:  $F_1 = 1, F_2 = 1$

Recursive step:  $F_n = F_{n-1} + F_{n-2}$  for  $n > 2$

The sequence is 1,1,2,3,5,8,13,21,... Otherwise known as the Fibonacci sequence.

2 Give a recursive definition of the sequence  $a_1, a_2, a_3, \dots$ , where  $a_n = 4n - 2$  for  $n \geq 1$

Basis Step:  $a_1 = 2$

Recursive step:  $a_n = a_{n-1} + 4$  for  $n \geq 2$

TODO (if needed): Add Fibonacci Proof.

## Recursively Defined Sets

A set might be defined recursively by explicitly describing one or more simple elements and then defining other elements in terms of existing simpler elements in the set. This is done by using an implication;  $x \in S \implies F(x) \in S$  where  $F(x)$  is some operation based on the simpler  $x$  known to be in the set to get the next item in the set.

<sub>1</sub> The set of positive integers, denoted by  $\mathbb{N}^+$  has the recursive definition:

1 is  $\mathbb{N}^+$

If  $n$  is in  $\mathbb{N}^+$ , then  $n+1$  is in  $\mathbb{N}^+$

<sub>2</sub> Give a recursive definition of the set  $S$  of positive integers that are multiples of 5.

Basis Step:  $5 \in S$

Recursive step: If  $x \in S$ , then  $x + 5 \in S$  (or  $x \in S \implies x + 5 \in S$ )

The way this works is by this logic; we know 5 is in  $S$ , so that means 10 is in  $S$ , since 10 is in  $S$ , then 15 is in  $S$  and so on...

<sub>3</sub> Give a recursive definition of the set of strings, that, is  $\Sigma^* = "", "a", "amigien", "words", "school", "ziemg", "dslfkjfsdkl" \dots$

Notations:

$\lambda$  is the empty string "".

$\Sigma$  is the set of all letters a,b,c...

Let  $x \in \Sigma^*$  and  $y \in \Sigma^*$ .  $xy$  is the concatenation of  $x$  and  $y$ .

Recursive Definition:

Basis step:  $\lambda \in \Sigma^*, x \in \Sigma^*$  where  $x \in \Sigma$

Recursive step:  $x \in \Sigma^* \implies xy \in \Sigma^*$  where  $y \in \Sigma$  (where  $y$  is a letter)

basically means you can append any letter to any of the existing strings (including empty string) to generate more strings ad infinitum

Alternate Recursive step:  $x \in \Sigma^* \wedge y \in \Sigma^* \implies xy \in \Sigma^*$

There's a ton of exercises and further descriptions of the examples in the videos and slides, add those if needed!



## Recursively Defined Sequence

### 4.2 Closed Form Solution

#### Intro/Motivation

Consider the following recursively defined sequence;

Basis step:  $S_1 = 2$

Recursive Step:  $S_n = 2S_{n-1}$  for  $n \geq 2$

$S$  would be the sequence 2,4,8,16,32 *notice a pattern here?*

If you were to represent this sequence in code you'd get something like one of these;

```
int S_prev = 2;                                int CompSn(int n)
for(int i = 2; i <= n; ++i)                    {
{
    S = 2*S_prev;                                if(n == 1)
    S_prev = S;                                return 2;
}                                              return 2*CompSn(n-1);
}                                              }
```

Note that both of these would be  $O(n)$ , quite a gross time complexity for something with a clear trend.

Looking back at our sequence  $S_n$  is just  $2^n$ ! In other words, our two sets of code could be replaced with an  $O(\log n)$  `int Sn = pow(2,n).`

ⓘ This time complexity comes from the implementation of pow

## Definitions

What we did above is an example of finding/solving the **closed-form solution**.

An equation, where we can substitute values and get the output value back directly, is called a closed-form solution.

Another example would be  $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$  as the closed-form solution to  $ax^2 + bx + c = 0$ . Note that an algorithm is not a closed-form solution because you cannot get an output value directly.

Not all kinds of recurrence relations can be solved.

A recurrence relation for a sequence  $S_1, S_2, S_3, \dots$  is a linear recurrence relation if  $S_n$  is a linear function of the previous elements.

- › The general linear recurrence relation has the form:

$$S_n = f_1(n)S_{n-1} + f_2(n)S_{n-2} + \dots + f_k(n)S_{n-k} + g(n)$$

where  $1 \leq k \leq n-1$ , the  $f_i$ 's and  $g$  can be expressions involving  $n$ .

- › The recurrence relation has constant coefficients if the  $f_i$ 's are all constants.

A recurrence relation is first-order if the  $n$ th element depends only on the  $(n-1)$ th element.

$$S_n = 2S_{n-1} \quad \text{Linear, first-order.}$$

examples:  $F_n = F + n - 1 + F_{n-2}$  Linear but not first order.

$$S_n = S_{n-1}S_{n-2} \quad \text{Not Linear.}$$

- › The general form solution with a constant coefficient  $S_n = cS_{n-1} + g(n)$  for  $n \geq 2$  can be expanded  $k$  times to look like;

$$c^k S_{n-k} + c^{k-1}g(n - (k-1)) + \dots + cg(n-1) + g(n)$$

This series of expansions will stop when  $n-k=1$  So we can say that  $k=n-1$ . Giving us a better solution of  $c^{n-1}S_1 + c^{n-2}g(2) + \dots + cg(n-1) + c^0g(n)$ . Finally we can simplify this further by using summation notation;

$$S_n = c^{n-1}S_1 + \sum_{i=2}^n c^{n-i}g(i)$$

So to solve for linear first-order, constant coeff recurrence relations you must identify  $c$  and  $g(n)$  and plug into the form above. You can identify  $c$  and  $g(n)$  by arranging the recurrence relation into the  $S_n = cS_{n-1} + g(n)$  form.

## For Quick Reference

$$S_n = \overbrace{cS_{n-1} + g(n)}^{\text{Recurrence Relation of this form}} = \underbrace{c^{n-1}S_1 + \sum_{i=2}^n c^{n-i}g(i)}_{\text{Has this solution}}$$

## Examples

<sub>1</sub> Solve  $S_n = 2S_{n-1} + 3$  for  $n \geq 2$  with  $S_1 = 4$

Match and identify  $c$  and  $g(n)$

$$c = 2 \quad g(n) = 3$$

Substitute in  $S_n = c^{n-1}S_1 + \sum_{i=2}^n c^{n-i}g(i)$

$$\begin{aligned} S_n &= 2^{n-1} * 4 + \sum_{i=2}^n 2^{n-1} * 3 \\ &= 2^n + 1 + 3(2^{n-1} - 1) \end{aligned}$$

We're Simplifying the summation here by using the identity:  $1 + 2 + 2^2 + \dots + 2^m = 2^{m+1} - 1$  where  $m = n - 2$

<sub>2</sub> Solve  $T_n = T_{n-1} + (n + 1)$  for  $n \geq 2$  with  $T_1 = 2$

Match and identify  $c$  and  $g(n)$

$$c = 1 \quad g(n) = n + 1$$

Substitute


$$\begin{aligned} T_n &= 1^{n-1} * 2 + \sum_{i=2}^n 1^{n-i}(i + 1) \\ &= 2 + (3 + 4 + \dots + (n + 1)) \\ &= \frac{(n+1)(n+2)}{2} - 1 \end{aligned}$$

We're simplifying using the identity:  $1 + 2 + 3 + \dots + m = \frac{m(m+1)}{2}$

## 5 Counting

### 5.1 Basics

---

 Counting is the process of determining the number of a set of objects with certain properties.

