ECE 606, Fall 2022, Syllabus, Logistics and Schedule

Algorithms are at the very foundations of computing. It is important that one understands how to design them, and analyze them for correctness and efficiency. It is important also that one recognizes whether a problem is intractable so one does not naively seek an efficient algorithm when none may exist. The intent of this course is to provide students with fundamental training in these aspects.

Target audience	Graduate students in engineering at Waterloo
Recommended prior knowledge	ECE 250 or an equivalent `www.ucalendar.uwaterloo.ca/1920/COURSE/course-ECE.html`
Lectures	See the schedule of classes: `classes.uwaterloo.ca/grad.html` Technology permitting, I will record and post my lectures.
Instructor	Mahesh Tripunitara, `tripunit@uwaterloo.ca` "Mahesh" "Dr. T" "Prof. T"
Office hours	Mondays, 5-6pm via the team for the course on MS teams. Or by appointment — schedule via email/private Piazza post.
TA(s)	I do have some help with marking; however, those folks do not have sufficient bandwidth to interact with you. Please address all concerns, e.g., regarding marks you receive on an assignment problem with me via email/private Piazza post.
Course materials	`learn.uwaterloo.ca`
"Textbook"	Tripunitara, "ECE 606 – Algorithms" Available on Learn. May be posted in stages only.
Discussions	Self signup as of Sept. 1, 2022 at `piazza.com/uwaterloo.ca/fall2022/ece606`
Marking	Weekly assignments 50% Final exam 50%
Assignments	Weekly, Due: 11:59pm Tuesdays. Administered through Crowdmark: `app.crowdmark.com/sign-in/waterloo`
Lateness policy	No late submissions accepted for any reason whatsoever.
Audit	All deliverables (assignments + final exam) must be met. A mark of 50 on the course must be achieved.
AccessAbility	`uwaterloo.ca/accessability-services`
Academic Integrity	`uwaterloo.ca/academic-integrity` $\longrightarrow$ Students

Content Schedule

Week		*Topics*
(1)	Sep 07 – Sep 13	Intro to the course; Discrete math review; intro to Python 3
(2)	Sep 14 – Sep 20	Expressing algorithms; Data structures review
(3)	Sep 21 – Sep 27	Properties of algorithms: existence, correctness, efficiency
(4)	Sep 28 – Oct 04	Design strategy I: incremental
(5)	Oct 05 – Oct 11	Design strategy II: divide-n-conquer
(-)	Oct 12 – Oct 18	(nothing; reading week)
(6)	Oct 19 – Oct 25	Design strategy III: greedy
(7)	Oct 26 – Nov 01	Design strategy IV: dynamic programming
(8)	Nov 02 – Nov 08	Randomization, Probabilistic and approximation algorithms
(9)	Nov 09 – Nov 15	Non-determinism; computational complexity; the class **NP**; other complexity classes
(10)	Nov 16 – Nov 22	Cook- and Karp-reductions; hardness and completeness for a complexity class
(11)	Nov 23 – Nov 29	**NP**-complete problems and reductions between them
(12)	Nov 30 – Dec 06	Machine learning — Probably Approximately Correct (PAC)
Dec 9 – 23, final exam		

Assignments

There will be weekly assignments, for a total of 12 assignments across the course. Each comprises a few problems that the TAs will mark. There may be problems in the assignment that involve programming in Python 3; each such problem will be annotated with "[**python3**]." Assignments will be published by midnight every Tuesday. They are due by 11:59pm the following Tuesday. Written solutions must be typeset, or written legibly and scanned, and uploaded to Crowdmark. Some subset of the problems on each assignment will be marked by us. This subset will not be announced beforehand.

Lateness policy: no late submissions accepted.

Collaboration policy: you may collaborate with your colleagues when working on your assignments in that you can discuss ideas with one another. However, your final submission must be your own. That is, when you sit down to write your solutions, you should do so on your own. Any sources you use, whether they are your colleagues, books, papers or online resources, should be appropriately credited in your submission. There is no penalty for utilizing such (re)sources, provided they are credited explicitly. Otherwise, it is regarded as plagiarism, and is an academic offence.

Originality detection: We may use plagiarism-detection software to check that your submissions are indeed original, and not plagiarized. Such software includes Turnitin, iThenticate and Moss.

Final Exam

The final exam will be published similarly as the assignments. However, you will have 24 hours only to turn in your solutions. Your submission is expected to be your own; you are not to collaborate with anyone, in the course nor outside. However, you're free to use any resources, e.g., books/papers/online resources, that you like. You should credit any (re)source you use in your submission.

I am often asked what the best preparation for this course is. I suggest that a prospective student have a good grasp of basic discrete math, logic and proof techniques — at the level we teach in our ECE 108 course: `www.ucalendar.uwaterloo.ca/1920/COURSE/course-ECE.html`. Note that ECE 108 is a pre-requisite to ECE 250, which I mention as recommended prior knowledge for ECE 606 in the table on the first page. I attach a "textbook" for ECE 108; I recommend strongly that a prospective student in ECE 606 peruse it beforehand.

ECE 108, Discrete Math & Logic

John Thistle Mahesh Tripunitara

{jthistle,tripunit}@uwaterloo.ca
ECE, University of Waterloo

Acknowledgements

This book relies partly on material from the following.

- W. Conradie and V. Goranko, "Logic and Discrete Mathematics, a Concise Introduction," Wiley.
- G. P. Hochschild, "Perspectives of Elementary Mathematics," Springer-Verlag.
- P. J. Cameron, "Sets, Logic and Categories," Springer.
- M. Huth and M. Ryan, "Logic in Computer Science, Modelling and Reasoning about Systems," Cambridge.
- T. H. Cormen, C. E. Leiserson, R. L. Rivest and C. Stein, "Introduction to Algorithms, Third Edition," MIT Press.

Contents

Chapter 1

Introduction

What is "discrete math?"

Discrete math is a collection of branches of mathematics that deals with discrete, as opposed to continuous, structures. An example of a discrete structure is the set of integers, $\{\ldots, -2, -1, 0, 1, \ldots\}$. We call those "discrete" because they are a collection of "distinct and unconnected elements," as defined in the Merriam-Webster's dictionary. The real numbers, on the other hand, are not discrete: between any two real numbers, we can find another real number.

Discrete math and logic is at the very foundations of several aspects of Electrical and Computer Engineering (ECE).

For example, consider a fundamental problem in communications, which itself is an important topic in ECE. The problem is that of efficiently encoding a message so it can then be transmitted. Suppose the message we want to send is:

> *this is a test this is only a test*

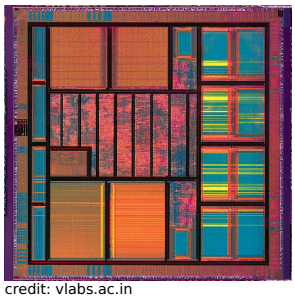
One way of encoding the above message is to allocate a fixed number of bits per character, e.g., 8-bits, as done by the American Standard Code for Information Interchange, ASCII. This results in an encoding of 272 bits for the above message, including the spaces.

What if we, instead, assign a sequence of bits to a character based on its frequency of occurrence in the message? Such an approach is called a *Huffman*

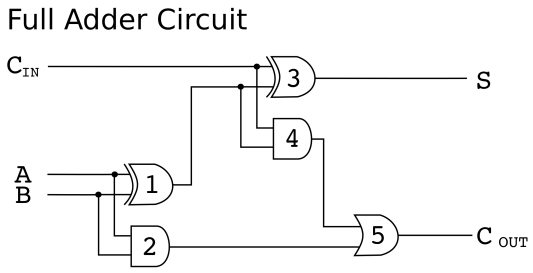
code. The more frequently a character occurs, the fewer number of bits we associate with it. Under such an encoding, for the above message, we may associate, for example, 01 with a space, 100 with each "i," 1110 with each "h," 111101 with each "n," and so on. This results in only 106 bits to encode the above message; a significant savings.

See `https://people.ok.ubc.ca/ylucet/DS/Huffman.html` for a cool applet that constructs such an encoding by building a particular kind of tree data structure. The ideas behind the construction of such a code, and an analysis of why it works, are all based in discrete math.

Another example of where discrete math and logic shows up in ECE is in the context of Digital Integrated Circuits (ICs). ICs are fundamental to modern computers. An IC can be seen a kind of directed graph of logic gates. (We discuss graphs briefly in this course in the context of relations in Chapter 3.) The following picture shows a modern IC to the left with a detailed view of a full adder circuit to the right. The full adder circuit adds the bits A and B, with a carry-in bit, C_{IN}, and outputs two bits: the sum, S, and a carry-out bit, C_{OUT}. In the picture, the gates labelled 1 and 3 are XOR gates, the gates labelled 2 and 4 are AND gates, and the gate labelled 5 is an OR gate. For example, the result of $A = 0, B = 1, C_{IN} = 1$ is $S = 0, C_{OUT} = 1$.



credit: vlabs.ac.in



As a final example of where discrete math and logic shows up in ECE, we point to algorithms. An algorithm can be thought of as a procedure to compute a function. (We discuss what a function is in Chapter 3.) Algorithms underlie computer programs, e.g., those written in C++, and show up in various aspects of our lives, e.g., in the computer equipment and cellphones we use. The design and analysis of algorithms is rooted deeply in discrete math

and logic. It is typical, for example, to adopt a data structure to represent and store data on which an algorithm operates. A data structure is often a discrete structure, e.g., an array, or a graph. To analyze the correctness and efficiency of an algorithm, we often use concepts we introduce in this course, such as proof by induction and contradiction.

Layout The remainder of this book, and the course, are structured roughly as follows: (i) Chapter 2, propositional logic and proof techniques, 3 weeks, (ii) Chapter 3, sets, functions and cardinality, 4 weeks, and, (iii) Chapter 4, combinatorics, 5 weeks.

Chapter 2

Propositional Logic and Proof Techniques

In this chapter, we'll define the precise language of *propositional logic*. You'll find that it is very closely related to switching algebra – or the two-element boolean algebra – that you will be studying in ECE 124, Digital circuits and systems.

Definition 1 (Proposition)**.** *A proposition is a statement with which we are able to associate* true *or* false*.*

Examples of propositions:

1. "The Earth is flat."
2. "Not all birds can fly."
3. "A dog is a mammal, and not a bird."

Of course, in the above, Proposition (1) happens to be false, and Propositions (2) and (3) are true.

Examples of statements that are not propositions:

1. "Hey, you!"
2. "Which way is the hotel?"
3. "This statement is false."

4. "The variable x is non-negative."

The first of the above is an exclamation, and the second is a question. As for the third, if it is true, then it is false, and if it is false, then it is true. Thus, we are able to associate neither true nor false with that statement. The fourth refers to a variable that can take on one of several values. Without knowledge of exactly what value x takes at a given moment, we cannot assess the truthfulness of the statement.

In this context, it is interesting and fun to address an old riddle. Suppose one is faced with two persons, call them Alice and Bob, one of whom always speaks the truth, and the other of whom always lies. What questions, when asked of Alice and/or Bob, would reveal which one amongst them is the truth-teller, and which one is the liar?

Suppose we ask one of them, say Alice, whether the other, Bob, would say 'yes' if asked whether Alice is the liar. If Alice is the truth-teller, then she would say 'yes,' because Bob is the liar, and he would answer 'yes' to our question to him, when the correct answer is 'no.' If Alice is the liar, then she would say 'no,' because Bob, as the truth-teller, would say 'yes' if we asked him whether Alice is the liar, and because Alice always lies, she would negate that expected response from Bob.

While devising the right question to ask above certainly takes creativity, underlying the entire exercise is careful logical reasoning. Communicating and inculcating this is exactly our intent with our discussions on propositional logic.

To develop an understanding of propositional logic, we will often deal with propositions abstractly. Specifically, we will adopt usages such as: "Assume that p is a proposition." When we say that, we do not know exactly what the proposition p is. All we know is that p is either true or false.

Given propositions, we can compose them in certain ways to yield other propositions. Some refer to such a new proposition as a *compound* proposition. A proposition that is not compound is called an *atomic* proposition.

The third example of a proposition above, "A dog is a mammal, and not a bird" is an example of a compound proposition. As another example, consider the following two propositions: (i) "The glass is not empty." (ii) "The glass

is not full." We can compose them and say, (iii) "The glass is neither empty nor full." Given such a compound proposition, it is necessary to clarify its *semantics*, that is, what the truth value of the compound proposition (iii) is as a function of the truth values of its constituent, atomic propositions.

To clarify what we mean, suppose the glass is indeed empty. Then Proposition (i) above is false. This implies that Proposition (iii) is false as well. Similarly, suppose Proposition (iii) is false. Then at least one of Proposition (i) and (ii) is false. A customary way, in propositional logic, to specify a semantics for a proposition that is composed of other propositions is to specify a *truth table*. For our example of Propositions (i)–(iii) above, such a truth table may look like the following.

If "the glass is not empty" is	and "the glass is not full" is	then "the glass is neither empty nor full" is
true	true	true
true	false	false
false	true	false
false	false	false

An important aspect of logic is to carefully distinguish *syntax* from semantics. Syntax refers to the way we write things down. Semantics refers to what they mean. We now specify a syntax for compound propositions. We then clarify what the semantics of each is, via truth tables. The manner in which we specify a syntax for compound propositions is by introducing logical *connectives*, and then asserting that the use of such connectives in particular ways is syntactically valid.

Logical connectives – syntax Given that each of p and q is a proposition, so are the following:

- (p): parenthesization – used to force precedence.
- $\neg p$: negation.
- $p \wedge q$: conjunction.
- $p \vee q$: disjunction.

- $p \implies q$: implication.
- $p \impliedby q$: inference.
- $p \iff q$: if and only if.

Given the above syntax for the use of logical connectives to make new propositions, we can further propose rules via which even more propositions can be derived. They would be similar to the axioms of boolean algebra, which you will likely see in ECE 124. We present an example here, but leave more for a future course. For this course, we focus on employing semantics, which we specify using truth tables, to infer more propositions. Similarly, in ECE 124, you will generally use "truth tables," like those employed here, rather than proofs based on the axioms of boolean algebra.

We point out that more connectives can be introduced, for example, $\oplus$, "exclusive-or." It turns out that in propositional logic, the connectives $\neg, \vee$ and $\wedge$ suffice, and all other connectives can be defined using those three only. Analogously, in ECE 124, you see that AND, OR, and NOT gates suffice to implement any boolean function; but you'll consider XOR and other gates, which may be more convenient for the implementation of specific functions. We introduced $\implies$, $\impliedby$ and $\iff$ as well because those are used heavily in this course for proofs. Consequently, it is useful to directly specify and understand those connectives as well.

As an example of the use of purely syntactic derivation, see `proofwiki.org/wiki/Rule_of_Material_Implication/Formulation_1/Forward_Implication/Proof`, which shows a derivation from $p \implies q$ to $\neg p \vee q$.

Logical connectives – semantics The following truth tables are customarily associated with the above propositions that are formed using logical connectives. A truth table specifies, for every possibility of a truth value for the constituent propositions, what the truth value of a compound proposition is. We use T for true, and F for false.

- parenthesization:

p	(p)
T	T
F	F

  The above truth table merely emphasizes that the truth value of p is unaffected by parenthesization.

- negation:

p	$\neg p$
T	F
F	T

Example: suppose "the Sun is hot" is true. Then, "the Sun is not hot" is false. The second statement is the manner in which we customarily write the negation of "the Sun is hot" in English.

- conjunction:

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

Example: suppose "the Moon is made of cheese" is false, and "the Sun is hot" is true. Then, "the Moon is made of cheese and the Sun is hot" is false.

- disjunction:

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

Example: suppose "the Moon is made of cheese" is false, and "the Sun is hot" is true. Then, "either the Moon is made of cheese, or the Sun is hot, or both" is true.

- implication:

p	q	$p \implies q$
T	T	T
T	F	F
F	T	T
F	F	T

Example: suppose "the Moon is made of cheese" is false, and "the Sun is hot" is true. Then:

  - "If the Sun is hot, then the Moon is made of cheese" is false.
  - "If the Moon is made of cheese, then the Sun is hot" is true.
  - "If the Sun is not hot, then the Moon is made of cheese" is true.

The last two examples illustrate that, in propositional logic, "if p then q" may have a very different meaning than in natural language. In English, it is often used, for instance, to imply a causal relationship between p and q. But given a premise p that is false – for example, "the Sun is not hot" – the implication $p \implies q$ is true for any q, even a completely unrelated proposition q such as "the Moon is made of cheese." So the current truth of $p \implies q$ does not mean that, when the Sun eventually cools, the Moon will then be composed entirely of fermented curd; rather, when the Sun cools, the implication itself will be false: in our truth-functional semantics, the truth value of the compound proposition reflects only the specific truth values of the constituent propositions, and no more profound relationship between those constituent propositions. It may be helpful to think of "if p then q" as shorthand for, "(in any row of the truth table in which $p \implies q$ is true), if p is true, then q is true."