For example;

- The number of students in a classroom
  - Number of phone numbers in the US
  - Least number of students out of 15 born on the same day of the week.
- 

Counting problems can be very difficult and now obvious to solve. The general technique and solution to counting problems is to divide and conquer, simplifying the problem by decomposing it.

More specifically, we'll be working with four counting principles;

Multiplication Principle	Addition Principle
Principle of inclusion and exclusion	Pigeonhole principle

### 5.1.1 Multiplication Principle

Suppose that a task can be broken down into a sequence of two independent steps. If there are  $n_1$  ways to do the first step and for each of ways of doing the first step, there are  $n_2$  ways to do the second step, then there are  $n_1 n_2$  ways to complete the task.

Set Representation: Let  $A$  and  $B$  denote the set of ways to do the first and second step, respectively. Then  $|A \times B| = |A| \cdot |B|$

Generalization: If a task can be broken into a sequence of  $m$  **independent** steps, where step  $i$  can be done in  $n_i$  ways,  $i = 1, 2, \dots, m$ , then the number of ways to complete the task is;

$$\prod_{i=1}^m n_i = n_1 \cdot n_2 \cdot n_3 \cdot \dots \cdot n_m$$

**Note that**  
 $\prod$  is the product of everything in the sequence.

### Examples

<sub>1</sub> The chairs of an auditorium are to be labeled with an uppercase English letter followed by a positive integer not exceeding 100. What is the largest number of chairs that can be labeled differently?

Label a chair by a sequence of 2 steps:

- Step 1: Choose an uppercase English letter    26 ways  $\{A, B, C, \dots, Z\}$   
Step 2: Choose a positive integer  $\leq 100$     100 ways  $\{1, 2, \dots, 100\}$

Therefore, there are  $26 \times 100 = 2600$  different labels.

<sub>2</sub> The last part of your telephone number consists of four digits. How many such four-digit numbers are there?

Construct a four-digit number by a sequence of 4 steps:

- Step 1: Choose the 1st digit    10 ways  $\{0, 1, 2, \dots, 9\}$   
Step 2: Choose the 2nd digit    10 ways  $\{0, 1, 2, \dots, 9\}$   
Step 3: Choose the 3rd digit    10 ways  $\{0, 1, 2, \dots, 9\}$   
Step 4: Choose the 4th digit    10 ways  $\{0, 1, 2, \dots, 9\}$

Therefore, there are  $10^4$  different numbers.

### 5.1.2 Addition Principle

If a task can be done either in one of  $n_1$  ways or in one of  $n_2$  ways, where these two sets have no common ways, then there are  $n_1 + n_2$  ways to do the task.

Set representation: Let  $A$  and  $B$  denote two disjoint sets of ways, then  $|A \cup B| = |A| + |B|$

Generalization: If a task can be done either in one of  $n_1$  ways, in one of  $n_2$  ways,... or in one of  $n_m$  ways, **where no two sets share common ways**, then the number of ways to complete a task is:

$$\sum_{i=1}^m n_i = n_1 + n_2 + n_3 + \dots + n_m$$

#### Example

One restaurant has 2 types of salad and 3 types of soup. Choose one item as appetizer. How many options are there?

$A = \{\text{salad1, salad2}\}$

$B = \{\text{soup1, soup2, soup3}\}$

The total number of options are  $2 + 3 = 5$

#### Example - Combining Multiplication and Addition

How many binary strings of length 6 end with 00 or 01?

$C_1$ : Strings ending with 00

Step 1: Select the 1st digit    2 ways  $\{0,1\}$

Step 2: Select the 2nd digit    2 ways  $\{0,1\}$

Step 3: Select the 3rd digit    2 ways  $\{0,1\}$

Step 4: Select the 4th digit    2 ways  $\{0,1\}$

Step 5: Select the 5th digit    1 way  $\{0\}$

Step 6: Select the 6th digit    1 way  $\{0\}$

By the multiplication principle, there are  $2^4$  strings

$C_2$  Strings ending with 01

By the multiplication principle, there are  $2^4$  strings

By addition principle there are  $2^4 + 2^4 = 32$  strings.

These two methods together are not enough, and can actually lead to us getting incorrect answers!

For example;

How many binary strings of length 8 either start with 1 or end with 00?

- › Strings starting with 1:  $2^7$
- › Strings ending with 00:  $2^6$
- › Thus the answer would be  $2^7 + 2^6$

Except this answer is **wrong!**

Strings starting with 1 and ending with 00 are counted twice!

We're overcounting  $2^5$  strings, we need to subtract this double-counted amount to have the right answer. The correct answer is actually  $2^7 + 2^6 - 2^5 = 160$

This fix leads us into our next principle...

### 5.1.3 Principle of Inclusion and Exclusion (2-way)

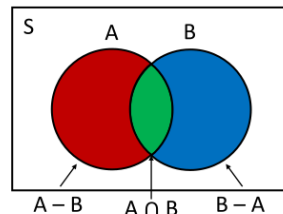
If a task can be done either in one of  $n_1$  ways **or** in one of  $n_2$  ways, then the number of ways to do the task is  $n_1 + n_2$  minus the number of *common* ways in these sets.

Set Representation:  $|A \cup B| = |A| + |B| - |A \cap B|$

It's easier to understand this set representation of the size given a Venn diagram (pictured rightside).

However, from this diagram it's important to also notice that the red area,  $|A - B| = |A| - |A \cap B|$  (similar for  $|B - A|$ ).

This equation ends up being extremely valuable for many counting problems, so keep it in mind.



## Examples

A computer company receives 350 applications for a job. Suppose that 220 of these applicants majored in computer science, 147 majored in business, and 51 majored in both computer science and business.

1 How many of these applicants majored in neither computer science nor business?

S: set of all applicants  $|S| = 350$

C: set of all applicants that majored in CS,  $|C| = 220$

B: set of applicants majored in business,  $|B| = 147$

Meaning  $|C \cap B| = 51$

What is  $|C' \cap B'|$ ?

By DeMorgans law, we know that  $|C' \cap B'| = |(C \cup B)'|$

$= |S - (C \cup B)|$  by complement definition

$= |S| - |C \cup B|$  from the venn diagram observation

› Now we just need  $|C \cup B|$ , this is where we apply princ of inc/exclusion

$= |S| - (|C| + |B| - |C \cap B|)$

› Now its just simple substitution

$= 350 - (220 + 147 - 51) = 34.$

2 How many of these applicants majored in CS but not in business?

$|C| = 220 \quad |B| = 147 \quad |C \cap B| = 51$

$|C - B| = |C| - |C \cap B|$  from venn diagram

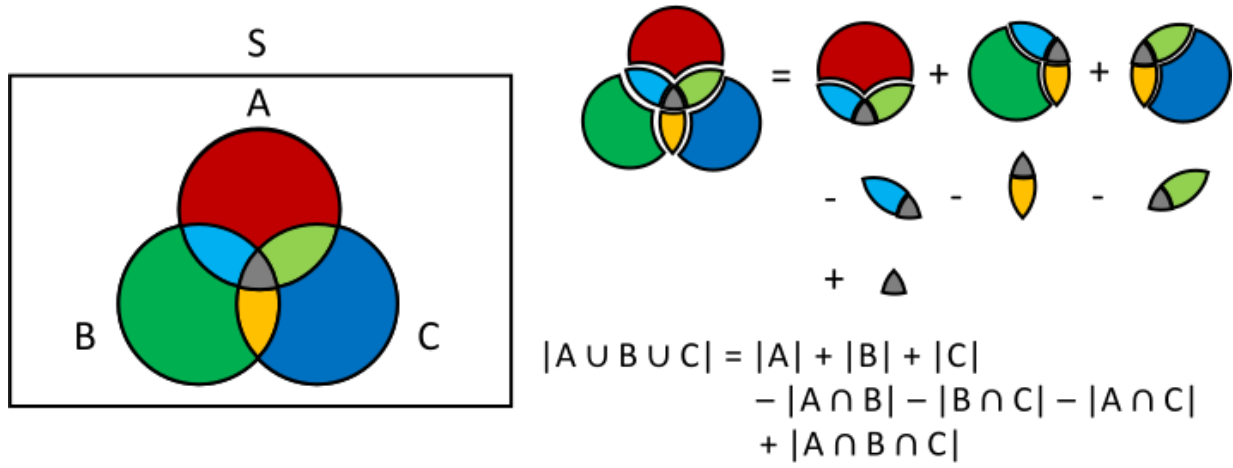
$= 220 - 51 = 169$

⚠ Its important to remember that all this [...] junk means "size of..."



### 5.1.4 Principle of Inclusion and Exclusion (n-way)

Before looking at the generalized solution, let's look at 3 sets with a venn diagram.



Notice the pattern? We're first adding the sets then subtracting the intersections every set. Then we add back the intersection of all the sets because just subtracting them would lead to an undercounting issue (we're missing out on the middle piece of the venn diagram).

This pattern can be compiled into our generalization:

$$\begin{aligned}
 |A_1 \cup A_2 \cup \dots \cup A_n| = & \sum_{1 \leq i \leq n} |A_i| \\
 & - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| \\
 & + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| \\
 & - \dots \\
 & \dots \\
 & + (-1)^{n+1} |A_1 \cap A_2 \cap \dots \cap A_n|
 \end{aligned}$$

For example, when  $n = 3$ :

$$\begin{aligned}
 |A_1 \cup A_2 \cup A_3| = & |A_1| + |A_2| + |A_3| \\
 & - |A_1 \cap A_2| - |A_2 \cap A_3| - |A_1 \cap A_3| \\
 & + |A_1 \cap A_2 \cap A_3|
 \end{aligned}$$

## Examples

In a class, 19 students are math majors, 23 are CS majors, and 10 are physics majors. In addition, 9 students are math and CS majors, 2 students are physics and CS majors, 4 students are math and physics majors. There is 1 student majoring all three majors.

<sub>1</sub> How many students are there?

$M$ : set of students majoring in math,  $|M| = 19$

$C$ : set of students majoring in CS,  $|C| = 23$

$P$ : set of students majoring in physics,  $|P| = 10$

$|M \cap C| = 9$ ,  $|P \cap C| = 2$ ,  $|M \cap P| = 4$ , and  $|M \cap C \cap P| = 1$

Answer:  $|M| + |C| + |P| - |M \cap C| - |P \cap C| - |M \cap P| + |M \cap C \cap P|$   
 $= 19 + 23 + 10 - 9 - 2 - 4 + 1 = 38$ .

<sub>2</sub> How many students major in math only?

$|M| = 19$ ,  $|C| = 23$ ,  $|P| = 10$

$|M \cap C| = 9$ ,  $|P \cap C| = 2$ ,  $|M \cap P| = 4$ , and  $|M \cap C \cap P| = 1$

Need  $|M - (C \cup P)|$   
 $= |M| - |M \cap (C \cup P)|$  (Venn:  $|A - B| = |A| - |A \cap B|$ )  
 $= |M| - |(M \cap C) \cup (M \cap P)|$  (Distributive Law)  
 $= |M| - (|M \cap C| + |M \cap P| - |M \cap C \cap P|)$  (Principle of I&E).  
 $= 19 - (9 + 4 - 1) = 7$

<sub>3</sub> How many students major in math or CS but not physics?

$|M| = 19$ ,  $|C| = 23$ ,  $|P| = 10$

$|M \cap C| = 9$ ,  $|P \cap C| = 2$ ,  $|M \cap P| = 4$ , and  $|M \cap C \cap P| = 1$

Need  $|M \cup C - P|$   
 $= |M \cup C| - |(M \cup C) \cap P|$  (Venn:  $|A - B| = |A| - |A \cap B|$ )  
 $= |M \cup C| - |(M \cap P) \cup (C \cap P)|$  (Distributive)  
 $= |M| + |C| - |M \cap C| - (|M \cap P| + |C \cap P| - |M \cap C \cap P|)$   
 $= 19 + 23 - 9 - (4 + 2 - 1) = 28$

### 5.1.5 Pigeonhole Principle

**📖** If more than  $k$  pigeons are placed into  $k$  pigeonholes, then at least one hole contains more than one pigeon. This principle is used to answer questions of the form "at least how many objects satisfy a certain property"

To use the pigeonhole principle, we need to;

- › Identify "pigeons" and identify "pigeonholes"
- › Associate between pigeons and pigeonholes.

Generalization: If  $n$  objects are placed into  $k$  boxes, then there is at least one box containing at least  $\underbrace{\lceil n/k \rceil}_{\text{"ceiling" of } n/k}$  objects.

❗ The "ceiling" operation rounds up to the nearest whole integer.  
ex;  $\lceil 2.2 \rceil = 3$

This can be proven by contradiction;

- › Assume to the contrary that none of the boxes contain more than  $\lceil n/k \rceil - 1$  objects.
- › Then the total number of objects is at most;  $k(\lceil n/k \rceil - 1) < k((n/k + 1) - 1) = n$
- › This is a contradiction because there are a total of  $n$  objects.

### Examples

1 Seven points lie inside a hexagon of side length 1.

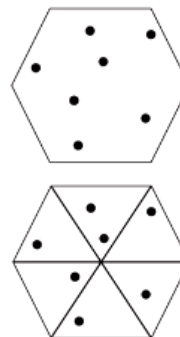
Show that there must exist at least two points whose distance apart is at most 1.

Pigeons: points.

Pigeonholes: Triangles

- › We can set up our pigeonhole by dividing our hexagon into 6 triangles. The lengths of these triangle sides are at most one, so the distance between any two points contained in the triangle can be at most one.

At least two points are inside one of these triangles by pigeonhole principle, so at least one set of points satisfies the "distance of at most one" setup from the triangle info above.



<sup>2</sup> There are some people in a room. Some are acquaintances; some are not. Assume that if  $a$  is acquainted to  $b$ , then  $b$  is acquainted to  $a$ . Also, no one is acquainted to him- or herself. Show that at least two people have the same number of acquaintances.

Let  $n$  be the number of people in the room.

Pigeons: People in the room.

Pigeonholes: Number of acquaintances.

‣ Possible acquaintances:  $0, 1, 2, \dots, n - 1$

Two Possible Cases:

1. Someone has 0 acquaintances

‣ This implies that no one has  $n - 1$  acquaintances.

‣ Pigeonholes =  $\{0, 1, 2, \dots, n - 2\}$ ,  $n - 1$  pigeonholes.  $n$  pigeons.

2. No one has 0 acquaintances

‣ Pigeonholes =  $\{1, 2, \dots, n - 1\}$ ,  $n - 1$  pigeonholes.  $n$  pigeons.

By pigeonhole principle, there must be 2 people that have the same number of acquaintances.

<sup>3</sup> Among 15 students, at least how many were born on the same day of the week?

Objects: students

Boxes: days of the week

There are at least  $\lceil 15/7 \rceil = 3$  students born on the same day of the week.

<sup>4</sup> How many students, each of whom comes from one of the 50 states, must be enrolled in a university to guaranteed that there are at least 100 who come from the same state?

Objects: students.

Boxes: 50 states.