In mathematics, because we use these same truth-functional semantics, if p is false, we say that $p \implies q$ is *vacuously true*, to mean that the implication is true simply by virtue of the falsity of its premise. For example, if p is "x is an element of the empty set," and q is "x has property Q," then $p \implies q$ is (vacuously) true, whatever the property Q: the elements of the empty set can be said to have any property that you like, because there are no such elements.

It is not necessary to read $p \implies q$ as "if p then q"; another common way is to say "p only if q." Again, the proper interpretation is truth-functional.

In other words, in our truth-functional semantics, the following two statements are completely equivalent:

> If the Sun is hot, then the Moon is made of cheese.
>
> The Sun is hot only if the Moon is made of cheese.

- inference:

p	q	$p \impliedby q$
T	T	T
T	F	T
F	T	F
F	F	T

Here the compound proposition is a different way of writing $q \implies p$. It is commonly read, "p if q," but should be interpreted only truth-functionally, and not as implying some deeper relationship between p and q.

Example: suppose "the Moon is made of cheese" is false, and "the Sun is hot" is true. Then:

- "the Sun is hot if the Moon is made of cheese" is true.
- "the Moon is made of cheese if the Sun is hot" is false.
- "the Moon is made of cheese if the Sun is not hot" is true.

- if and only if:

p	q	$p \iff q$
T	T	T
T	F	F
F	T	F
F	F	T

Example: suppose "the Moon is made of cheese" is false, and "the Sun is hot" is true. Then:

- "The Sun is hot if and only if the Moon is made of cheese" is false.
- "The Moon is made of cheese if and only if the Sun is not hot" is true.

Given the above semantics via truth tables, we can now infer several more propositions.

Claim 1. $(p \implies q) \iff (\neg p \vee q)$.

Proof. By truth-table.

p	q	$\neg p$	$p \implies q$	$\neg p \vee q$	$(p \implies q) \iff (\neg p \vee q)$
F	F	T	T	T	T
F	T	T	T	T	T
T	F	F	F	F	T
T	T	F	T	T	T

□

We claim that the above is a valid proof for the claim because for every possible combination of truth values for p and q, we have shown that the

proposition in the claim is true. We now make and prove two more claims. The first, which is an implication, has a special name, and is useful for carrying out some proofs. Given $p \implies q$, we call the proposition $\neg q \implies \neg p$ its *contrapositive*. The contrapositive of an implication is different from the *converse*: the converse of $p \implies q$ is $q \implies p$. It turns out that $(p \implies q) \iff (\neg q \implies \neg p)$, that is, an implication and its contrapositive are completely equivalent from the standpoint of their respective truth values. However, given a proposition $p \implies q$, its converse, $q \implies p$, is not necessarily true.

For example, suppose you know that if it rains, then I carry an umbrella. You happen to observe that I am carrying an umbrella. Can you infer anything, for example, that it is raining? The answer is no, not necessarily. On the other hand, suppose you observe that I am not carrying an umbrella. Can you infer anything? The answer is yes, you can infer that it is not raining.

Claim 2. $(p \implies q) \iff (\neg q \implies \neg p)$.

Proof. We prove by truth table.

p	q	$\neg p$	$\neg q$	$p \implies q$	$\neg q \implies \neg p$	$(p \implies q) \iff (\neg q \implies \neg p)$
F	F	T	T	T	T	T
F	T	T	F	T	T	T
T	F	F	T	F	F	T
T	T	F	F	T	T	T

□

We now assert something that is perhaps not as easy to prove. If only because it involves three propositions, p, q and r. But again, careful use of the truth table enables us to carry out the proof.

Claim 3. $(p \implies q) \implies (p \vee r \implies q \vee r)$.

Proof. By truth table.

p	q	r	$p \vee r$	$q \vee r$	$p \implies q$	$p \vee r \implies q \vee r$	$(p \implies q) \implies (p \vee r \implies q \vee r)$
F	F	F	F	F	T	T	T
F	F	T	T	T	T	T	T
F	T	F	F	T	T	T	T
F	T	T	T	T	T	T	T
T	F	F	T	F	F	F	T
T	F	T	T	T	F	T	T
T	T	F	T	T	T	T	T
T	T	T	T	T	T	T	T

□

Perhaps the trickiest part of the truth table in the above proof is intuiting the truth value of the last column when $p \implies q$ is false. Recall that the proposition $\phi \implies \psi$ is true whenever ϕ is false. And in this case, ϕ is $p \implies q$.

A number of other useful propositions can similarly be inferred from the truth tables. Following are some useful propositions, and names we associate with them when perceived as properties.

- $(p \vee q) \iff (q \vee p)$ – commutativity of $\vee$.
- $(p \wedge q) \iff (q \wedge p)$ – commutativity of $\wedge$.
- $((p \vee q) \vee r) \iff (p \vee (q \vee r))$ – associativity of $\vee$.
- $((p \wedge q) \wedge r) \iff (p \wedge (q \wedge r))$ – associativity of $\wedge$.
- $(\neg(p \vee q)) \iff (\neg p \wedge \neg q)$ – De Morgan's law ($\neg$ over $\vee$).
- $(\neg(p \wedge q)) \iff (\neg p \vee \neg q)$ – De Morgan's law ($\neg$ over $\wedge$).
- $(p \vee (q \wedge r)) \iff ((p \vee q) \wedge (p \vee r))$ – distributivity of $\vee$ over $\wedge$.
- $(p \wedge (q \vee r)) \iff ((p \wedge q) \vee (p \wedge r))$ – distributivity of $\wedge$ over $\vee$.
- $(p \implies q) \iff (q \impliedby p)$.
- $(p \iff q) \iff ((p \implies q) \wedge (p \impliedby q))$.

Quantifiers We now introduce constructs that are not part of propositional logic, but a higher-order logic called *predicate* logic. However, as they are useful for this course in intuiting properties in various contexts, we introduce and discuss them here. The constructs are called *quantifiers*, and they are useful when we want to make assertions that have variables in them.

An example of the use of a quantifier is the following: "every star is hot." Another way of saying the same thing, while explicating the use of a variable and a quantifier is: "for every star x, x is hot." The "for every" part is a quantifier, specifically the *universal* quantifier. The other quantifier of interest to use is the *existential* quantifier. An example of its use is: "there exists x such that x is a bird and x can fly." (More simply, in English we would say, "there exists a bird that can fly," or "some birds can fly.")

The notation we use for the universal quantifier is "$\forall$" and for the existential quantifier is "$\exists$." For example, we might write: "$\exists$ rational y such that $y^2 = 2$." As another example, "$\forall$ integer x, x^3 is an integer ." We can use the logical connectives $\neg, \vee$ and $\wedge$ along with quantifiers. For example, to express that there exists no rational y such that $y^2 = 2$, we could write: "$\neg(\exists$ rational y such that $y^2 = 2)$,"

In the context of that last example, it is useful to be able to intuit equivalent assertions. We could equivalently assert: "$\forall$ rational $y, \neg(y^2 = 2)$," for that example, or, "$\forall$ rational $y, y^2 \neq 2$," if we define the symbol "$\neq$" as the complement of "$=$." Indeed, following are the rules, in general, of negating an assertion with a quantifier. In the following, we assume that $p(x)$ is an assertion that involves the variable x.

- $\neg(\exists x, p(x)) \iff \forall x, \neg p(x)$.
- $\neg(\forall x, p(x)) \iff \exists x, \neg p(x)$.

We can quantify over more than one variable. For example: "$\forall$ positive integer a, $\exists$ real b such that $b = \sqrt{a}$." Note that, when different quantifiers are used, as in this example, their order matters: in general, "$\forall$ person a, $\exists$ person b such that b is a's mother" is not equivalent to "$\exists$ person b, such that, $\forall$ person a, b is a's mother"; the first formula asserts that every person has a mother, the second that there is a person who is mother to everyone (even herself).

Sometimes, when we use the same quantifier over multiple variables, we write

one instance of a quantifier only, and not several. For example:

$$\forall \text{ real } a, b, (a \leq b \vee b \leq a)$$

When we really should write "$\forall$ real a, $\forall$ real $b \ldots$."

We have already been using quantifiers implicitly. For example, consider Claim 3 above. When we refer to p, q and r in the statement of the claim, what we really mean to say is, "for all propositions p, q and r, it is true that…" The "for all" quantifiers on each of p, q and r were left implicit in the statement of the claim.

Proof techniques

We now discuss proof techniques that are useful in this course, and in future, to you in your engineering profession. The mindset and systematic thinking that working out a proof develops is critical to one's success as an engineer. The kinds of proofs we develop, and the underlying mindsets and techniques we use, are not only of esoteric or theoretical interest. They have immediate, practical consequence. Also, the precise communication that such proofs require also are very valuable for one to develop as an engineer. Precise technical communication is an invaluable skill, that is highy prized not only in academia, but also industry and business settings. We return to this somewhat philosophical discussion once we have discussed the proof techniques we seek to impart as part of this course.

Logical deduction The overarching technique we use is logical deduction: going from a set of known or assumed statements to new statements, that are typically derived by logic implication. We have already seen some examples of this in our discussions on logic in this chapter.

Consider the following joke. Three logicians walk into a bar. The bartender asks, "would y'all like something to drink?" Logician 1 says, "I don't know." Logician 2 says, "I don't know." Logician 3 says, "yes."

The joke is a play on the wording of the bartender's question, specifically, her use of "all." She seems to be asking whether all three of the logicians want a drink. Presumably, each of Logicians 1 and 2 would like a drink. But they do not know yet as to whether all of them want a drink. Therefore, they are compelled to say, "I don't know." Logician 3 infers that the other two would each like a drink; otherwise, one of them would have said, "no." She knows that she wants a drink herself, and therefore says, "yes."

Imagine that Logician 3 had said, "no." Then, presumably Logicians 1 and 2 want a drink each, but Logician 3 does not. While this is admittedly a joke, it exercises logical deduction in a good way. Such logical deduction is at the foundations of every proof we carry out. Following are some specific strategies one could adopt to carry out a proof. Each strategy provides a kind of framework within which logical deduction is used. More than one strategy may be useful in carrying out a proof, and a proof does not require any particular strategy to be adopted to be carried out successfully. It is

important also to recognize when one has successfully carried out a proof; the strategy helps with this aspect as well.

Some of the strategies that arise in this course, and in future courses are:

- Case analysis: we enumerate, exhaustively, all possible cases that can occur, and prove each, in turn. Following is an example.

  Claim 4. *For any three natural numbers x, y, z, where $x + y = z$, if any two of x, y, z are divisible by 3, then so is the third.*

  Proof. By case analysis.

  1. x, y are divisible by 3. Then, $x = 3a, y = 3b$ for some natural numbers a, b. Then, because $z = x+y, z = 3(a+b)$, which implies that z is divisible by 3.
  2. x, z are divisible by 3. Then, $x = 3a, z = 3b$ for some natural numbers a, b. As y is a natural number, i.e., $y \geq 0$ and $x + y = z$, $b \geq a$. And, $y = 3(b - a)$. As $b \geq a$, $b - a$ is a natural number, and therefore y is a natural number that is divisible by 3.
  3. y, z are divisible by 3. This is identical to the previous case as x and y are interchangeable.

  □

  An interesting observation about the above claim is that its converse is not necessarily true. That is, for three natural numbers x, y, z with $x+y = z$, if one of them is divisible 3, it does not necessarily imply that the other two are as well. A *counterexample* can be used to establish this. A counterexample is $x = 1, y = 2, z = 3$.

- Contradiction: we recall the truth table for an implication, and observe that the only case such a proposition is false is when ϕ is true, and ψ is false. For a proof by contradiction of a proposition $\phi \implies \psi$, we assume that the premise, ϕ is true, and yet, the implication, ψ, is false. We then establish by logical deduction that something that is false must be true, or that something that is true must be false – this is the contradiction we deduce.

  For example, consider the following claim, and its proof by contradiction.

Claim 5. *$\sqrt{2}$ is not rational.*

Proof. To perceive the statement the claim as an implication, we can rephrase it as: $x = \sqrt{2} \implies x$ is not a rational number.

For the purpose of contradiction, assume that $x = \sqrt{2}$, and x is rational. Then, $x = p/q$, where p and q are integers. We assume, without loss of generality, that p and q have only 1 as a common factor, i.e., p/q is in its simplest form. Then, $x^2 = 2 = p^2/q^2 \implies p^2 = 2q^2$.

Thus, p^2 is even. This implies that p is even, because if p is odd, then p is of the form $2x+1$ where x is an integer, and $(2x+1)^2 = 4x^2+4x+1$, which is odd. Thus, $p = 2y$, for some integer y.

Therefore, $p^2/2 = (2y)^2/2 = 2y^2 = q^2$. Thus, q^2 is even as well, and therefore q is even. Thus, both p and q are even, which means p/q is not in its simplest form, which is our desired contradiction.

□

Another example, which was on the final exam of the Spring'18 offering of the course is the following claim. We define an even number as follows: x is an even number if $x = 2y$, where y is an integer.

Claim 6. *If a, b, c are positive integers, then at least one of $a-b, b-c, c-a$ is even.*

An example is $a = 13, b = 8, c = 5$. Then, $c - a = -8$, which is even.

Proof. Assume, for the purpose of contradiction, that none of $a-b, b-c, c-a$ is even. Then, $a-b = 2k+1$ for some integer k, and $b-c = 2l+1$ for some integer l. then, $c-a = -(b-c+a-b) = -(2l+1+2k+1) = 2(-l-k+1)$, which is an integer because l, k are integers, and is even. This contradicts our assumption that $c - a$ is odd. □

- Contrapositive: recall that $(\phi \implies \psi) \iff (\neg\psi \implies \neg\phi)$; the two implications are contrapositives of one another. Given a claim $\phi \implies \psi$ a proof of the contrapositive proves, instead, $\neg\psi \implies \neg\phi$.

  Following is an example of proof by contrapositive.

Claim 7. *For x, y positive integers,* $\left(\sum_{i=1}^{x} i = \sum_{i=1}^{y} i\right) \implies (x = y)$.

Proof. We prove the contrapositive, that is, for x, y positive integers, $(x \neq y) \implies \left(\sum_{i=1}^{x} i \neq \sum_{i=1}^{y} i\right)$.

Given that $x \neq y$, either (i) $x > y$ or (ii) $x < y$. In case (i), $\left(\sum_{i=1}^{x} i\right) = \left(\sum_{i=1}^{y} i + \sum_{i=y+1}^{x} i\right) \geq \left(y + 1 + \sum_{i=1}^{y} i\right) > \left(1 + \sum_{i=1}^{y} i\right)$, because $x \geq y+1$ and $y > 0$. This implies that $\sum_{i=1}^{x} i \neq \sum_{i=1}^{y} i$, as desired.

Case (ii) is proven identically, by interchanging x and y. □

- Construction: this is typically for statements of the form "there exists..." That is, a natural way to prove that something exists is to construct, or present, one. For example, if we all agree on what an elephant is, and I am challenged to prove that elephants exist, I can simply produce and present an elephant. Following is an example.

  Claim 8. *Given any two real numbers, x, y such that $x < y$, there exists a real number z such that $x < z < y$.*

  Proof. By construction. Let $z = (x + y)/2$. Then z is real because the sum of two real numbers is real, and dividing a real by another that is not zero yields a real. To establish that $x < z < y$, we observe:

$$\begin{aligned} x < z < y &\impliedby x < \frac{x+y}{2} < y \\ &\impliedby 2x < x + y < 2y \\ &\impliedby x + x < x + y < y + y \\ &\impliedby x < y \end{aligned}$$

  □

The above proof demonstrates a useful strategy: to begin with what we seek to prove, and then work backwards to a sufficient condition for that to be true, in this case, $x < y$, which we know to be true.

- Induction: a proof by induction is usually put to use when we have a statement that involves a universal quantifier, for a sequence of items, for example, all natural numbers. A proof by induction is structured as follows:
  - We first prove that the statement is true for the *base case*. The base case is the statement for the first natural number, 0.
  - We then prove the *step*, i.e., the following implication: if the statement is true for all natural numbers, $0, 1, \ldots, i-1$, then the statement is true for the natural number i.

  Together, the two steps above prove the statement for all items in the sequence, for example, every natural number. This is because proving the (i) base case, i.e., the statement for 0, and, (ii) the step, implies that the statement is true for the second natural number, 1. This, with the step, in turn implies that the statement is true for 2. And, 3, and so on, for all natural numbers. Following is an example.

Claim 9. $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$.

Proof. By induction on n.

Base case: $n = 1$. When $n = 1$, the left hand side is 1. And the right hand-side is $\frac{1\times 2}{2} = 1$. Thus, we have proved that the statement is true for the base case.