However, this time we don't know the number of students.

‣ We want to find the minimum  $n$  so that  $\lceil n/50 \rceil = 100$

‣ This happens when the quotient is 99 and the remainder is 1.

‣ Thus,  $n = 50 * 99 + 1 = 4951$

## 5.2 Permutation and Combination

Many counting problems can be solved by finding the number of ways to select a specified number of objects out of a set.

When order matters: Permutations.

When order doesn't matter: Combinations.

Recall:  
Multiplication Principle  
 $|A \times B| = |A| \cdot |B|$   
  
Addition Principle  
 $|A \cup B| = |A| + |B|$   
  
Prnc' of Incls'n & Excls'n  
 $|A \cup B| = |A| + |B| - |A \cap B|$

For example:

In how many ways can we select three students from a group of students to stand in line for a picture?

› Order matters here, so permutation

How many different committees of three students can be formed from a group of five students?

› Order doesn't matter here, so combinations

### 5.2.1 Permutation

A permutation of a set of elements is an ordered arrangement of these elements.

For Example;

$$S = \{a, b, c\}$$

Permutations of S: abc, acb, bac, bca, cab, cba.

The number of permutations of  $S = P(n, n) = n!$

Since we have a sequence of  $n$  selection steps;

Step 1: select the 1st element  $n$  ways

Step 2: select the 2nd element  $n - 1$  ways

Step 3: select the 3rd element  $n - 2$  ways

...

Step  $n$ : select the  $n$ th element  $1$  way.

by the multiplication principle we get our  $\underbrace{P(n, n)}_{\substack{n \text{ elements in the set,} \\ \text{selecting a range of } n \text{ elements}}} = n \times (n - 1) \times (n - 2) \times \dots \times 1 = n!$ .

An **r-permutation** is an ordered arrangement of  $r$  elements of a set.  $r$  now being a smaller range of the set than all  $n$  items.

The number of  $r$ -permutations  $P(n, r) = \frac{n!}{(n-r)!}$

Since we have a sequence of  $r$  selection steps;

Step 1 select the 1st element  $n$  ways

Step 2 select the 2nd element  $n - 1$  ways

Step 3 select the 3rd element  $n - 2$  ways

...

Step  $r$  select the  $r$ th element  $(n - r + 1)$  ways

By the multiplication principle  $\underbrace{P(n, r)}_{\substack{n \text{ elements in the set,} \\ \text{selecting a range of } r \text{ elements}}} = n \times (n - 1) \times (n - 2) \times \dots \times (n - r + 1)$

## Examples

<sub>1</sub> How many 2-permutations of set  $\{a, b, c\}$  are there?

$$P(3, 2) = 3 \times 2 = 6$$

ab,ac,ba,bc,ca,cb

<sub>2</sub> Suppose that there are eight runners in a race. How many ways are there to award the gold, silver, and bronze medals?

$$P(8, 3) = 8 \times 7 \times 6 = 336$$

<sub>3</sub> How many strings consisting of the letters A, B, C, D, E, F, G, H contain the string ABC?

Idea: consider ABC as one element and D E F G H as other 5 elements for a total of 6 elements.

It is equivalent to counting the number of permutations of these 6 elements:  $P(6, 6) = 6! = 720$

### 5.2.2 Combinations

An  $r$ -combination of a set of elements is an unordered selection of  $r$  elements from a set. For example;

$$S = \{a, b, c\}$$

2-combinations of  $S$ :  $\{a, b\}, \{a, c\}, \{b, c\}$

**i** *Since order doesn't matter, these are all the same as  $\{b, a\}, \{c, a\}, \{c, b\}$  so we don't include those as separate elements.*

Using just  $P(n, r)$  would be overcounting by  $r!$  since it counts different orderings of the same elements. So we need a different equation for combinations;

The number of  $r$ -combinations of a set with  $n$  elements is;

$$\underbrace{C(n, r)}_{\text{set of size } n, \text{ selecting } r \text{ elements}} = \frac{P(n, r)}{r!} = \frac{n!}{r!(n-r)!}$$

Where we are selecting  $r$  elements ( $C(n, r)$ ) and arranging them ( $P(r, r) = r!$ ).

#### Examples

<sub>1</sub> How many ways can we select a committee of 4 out of a group of 8 people?

$$C(8, 4) = \frac{8!}{4!(8-4)!} = 70$$

<sub>2</sub> Prove  $C(n, r) = C(n, n-r)$

$$\begin{aligned} C(n, r) &= \frac{n!}{r!(n-r)!} \\ &= \frac{n!}{(n-(n-r))!(n-r)!} \\ &= C(n, n-r) \end{aligned}$$

TODO: add card game example if needed



## 5.3 More Counting

### 5.3.1 Selecting Different Types Of Identical Objects

---

**Theorem/General Equation:** The number of  $r$ -combinations of a set of  $n$  types of identical objects is...

$$C(n + r - 1, r)$$

---

**Motivating Example** How many ways are there to select four pieces of fruit from a bowl containing apples, oranges, and pears?

There are at least four pieces of each type of fruit.

Only the type of fruit matters, but not the individual piece.

We can begin counting by finding every possible group...

3 sets of all the same fruit - 4 apples, 4 oranges, 4 pears.

6 sets of 3 of one fruit and one of the other;

› 3 apples and 1 pear or 1 orange      3 oranges and 1 apple or 1 pear      3 pears and 1 apple or 1 one other.

3 sets where there's 2 pieces of the same type, 2 pieces of a different type

› 2 apple, 2 orange.      2 apple, 2 pear.      2 orange, 2 pear.

3 sets where two items are of the same type, but the other two are all different.

› 2 apples, 1 orange, 1 pear      2 oranges, 1 pear, 1 apple      2 pears, 1 orange, 1 apple

All this adds up to 15 combinations/ways we can select 4 pieces from this bowl.

This solution is the number of 4-combinations with identical objects from a three-object set, (being apple orange and pear).

Since this set is small, it's easy to visualize and see all the possible combinations - however we need a general solution for a set and selection of any size! Leading to our formula above.

TODO: im not a huge fan of the cash box example, only add later if you need it.

### Example

1 Suppose that a cookie shop has four kinds of cookies. How many ways can six cookies be chosen? Assume that only the type of cookie, and not the individual cookies or the order in which they are chosen, matters.

$n = 4, r = 6 \mapsto C(9, 6)$  ways

### 5.3.2 Arranging Different Types of Identical Objects

We cannot just use factorial because that would lead to overcounting since factorial would treat every element is independent instead of ignoring identical elements. 4 apples is 4 apples, no matter the order they are in!

---

**Theorem/General Equation:** The number of different permutations of  $n$  objects of  $k$  types, where there are  $n_i$  identical objects of type  $i$ , for  $1 \leq i \leq k$  is

$$\frac{n!}{n_1!n_2!\dots n_k!}$$

---

#### Examples

- <sub>1</sub> How many ways can 4 blue balls and 3 red balls be arranged in a row?

Solution:  $\frac{(4+3)!}{4!3!} = \frac{7!}{4!3!} = 35$  ways to arrange them

- <sub>2</sub> How many strings can be constructed by reordering the letters of “SUCCESS”?  
7 letters,  $n = 7$ . 4 unique letters, so  $k = 4$ ...

Solution:  $\frac{7!}{\underbrace{3!1!2!1!}} = \frac{7!}{3!2!} = 420$  ways to arrange them.

3 S's, 1 U, 2 C's, 1 E

### 5.3.3 Arranging Objects in a Circle

---

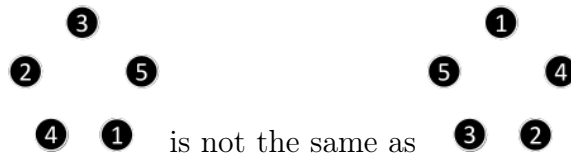
**Theorem/General Equation:** The number of ways to arrange  $n$  objects in a circle is

$$(n - 1)!$$

---

**Motivating Example** How many ways can 5 people be arranged in a circle? For a circle, only the relative positions matter.

It's not just  $5!$  since



Only the relative positions (the overall wrapping-round order) matters!

The correct answer would be  $(5 - 1)! = 4! = 24$  ways to arrange 5 people in a circle.

### 5.3.4 Arranging Objects with Constraints (examples)

<sub>1</sub> How many ways can 6 dogs and 2 cats be arranged in a row such that the 2 cats are together?



We can treat the 2 cats as one "unit", meaning there's 7 units to arrange.  $7!$  ways to arrange these units

The cats then can be arranged themselves in  $2!$  ways.

So the total number of ways to arrange them is  $7! * 2 = 10,080$

<sub>2</sub> How many ways can 6 dogs and 2 cats be arranged in a row such that the 2 cats are not together?



We can just find all the arrangements and subtract out the ones where the cats are together! (previous example)

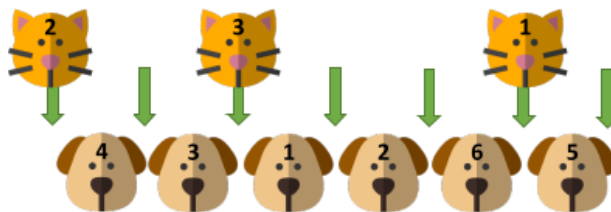
Number of ways:  $8! - 10080 = 30,240$

<sub>3</sub> How many ways can 6 dogs and 3 cats be arranged in a row, such that the 3 cats are separate from each other?

Start by arranging our 6 dogs in a row. There are  $6!$  ways.

In order to keep the cats separate, they need to be put into slots between each of the dogs. There are  $P(6, 3) = 7 * 6 * 5$  ways to fit 3 cats into the 7 slots.

Meaning there is a total of  $6! * 7 * 6 * 5$  ways to arrange them.



## 6 Probability

### 6.1 Basics

Probability is closely related to counting!

The simplest equation in probability is when the outcomes are equally likely, in that case;

$$\text{Probability} = \frac{\text{Number of target outcomes}}{\text{Number of all outcomes}}$$

#### Examples

<sub>1</sub> Coin Flipping - Assume 2 outcomes (head and tail) are equally likely. The probability of seeing;

a head is 0.5

a tail is 0.5

<sub>2</sub> Dice Rolling - There are 6 different outcomes, namely, 1, 2, 3, 4, 5, and 6. Each of them is equally likely.

The probability of seeing each outcome is  $1/6$ .

The probability of seeing an odd number is  $1/2$ .

$$> p(\text{odd}) = \frac{|\{1,3,5\}|}{|\{1,2,3,4,5,6\}|} = 1/2$$

---

#### Terminology

**Experiment** - A procedure that yields one of a given set of possible outcomes.

The **Sample Space** of an Experiment - is the set of possible outcomes.

An **event** is a subset of the sample space.

If  $S$  is a finite nonempty sample space of equally likely outcomes, and  $E$  is an event, then the **probability** of  $E$  is;

$$p(E) = \frac{|E|}{|S|}$$

## Examples

<sub>1</sub> A box has 4 red balls and 6 blue balls. What is the probability that a ball chosen at random from the box is blue?

Sample space: 10 outcomes

Event: 6 blue balls

$$p(\text{ball is blue}) = 6/(4+6) = 0.6$$

<sub>2</sub> What is the probability that when two dice are rolled, the sum of the numbers on the two dice is 7?

Sample space:

› By multiplication principle, there are 36 possible outcomes.

Event:

› 6 outcomes leading to 7:  $\{(1, 6), (2, 5), (3, 4), (4, 3), (5, 2), (6, 1)\}$

$$p(\text{sum} = 7) = 6/36 = 1/6$$

<sub>3</sub> In each Powerball game, players select five numbers from 1-69 for white balls and one number from 1-26 for the red ball. In order to win the jackpot, all 6 balls must match those in the drawing. What is the probability of winning a jackpot?

Sample Space:

›  $C(69,5) * C(26,1) = 292,201,338$  outcomes

Event (Winning a jackpot): 1 outcome

$$p(\text{jackpot}) = 1/292,201,338$$

<sub>4</sub> In each Powerball game, players select five numbers from 1-69 for white balls and one number from 1-26 for the red ball (Powerball). What is the probability of winning the third prize (\$50,000), matching exactly 4 white balls and the powerball?

Sample space:  $C(69, 5) \times C(26, 1) = 292,201,338$  outcomes

Event (winning the third prize):  $C(5, 4) \times C(69-5, 1) = 320$  outcomes

$$p(\text{third prize}) = 320/292,201,338 \approx 1/913,129.$$

## Probability of Complements of Events

Let E be an event in a sample space S. The probability of its complement E' is;

$$p(E') = 1 - p(E)$$

### Examples

<sub>1</sub> A sequence of 10 bits is randomly generated. What is the probability that at least one of these bits is 0?

Event: seeing no-zero string

$$> p(E) = \frac{1}{2^{10}} \text{ (only 1111111111)}$$

Complement event: seeing at least one 0 in the string.

$$> p(E') = 1 - p(E) = 1 - \frac{1}{2^{10}}$$

<sub>2</sub> How large must a class be to make the probability of finding at least two people with the same birthday at least 50%? Assume that a year is always 365 days long.

Let n be the number of students in a class.

The probability of no two have the same birthday is:

$$> \frac{P(365, n)}{365^n}$$

To make  $\frac{P(365, n)}{365^n} < 0.5$ , n must be at least 23.

## Probability of Unions of Events

Let  $E_1$  and  $E_2$  be two events in the sample space  $S$ . Then:

$$p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2)$$

**Example** What is the probability that a randomly selected positive integer not exceeding 100 is divisible by either 2 or 5?

$E_1$  is divisible by 2

$E_2$  is divisible by 5

$E_1 \cup E_2$ : divisible by either 2 or 5

$E_1 \cap E_2$ : divisible by 2 and 5, or equivalently by 10

$$p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2)$$

$$= 0.5 + 0.2 - 0.1$$

$$= 0.6$$



### Three Axioms in Discrete Probability Theory

So far, all of our probability calculations assume *equal probability*, we need some new rules when this isn't the case!

1. The probability of an event  $E$  is:

$$0 \leq p(E) \leq 1$$

2. The sum of probabilities of all outcomes is equal to 1.
3. For any two events  $E_1$  and  $E_2$ :

$$p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2)$$

### Example

What are the probabilities of the outcomes when the coin is biased so that heads come up twice as often as tails?

$p(H)$  is the probability of head coming up.

$p(T)$  is the probability of tail coming up

We have  $p(H) = 2p(T)$  and  $p(H) + p(T) = 1$ .

Therefore,  $p(H) = 2/3$ , and  $p(T) = 1/3$ .

## Random Variables

A **random variable** is a function from the sample space of an experiment to the set of real numbers. That is a random variable assigns a real number to each possible outcome.