Step: we adopt the induction assumption, that the statement is true for all $n = 1, 2, \ldots, i-1$, for some $i \geq 2$. Under that premise, we seek to prove the statement for $n = i$. We observe:

$$\begin{aligned} 1 + 2 + \ldots + i - 1 + i &= \frac{(i-1)i}{2} + i \qquad \because \text{induction assumption} \\ &= \frac{i^2 - i + 2i}{2} \\ &= \frac{i^2 + i}{2} = \frac{i(i+1)}{2} \end{aligned}$$

Thus, we have proven the base case and the step, and therefore we have successfully carried out our proof by induction on n.

□

As the base case, we have proved that the statement is true when $n = 1$. As a consequence of proving the step, then, we have proved that the statement is true for $n = 2$. And with that, and as a consequence of the step, we have proved that the statement is true for $n = 3$. And so on.

We now carry out several proofs as examples to demonstrate the above strategies. We begin with a problem from the final exam of the Spring'18 offering of the course.

Claim 10. *For every natural number $n \geq 12$, there exist natural numbers m_1, m_2 such that $n = 4m_1 + 5m_2$.*

Proof. By induction on n.

Base cases: we prove the statement for the following cases: $n = 12, 13, 14, 15$. The reason we consider several base cases becomes apparent once we get in to proving the step. We observe:

- $12 = 4 \times 3 + 5 \times 0$.
- $13 = 4 \times 2 + 5 \times 1$.
- $14 = 4 \times 1 + 5 \times 2$.
- $15 = 4 \times 0 + 5 \times 3$.

Step: we assume that the assertion is true for all $n = 12, 13, \ldots, i - 1$ for some $i \geq 13$. For $n = i$, we first observe that $i = i - 1 + 1 = 4k_1 + 5k_2 + 1$, for some natural numbers k_1, k_2, from the induction assumption. We do a case analysis.

Case (i): $k_1 > 0$. Then, $i = 4k_1 + 5k_2 + 1 = 4(k_1 - 1) + 5(k_2 + 1)$.

Case (ii): $k_1 = 0$. Then, because $i > 12$, $k_2 \geq 3$. Then, $i = 5k_2 + 1 = 4 \times 4 + 5(k_2 - 3)$.

The reason we prove several base cases is to address Case (ii) of the step. Because the smallest n for which $k_2 \geq 3$ is $n = 15$. By addressing several

base cases, we ensure that our proof is indeed correct, i.e., that we can indeed make the inductive argument. □

Claim 11. *For every non-negative integer n, exactly one of the following is true:*

- *there exists a non-negative integer m such that $n = 3m$.*
- *there exists a non-negative integer m such that $n = 3m + 1$.*
- *there exists a non-negative integer m such that $n = 3m + 2$.*

We need to be careful here in that the statement says that exactly one of those cases is true. That is, for a particular n, one of the cases is true, and neither of the others is true. We need to prove both those properties.

Proof. By induction on n. Again, we are careful to address several base cases.

Base cases: for each of $n = 0, 1, 2$, we prove the first part by construction, i.e., by producing an m that demonstrates that the statement is true.

For $n = 0$, we observe that $0 = 3 \times 0$, i.e., $m = 0$, which proves that the statement is true. For $n = 1$, we again propose $m = 0$, and observe that $n = 1 = 3 \times 0 + 1$. And for $n = 2$, we propose $m = 0$, and observe that $n = 2 = 3 \times 0 + 2$. Thus, we have shown one part of the statement for each of $n = 0, 1, 2$, which is that there exists such an m.

We now prove the other part of the statement: that given that $0 = 3m$ for some m, then it can be neither $3m' + 1$ nor $3m' + 2$ for any non-negative integer m'. Suppose, for the purpose of contradiction, there exists such an m', that is, $0 = 3m' + 1$. Then, $m' = -1/3$, which contradicts the assumption that m' is a non-negative integer. Similarly, $0 = 3m' + 2 \implies m' = -2/3$, again a contradiction.

And similarly, if $1 = 3m'$, then $m' = 1/3$ and if $1 = 3m' + 2$, then $m' = -1/3$, in each case a contradiction to the assumption that m' is a non-negative integer. And finally, if $2 = 3m'$, then $m' = 2/3$, and if $2 = 3m' + 1$, then $m' = 1/3$.

Step: we assume that the statement is true for all $n = 0, 1, 2, \ldots, i - 1$ for some $i \geq 1$. For $n = i$, we do a case analysis, and in each case, produce an m.

- if $i - 1 = 3m$ for some non-negative integer m, then, $i = 3m + 1$.
- if $i - 1 = 3m + 1$ for some non-negative integer m, then, $i = 3m + 2$.
- if $i - 1 = 3m + 2$ for some non-negative integer m, then, $i = 3(m + 1)$. And because m is a non-negative integer, so is $m + 1$.

To establish that no other case applies, assume that a non-negative integer m' exists that corresponds to one of the other cases, for the purpose of contradiction. We again do a case analysis.

- if $i = 3m$ and $i = 3m' + 1$, then $m' = m - 1/3$, which is a contradiction to the assumption that m' is a non-negative integer. And if $i = 3m' + 2$, then $m' = m - 2/3$, which is a similar contradiction.
- if $i = 3m + 1$ and $i = 3m'$, then $m' = m + 1/3$, and if $i = 3m' + 2$, then $m' = m - 1/3$, each of which is a contradiction.
- if $i = 3m + 2$ and $i = 3m'$, then $m' = m + 2/3$, and if $i = 3m' + 1$, then $m' = m + 1/3$, both of which contradict our assumption that m' is a non-negative integer.

□

We now consider a proof by induction for a statement that is obviously not true. The statement is: all horses have the same colour. The proof is as follows. For the base case, pick a horse. Obviously it is the same colour as itself. Therefore, the base case has been proved. The induction assumption is that given up to $n = i - 1$ horses, for some $i \geq 2$, they all have the same colour. Now consider that we are given $n = i$ horses. We pick some horse, and temporarily remove it from the set. Then we are left with $i - 1$ horses which, by the induction assumption all have the same colour. We now temporarily remove one of those $i - 1$ horses from the set, and add back in the horse that we first removed. Again, we are left with $i - 1$ horses which, by the induction assumption must all have the same colour.

A flaw in the above proof is in the manner in which we prove the step. While it is certainly ok to remove a horse, call it H, from the set and then assert that the remainder all have the same colour, what we now need to do is prove

that H has the same colour as the other $i-1$ horses. We cannot again appeal to the induction assumption to do that, as the above flawed proof does.

We now present one more correct example of proof by induction. In the following claim, we address a situation that there appears to be more than one choice for the parameter on which we carry out induction.

Claim 12. *Suppose n is a natural number whose digits, in order of most- to least-significant, are $n_{k-1}\, n_{k-2}\, \ldots, n_0$, where each n_i is one of $0, \ldots, 9$. If the sum of the digits of n, $S_n = \sum_{i=0}^{k-1} n_i$, is divisible by 3, then n is divisible by 3.*

An example is $n = 809173$. Then, $S_n = 28$, which is not divisible by 3. Therefore, from the statement in the claim, we cannot infer anything as to whether n is divisible by 3. On the other hand, the digits of 82907370 add up to 36, and therefore, if the claim is true, then 82907370 is divisible by 3.

We emphasize that the implication in the statement goes in one direction only. "...if S_n is divisible by 3, then n is divisible by 3..." It says nothing about what S_n may be if n is divisible by 3.

The above claim presents an example of where if we choose to carry out a proof by induction, then we need to clearly say on what parameter we carry out induction. For the above claim, there appear to be at least two choices: induction on n, and induction on k. In the following proof, we carry out induction on k, i.e., the number of digits when we write n in decimal.

Proof. Base case: $k = 1$. Then, $n = n_0 = S_n$, i.e., n has only one digit. Then, for S_n to be divisible by 3, S_n must be one of $3, 6$ or 9. In each case, because $n = S_n$, we observe that n is divible by 3 as well.

Step: our induction assumption is that given any n that has $k = 1, \ldots, i-1$ digits, for some $i \geq 2$, if S_n is divisible by 3, then so is n. We need to now prove that given some n of i digits, if S_n is divisible by 3, then so is n. Henceforth, we use the notation $(\,)_{10}$ to indicate when we write a number in base-10, i.e., its digits from most- to least-significant.

We have $n = (n_{i-1}\, n_{i-2} \ldots n_0)_{10}$. Therefore, $n = 10^{i-1} n_{i-1} + 10^{i-2} n_{i-2} + \ldots +$

$10^0 n_0 = 10^{i-1} n_{i-1} + (n_{i-2} \ldots n_0)_{10}$. Also, $S_n = \sum_{j=0}^{i-1} n_j = n_{i-1} + \sum_{j=0}^{i-2} n_j$. We do a case analysis on $\sum_{j=0}^{i-2} n_j$ as to whether it is divisible by 3. We appeal often to Claim 4. Recall that that claim is: given three natural numbers x, y, z such that $x + y = z$ and any two are divisible by 3, then so is the third.

- Suppose $\sum_{j=0}^{i-2} n_j$ is divisible by 3. Then, for S_n to be divisible by 3, n_{i-1} must be divisible by 3 by Claim 4. That is, $n_{i-1} = 3a$ for some natural number a. Then, $n = 10^{i-1} \times 3a + (n_{i-2} \ldots n_0)_{10}$. As $\sum_{j=0}^{i-2} n_j$ is divisible by 3, by the induction assumption, $(n_{i-2} \ldots n_0)_{10}$ is divisible by 3. Therefore, by Claim 4, $n = 10^{i-1} \times 3a + (n_{i-2} \ldots n_0)_{10}$ is divisible by 3, because it is the sum of two numbers, each of which is divisible by 3.

- Suppose $\sum_{j=0}^{i-2} n_j$ is not divisible by 3. Then, $\sum_{j=0}^{i-2} n_j = 3a + b$, for some natural number a, and for b either 1 or 2. We now do a case analysis of those two cases for b.

  - If $b = 1$, then $n_{i-1} = 3a' + 2$ for some natural number a', because otherwise, S_n is not divisible by 3. And we have:

$$\begin{aligned} n &= 10^{i-1} n_{i-1} + (n_{i-2} \ldots n_0)_{10} \\ &= 10^{i-1}(3a' + 2) + (n_{i-2} \ldots n_0)_{10} \\ &= 10^{i-1} \times 3a' + 10^{i-2} \times 20 + (n_{i-2} \ldots n_0)_{10} \end{aligned}$$

    Now, we do a further case analysis on n_{i-2}:

    * If $n_{i-2} = 0$, then, we choose to write n as:

$$n = 10^{i-1} \times 3a' + 10^{i-2} \times 18 + (2\, n_{i-3} \ldots n_0)_{10}$$

      Now, each of $10^{i-1} \times 3a'$ and $10^{i-2} \times 18$ is divisible by 3. And the digits of $(2\, n_{i-3} \ldots n_0)_{10}$ are divisible by 3, because

$\sum_{j=2}^{i-2} n_j = 3a + 1$. Therefore, by the induction assumption, $(2\, n_{i-3} \ldots n_0)$ is divisible by 3. Thus, n is the sum of three numbers, each of which is divisible by 3, and therefore n is divisible by 3.

* If $n_{i-2} > 0$, then, we choose to write n as:

$$n = 10^{i-1} \times 3a' + 10^{i-2} \times 21 + ((n_{i-2} - 1)\, n_{i-3} \ldots n_0)_{10}$$

Again, n is the sum of three numbers each of which is divisible by 3.

– If $b = 2$, then $n_{i-1} = 3a' + 1$ for some natural number a', because otherwise, S_n is not divisible by 3. And we have:

$$\begin{aligned} n &= 10^{i-1} n_{i-1} + (n_{i-2} \ldots n_0)_{10} \\ &= 10^{i-1}(3a' + 1) + (n_{i-2} \ldots n_0)_{10} \\ &= 10^{i-1} \times 3a' + 10^{i-2} \times 10 + (n_{i-2} \ldots n_0)_{10} \end{aligned}$$

As before, we do a further case analysis on n_{i-2}:

* If $n_{i-2} = 0$ or $n_{i-2} = 1$, then we choose to write n as:

$$n = 10^{i-1} \times 3a' + 10^{i-2} \times 9 + ((n_{i-2} + 1)\, n_{i-3} \ldots n_0)_{10}$$

And n is the sum of three numbers each of which is divisible by 3.

* If $n_{i-2} \geq 2$, then we choose to write n as:

$$n = 10^{i-1} \times 3a' + 10^{i-2} \times 12 + ((n_{i-2} - 2)\, n_{i-3} \ldots n_0)_{10}$$

And n is the sum of three numbers each of which is divisible by 3.

□

Chapter 3

Sets, Functions and Cardinality

A *set* is a collection of distinct item or *elements*. For example, {apple, orange, pear} is a set, as is $\{1, 2, aardvark, x\}$.

The above definition is somewhat vague and incomplete, and as will be seen shortly, it can lead to paradoxes. A thorough treatment of the way it needs to be qualified is beyond the scope of this course. Suffice it to say that it is safe to consider the standard collections normally encountered in engineering – such as those of the integers, rationals and real numbers – to be sets; and we will introduce some restrictions on the manner in which new sets can be defined – these will be sufficient to keep us out of trouble.

A set is completely determined by its elements: two sets A and B are identical, or *equal*, written $A = B$, if they have exactly the same elements. Otherwise, they are distinct, different or unequal: $A \neq B$.

We emphasize two important properties of a set:

- a set imposes no ordering on the items it contains. A set is an unordered collection. For example, $\{1, 2, 3\} = \{2, 1, 3\}$.
- each element of a set is distinct. No two elements can be identical. As an example, this precludes $\{1, 1, 2, 3\}$ from being deemed a set. (It is, rather, a *multiset*.)

An element of a set can also be called a *member*, and we say that the set *contains* that member. We use "$\in$" to denote set membership. E.g., $1 \in$

$\{1, 2, 3\}$, and, $x \in \{a, x, y, z\}$. The complement of $\in$ is $\notin$, e.g., $b \notin \{a, x, y, z\}$. We can define $\notin$ terms of $\in$ as follows, using logic: $x \notin S \iff \neg(x \in S)$.

The *empty set* is a set which has no members. By definition, any two such sets are in fact one and the same: they have exactly the same members. There is therefore a unique empty set. It is denoted $\emptyset$, or $\{\,\}$.

An alternative to denoting a set by enumerating elements is *set-builder notation*. An example of the specification of a set using set-builder notation is as follows: $\{x \mid x \text{ is an integer} > 0 \text{ and } \leq 5\}$. Of course, that specifies the set $\{1, 2, 3, 4, 5\}$. As the example suggests, in set-builder notation, we use the vertical bar, "$\mid$" to specify conditions on the members of the set.

The complement of the empty set, $\emptyset$, is the set of everything, which is called the *universal set*, or simply, the *universe* and is denoted $\mathcal{U}$. We need to be careful with what we include in $\mathcal{U}$, i.e., what "everything" means in this context, as our discussions on Russell's paradox below indicate. Typically, we associate our discussions with a *domain of discourse*, and the domain of discourse specifies what $\mathcal{U}$ is. For example, our domain of discourse may be all natural numbers, in which case $\mathcal{U}$ would be the set of all natural numbers. As another example, our domain of discourse may be all people, in which case $\mathcal{U}$ would be the set of all people. The domain of discourse, and therefore what $\mathcal{U}$ is, is typically clear from context.

Special sets We now identify sets that we and others refer to frequently. The set of natural numbers, denoted $\mathbb{N}$ is $\{1, 2, \ldots\}$. The set of whole numbers, $\mathbb{W} = \{0, 1, 2, 3, \ldots\}$. The set of integers, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$. The set of positive integers, $\mathbb{Z}^+ = \{1, 2, 3 \ldots\} = \mathbb{N}$. The set of non-negative integers, $\mathbb{Z}_0^+ = \{0, 1, 2, \ldots\} = \mathbb{W}$. The set of negative, and non-positive integers are similarly specified, and denoted $\mathbb{Z}^-$ and $\mathbb{Z}_0^-$, respectively. The set of real numbers is denoted $\mathbb{R}$, and correspondingly, we have the of positive real numbers, $\mathbb{R}^+$, the set of non-negative reals $\mathbb{R}_0^+$, the set of negative reals, $\mathbb{R}^-$, and the set of non-positive reals, $\mathbb{R}_0^-$.

The set of rational numbers, denoted $\mathbb{Q}$, can be defined using the set-builder notation as follows: $\mathbb{Q} = \{p/q \mid p \in \mathbb{Z}, q \in \mathbb{Z}^+, p \text{ and } q \text{ have no factor, or divisor, in common other than 1}\}$. Such a specification using the set-builder notation brings us to the issue of care we need to take when using the set-builder notation.

Russell's paradox A set is a collection of items. A set itself can be perceived as an item. Therefore, it is possible to specify a set of sets. For example, $\{\{1\}, \emptyset, \{1, 2, 3, 4, 5\}\}$ is a set of sets of integers, which has three members. An immediate question that then arises is: can a set be a member of itself? It does not seem meaningful to allow this, and therefore we may mandate that no set is allowed to be a member of itself.