### Examples

<sub>1</sub> Suppose that a coin is flipped 3 times. Let  $X(t)$  denote the number of heads that appear when  $t$  is the outcome.

$$X(\text{HHH}) = 3$$

$$X(\text{HHT}) = X(\text{HTH}) = X(\text{THH}) = 2$$

$$X(\text{TTH}) = X(\text{THT}) = X(\text{HTT}) = 1$$

$$X(\text{TTT}) = 0$$

<sub>2</sub> Assume a coin is flipped for 5 times.  $p(\text{H}) = 0.6$  and  $p(\text{T}) = 0.4$ . Each coin flip is independent of the previous.

Let  $X$  be the number of heads in the outcome.

$$p(X = 0) = 0.60 \times 0.45$$

$$p(X = 1) = C(5, 1) \times 0.6 \times 0.44$$

$$p(X = 2) = C(5, 2) \times 0.62 \times 0.43$$

$$p(X = 3) = C(5, 3) \times 0.63 \times 0.42$$

$$p(X = 4) = C(5, 4) \times 0.64 \times 0.4$$

$$p(X = 5) = 0.65 \times 0.40$$

## Expected Value

The **expected values** (**expectation** or **mean**) of the random variable  $X$  on the sample space  $S$  is equal to

$$E(x) = \sum_{s \in S} p(s)X(s)$$

## Examples

<sub>1</sub> Roll a dice. Let  $X$  denote the number. What is the expected value of  $X$ ?

$$E(X) = 1 \times 1/6 + 2 \times 1/6 + 3 \times 1/6 + 4 \times 1/6 + 5 \times 1/6 + 6 \times 1/6$$

$$E(X) = 7/2$$

<sub>2</sub> Flip a fair coin 3 times. Let  $X$  denote the number of heads. What is the expected value of  $X$ ?

Possible Outcomes:

$$\left\{ \begin{array}{cccccccc} \text{HHH} & \text{HHT} & \text{HTH} & \text{THH} & \text{HTT} & \text{THT} & \text{TTH} & \text{TTT} \\ 3 & 2 & 2 & 2 & 1 & 1 & 1 & 0 \end{array} \right\}$$

Expected Value:

$$\triangleright E(X) = 1/8 \times (3 + 3 \times 2 + 3 \times 1 + 0) = 3/2$$


<sub>3</sub> You have 100 dollars and can invest into a stock. The returns are You have 100 dollars and can invest into a stock. The returns are \$90 with probability 0.6. Should you invest?

Let  $X$  denote the return.

$$E(X) = 0.4 \times 120 + 0.6 \times 90 = 102.$$

Yes! On average you'll make a profit.

## 6.2 Conditional Probability

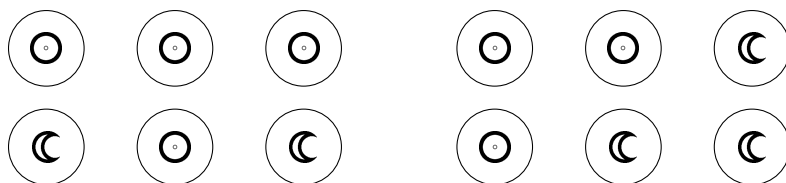
 Let  $E$  and  $F$  be two events such that  $p(F) > 0$ . The **conditional probability** of  $E$  given  $F$  is;

$$P(E|F) = \frac{P(E \cap F)}{p(F)}$$

In other words, what is the probability of  $E$  given that  $F$  has already occurred.

<sup>ex</sup> If we flip a coin three times, what is the probability of seeing at least 2 tails, given that the first one is a tail?

There are only 4 outcomes



Let  $E$  denote the event of seeing 2 pairs

Let  $F$  denote that the first one is a tail


$$\frac{|E \cap F|}{|F|} = \frac{p(E \cap F)}{p(F)} = \frac{3}{4}$$

<sup>ex</sup> What is the conditional probability that a family with two children has two boys, given they have at least one boy? Assume that each of the possibilities BB, BG, GB, and GG is equally likely, where B represents a boy and G represents a girl.

$E$ : both children are boys (1 outcome)

$F$ : at least is a boy (3 outcomes)

$$P(E|F) = \frac{P(E \cap F)}{p(F)} = \frac{\frac{|E \cap F|}{S}}{\frac{|F|}{S}} = \frac{1/4}{3/4} = \frac{1}{3}$$

 remember the probability of each of an event happening is the amount of cases of it occurring divided by the set of all possible cases

### 6.2.1 Corollary of Conditional Probability

We can move around the variables of the conditional probability eq to get

$$p(E \cap F) = p(E|F)p(F)$$

This formula is useful to use when the conditional probability is easier to estimate.

ex The probability of getting a flu is 0.2. The probability of having a fever given the flu is 0.9. What is the probability of getting a flu with a fever?

E: fever

F: flu,  $p(F) = 0.2$ .

$$p(E|F) = 0.9$$

$$p(E \cap F) = p(E|F)p(F) = 0.18$$

### 6.2.2 Independence

Two events  $E$  and  $F$  are independent iff;

$$p(E \cap F) = p(E)p(F)$$

**Motivating Example:** Say you flip a coin three times, what is the probability of the third being a head? What is the probability given the first two are heads?

First Part;

E: the third one is a head,  $|E| = 4$

F: the first two are heads

Total # of possible flips:  $2^3 = 8$

$$p(E) = \frac{4}{8} = \frac{1}{2}$$

Second Part;

$$P(E|F) = \frac{P(E \cap F)}{p(F)}$$

▷  $|E \cap F| = 1 \mapsto p(E \cap F) = \frac{1}{8}$  - only one case where they're all heads!

▷  $p(F) = \frac{2}{8}$  based on the fact that we're only relying on the prob from the last coin flip (first two are assumed heads)

$$P(E|F) = \frac{\frac{1}{8}}{\frac{2}{8}} = \frac{1}{2}$$

Note how these probabilities are the same!

## Independence Examples

<sub>1</sub> Let  $E$  denote that the family has three children of both sexes and  $F$  denote that the family has at most one boy. Are  $E$  and  $F$  independent?

Total sample space ( $S$ ) = 8.

Both sexes ( $E$ ) = {GGB, GBG, GBB, BGB, BBG, BGG},  $|E| = 6$

At most one boy ( $F$ ) = {GGG, GGB, GBG, BGG},  $|F| = 4$

$E \cap F = \{GGB, GBG, BGG\}$

$p(E \cap F) = \frac{3}{8}$ , and  $p(E)p(F) = \frac{3}{8}$

Therefore,  $E$  and  $F$  are independent.

<sub>2</sub> The probability of getting a flu is 0.2. The probability of having a fever is 0.3. The probability of having a fever given the flu is 0.9. Are flu and fever independent?

$E$ : flu,  $p(E) = 0.2$

$F$ : fever  $p(F) = 0.3$

$p(F|E) = 0.9$

We need  $p(E \cap F)$

› By corollary def,  $p(E \cap F) = p(E|F)p(F)$

› We need the other way round of the given  $p(F|E)$ !

\* Since it's based on intersection, we can just flip every part of the corollary def!

→  $p(E \cap F) = p(F \cap E) = p(F|E)p(E)$

\*  $p(F|E)p(E)$ , all known values,  $0.9 * 0.2 = 0.18$

\*  $p(E)p(F) = 0.06$

› Therefore, these events are not independent

### 6.2.3 Bayes Theorem

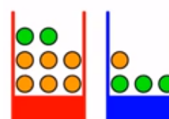
Bayes Theorem is another relation/equation we can use to evaluate conditional probability problems. The Theorem is defined by the following eq;

$$P(E|F) = \frac{P(F|E)p(E)}{p(F)}$$

---

#### Motivating Example

We have two colored boxes, and each contains two types of fruits, apples (shown in green) and oranges (shown in orange). We randomly select a fruit by first randomly choosing a box with probability 0.4 for red and 0.6 for blue, respectively, and then selecting one fruit in the box uniformly at random.



Also note that the probability of choosing an apple is  $\frac{11}{20} = 0.55$  example excluded from notes, 11/14 vid 2. Given that we have chosen an orange, what is the probability that the box we chose was red?

Using our original conditional eq we would have:  $P(B = r|F = o) = \frac{p(B=r \cap F=o)}{P(F=O)}$

However,  $p(B = r \cap F = o)$  is very hard to determine. So we need a new definition for conditional probability we can work with!

Using Bayes Theorem...

$$p(B = r|F = o) = \frac{p(F = o | B = r) \cdot p(B = r)}{p(F = o)}$$

6 oranges of 8 total in red box

$$p(B = r|F = o) = \frac{\overbrace{3/4}^{6 \text{ oranges of 8 total in red box}} \cdot (0.4)}{p(F = o)}$$

and note that:  $p(F = o) = 1 - p(F = a) = 1 - 0.55 = 0.45$

$$\frac{(3/4) \cdot 0.4}{0.45} = \frac{2}{3}$$

Bayes theorem is used to estimate probabilities based on *partial evidence*. Mathematically, we often are unable to determine or know  $p(F)$  directly, so this equation can be rewritten to calculate  $p(F)$ .

$$p(E|F) = \frac{p(F|E)p(E)}{p(F)} = \frac{P(F|E)p(E)}{p(F)} = \frac{P(F|E)p(E)}{p(F|E)p(E) + p(F|E')p(E')}$$

Note that  $P(E') = 1 - p(E)$ , meaning if we can calculate  $p(E)$  we can easily get  $p(E')$ . So the only information that requires extra work is finding  $p(F|E')$

## Examples

<sub>1</sub> The probability of getting a flu is 0.2. The probability of having a fever is 0.3. The probability of having a fever given the flu is 0.9. What is the probability of getting a flu given the fever?

$$p(flu|fever) = \frac{p(fever|flu) \cdot p(flu)}{p(fever)}$$

All of these values are defined in the problem, just plug in;  $\frac{0.9 \cdot 0.2}{0.3} = 0.6$

<sub>2</sub> The probability of getting a flu is 0.2. The probability of having a fever given the flu is 0.9. The probability of having a fever given no flu is 0.15. What is the probability of getting a flu given the fever?

Notice that we don't know  $p(fever)$ , we have to use the big version of Bayes theorem

Want  $p(flu|fever)$

Everything we need in the large Bayes theorem is given except for  $p(E')$

(Note that  $p(F|E') = 0.15$ , "The probability of having a fever given no flu is 0.15")

Remember that  $p(E') = 1 - p(E) = 1 - 0.2 = 0.8$ . Now we have everything and can just plug-in.

$$\frac{0.9 \cdot 0.2}{0.9 \cdot 0.2 + 0.15 \cdot 0.8} = 0.6$$



## 7 Relations

### 7.1 Basics

---

 A **relation** is a structure to represent the relations among elements of sets. In terms of sets, a relation is a subset of the **Cartesian Product** of the sets

---

#### 7.1.1 Binary Relation

One of the simpler cases of a relation;

Let  $A$  and  $B$  be sets. A **binary relation from  $A$  to  $B$**  is a subset of  $A \times B$ .

In other words, a binary relation from  $A$  to  $B$  is a set  $R$  of ordered pairs of form  $(a, b)$ , where  $a \in A$  and  $b \in B$ .

Let  $a R b$  denote that  $(a, b) \in R$  and  $a \not R b$  denote that  $(a, b) \notin R$

If  $a R b$ , we say  $a$  is related to  $b$  by  $R$

Since  $R$  is a set, we can describe this idea in many ways, we can list all the elements of  $R$ , define it in some way by describing the properties of its elements or by describing the relation  $R$  represents.

#### Examples

<sub>1</sub> Let  $A$  be the set of students at Mines, and let  $B$  be the set of courses. Let  $R$  be the relation that consists of those pairs  $(a, b)$ , where  $a$  is a student enrolled in course  $b$ .

Here we're defining  $R$  by describing the relation it represents...

If Alice and Bob are enrolled in CSCI101, then  $(\text{Alice}, \text{CSCI101}) \in R$  and  $(\text{Bob}, \text{CSCI101}) \in R$

If Alice is also enrolled in CSCI200, then  $(\text{Alice}, \text{CSCI200}) \in R$ .

However, if Bob is not in CSCI200, then  $(\text{Bob}, \text{CSCI200}) \notin R$ .

<sub>2</sub> Let  $A = \{a, b, c\}$  and  $B = \{1, 2, 3\}$ .

Is  $R = \{(a, 1), (b, 2), (c, 2)\}$  a relation from  $A$  to  $B$ ?      Yes

Is  $Q = \{(1, a), (2, b)\}$  a relation from  $A$  to  $B$ ?      No, but it is from  $B$  to  $A$ .

Is  $P = \{(a, a), (b, c), (b, a)\}$  a relation from  $A$  to  $A$ ?      Yes

### 7.1.2 Graph Representation

Graphs are a whole section later, this is just a brief introduction needed to represent relations ☺.

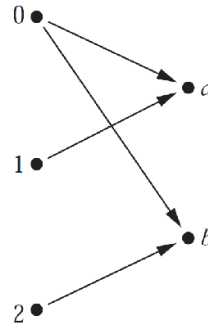
We can graphically represent a binary relation  $R$  by...

If  $a R b$ , then we draw an arrow from  $a$  to  $b$ .

Example:

Let  $A = \{0,1,2\}$  and  $B = \{a,b\}$ ,

Then  $\{(0,a), (0,b), (1,a), (2,b)\}$  is a relation from  $A$  to  $B$ ;



---

### 7.1.3 Table Representation

We can represent a binary relation  $R$  with a table by...

If  $a R b$ , then we mark the cell corresponding to  $a$  and  $b$ .

Example:

Let  $A = \{0,1,2\}$  and  $B = \{a,b\}$ ,

Then  $\{(0,a), (0,b), (1,a), (2,b)\}$  is a relation from  $A$  to  $B$ .

R	$a$	$b$
0	×	×
1	×	
2		×

### 7.1.4 Relation on One Set

A **relation on a set A** is a relation from A to A. Meaning that a relation on a set A is a subset of  $A \times A$ .

The number of binary relations on a set A of size  $n$  is  $2^{n^2}$

#### Examples

<sub>1</sub> Let  $A = \{1,2,3,4\}$ . What are in  $R_{\text{div}} = \{(a,b) | a \text{ divides } b\}$

$$R_{\text{div}} = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,4), (3,3), (4,4)\}$$

<sub>2</sub> Let  $A = \{1,2,3,4\}$ . Define  $aR_{\neq}b$  iff  $a \neq b$ . What is  $R_{\neq}$

$$R_{\neq} = \{(1,2), (1,3), (1,4), (2,1), (2,3), (2,4), (3,1), (3,2), (3,4), (4,1), (4,2), (4,3)\}$$

<sub>3</sub> Which of the following relations contain  $(1, 1)$ ,  $(1, 2)$ ,  $(2, 1)$ ,  $(1, -1)$ , and  $(2, 2)$ ?

$$R_1 = \{(a,b) | a \leq b\} \quad \text{✗} \quad 2 \not\leq 1$$

$$R_2 = \{(a,b) | a > b\} \quad \text{✗} \quad 1 \not> 1$$

$$R_3 = \{(a,b) | a = b \text{ or } a = -b\} \quad \text{✗} \quad 1 \neq \pm 2$$

$$R_4 = \{(a,b) | a = b\} \quad \text{✗} \quad 1 \neq 2$$

$$R_5 = \{(a,b) | a = b + 1\} \quad \text{✗} \quad 1 \neq 1 + 1$$

$$R_6 = \{(a,b) | a + b \leq 4\} \quad \text{✓}$$

## 7.2 Relation Properties

---

Reflexivity   Symmetry   Antisymmetry   Transitivity

---

A relation  $R$  on a set  $A$  is **reflexive** if;  
 $\forall a((a, a) \in R)$

Examples:

Let  $R_{\text{Div}} = \{(a, b) \mid a \text{ divides } b\}$  be a relation on  $A = \{1, 2, 3, 4\}$

›  $R_{\text{div}}$  is reflexive.