However, it turns out that this by itself does not preclude contradictions that can occur in the specification of a set. A particular contradiction is Russell's paradox, which is demonstrated by the following specification of a set using set-builder notation.

$$\text{Let } S = \{x \mid x \text{ is a set such that } x \notin x\}$$

That is, S is the set of all sets that do not contain themselves. Now, we ask: does S contain itself?

- If the answer is 'yes,' then:

  $$S \in S \implies S \text{ is a set that does not contain itself} \implies S \notin S$$

  Thus, we have a contradiction.

- If the answer is 'no,' then:

  $$S \notin S \implies S \text{ is a set that does not contain itself} \implies S \in S$$

  Thus, we again have a contradiction.

A thorough discussion on "clean" specifications of sets and other constructs is beyond the scope of this course. The above discussion on Russell's paradox reveals, however, that care must be taken. In our case, a quick "hack" is to restrict the manner in which the set-builder notation is used. We require that when specifying a set using the set-builder notation, it must look like the following:

$$\{x \in A \mid \text{conditions on } x\}$$

That is, we must specify of what superset A this set being specified is a subset. (See below for definitions of super- and subsets.) And the conditions that

appear after "$|$" are then used to specify which members of A are members of this set. Under these requirements, the earlier specification, $S = \{x \mid x \notin x\}$ is no longer allowed.

And if we specify, for example, $S = \{x \in A \mid x \notin x\}$, we no longer have a paradox. Because suppose $S = \{x \in A \mid x \notin x\}$ is our specification of S, and we again ask: is $S \in S$?

- If the answer is 'yes,' then:

$$S \in S \implies S \in A \wedge S \notin S \implies S \notin S$$

  Thus, we have a contradiction.

- If the answer is 'no,' then:

$$S \notin S \implies S \notin A \vee (S \in A \wedge S \notin S)$$

  Now, if $S \in A$, then $S \in A \wedge S \notin S \implies S \in S$, a contradiction.

Thus, we have a possibility without a contradiction, and that is that $S \notin A$. Which implies $S \notin S$, and the answer to the question "is $S \in S$?" is "no."

Set relationships and operations We now continue with our discussions on basic notions regarding sets.

A is a *subset* of B, denoted $A \subseteq B$, if every member of A is a member of B. That is, $A \subseteq B \iff (x \in A \implies x \in B)$. We say that A is a *strict subset* of B, denoted $A \subset B$, if A is a subset of B, but is not equal to B. That is, $A \subset B \iff (A \subseteq B \wedge A \neq B)$.

We say that A is a *superset* of B, denoted $A \supseteq B$ if and only if $B \subseteq A$. We say that A is a *strict superset* of B, denoted $A \supset B$ if and only if $A \supseteq B \wedge A \neq B$.

Claim 13. *For any two sets A, B, $(A = B) \iff (A \subseteq B \wedge A \supseteq B)$.*

Proof. By deduction.

$$\begin{aligned} A = B &\iff (x \in A \iff x \in B) \\ &\iff ((x \in A \implies x \in B) \wedge (x \in A \impliedby x \in B)) \\ &\iff (A \subseteq B \wedge A \supseteq B) \end{aligned}$$

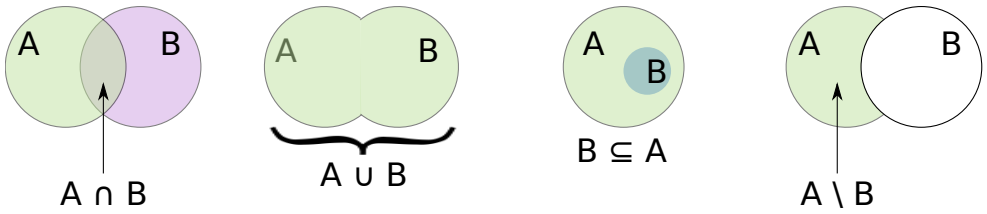
□

For two sets A, B, their *union*, denoted $A \cup B$ is the set with the property: $x \in A \cup B \iff (x \in A \vee x \in B)$.

Their *intersection*, denoted $A \cap B$ is the set with the property: $x \in A \cap B \iff (x \in A \wedge x \in B)$.

Their *difference*, denoted $A \setminus B$ or $A - B$, is the set $\{x \in A \mid x \notin B\}$.

Venn diagrams and their limitations We can visualize some set relationships and operations using Venn diagrams. Examples of Venn diagrams for intersection, union, subset and difference between two sets are shown below.



Venn diagrams are certainly useful to gain an understanding of what's going on in some limited situations with sets. However, they are not a proof strategy for several reasons. One is that they do not deal well with special cases, e.g., if one of the sets is empty, or the universe. They also do not scale to assertions, for example, that involve n sets, where n is some natural number. And they are not necessarily useful to intuit somewhat complex assertions, for example, the following from the final exam in Spring '18: "prove that for sets A, B, $(A \setminus B = B) \implies (A = \emptyset)$." Therefore, while Venn diagrams are useful to get an idea of what's going on, it is important to be able to work more abstractly, and be able to work with the proof strategies we discuss in this course.

We now present some properties of set operations.

Claim 14. *For any two sets A, B, $A \setminus B = A \setminus (A \cap B)$.*

Proof.

$$
\begin{aligned}
y \in A \setminus (A \cap B) &\iff y \in A \wedge (y \notin A \cap B) && (3.1)\\
&\iff y \in A \wedge (y \notin A \vee y \notin B) && (3.2)\\
&\iff (y \in A \wedge y \notin A) \vee (y \in A \wedge y \notin B) && (3.3)\\
&\iff \mathsf{false} \vee (y \in A \wedge y \notin B) && (3.4)\\
&\iff y \in A \wedge y \notin B && (3.5)\\
&\iff y \in A \setminus B && (3.6)
\end{aligned}
$$

Rationale for each line in the above proof:

(3.1) definition of set difference.

(3.2) $y \in A \cap B \iff (y \in A \wedge y \in B)$. Now, we negate each side, and we have: $\neg(y \in A \cap B) \iff \neg(y \in A \wedge y \in B)$. Which is the same as: $y \notin A \cap B \iff (y \notin A \vee y \notin B)$.

(3.3) $\wedge$ distributes over $\vee$.

(3.4) $\phi \wedge \neg\phi \iff \mathsf{false}$.

(3.5) $(\mathsf{false} \vee \phi) \iff \phi$.

(3.6) definition of set difference.

□

We can establish several properties of $\cup$ and $\cap$, for example, that they are commutative and associative, and how they work for the special sets, $\emptyset$ and $\mathcal{U}$. An interesting property is the manner in which $\cup$ and $\cap$ distribute over one another.

Claim 15. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Proof. The proof is pretty much directly from the distributivity of $\vee$ over $\wedge$. This is not a coincidence — $\cup$ between sets has a very similar semantics to $\vee$ between propositions, and $\cap$ between sets is similar to $\wedge$ between

propositions. The proof is as follows:

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

□

Similarly, we can show that $\cap$ distributes over $\cup$, i.e., $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

We can generalize the notion of union and intersection to more than just between two sets. Given a set $\mathcal{X}$, we define

$$\bigcup \mathcal{X} = \{y \in X \mid X \in \mathcal{X}\} \ .$$

For $\mathcal{X} \neq \emptyset$, let $X \in \mathcal{X}$. Then, we define:

$$\bigcap \mathcal{X} = \{x \in X \mid \forall X' \in \mathcal{X}, x \in X'\} \ .$$

For example, $\bigcup\{\{1,2\},\{2,3\},\{3,4\}\} = \{1,2,3,4\}$, and $\bigcap\{\{1,2,3\}, \{2,3,4\}, \{3,4,5\}\} = \{3\}$.

Claim 16. *Suppose* $\mathcal{X} = \{X_1, \ldots, X_n\}$ *for some* $n \in \mathbb{N}, n > 0$. *Then,* $\bigcup \mathcal{X} = X_1 \cup X_2 \cup \ldots \cup X_n$, *and* $\bigcap \mathcal{X} = X_1 \cap X_2 \cap \ldots \cap X_n$.

The claim can be proved by induction on n.

The *complement* of a set A, denoted $\overline{A}$ is $\overline{A} = \mathcal{U} \setminus A$, where $\mathcal{U}$ is the universal set. Thus, as special cases, we have: $\overline{\emptyset} = \mathcal{U}$, and $\overline{\mathcal{U}} = \emptyset$. As an example of the complement of a set, suppose $\mathcal{U} = \mathbb{Z}$, the set of integers. Then, $\overline{\mathbb{Z}^+} = \mathbb{Z} \setminus \mathbb{Z}^+ = \mathbb{Z}_0^-$, i.e., the set of all negative integers and zero.

Complement for sets is akin to negation in propositional logic.

Claim 17. $\overline{(\overline{A})} = A$.

Proof.

$$\begin{aligned}
x \in \overline{(\overline{A})} &\iff x \in \mathcal{U} \setminus \overline{A} \\
&\iff x \in \mathcal{U} \wedge x \notin \overline{A} \\
&\iff x \in \mathcal{U} \wedge x \notin (\mathcal{U} \setminus A) \\
&\iff x \in \mathcal{U} \wedge \neg(x \in \mathcal{U} \setminus A) \\
&\iff x \in \mathcal{U} \wedge \neg(x \in \mathcal{U} \wedge \neg(x \in A)) \\
&\iff x \in \mathcal{U} \wedge (x \notin \mathcal{U} \vee x \in A) \\
&\iff (x \in \mathcal{U} \wedge x \notin \mathcal{U}) \vee (x \in \mathcal{U} \wedge x \in A) \\
&\iff \mathsf{false} \vee (x \in \mathcal{U} \wedge x \in A) \\
&\iff x \in \mathcal{U} \wedge x \in A \\
&\iff x \in \mathcal{U} \cap A \iff x \in A
\end{aligned}$$

□

Ordered pairs and Cartesian product An *ordered pair* of two items, x and y, denoted $\langle x, y\rangle$ is defined as:

$$\langle x, y\rangle = \begin{cases} \{\{x\}\} & \text{if } x = y \\ \{\{x\}, \{x, y\}\} & \text{otherwise} \end{cases}$$

The main point of an ordered pair is to impose an ordering between the two items x and y; that is, if $x \neq y$, then $\langle x, y\rangle \neq \langle y, x\rangle$. This is captured by the following claim.

Claim 18. *Given two ordered pairs,* $\langle x_1, y_1\rangle, \langle x_2, y_2\rangle$*,*

$$(\langle x_1, y_1\rangle = \langle x_2, y_2\rangle) \iff ((x_1 = x_2) \wedge (y_1 = y_2))$$

Proof. For the " $\Longrightarrow$ " direction: we assume $\langle x_1, y_1\rangle = \langle x_2, y_2\rangle$ and consider two cases.

- $x_1 = y_1$ or $x_2 = y_2$. The two cases are the same, so we address the former only. $x_1 = y_1 \implies \langle x_1, y_1\rangle$ has one member only, which implies $x_2 = y_2$, as otherwise, $\langle x_2, y_2\rangle$ has two members. Furthermore, $\langle x_1, y_1\rangle = \{\{x_1\}\} = \{\{x_2\}\} = \langle x_2, y_2\rangle$, and therefore, $x_1 = x_2 = y_1 = y_2 \implies (x_1 = x_2) \wedge (y_1 = y_2)$.

- $x_1 \neq y_1$ or $x_2 \neq y_2$. The two cases are the same, so we address the former only. $\langle x_1, y_1 \rangle = \{\{x_1\}, \{x_1, y_1\}\} = \{\{x_2\}, \{x_2, y_2\}\} = \langle x_2, y_2 \rangle$. Thus, $\{x_1\} = \{x_2\} \implies x_1 = x_2$. And $\{x_1, y_1\} = \{x_2, y_2\} \implies y_1 = y_2$ as well.

The " $\Longleftarrow$ " direction is proven similarly. □

Ordered pairs are used when the ordering of two items is important, which means that making them members of a set does not suffice, as a set is unordered. For example, we may want ordered pairs of $\langle \text{parent}, \text{child} \rangle$, and then the ordered pair $\langle \text{Alice}, \text{Bob} \rangle$ is different from $\langle \text{Bob}, \text{Alice} \rangle$, because the former says that Alice is a parent of Bob, while the latter says that Bob is a parent of Alice.

Now that we have a characterization of ordered pairs, we can define the *Cartesian product*. The Cartesian product of two sets, A, B, denoted $A \times B$ is defined as:

$$A \times B = \{\langle x, y \rangle \mid x \in A \text{ and } y \in B\}$$

For example, if $A = \{1, 2, 3\}, B = \{a, b\}$, then $A \times B = \{\langle 1, a \rangle, \langle 1, b \rangle, \langle 2, a \rangle, \langle 2, b \rangle, \langle 3, a \rangle, \langle 3, b \rangle\}$.

A special case of a Cartesian product is that of a set with itself. For example, if $A = \{1, 2, 3\}$ as above, then $A \times A = \{\langle 1, 1 \rangle, \langle 1, 2 \rangle, \langle 1, 3 \rangle, \langle 2, 1 \rangle, \langle 2, 2 \rangle, \langle 2, 3 \rangle, \langle 3, 1 \rangle, \langle 3, 2 \rangle, \langle 3, 3 \rangle\}$. The Cartesian product provides us a nice way to define the set of rational numbers. $\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}^+$; that is, $\mathbb{Q}$ is the set of all ordered pairs $\langle \text{integer}, \text{positive integer} \rangle$.

A particularly interesting and useful notion is that of a *relation* on the sets A, B. A relation, R, on A, B is: $R \subseteq A \times B$. The intent with a relation is to model a relationship between items in A and items in B. R is required to be a subset only of $A \times B$; this allows for only some items in A to be related to items in B. For example, suppose $A = \{-1, 0, 1\}, B = \langle 1, 2, 3 \rangle$. Then $R = \{\langle -1, 1 \rangle, \langle 1, 1 \rangle\}$ is a relation, which we may call the "is the square of" relation. That is, $\langle x, y \rangle \in R$ only if $y = x^2$.

Relations play a particularly important role in modern computing. A relational database is an approach to storing information by perceiving the information as comprising relations on sets. Before we discuss relational

databases, we first generalize the notions of ordered pairs and Cartesian products.

An *n-tuple* is an ordered sequence, $\langle x_1, x_2, \ldots, x_n \rangle$, of n items. When the number of items is inferred from context, or does not matter, we refer to such a structure as simply a *tuple*. Two tuples, $\langle x_1, \ldots, x_n \rangle$ and $\langle y_1, \ldots, y_m \rangle$ are said to be equal, or the same, denoted, $\langle x_1, \ldots, x_n \rangle = \langle y_1, \ldots, y_m \rangle$ if two conditions are met: (i) $n = m$, and, (ii) $x_1 = y_1, \ldots, x_n = y_n$. Note that (ii) is the length-n counterpart of Claim 18.

Now, we can define the Cartesian product of n sets, $A_1 \times A_2 \times \ldots \times A_n = \{\langle x_1, \ldots, x_n \rangle \mid x_1 \in A_1, \ldots, x_n \in A_n\}$. And we can then define a relation on $A_1, \ldots, A_n$; $R \subseteq A_1 \times \ldots \times A_n$ is such a relation. Rather than a relationship between items from only two sets, such a relation expresses a relationship between items from the n sets.

A relational database comprises tables. Each such relational table is a relation as we define above. For example, here at the University of Waterloo, the registrar likely maintains a relational database where the tables are a relation $R \subseteq I \times N \times Y$, where I is the set of IDs, N is the set of names, and Y is the set of years of entry. We can now query such tables; for example, we can ask what the ID of a particular student is, given her name, and how many students entered the university in the year 2018.

Another example of the use of relations is a social network, such as Facebook. The "is a Facebook friend of" may be seen as a relation that is a subset of $U \times U$, where U is the set of all users in Facebook. Facebook may impose additional properties on such relations. For example, the "is a Facebook friend of" relation may be *symmetric*: Alice is a Facebook friend of Bob only if Bob is a Facebook friend of Alice. We discuss relations more at the end of this chapter.

Intervals Another notation that is associated with sets is that of intervals. For example, $[-5.3, 4.82]$ represents the set of all real numbers between -5.3 and 4.82, inclusive. There are three kinds of intervals:

- $[a, b]$ where $a, b \in \mathbb{R}$ is called a *closed interval*. It represents the set $\{r \in \mathbb{R} \mid a \leq r \leq b\}$.
- $(a, b]$ and $[a, b)$, where $a, b \in \mathbb{R}$ are called a *half-open intervals*. The

former represents the set $\{r \in \mathbb{R} \mid a < r \leq b\}$, and the latter represents $\{r \in \mathbb{R} \mid a \leq r < b\}$.

- (a, b) where $a, b \in \mathbb{R}$ is called an *open interval*. It represents the set $\{r \in \mathbb{R} \mid a < r < b\}$.

Sometimes, when we want the convenience of the above notation but want to restrict ourselves to subsets of reals, we intersect an interval with a set. For example, we could represent the set of all integers between -10 and 8, which excludes -10, but includes 8, as $(-10, 8] \cap \mathbb{Z}$. Of course, that set is $\{-9, -8, \ldots, -1, 0, 1, \ldots, 8\}$.

Powerset Given a set A, the *powerset* of A is the set of all subsets of A. We denote it as $\mathscr{P}(A)$. For example, if $A = \{1, 2, 3\}$, then $\mathscr{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$. We can establish lots of properties of the powerset; following is an example.

Claim 19. $A \in \mathscr{P}(X) \wedge B \in \mathscr{P}(X) \implies A \cup B \in \mathscr{P}(X)$.

Proof.

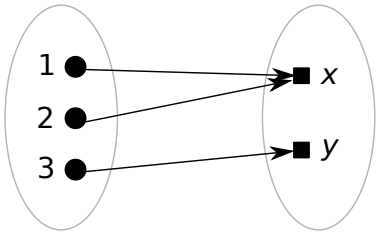
$$
\begin{aligned}
& A \in \mathscr{P}(X) \wedge B \in \mathscr{P}(X) \\
\iff & (A \subseteq X) \wedge (B \subseteq X) \\
\iff & (x \in A \implies x \in X) \wedge (x \in B \implies x \in X) \\
\iff & (x \notin A \vee x \in X) \wedge (x \notin B \vee x \in X) \\
\iff & (x \notin A \wedge x \notin B) \vee (x \in X) \\
\iff & \neg(x \in A \vee x \in B) \vee (x \in X) \\
\iff & (x \in A \vee x \in B) \implies x \in X \\
\iff & (x \in A \cup B) \implies x \in X \\
\iff & A \cup B \subseteq X \iff A \cup B \in \mathscr{P}(X)
\end{aligned}
$$

□

Functions A *function* from a set A to a set B is a relation, $F \subseteq A \times B$ such that every $a \in A$ appears as the first component in exactly one ordered pair in F. For example, given $A = \{1, 2, 3\}, B = \{x, y\}$, the relation $F = \{\langle 1, x\rangle, \langle 2, x\rangle, \langle 3, y\rangle\}$, is a function from A to B.

Apart from this perspective of a function as a particular kind of relation, there are other ways to perceive a function that are meaningful. One is

the perspective that the function is a mapping of each item in A to exactly one item in B. This perspective can be visualized for the above example as follows.



The notion of a function is quite fundamental, and surprisingly powerful. It plays an important role in many aspects of electrical and computer engineering. Many algorithms, for example, compute functions. And algorithmic problems can be expressed as problems of computing functions. As an example, consider the problem of sorting, in non-decreasing order, an array of integers. This can be seen as the problem of mapping an array of integers to its sorted permutation (or rearrangement), and such a mapping is a function, because every such array is associated with a unique sorted permutation.

Functions are often represented using lower-case letters, e.g., f, and to emphasize that f is a function from A to B, we write $f\colon A \to B$. The set A is called f's *domain*, and the set B is called its *codomain*. We write *domain*(f) and *codomain*(f) to refer to the domain and codomain, respectively, of a function f. We observe that the mindset behind such notation is to perceive the mnemonics *domain* and *codomain* as functions. Each maps a function to a set.

If f maps $a \in A$ to $b \in B$, we write this as $f(a) = b$. To specify the manner in which f maps a particular $a \in A$ to $b \in B$, we use "$\mapsto$." For example, a function, f, whose domain and range are the set of integers, and which maps every integers to double that integer is written as:

$$f\colon \mathbb{Z} \to \mathbb{Z}, f : a \mapsto 2a$$

If $f\colon A \to B$ is a function under which $f(a) = b$ for some $a \in A, b \in B$, we call b the *image* of a under f. We call a the *preimage* of b under f. The set of all images is called the *range* of the function; we denote it as *range*(f). That

is, $range(f) = \{b \in codomain(f) \mid \exists a \in domain(f) \text{ such that } f(a) = b\}$. As that specification for the range indicates, $range(f) \subseteq codomain(f)$.

For example, suppose $domain(f) = \{1, 2, 3\}$, $codomain(f) = \{p, q, r, s\}$, and $f(1) = f(3) = p, f(2) = q$, then $range(f) = \{p, q\}$.

If $range(f) = codomain(f)$, then we say that f is *surjective*, *onto* or *a surjection*. If f maps every $a \in domain(f)$ to a unique $b \in codomain(f)$, then we say that f is *injective*, *into*, *an injection* or *one-to-one*. That is, f is injective if, for every $a_1, a_2 \in domain(f)$, it is the true that:

$$f(a_1) = f(a_2) \implies a_1 = a_2$$

If f is injective, then we can define another function, which we call the *inverse* of f, denoted f^{-1}, as follows:

$$f^{-1} \colon range(f) \to domain(f), f^{-1} : f(x) \mapsto x$$

An injective function is also called *invertible* for exactly the reason that its inverse exists and can be defined as above. A special case of an invertible function f is when f is both injective and surjective. In this case f is called a *bijection*. Figure 3.1 shows, pictorially, examples of these kinds of functions.

Injections, surjections and bijections are related to one another, for example, as expressed by the following claims.

Claim 20. *If $f \colon A \to B$ is a bijection, then so is f^{-1}, and $f^{-1^{-1}} = f$.*

Proof. Because f is a surjection, $range(f) = B$. Thus, $f^{-1} \colon B \to A$. From the definition of f^{-1}, f^{-1} is a surjection. To show that f^{-1} is an injection as well, assume otherwise, for the purpose of contradiction. Then, there exist some $b_1, b_2 \in B$ with $b_1 \neq b_2$ such that $f^{-1}(b_1) = f^{-1}(b_2)$. But as $B = range(f)$, there exist $a_1, a_2 \in A$ such that $f(a_1) = b_1, f(a_2) = b_2$. Also, as f is a function, $b_1 \neq b_2 \implies a_1 \neq a_2$.

But, from the definition of f^{-1}, $a_1 = f^{-1}(b_1), a_2 = f^{-1}(b_2)$. Thus, we have a contradiction to the assumption that $f^{-1}(b_1) = f^{-1}(b_2)$. Therefore, f^{-1} is an injection.

To prove that $f^{-1^{-1}} = f$, we need to prove that for all $a \in A$, $f^{-1^{-1}}(a) = f(a)$. Let $g = f^{-1}$. Then, from the definition of f^{-1}:

$$g \colon B \to A, \quad g : f(a) \mapsto a$$

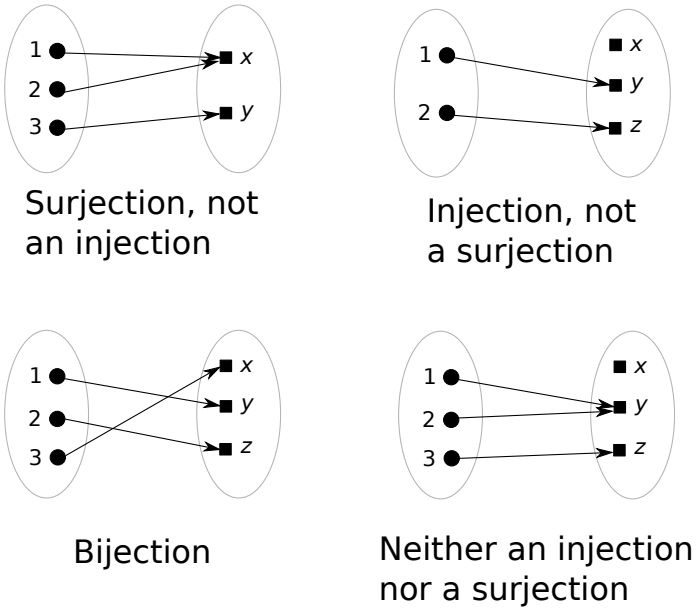


Figure 3.1: Injections, surjections and bijections

Then, $f^{-1^{-1}} = g^{-1}$, where:

$$g^{-1} : A \to B, \quad g^{-1} : g(b) \mapsto b$$

Now suppose $f(a) = b$ for some $a \in A, b \in B$. Then, $f^{-1}(b) = g(b) = a$. And $f^{-1^{-1}}(a) = g^{-1}(a) = b = f(a)$, as desired. □

Claim 21. *Suppose $f : A \to B$ is an injection. Then $f^{-1} : range(f) \to A$ is a bijection.*

Proof. From the definition of *range*(f), f^{-1} is a surjection. To show that f^{-1} is an injection, assume otherwise, for the purpose of contradiction. Then, there exist $b_1, b_2 \in range(f)$ with $b_1 \neq b_2$ such that $f^{-1}(b_1) = f^{-1}(b_2)$. But, from the definition of f^{-1}, $f^{-1}(b_1) = a_1$ for some $a_1 \in A$ such that $f(a_1) = b_1$, and similarly for b_2 and a_2. Thus, $a_1 = a_2$, yet $f(a_1) = b_1 \neq b_2 = f(a_2)$, which contradicts the assumption that f is a function. □

Claim 22. *There exists an injection $f : A \to B$ if and only if there exists a surjection $g : B \to A$.*

Proof. "only if": suppose such an f exists. Then by Claim 21 above, there exists $f^{-1}: \mathit{range}(f) \to A$ which is a bijection. Now pick some $a \in A$ and define g as follows.

$$g\colon B \to A, \quad g\colon b \mapsto \begin{cases} f^{-1}(b) & \text{if } b \in \mathit{range}(f) \\ a & \text{otherwise} \end{cases}$$

Then g is a surjection because $\mathit{range}(f) \subseteq B$.

"if": suppose such a g exists. Then, for every $a \in A$, there exists some $b \in B$ such that $g(b) = a$. Let $G\colon A \to \mathscr{P}(B), \quad G\colon a \mapsto \{b \in B \mid g(b) = a\}$, where $\mathscr{P}(B)$ is the powerset of B. For every $a \in A$, pick some $b \in G(a)$, and denote the choice as b_a. Then, $f\colon A \to B, \ f\colon a \mapsto b_a$ is an injection. $\square$

Cardinality of sets

The *cardinality* of a set intends to capture the notion of the number of members the set contains. We specify it based on the existence of particular kinds of functions from a set to a subset of the set of natural numbers, $\mathbb{N} = \{1, 2, 3, \ldots\}$.

Suppose, for some $n \in \mathbb{N}$, we refer to the subset $\{1, 2, \ldots, n\}$ of $\mathbb{N}$ as $\mathbb{N}_n$. We say that a set $S \neq \emptyset$ is *finite* if there exists some $n \in \mathbb{N}$ for which there exists a bijection $f : S \to \mathbb{N}_n$.

For example, the set $S = \{-3, 0, 1, 3, 4\}$ is finite, because there is a bijection, $f : S \to \mathbb{N}_5$. Such an f may be: $f(-3) = 5, f(0) = 1, f(1) = 3, f(3) = 2, f(4) = 3$.

Claim 23. *If there exists an injection $f : S \to \mathbb{N}_n$ for some $n \in \mathbb{N}, S \neq \emptyset$, then S is finite.*

Proof. We need to prove that there exists a bijection $g : S \to \mathbb{N}_m$, for some $m \in \mathbb{N}$. We do so by construction. Define g as follows.

$$g : s \mapsto \begin{cases} 1 & \text{if } f(s) = \min\limits_{s' \in S}\{f(s')\} \\ g(s') + 1 & \text{otherwise, for } s' \in S \text{ with} \\ & f(s') = \max\limits_{s'' \in S}\{f(s'') \mid f(s'') \in \{1, 2, \ldots, f(s) - 1\}\} \end{cases}$$

We claim that the above g is a bijection from S to N_m, where $m = \max_{s \in S}\{g(s)\}$. We can prove this by, for example, induction on n. □

We say that a set $S \neq \emptyset$ is *infinite* if it is not finite.

Claim 24. $\mathbb{N}$ *is infinite.*

Proof. Assume otherwise, for the purpose of contradiction. Then, there exists some $n \in \mathbb{N}$ such that there is a bijection $f : \mathbb{N} \to \mathbb{N}_n$. Now let $m = \max\limits_{1 \leq i \leq n}\left\{f^{-1}(i)\right\}$. Now, $m \in \mathbb{N} \implies m + 1 \in \mathbb{N}$. Let $f(m+1) = j \in \mathbb{N}_n$. Then, as f is a bijection, $f^{-1}(j) = m + 1 > m$, a contradiction to the assumption that m is the maximum across all $f^{-1}(i)$'s. □

Thus, from the standpoint of the cardinality of a non-empty set, we have two classes: finite and infinite. And we have an example of the former and the latter. From the standpoint of the latter, the following claim should be easy to prove: if S is infinite and $T \supseteq S$, then T is infinite. We have a similar claim from the existence of functions as well: if S is infinite and there exists an injection from S to T, then T is infinite. Thus, starting from $\mathbb{N}$, we can infer that some of the sets we know are infinite, e.g., $\mathbb{Z}, \mathbb{Q}$ and $\mathbb{R}$.

We now further classify within infinite sets. We say that a set $S \neq \emptyset$ is *countably infinite* if there exists a bijection $f : S \to \mathbb{N}$. If $S \neq \emptyset$ is either finite or countably infinite, we say that it is *countable*. If $S \neq \emptyset$ is not countable, we say that it is *uncountable* or *uncountably infinite*.

Claim 25. *For $S \neq \emptyset$, if there exists an injection $f : S \to \mathbb{N}$, then S is countable.*

Proof. Let f be some injection from S to $\mathbb{N}$. Then, we have two cases:

- there exists some $n \in \mathbb{N}$ such that f is an injection from S to $\mathbb{N}_n$. Then, by Claim 23, S is finite and therefore countable.

- no such n exists. Then, we construct a bijection g as in the proof for Claim 23 from S to $\mathbb{N}$. This establishes that S is countably infinite and therefore countable.

□

We now establish that there exist sets that are not countable. We show this by contradiction; the particular proof strategy is called "diagonalization," and is useful in other contexts as well, to show non-existence.

Claim 26. $(0, 1)$*, i.e., the set of reals between* 0 *and* 1*, is uncountable.*

Proof. We assume that every real $r \in (0, 1)$ can be represented in decimal as $0.n_1\, n_2\, n_3\, \ldots$, where each $n_i \in \{0, \ldots, 9\}$. That is, a non-terminating string of digits after the decimal point. Let f be any function $f : \mathbb{N} \to (0, 1)$. Then,

we claim that f cannot be surjective. Thus, no bijection from $(0,1)$ to $\mathbb{N}$ can exist, and therefore $(0,1)$ is uncountable.

To show that f is not a surjection, consider how f maps each of $1, 2, \ldots$ to some member of $(0,1)$.

$$\begin{aligned} f(1) &= 0.n_{1,1}\, n_{1,2}\, n_{1,3} \ldots \\ f(2) &= 0.n_{2,1}\, n_{2,2}\, n_{2,3} \ldots \\ &\ldots \\ f(i) &= 0.n_{i,1}\, n_{i,2} \ldots n_{i,i} \ldots \\ &\ldots \end{aligned}$$

Where each $n_{i,j} \in \{0, \ldots, 9\}$. Now, we specify a new $r \in (0,1)$ as follows. $r = 0.n_1\, n_2\, \ldots$ where:

$$n_i = \begin{cases} 1 & \text{if } n_{i,i} > 5 \\ 7 & \text{otherwise} \end{cases}$$

We claim there exists exists no $j \in \mathbb{N}$ such that $f(j) = r$. Specifically, for every $j \in \mathbb{N}$, $n_{j,j} \neq n_j$. Therefore, $f(j) \neq r$. □

As $(0,1)$ is uncountable, so are all of its supersets. Specifically, $\mathbb{R}$ is uncountable. Note that the proposition, "$((S \text{ is uncountable }) \wedge (T \supseteq S)) \implies (T \text{ is uncountable})$" is subject to proof, but the proof should be easy to carry out.

Some countably infinite sets We now establish that some sets with which we are familiar are indeed countable, perhaps counterintuitively.

Claim 27. $\mathbb{Z}_0^+ = \{0, 1, 2, \ldots\}$ *is countable.*

Proof. Let f be the following function.

$$f : \mathbb{Z}_0^+ \to \mathbb{N}, \quad f : z \mapsto z + 1$$

Then f is a bijection that establishes that $\mathbb{Z}_0^+$ is countable. □

Claim 28. $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, \ldots\}$ *is countable.*

Proof. Let $f : \mathbb{Z} \to \mathbb{N}$ be as follows.

$$f(i) = \begin{cases} 2|i| + 1 & \text{if } i \leq 0, \text{where } |\cdot| \text{ is absolute value} \\ 2i & \text{otherwise} \end{cases}$$

We claim that f above is a bijection. Given any $i, j \in \mathbb{Z}$, with $i \neq j$, we have the following three cases. (i) Both $i, j \leq 0$. Then, $f(i) = -2i + 1 \neq -2j + 1 = f(j)$. (ii) Both $i, j > 0$. Then, $f(i) = 2i \neq 2j = f(j)$. (iii) $i \leq 0, j > 0$. Then, $f(i)$ is odd and $f(j)$ is even, and therefore $f(i) \neq f(j)$.