Let  $R$  on  $A = \{1, 2, 3, 4\}$  be defined as  
 $R = \{(1, 2), (2, 2), (3, 3)\}$ .

›  $R$  is not reflexive, because  $(1, 1) \notin R$

---

A relation  $R$  on a set  $A$  is **symmetric** if;  
 $\forall a \forall b((a, b) \in R \implies (b, a) \in R)$

Examples:

Let  $R_{\text{div}} = \{(a, b) \mid a \text{ divides } b\}$  be a relation on  $A = \{1, 2, 3, 4\}$

› Not symmetric because  $(1, 2) \in R_{\text{div}}$   
but  $(2, 1) \notin R_{\text{div}}$

Let  $R_{\neq} = \{(a, b) \mid a \neq b\}$  be a relation on  
 $A = \{1, 2, 3, 4\}$ .

› This is symmetric.

---

A relation  $R$  on a set  $A$  is **antisymmetric** if;  
 $\forall a \forall b((a, b) \in R \wedge (b, a) \in R \implies a = b)$

Examples:

Let  $R_{\text{div}} = \{(a, b) \mid a \text{ divides } b\}$  be a relation on  $A = \{1, 2, 3, 4\}$

› This is antisymmetric

Let  $R_{\neq} = \{(a, b) \mid a \neq b\}$  be a relation on  
 $A = \{1, 2, 3, 4\}$ .

› Not antisymmetric,  $(1, 2) \in R_{\neq}$  and  
 $(2, 1) \in R_{\neq}$  but  $1 \neq 2$

---

A relation  $R$  on a set  $A$  is **transitive** if;  
 $\forall a \forall b \forall c((a, b) \in R \wedge (b, c) \in R \implies (a, c) \in R)$

Examples:

Let  $R_{\text{div}} = \{(a, b) \mid a \text{ divides } b\}$  be a relation on  $A = \{1, 2, 3, 4\}$

› Transitive.

Let  $R_{\neq} = \{(a, b) \mid a \neq b\}$  be a relation on  
 $A = \{1, 2, 3, 4\}$ .

› No, since  $(1, 2) \in R_{\neq}$  and  $(2, 1) \in R_{\neq}$   
but  $(1, 1) \notin R_{\neq}$

---

## Examples

$$_1 S = \mathbb{N}; x R y \iff x + y \text{ is even}$$

Reflexive:  $x + x = 2x$

Symmetric:  $x + y \text{ is even} \implies y + x \text{ is even}$

Not Antisymmetric:  $3 + 5$  is even and  $5 + 3$  is even, but  $3 \neq 5$

Transitive:  $x + y \text{ is even}$ , then  $x + y = 2m$ ;  $y + z \text{ is even}$ , then  $y + z = 2n$ ;  $x + z = 2m + 2n - 2y = 2(m + n - y)$

$$_2 S = \mathbb{Z}^+; x R y \iff x \text{ divides } y$$

Reflexive:  $x$  divides  $x$

Not symmetric:  $3$  divides  $6$ , but  $6$  does not divide  $3$ .

Antisymmetric:  $x$  divides  $y$ , then  $y = mx$ ;  $y$  divides  $x$ , then  $x = ny$ ; Hence  $nm = 1$  and  $n = m = 1$ . So  $x = y$ .

Transitive:  $x$  divides  $y$ , then  $y = mx$ ;  $y$  divides  $z$ , then  $z = ny$ . Hence  $z = nm x$ .

$$_3 S = \mathbb{N}; x R y \iff x = y^2$$

Not reflexive:  $2 \neq 2^2$

Not symmetric:  $9 = 3^2$ , but  $3 \neq 9^2$

Antisymmetric:  $x = y^2$  and  $y = x^2$ , then  $x = x^4$  and thus  $x = 0$  or  $1$ . Hence  $x = y = 0$  or  $1$ .

Not transitive:  $16 = 4^2$  and  $4 = 2^2$ , but  $16 \neq 2^2$

$$_4 S = \{x \mid x \text{ is a student in CSCI101}\}; x R y \iff x \text{ sits in the same row as } y$$

Reflexive: A student sits in the same row as themselves.

Symmetric: If  $x$  sits in the same row as  $y$ , then  $y$  sits in the same row as  $x$ .

Not Antisymmetric: Two different students sit in the same row.

Transitive: If  $x$  sits in the same row as  $y$ , and  $y$  sits in the same row as  $z$ , then  $x$  sits in the same row as  $z$ .

$$_5 S = \{0, 1\}; x R y \iff x = y^2$$

Reflexive:  $0 = 0^2$  and  $1 = 1^2$

Symmetric:  $0 = 0^2$  and  $1 = 1^2$

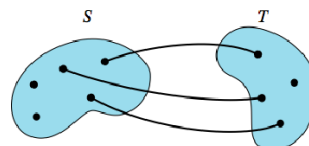
Antisymmetric:  $x = y^2$  and  $y = x^2$ , then  $x = x^4$  and thus  $x = 0$  or  $1$ . Hence  $x = y = 0$  or  $1$

Transitive:  $x = y^2$  and  $y = z^2$ , then  $x = y = z = 0$  or  $1$ . Hence  $x = z^2$

## 7.3 Types of Relations

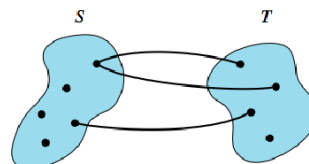
Let  $R$  be a binary relation from  $S$  to  $T$ , that is  $x R y$  where  $(x,y) \in S \times T$ . Then  $R$  is...

**One-to-One:** each element in  $S$  is paired with at most one element in  $T$ , and each element in  $T$  is paired with at most one element in  $S$ .



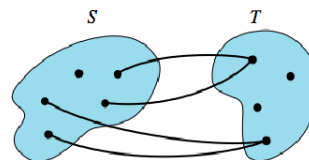
One-to-one

**One-to-Many:** some element in  $S$  is paired with more than one element in  $T$ , but each element in  $T$  is paired with at most one element in  $S$ .



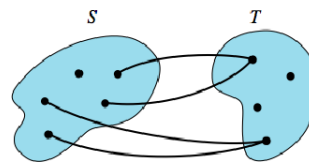
One-to-many

**Many-to-One:** each element in  $S$  is paired at most one element in  $T$ , but some element in  $T$  is paired with more than one element in  $S$ .



Many-to-one

**Many-to-Many:** some element in  $S$  is paired with more than one element in  $T$  and some element in  $T$  is paired with more than one element in  $S$ .



Many-to-many

ex Let  $S = \{2, 5, 7, 9\}$ . Identify the types of the following relations on  $S$ .

$$R = \{(5,2), (7,5), (9,2)\}$$

> many-to-one

$$R = \{(2,5), (5,7), (7,2)\}$$

> one-to-one

$$R = \{(7,9), (2,5), (9,9), (2,7)\}$$

> many-to-many