Thus, f is an injection. To show that f is a surjection, suppose $i \in \mathbb{N}$. Then, we have two cases. (i) i is even. Then $i = f(i/2)$. (ii) i is odd. Then, $i = f((1 - i)/2)$. Thus, f is surjective. □

Claim 29. $\mathbb{N} \times \mathbb{N}$ *is countable.*

Proof. A natural way to prove the claim is by construction; i.e., we devise a bijection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$. We can do this in many ways. Following is a strategy. We group pairs, $\langle i, j \rangle \in \mathbb{N} \times \mathbb{N}$, systematically, and then map each pair to a natural number. The following table suggests such a grouping and mapping to natural numbers.

Group #	*Pair(s)*	*# pairs*	*Map to*
1	$\langle 1, 1 \rangle$	1	1
2	$\langle 1, 2 \rangle, \langle 2, 2 \rangle, \langle 2, 1 \rangle$	3	$2, 3, 4$
3	$\langle 1, 3 \rangle, \langle 2, 3 \rangle, \langle 3, 3 \rangle$ $\langle 3, 1 \rangle, \langle 3, 2 \rangle$	5	$5, \ldots, 9$
4	$\langle 1, 4 \rangle, \ldots, \langle 3, 4 \rangle, \langle 4, 4 \rangle$ $\langle 4, 1 \rangle, \ldots, \langle 4, 3 \rangle$	7	$10, \ldots, 16$
...	...	...	...
k	$\langle 1, k \rangle, \ldots, \langle k - 1, k \rangle, \langle k, k \rangle$ $\langle k, 1 \rangle, \ldots, \langle k, k - 1 \rangle$	$2k - 1$	$(k - 1)^2 + 1, \ldots, k^2$
...	...	...	...

Based on the above table, consider the following function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$:

$$f(i, j) = \begin{cases} (j - 1)^2 + i & \text{if } i \leq j \\ (i - 1)^2 + i + j & \text{otherwise} \end{cases}$$

We now need to prove that f is indeed a bijection. We first observe that $(\max\{a, b\} - 1)^2 + 1 \leq f(a, b) \leq (\max\{a, b\})^2$. We can prove this by a case

analysis.

Case 1: $a \leq b$. In this case, $\max\{a, b\} = b$, and $f(a, b) = (b-1)^2 + a$. And $f(a, b) \geq (b-1)^2 + 1$ because $a \geq 1$. And $f(a, b) \leq b^2$ because $f(a, b) = b^2 - 2b + 1 + a = b^2 - (b-1) - (b-a) \leq b^2$ because $b \geq 1$ and $b \geq a$.

Case 2: $a > b$. In this case, $\max\{a, b\} = a$, and $f(a, b) = (a-1)^2 + a + b$. And $f(a, b) \geq (a-1)^2 + 1$ because $a + b \geq 1$. And $f(a, b) \leq a^2$ because $f(a, b) = a^2 - 2a + 1 + a + b = a^2 - a + 1 + b = a^2 - (a - (b+1)) \leq a^2$ because $a > b \implies a \geq b + 1$.

Now, to prove that f is injective, assume $\langle a, b\rangle \neq \langle c, d\rangle$, for $a, b, c, d \in \mathbb{N}$. We seek to prove that $f(a, b) \neq f(c, d)$. We consider two cases.

Case 1: $\max\{a, b\} \neq \max\{c, d\}$. Let $\max\{a, b\} = p, \max\{c, d\} = q$. Then, $f(a, b) \in \{(p-1)^2 + 1, \ldots, p^2\}, f(c, d) \in \{(q-1)^2 + 1, \ldots, q^2\}$, in which case $f(a, b) \neq f(c, d)$, because

$$p \neq q \implies \left\{(p-1)^2 + 1, \ldots, p^2\right\} \cap \left\{(q-1)^2 + 1, \ldots, q^2\right\} = \emptyset$$

Case 2: $\max\{a, b\} = \max\{c, d\}$. We consider two subcases.

- Case (a): $a \leq b$. Then, $\max\{a, b\} = b$ and $f(a, b) = (b-1)^2 + a$. We consider two subcases.
  - Case (i): $c > d$. Then, $\max\{c, d\} = c$, $c = b$ and $f(c, d) = (b-1)^2 + b + d$. And $f(a, b) = f(c, d) \implies (b-1)^2 + a = (b-1)^2 + b + d \implies a = b + d$. This is impossible because $a \leq b$ and $d \geq 1$, and therefore, $a < b + d$.
  - Case (ii): $c \leq d$. Then, $\max\{c, d\} = d$, $d = b$ and $f(c, d) = (b-1)^2 + c$. And $f(a, b) = f(c, d) \implies (b-1)^2 + a = (b-1)^2 + c \implies a = c$, which contradicts the assumption that $\langle a, b\rangle \neq \langle c, d\rangle$.
- Case (b): $a > b$. Then, $\max\{a, b\} = a$ and $f(a, b) = (a-1)^2 + a + b$. We consider two subcases.
  - Case (i): $c > d$. Then, $\max\{c, d\} = c$, $c = a$ and $f(c, d) = (a-1)^2 + a + d$. And $f(a, b) = f(c, d) \implies b = d$. This contradicts the assumption that $\langle a, b\rangle \neq \langle c, d\rangle$.

– Case (ii): $c \leq d$. Then, $\max\{c, d\} = d$, $d = a$ and $f(c, d) = (a-1)^2 + c$. And $f(a, b) = f(c, d) \implies (a-1)^2 + a + b = (a-1)^2 + c \implies a + b = c$, which is impossible because $c \leq a = d$ and $b \geq 1$.

Thus, f is injective. To prove that f is surjective, pick some $n \in \mathbb{N}$. We seek to show that there exists some $\langle a, b\rangle \in \mathbb{N} \times \mathbb{N}$ such that $f(a, b) = n$.

For every $n \in \mathbb{N}$, there exists $m \in \mathbb{N}$ such that $n \in \{(m-1)^2 + 1, \ldots, m^2\}$. Thus, $n = (m-1)^2 + p$, for some $p \in \{1, \ldots, 2m-1\}$. We observe that if $p \leq m$, then from the definition of f, $n = f(p, m)$, and if $m < p \leq 2m - 1$, then $n = f(m, p - m)$. Thus, f is surjective. □

Claim 30. $\mathbb{Q}$ *is countable.*

Proof. Recall that $\mathbb{Q} = \{\langle n, m\rangle \in \mathbb{Z} \times \mathbb{Z}^+\}$. We can compose the bijection from $\mathbb{Z}$ to $\mathbb{N}$ that is used to establish that $\mathbb{Z}$ is countable with the bijection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$ to establish that $\mathbb{N} \times \mathbb{N}$ is countable to establish that $\mathbb{Z} \times \mathbb{Z}$ is countable. Now, as $\mathbb{Q} \subseteq \mathbb{Z} \times \mathbb{Z}$, $\mathbb{Q}$ is countable as well. □

Returning to set-cardinality and associated notation, given a set S, its cardinality is denoted $|S|$. We have distinguished: the empty set, finite sets, countably infinite sets and uncountable sets.

- $|\emptyset| = 0$, i.e., the cardinality of the empty set is 0.
- If S is not empty, and is countable, let $n \in \mathbb{N}$ for which there exists a bijection $f : S \to \mathbb{N}_n$. Then, $|S| = n$.
- We denote $|\mathbb{N}| = \aleph_0$, which is read "aleph zero." That is, we introduce a special symbol to represent the cardinality of $\mathbb{N}$. Note that this implies, for example, that $|\mathbb{Q}| = |\mathbb{Z}| = \aleph_0$.

We can also compare cardinalities. Recall that the empty set is unique. That is, if sets A and B are both the empty set, then $A = B$. For non-empty sets A, B, we say that $|A| = |B|$ if and only if there exists a bijection $f : A \to B$. If there exists an injection $g : A \to B$ then, we say that $|A| \leq |B|$. And if there exists an injection $h : A \to B$, but no surjection, then $|A| < |B|$. So, for example, if A is finite, then $|A| < \aleph_0 < |\mathbb{R}|$. The symbols "$\geq$" and "$>$" can be defined as analogues of "$\leq$" and "$<$," respectively.

Relations

We now revisit relations. Recall that a relation between sets $A_1, A_2, \ldots, A_n$ is a subset of $A_1 \times A_2 \times \ldots \times A_n$. A special case is $n = 2$, i.e., a relation between two sets. Another special case is when all the sets $A_1, \ldots, A_n$ are the same. The notion of a relation naturally captures what we think of as relationships.

In our discussions in this portion of the book, we restrict ourselves to *binary relations*, i.e., subsets of $A \times B$. So when we simply say "relation," we mean a binary relation. In particular, we focus on the case that $A = B$, i.e., relations of the form $R \subseteq A \times A$ for some set A. We often write $A \times A$ as A^2, and call a relation $R \subseteq A^2$ a "relation on the set A."

For example, suppose we have a set of people, $P = \{\text{Alice}, \text{Bob}, \text{Carol}, \text{Dave}, \text{Eve}\}$. We may now specify a relation, ParentOf $\subseteq P \times P$, where ParentOf $= \{\langle \text{Alice}, \text{Bob}\rangle, \langle \text{Alice}, \text{Carol}\rangle, \langle \text{Bob}, \text{Dave}\rangle, \langle \text{Eve}, \text{Carol}\rangle\}$. Presumably what we seek to express via the set of ordered pairs ParentOf is that Alice is a parent of both Bob and Carol, Bob is a parent of Dave and Eve is a parent of Carol.

We use the above example to make several observations about relations in general.

- A relation may or may not be a strict subset of the cartesian product of the underlying sets. In our example above, $|P \times P| = 25$, and $|\text{ParentOf}| = 4$.

- A relation may or may not be a function. The relation ParentOf is not a function. We observe that Alice maps to both Bob and Carol.

- A relation may or may not be *symmetric*. A symmetric relation, $R \subseteq A^2$ is one which satisfies the following property:

$$\forall \langle x, y\rangle \in A^2,\ \langle x, y\rangle \in R \iff \langle y, x\rangle \in R$$

  We observe that $\langle \text{Alice}, \text{Bob}\rangle \in \text{ParentOf}$, but $\langle \text{Bob}, \text{Alice}\rangle \notin \text{ParentOf}$. Indeed, ParentOf above is *asymmetric*. A relation $R \subseteq A^2$ is said to be asymmetric if:

$$\forall \langle x, y\rangle \in A^2,\ \langle x, y\rangle \in R \implies \langle y, x\rangle \notin R$$

An immediate question that arises is whether R is symmetric if and only if R is not asymmetric, i.e., whether the notion of symmetric is the complement of the notion of asymmetric. We can deploy our understanding of logic to intuit this.

Based on the definition of symmetry above, $R \subseteq A^2$ is not symmetric if:

$$\begin{aligned}
&\neg\big(\forall\langle x,y\rangle \in A^2,\ \langle x,y\rangle \in R \iff \langle y,x\rangle \in R\big)\\
\iff &\exists\langle x,y\rangle \in A^2,\ \neg(\langle x,y\rangle \in R \iff \langle y,x\rangle \in R)\\
\iff &\exists\langle x,y\rangle \in A^2,\ \neg((\langle x,y\rangle \notin R \vee \langle y,x\rangle \in R) \wedge (\langle y,x\rangle \notin R \vee \langle x,y\rangle \in R))\\
\iff &\exists\langle x,y\rangle \in A^2,\ ((\langle x,y\rangle \in R \wedge \langle y,x\rangle \notin R) \vee (\langle y,x\rangle \in R \wedge \langle x,y\rangle \notin R))
\end{aligned}$$

That is, for R to not be symmetric, all we need is a pair $\langle x,y\rangle \in R$ such that $\langle y,x\rangle \notin R$. Whereas asymmetric requires this for every pair $\langle x,y\rangle \in R$. So, for example, consider $R \subseteq \{1,2,3\}^2$ where $R = \{\langle 1,2\rangle, \langle 2,1\rangle, \langle 1,3\rangle\}$. Then R is not symmetric because $\langle 1,3\rangle \in R$, yet $\langle 3,1\rangle \notin R$. R is also not asymmetric because both $\langle 1,2\rangle, \langle 2,1\rangle \in R$.

There is another notion that is in customary use in this context; the notion of *antisymmetry*. A relation $R \subseteq A^2$ is said to be antisymmetric if:

$$\forall\langle x,y\rangle \in A^2,\ \langle x,y\rangle \in R \wedge \langle y,x\rangle \in R \implies x = y$$

Unlike a relation that is symmetric, an antisymmetric relation cannot contain both $\langle x,y\rangle$ and $\langle y,x\rangle$ when $x \neq y$. Unlike a relation that is asymmetric, an antisymmetric relation does not preclude both $\langle x,y\rangle$ and $\langle y,x\rangle$ from being in the relation.

The ParentOf relation above is antisymmetric: for distinct $\langle x,y\rangle$, it is never the case that both $\langle x,y\rangle$ and $\langle y,x\rangle$ are in ParentOf. Thus, the premise in the implication in the definition of antisymmetry is always false for ParentOf, and therefore the implication holds true.

The relation R over $\{1,2,3\}$ above, on the other hand, is not antisymmetric: both $\langle 1,2\rangle$ and $\langle 2,1\rangle$ are in R, yet $1 \neq 2$. Thus, this R is

an example of a relation that is neither symmetric nor antisymmetric. There can also exist relations that are both symmetric and antisymmetric. Consider, for example, $S \subseteq \{1,2,3\}^2$, where $S = \{\langle 1,1\rangle, \langle 3,3\rangle\}$. Then, S is both symmetric and antisymmetric.

What about asymmetry and antisymmetry? We observe that if a relation R over A is asymmetric, then R is antisymmetric, but the converse is not necessarily true. We state a claim for an "if and only if" relationship between asymmetry and antisymmetry once we discuss notions of reflexivity below.

- A relation, $R \subseteq A^2$, may be *reflexive*. We say that such an R is reflexive if:

$$\forall x \in A,\ \langle x, x\rangle \in R$$

We can also define *irreflexivity*; we say that $R \subseteq A^2$ is irreflexive if:

$$\forall x \in A,\ \langle x, x\rangle \notin R$$

It should not be difficult to see that some relation $R \subseteq A^2$ may be neither reflexive nor irreflexive. E.g., $R \subseteq \{1,2\}^2$ where $R = \{\langle 1,1\rangle\}$ is neither reflexive nor irreflexive. This R is not reflexive because $2 \in A$ and yet $\langle 2,2\rangle \notin R$, and it is not irreflexive because $\langle 1,1\rangle \in R$.

Is it possible that a relation R on a set A is both reflexive and irreflexive? This is not possible if $A \neq \emptyset$. However, if $A = \emptyset, R = \emptyset$, then R is both reflexive and irreflexive.

The notion of reflexivity also helps us clarify the distinction between asymmetry and antisymmetry.

Claim 31. *Suppose $R \subseteq A^2$. Then R is asymmetric if and only if R is antisymmetric and irreflexive.*

Proof. "$\Longrightarrow$": we prove the contrapositive. We have two cases:

1. R is not antisymmetric.

$$
\begin{aligned}
&R \text{ is not antisymmetric} \\
&\iff \neg\big(\forall\langle x,y\rangle \in A^2,\ \langle x,y\rangle \in R \wedge \langle y,x\rangle \in R \implies x = y\big) \\
&\iff \exists\langle x,y\rangle \in A^2,\ \neg(\langle x,y\rangle \in R \wedge \langle y,x\rangle \in R \implies x = y) \\
&\iff \exists\langle x,y\rangle \in A^2,\ \neg(\langle x,y\rangle \notin R \vee \langle y,x\rangle \notin R \vee x = y) \\
&\iff \exists\langle x,y\rangle \in A^2,\ \langle x,y\rangle \in R \wedge \langle y,x\rangle \in R \wedge x \neq y \\
&\implies \exists\langle x,y\rangle \in A^2,\ \langle x,y\rangle \in R \wedge \langle y,x\rangle \in R \\
&\iff \exists\langle x,y\rangle \in A^2,\ \neg(\langle x,y\rangle \notin R \vee \langle y,x\rangle \notin R) \\
&\iff \exists\langle x,y\rangle \in A^2,\ \neg(\langle x,y\rangle \in R \implies \langle y,x\rangle \notin R) \\
&\iff \neg\big(\forall\langle x,y\rangle \in A^2,\ \langle x,y\rangle \in R \implies \langle y,x\rangle \notin R\big) \\
&\iff R \text{ is not asymmetric}
\end{aligned}
$$

2. R is not irreflexive.

$$
\begin{aligned}
&R \text{ is not irreflexive} \\
&\iff \neg(\forall x \in A,\ \langle x,x\rangle \notin R) \\
&\iff \exists x \in A,\ \langle x,x\rangle \in R \\
&\iff \exists\langle x,y\rangle \in A^2,\ x = y \wedge \langle x,y\rangle \in R \wedge \langle y,x\rangle \in R \\
&\implies \exists\langle x,y\rangle \in A^2,\ \langle x,y\rangle \in R \wedge \langle y,x\rangle \in R \\
&\iff \exists\langle x,y\rangle \in A^2,\ \neg(\langle x,y\rangle \notin R \vee \langle y,x\rangle \notin R) \\
&\iff \exists\langle x,y\rangle \in A^2,\ \neg(\langle x,y\rangle \in R \implies \langle y,x\rangle \notin R) \\
&\iff \neg\big(\forall\langle x,y\rangle \in A^2,\ \langle x,y\rangle \in R \implies \langle y,x\rangle \notin R\big) \\
&\iff R \text{ is not asymmetric}
\end{aligned}
$$

"$\Longleftarrow$": we assume that R is antisymmetric and irreflexive.

$$
\begin{aligned}
&R \text{ antisymmetric } \wedge R \text{ irreflexive} \\
&\iff \big(\forall\langle x,y\rangle \in A^2,\ \langle x,y\rangle \in R \wedge \langle y,x\rangle \in R \implies x = y\big) \wedge \\
&\qquad \big(\forall\langle x,y\rangle \in A^2,\ x = y \implies \langle x,y\rangle \notin R\big) \\
&\implies \forall\langle x,y\rangle \in A^2,\ \langle x,y\rangle \in R \wedge \langle y,x\rangle \in R \implies \langle x,y\rangle \notin R \\
&\iff \forall\langle x,y\rangle \in A^2,\ \langle x,y\rangle \notin R \vee \langle y,x\rangle \notin R \vee \langle x,y\rangle \notin R \\
&\iff \forall\langle x,y\rangle \in A^2,\ \langle x,y\rangle \notin R \vee \langle y,x\rangle \notin R \\
&\iff \forall\langle x,y\rangle \in A^2,\ \langle x,y\rangle \in R \implies \langle y,x\rangle \notin R \\
&\iff R \text{ is asymmetric}
\end{aligned}
$$

□

- A relation $R \subseteq A^2$ may be *transitive*. We say that $R \subseteq A^2$ is transitive if:

$$\forall \langle x, y, z \rangle \in A^3, \langle x, y \rangle \in R \wedge \langle y, z \rangle \in R \implies \langle x, z \rangle \in R$$

  For example, the ParentOf relation above is not transitive, because $\langle \text{Alice}, \text{Bob} \rangle \in \text{ParentOf}$, and $\langle \text{Bob}, \text{Dave} \rangle \in \text{ParentOf}$, but $\langle \text{Alice}, \text{Dave} \rangle \notin \text{ParentOf}$. Similarly, the $R \subseteq \{1, 2, 3\}^2$ we specified above, where $R = \{\langle 1, 2 \rangle, \langle 2, 1 \rangle, \langle 1, 3 \rangle\}$ is not transitive, because $\langle 1, 2 \rangle, \langle 2, 1 \rangle \in R$, but $\langle 1, 1 \rangle \notin R$. However, the following relation $S \subseteq \{1, 2, 3\}^2$ where $S = \{\langle 1, 2 \rangle, \langle 1, 3 \rangle\}$, is transitive.

Now that we have discussed types of relations, we discuss situations that they show up. Comparison operators between, for example, integers, are a good example of where such relations such up. The comparator, "$\leq$," for example, can be seen as a relation between two integers, i.e., $\subseteq \mathbb{Z}^2$. Denote the relation induced by "$\leq$" between integers as the relation $R_{\mathbb{Z},\leq}$. That is:

$$R_{\mathbb{Z},\leq} = \left\{ \langle x, y \rangle \in \mathbb{Z}^2 \mid x \leq y \right\}$$

We observe that $R_{\mathbb{Z},\leq}$ is:

- Reflexive: because $\forall x \in \mathbb{Z}, x \leq x$ and therefore $\forall x \in \mathbb{Z}, \langle x, x \rangle \in R_{\mathbb{Z},\leq}$.
- Antisymmetric: because $\forall \langle x, y \rangle \in \mathbb{Z}^2, x \leq y \wedge y \leq x \implies x = y$.
- Transitive: because $\forall \langle x, y, z \rangle \in \mathbb{Z}^3, x \leq y \wedge y \leq z \implies x \leq z$.

There is a special name for a set and an operator that induce a relation that is reflexive, antisymmetric and transitive, like $\mathbb{Z}$ and $\leq$ above. And that is a *partial order*, a *partially ordered set* or a *poset*. We usually denote a poset as a pair of the set and the operator, e.g., we would say, "$\langle \mathbb{Z}, \leq \rangle$ is a poset."

The reason we call out posets specially is that they show up in various contexts, and we are able to establish additional properties about them. Another example of a poset is $\langle S, \subseteq \rangle$, where S is a set.

As a contrast, consider the relation that is induced on $\mathbb{Z}$ by "$<$." That is, consider the relation $R_{\mathbb{Z},<}$:

$$R_{\mathbb{Z},<} = \left\{ \langle x, y \rangle \in \mathbb{Z}^2 \mid x < y \right\}$$

We observe that $R_{\mathbb{Z},<}$ is:

- Irreflexive: because $\forall x \in \mathbb{Z}, x \not< x$.
- Asymmetric: because $\forall \langle x, y \rangle \in \mathbb{Z}^2, x < y \implies y \not< x$.
- Transitive: because $\forall \langle x, y, z \rangle \in \mathbb{Z}^3, x \leq y \wedge y \leq z \implies x \leq z$.

A relation that is irreflexive, asymmetric and transitive is called a *strict partial order*. Another example of a strict partial order is the relation induced by "$\subset$" on a set S.

Also interesting is a relation that is reflexive, symmetric and transitive. Such a relation is called an *equivalence*, and as its name suggests such a relation induces a kind of equality that is less strict than actual equality, but is useful in many contexts.

As an example, consider the relation between integers that is induced by the modulo operator, "mod," which is defined as follows.

$$\text{For } x \in \mathbb{Z}, y \in \mathbb{Z}^+,\ x \bmod y = r, \text{ where } r \in \{0, 1, \ldots, y-1\} \text{ such that } \exists q \in \mathbb{Z}, x = q \cdot y + r$$

For example, $29 \bmod 8 = 5$ and $-29 \bmod 8 = 4$.

Consider the relation induced on $\mathbb{Z}$ by "mod 4." That is, let $R_{\mathbb{Z},\, \text{mod } 4}$ be:

$$R_{\mathbb{Z},\, \text{mod } 4} = \left\{ \langle x, y \rangle \in \mathbb{Z}^2 \mid x \bmod 4 = y \bmod 4 \right\}$$

We observe that $R_{\mathbb{Z},\, \text{mod } 4}$ is:

- Reflexive: $\forall x \in \mathbb{Z}, x \bmod 4 = x \bmod 4$.
- Symmetric: $\forall \langle x, y \rangle \in \mathbb{Z}^2, x \bmod 4 = y \bmod 4 \implies y \bmod 4 = x \bmod 4$.
- Transitive: $\forall \langle x, y, z \rangle \in \mathbb{Z}^3, x \bmod 4 = y \bmod 4 \wedge y \bmod 4 = z \bmod 4 \implies x \bmod 4 = z \bmod 4$.

So $R_{\mathbb{Z},\,\mathrm{mod}\,4}$ is an equivalence, and what that conveys is that under mod 4, all integers that have the same value modulo 4 are not necessarily the same, but "equivalent" in this specific context.

Such an equivalence relation induces so called *equivalence classes* on the underlying set. For example, under " mod 4," the integers in $\{\ldots, -7, -3, 1, 5, 9, \ldots\}$ are equivalent to one another, in that they are all the same modulo 4. We use the following symbol to indicate equivalent: "$\equiv_{\mathrm{mod}\,4}$," e.g. we would write "$-7 \equiv_{\mathrm{mod}\,4} 5$ to indicate that -7 is equivalent to 5 under the "mod 4" relation. Such a set, i.e., $\{\ldots, -7, -3, 1, 5, 9, \ldots\}$ in this example, is called an equivalence class.

We observe that "mod 4" induces four equivalence classes on $\mathbb{Z}$:

$$\{\ldots, -8, -4, 0, 4, 8, \ldots\}$$
$$\{\ldots, -7, -3, 1, 5, 9, \ldots\}$$
$$\{\ldots, -6, -2, 2, 6, 10, \ldots\}$$
$$\{\ldots, -5, -1, 3, 7, 11, \ldots\}$$

As the members of each such class are equivalent to one another, we can simply pick a representative of each class to represent the entire class. From the standpoint of notation, we write this as $[0]_{\mathrm{mod}\,4}$, to refer to the set that is the equivalence class to which 0 belongs under "mod 4." That is, $[0]_{\mathrm{mod}\,4} = \{\ldots, -4, 0, 4, 8, \ldots\}$.

We observe that $[0]_{\mathrm{mod}\,4} = [116]_{\mathrm{mod}\,4}$, and $[0]_{\mathrm{mod}\,4} \neq [6]_{\mathrm{mod}\,4}$. In fact, given an equivalence $R \subseteq A^2$, suppose $[x_0]_R, [x_1]_R, \ldots, [x_n]_R$ are the equivalence classes induced by R. Then:

- The equivalence classes are pairwise disjoint. That is, for every i, j with $i \neq j$, $[x_i]_R \cap [x_j]_R = \emptyset$, and,
- The union of the equivalence classes is the set A, i.e., $\bigcup_{1 \leq i \leq n} [x_i]_R = A$.

That is, the equivalence classes *partition* the underlying set A.

As another example, for the set of all students that are currently enrolled in Waterloo-ECE, the year + term + cohort can be seen as an equivalence

relation. That is, Alice and Bob are in the same equivalence class if and only if they are in the same year, term and cohort. The class reps are representatives of each such equivalence class, and there is nothing special about them in the sense that they are perceived as members of the equivalence class, and any member of an equivalence class is a valid representative. The union of all equivalence classes is the set of all students in Waterloo-ECE.

As another example, consider the following way of modeling trust and a group of acquaintances.

- Everyone trusts him/herself, i.e., we assume trust is reflexive, and,
- If a trust b and b trusts c, then a trusts c, i.e., we assume trust is transitive.
- We have a set of acquaintances: A(lice), B(ob), C(arol), D(ave), E(dith) and F(rank). And it turns out:
  - A trusts B, C, D.
  - B trusts A, C, F.
  - C trusts A, B.
  - D trusts E.
  - E trusts D.

Let $T \subseteq \{A, \ldots, F\}^2$ be the above trust relation. Then, T is not an equivalence: for example, $\langle B, F\rangle \in T$, but $\langle F, B\rangle \notin T$, that is, T is not symmetric. Also, $\langle A, T\rangle$ is not a poset: for example, $\langle A, B\rangle \in T, \langle B, A\rangle \in T$, yet $A \neq B$, that is, T is not antisymmetric.

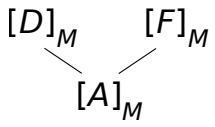
However, consider the following subset of T, $M \subseteq T$, which we can think of as "mutually trusting." $M = \{\langle x, y\rangle \in T \mid \langle y, x\rangle \in T\}$. Then, M is an equivalence, and it induces three equivalence classes: (i) $A \equiv_M B \equiv_M C$, i.e., $[A]_M = [B]_M = [C]_M = \{A, B, C\}$, (ii) $D \equiv_M E$, i.e., $[D]_M = [E]_M = \{D, E\}$, and, (iii) F, i.e., $[F]_M = \{F\}$.

Now suppose we define a relation between those equivalence classes, $C = \big\{\langle [x], [y]\rangle \in \{[A]_M, [D]_M, [F]_M\}^2 \mid \langle x, y\rangle \in T\big\}$.

For example, $\langle [A]_M, [A]_M\rangle \in C$ because $\langle A, A\rangle \in T$, because T is reflexive.

And $\langle [A]_M, [D]_M \rangle \in C$, because $\langle A, D \rangle \in T$. But, $\langle [D]_M, [A]_M \rangle \notin C$, because $\langle D, A \rangle \notin T$.

Now, $\langle \{[A]_M, [D]_M, [F]_M\}, C \rangle$ is a poset. That is, C is reflexive, transitive and antisymmetric. And it is meaningful to visualize the poset as follows.



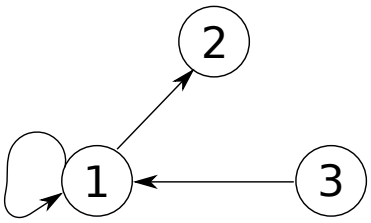
In the picture above, an edge "—" indicates unidirectional trust from an entity that is on the lower side of the edge to the upper side. For example, the edge from $[A]_M$ to $[D]_M$ indicates that everyone in the equivalence class $[A]_M$ trusts someone in the equivalence class $[D]_M$.

Thus the picture above indicates that the folks in the equivalence class $[A]_M$ are the most trusting from amongst $\{A, \ldots, F\}$. The equivalence classes $[D]_M$ and $[F]_M$ are incomparable to one another; indeed, the lack of an edge between them expresses that they are "islands" of trust, isolated from one another.

Another good example of the use of relations is in the context of social networks. Facebook, for example, employs a relation, "FriendOf." A semantics of FriendOf is that if $\langle \text{Alice}, \text{Bob} \rangle \in \text{FriendOf}$, then Alice can, for example, view photos that Bob posts. FriendOf is reflexive, in that Alice can view her own photos. It is also symmetric. However, it is not necessarily transitive. Facebook of course has other relations it employs as well. For example, it is possible for a user to "tag" another user in a photo. And "IsTagged" can be viewed as a relation between users that has particular semantics, e.g., with regards to whether a user can view particular photos.

Graphs Graphs provide a useful way to visualize and process (e.g., via algorithms) relations. A *graph* is an ordered pair, $\langle V, E \rangle$, where each of V, E is a set. The set V is called a set of *vertices* or *nodes*. The set E is called a set of *edges*. The set V is a set of identifiers, e.g., $V = \{1, 2, 3\}$. The set E is a relation on V, i.e., $E \subseteq V^2$. E.g., $E = \{\langle 1, 1 \rangle, \langle 1, 2 \rangle, \langle 3, 1 \rangle\}$. This example

graph can be visualized as follows.

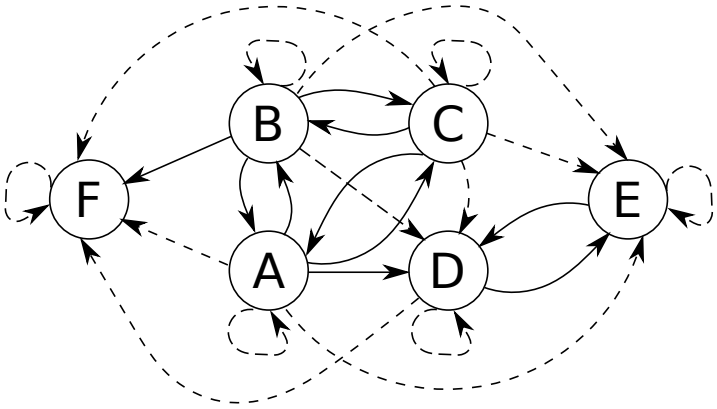


As the picture indicates, we typically draw a vertex as a labelled circle, and an edge as a line segment with an arrowhead that indicates the ordering within the ordered pair.

Depending on the semantics of the relation, E, we can now ask questions that may be meaningful in the particular context. For example, suppose in the above example, the vertices $1, 2, 3$ represent cities, and an edge $\langle x, y \rangle$ represents the fact that a transportation company is willing to deliver goods from x to y. Then, we observe that the *transitive closure* of the above graph, i.e., the minimum set of edges we would add to the graph so the relation is then transitive, tells us between which cities we can employ the transportation company provided we have a way to cache the goods in an intermediate city. For example, the transitive closure would include the edge $\langle 3, 2 \rangle$, but not the edge $\langle 2, 3 \rangle$.

As another example, following is a graph, call it $G = \langle V, E \rangle$, that expresses the trust relationships between $V = \{A, \ldots, F\}$ that we discussed above. We distinguish two kinds of edges: the solid edges are the "explicit" trust relationships – those that we mention under the third bullet above, in our specification of the trust relationships. The dotted edges are from our assumption that the relation is also reflexive and transitive; that is, the dotted edges result from computing the *reflexive closure* and the transitive closure

of the explicit trust relationships.



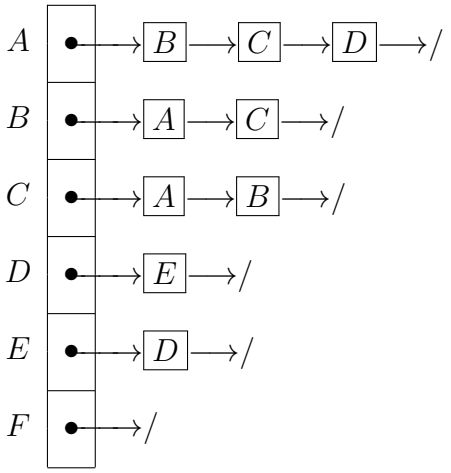
Now, we observe that sets of vertices that are *strongly connected* comprise an equivalence class in M, "mutually trust," that we discuss above. Two vertices, u, v are said to be strongly connected to one another if there is a path from u to v, and from v to u. We observe, for example, that this is indeed the case between the vertices in $\{A, B, C\}$. And if there is a dotted or solid edge $\langle u, v\rangle$, but no edge $\langle v, u\rangle$, then every vertex in $[u]_M$ has an edge to at least one vertex in $[v]_M$, but not vice versa.

From the standpoint of implementation, there are two customary ways to implement a graph. One is as an *adjacency matrix*, and the other is as an *adjacency list*. An adjacency matrix, call it J, is $|V| \times |V|$, i.e., has $|V|$ rows and $|V|$ columns, with one row and one column for every $u \in V$. An entry $J[u, v] = 1$ if $\langle u, v\rangle \in E$, otherwise $J[u, v] = 0$. Thus, an adjacency matrix of the above graph of the solid edges only is the following.

$$\begin{array}{c} \\ A \\ B \\ C \\ D \\ E \\ F \end{array} \begin{array}{c} \begin{array}{cccccc} A & B & C & D & E & F \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

An adjacency list, call it L, is an array of size $|V|$ for each $u \in V$, in which

the entry u is a linked list. An adjacency list for the above graph, for the solid edges only is the following.



Chapter 4

Combinatorics

This chapter addresses *combinatorics*, ways in which items can be chosen from a set. We will deal with finite sets only. We begin with some examples, which illustrate the different kinds of problems we deal with.

Example 1. *A committee comprises a chairperson, an outreach coordinator and a treasurer. There are* 10 *candidates, and one person may serve more than one role. In how many different ways can the committee be constituted?*

For each of the three positions, we have all 10 *candidates available. Thus, the total number of ways is* $10^3 = 1000$.

Example 2. *Suppose we have the same situation as Example 1, but one person may serve at most one role. In how many different ways can the committee be constituted?*

We have 10 *ways to choose a chairperson. Once we choose a chairperson, we have* 9 *ways in which we can choose the outreach coordinator, and then* 8 *ways in which we can choose the treasurer. Thus, the total number of ways is* $10 \times 9 \times 8 = 720$.

Example 3. *A committee comprises three officers, each of whom must be a different person, and there are* 10 *candidates. In how many different ways can the committee be constituted?*

In this case, we no longer distinguish the officers' roles, e.g., as chairperson, outreach coordinator and treasurer. But three distinct people must be chosen from the set of 10. *One way to count is to repeat the approach of Example 2*

above, and then account for the number of possibilities that should be treated as the same.

Example 2 tells us that there are 720 *ways, if we distinguish each officer's role. Suppose we have chosen a person, call her Alice to serve as officer* 1*, Bob to serve as officer* 2 *and Carol to serve as officer* 3*. This is the same as, for example, choosing Bob as officer* 1*, Carol as officer* 2 *and Alice as officer* 3*.*

Denoting Alice as a*, Bob as* b *and Carol as* c*, the number of different rearrangements of* $\langle a, b, c\rangle$ *is six:* $\langle a, b, c\rangle$*,* $\langle a, c, b\rangle$*,* $\langle b, a, c\rangle$*,* $\langle b, c, a\rangle$*,* $\langle c, a, b\rangle$ *and* $\langle c, b, a\rangle$*. Thus, to count all* 6 *of those ways as the same, we divide; i.e., our solution is* $720/6 = 120$*.*

That is, the 720 *different ways can be perceived as* 120 *groups of* 6 *each, where within each group, we have the same set of three officers.*

Example 4. *A committee comprises three officers, not all of whom need to be distinct individuals. There are* 10 *candidates. In how many different ways can the committee be constituted?*

In this case, we can either choose (i) one person to serve all three roles, (ii) two persons, one of whom serves two roles and the other one role, or, (iii) three persons. In case (ii), we need to distinguish which person serves two roles, i.e., for example, if the two chosen people are Alice and Bob, then we count Alice serving two roles and Bob one role as distinct from the situation that Bob serves two roles and Alice serves one role.

In case (i), we have 10 *different ways. In case (ii), we have* $10 \times 9 = 90$ *different ways. And in case (iii), we have* 120 *different ways, which we deduced in Example 3 above. Thus, the total is* 220 *different ways.*

The four examples above correspond to the four broad classes of selection we address. In Example 1, the selection is *ordered with replacement*. That is, the order of the choices matters, i.e., first vs. second vs. third, or chairperson vs. outreach coordinator vs. treasurer. But once a choice is made, e.g., of chairperson, the set from which we choose is replenished, i.e., the chosen one is replaced with a replica of that person.

In Example 2, the selection is *ordered without replacement*. The ordering

matters, e.g., if Alice is chosen as chairperson and Bob as outreach coordinator, that is different from Alice being chosen as outreach coordinator and Bob as chairperson. Also, the original set is not replenished once a choice is made. E.g., if Alice is chosen to be chairperson, then she is no longer available to serve any other role.

In Example 3, the selection is *unordered without replacement*. The "unordered" refers to the fact that all the members of the subset that is our selection are made simultaneously. There is no longer a first selection, then a second and so on. It is without replacement in that once a selection is made, the original set is not replenished.

In Example 4, the selection is *unordered with replacement*. The selection is unordered in that the subset that is our selection is contituted in one shot, and not one member of it at a time. However, there are limitlessly many replicas of each member in the original set from which we select the subset.

Principles

We now discuss the several underlying principles that help us navigate these sorts of questions regarding the number of possibilities in a particular setting.

"And" vs. "or" The first principle we discuss is a recognition of the use of "and" vs. "or" in the context of counting the number of different ways to make a selection. "And" is of course akin to conjunction, "$\wedge$," in propositional logic, and intersection, "$\cap$," between sets. "Or" is a bit more subtle in this context. It is not "inclusive or," which is akin to disjunction, "$\vee$," in propositional logic, and union, "$\cup$," between sets. Rather, it is "mutually exclusive or," which some folks represent using a new propositional logic operator "$\oplus$." Its semantics, expressed in English, is, "one or the other, but not both." Using $\neg, \vee$ and $\wedge$, $a \oplus b \iff (a \vee b) \wedge (\neg(a \wedge b)) \iff (a \wedge \neg b) \vee (b \wedge \neg a) \iff (a \vee b) \wedge (\neg a \vee \neg b)$.

"And" is typically used as part of putting together a selection. And when we use "and," we usually multiply the pieces that are and-ed together. "Or" is used to distinguish two different selections. And when we use "or," we usually add the different possibilities.

Example 5. *Jack has three books to read, Book 1, 2 and 3. He decides to either pick two of them, one to read during the day and the other at bedtime, or one only, to read during the day and at bedtime. How may different possibilities do we have for Jack's decision?*

This problem has both "and" and "or" components that can be called our clearly. The number of different possibilities can be expressed as:

Jack can pick:

(A) (*one book for daytime AND another for bedtime*)

OR

(B) (*one book for both day- and bedtime*)

The number of possibilities corresponding to (A) is 3×2*, i.e., a multiplication to correspond to the AND. The number of possibilities corresponding to (B) is* 3*. And we add the number of possibilities for (A) and (B) to correspond to the OR between them. So the solution is:* $3 \times 2 + 3 = 9$.

Pigeonhole principle The *pigeonhole principle* is: if we have n pigeonholes and more than n pigeons, then there must be a pigeonhole that houses more than one pigeon. It is called a "principle" because it is considered so self-evident that we do not bother proving it. However, can prove it by, for example, contradiction. Assume that we have n piegonholes, more than n pigeons, and that every pigeonhole has at most one pigeon. Then, if we sum the total number of pigeons across all pigeonholes, that sum $\leq n$, which contradicts the assumption that we have more than n pigeons.

The pigeonhole principle is useful in counting possibilities in certain situations.

Example 6. *How many people do we need in a group so we can guarantee that the birthdays of at least two of them fall in the same month?*

Answer: 13*. Because we have* 12 *"pigeonholes."*

Example 7. *We have* 30 *books that we want to put in* 20 *bags, each of which can hold all* 30 *books, if needed. Then, we know that there exists a bag with at least two books. And that is the strongest assertion we can make.*

Example 8. *In every set M of $n \geq 2$ integers, there exist distinct $a, b \in M$ such that the difference $a - b$ is divisible by $n - 1$.*

A special case of the above assertion is Claim 6 from Chapter 2, under "Proof techniques": given any set $\{a, b, c\}$ of integers, at least one of the differences $a-b, b-c, c-a$ must be divisible by 2, i.e., even. Another example is: given a set of 12 integers, at least one of the pairwise differences is divisible by 11.

For the original, general assertion, we can think of the "pigeonholes" as being $0, \ldots, n-2$, which is every value any integer can be modulo $n-1$. Thus, given n integers, there must exist at least two, i, j, such that $i \bmod (n-1) = j \bmod (n-1) \iff (i-j)$ is divisible by $n-1$.

Exponentiation When we make an ordered selection with replacement, we have repeated multiplications of the same number, i.e., exponentiation. An example is Example 1. Another example is the following.

Example 9. *The children at a school are taking field trips every day of the five days the following week, and need a teacher to act as chaperone for each trip. There are six teachers from which to choose a chaperone for each field trip. What is the total number of possiblities of assigning a chaperone to each field trip?*

The problem does not preclude the same teacher acting as chaperone for multiple field trips. Therefore, the total number of possibilities is 6^5.

Example 10. *The set of bit strings of length n, for some $n \in \mathbb{N}$, is:*

$$\underbrace{\{0,1\} \times \ldots \times \{0,1\}}_{n \text{ times}} = \{0,1\}^n$$

The number of bit strings of length n is $|\{0,1\}^n| = 2^n$. The number of bit strings of length n that all begin and end with the same bit $= \binom{2}{1} \times 2^{n-2} = 2^{n-1}$. The number that begin and end with different bits $= 2^n - 2^{n-1} = 2^{n-1}(2-1) = 2^{n-1}$. The number that have no consecutive bits the same $= 2$, because our choice of the first bit immediately gives us a choice for all n bits.

Factorial Recall that the *factorial* of n, denoted $n!$, for $n \in \mathbb{W} = \{0, 1, 2, \ldots\}$ is defined using a recurrence as follows:

$$n! = \begin{cases} 1 & \text{if } n = 0 \\ n \times (n-1)! & \text{otherwise} \end{cases}$$

The factorial function corresponds to the number of rearrangements of n distinct items. That is, if we have a set of n distinct items, the number of different ways in which they can be arranged is $n!$.

Example 11. *Eight friends go to a movie and buy tickets with assigned seating. The number of different ways in which they can occupy those seats is* $8! = 40,320$.

Example 12. *Bob has three different shirts and two different suits. How many different arrangements do we have in which he can hang them in his closet? What if every shirt is to be to the left of all the suits?*

The answer to the first question is $5!$ *because we have* 5 *items and* $5!$ *different ways to order them. The answer to the second is* $3! \times 2!$*. As a sanity check, we observe that* $5! > 3! \times 2!$*, which is what we would expect, because the second situation is more constrained than the first.*

Example 13. *How many different ways do we have to arrange* 8 *different math books,* 5 *different physics books and* 7 *different chemistry books such that all books of each subject are to be together?*

Answer: $3! \times 8! \times 5! \times 7!$*. The* $3!$ *is for the order of the subjects.*

Example 14. *How many rearrangements the letters does "BANANA" have?*

If all its letters were distinct, "BANANA" we would have $6!$*. However, in any such arrangement, a rearrangement of the A's and/or N's yields the same rearrangement of "BANANA." Thus, the solution is:*

$$\frac{6!}{3!\ 2!}$$

Permutation Given a set of n items, a *permutation*, or more specifically, a k-out-of-n permutation, is an arrangement of k of the n items from the set. For example, if the set $S = \{1, 2, 3\}$, then there are six 2-out-of-3 permutations: $\langle 1, 2\rangle$, $\langle 1, 3\rangle$, $\langle 2, 1\rangle$, $\langle 2, 3\rangle$, $\langle 3, 1\rangle$, $\langle 3, 2\rangle$.

A special case is when $k = n$, i.e., an n-out-of-n permutation, which is also simply called a permutation of the n items. We represent a k-out-of-n permutation as $P(n, k)$. And we can intuit what $P(n, k)$ is as follows. We

have n ways to pick the first item in the sequence, $n-1$ ways to pick the second, ..., and $n-k+1$ wants to pick the k^{th} item. Thus:

$$P(n,k) = \frac{n!}{(n-k)!}$$

Note that built into this notion of a permutation is that it is a kind of selection without replacement. Indeed, it is ordered selection without replacement. For example, Example 2 is exactly $P(10,3)$.

Example 15. *The number of* 4*-letter strings where each letter is one of the* 26 *in the English alphabet is* $P(26,4)$*.*

Example 16. *In how many different ways can be place* 8 *identical black pawns and* 8 *identical white pawns on a standard* 8×8 *chess board such that each pawn is in a square by itself?*

If the pawns were all distinct from one another, then our solution would be $P(64,16)$*. Given that we have two sets of* 8 *identical pawns each, we need to "factor" out duplicate arrangements. Once we have chosen the squares in which the* 8 *black pawns go, any rearrangement of those black pawns within those same squares is treated as the same arrangement. Thus, our solution is:*

$$\frac{P(64,16)}{8!\ 8!}$$

Example 14 and the above example are instances of what we can call *generalized permutation.* If we have n_1 indistinguishable items of Type_1, n_2 of Type_2, ..., n_k of Type_k, and $n_1 + \ldots + n_k = n$, then the number of ways to arrange them is:

$$\frac{n!}{n_1!\, n_2! \ldots n_k!}$$

Combination A k-out-of-n *combination* is a simultaneous, unordered selection of k items from a set of n items. We represent it as $\binom{n}{k}$, which is read as "n choose k." We can think of such a selection as first, an ordered

selection, i.e., $P(n,k)$, and then dividing by $k!$ so selections that should be counted as the same are indeed counted as the same.

That is, $\binom{n}{k} = P(n,k)/k!$, because the $k!$ rearrangements (permutations) of the k chosen items from n are all to be treated the same. Thus:

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

$\binom{n}{k}$ corresponds to unordered selection without replacement. An example is Example 3, in which we ask in how many different ways we can choose 3 distinct officers from 10 people. The answer is $\binom{10}{3}$.

Another example is Example 16, which we can approach as follows. We first pick the 16 squares on which the pawns are to be placed. Then, from amongst those 16, we choose 8 for the black pawns. Thus, the solution is:

$$\binom{64}{16} \times \binom{16}{8}$$

We can (and should) double-check that this yields the same solution as our approach using permutations does.

From permutations :

$$\frac{P(64,16)}{8!\ 8!} = \frac{64!}{48!\ 8!\ 8!}$$

From combinations :

$$\binom{64}{16} \times \binom{16}{8} = \frac{64!}{16!\ 48!} \times \frac{16!}{8!\ 8!} = \frac{64!}{48!\ 8!\ 8!}$$

Example 17. *In how many different ways can we arrange* 8 *identical copies of "Pride & Prejudice" and* 5 *identical copies of "Sense & Sensibility" on a shelf?*

One way to look at this is to observe that we have 13 *slots to fill on the shelf, and we choose* 8 *of them, unordered, for "Pride & Prejudice." This should be (and is) equivalent to choosing* 5 *of the slots for "Sense & Sensibility." So the solution is:*

$$\binom{13}{8} = \binom{13}{5}$$

The above example is a good illustration of the intuition behind the fact that $\binom{n}{k} = \binom{n}{n-k}$. Picking k items from a set of n is identical to picking the $n-k$ items to leave out. A special case is $\binom{n}{0} = \binom{n}{n} = 1$. That is, there is only one way to choose nothing from a set of size n, and this is the same number of ways in which we can choose everything from the set. We present one more example, before we discuss the binomial theorem.

Example 18. *In how many different ways can a pack of* 52 *distinct cards be dealt in to four hands of* 13 *cards each?*

We first select 13 *cards, unordered, for the first hand from all* 52*. For the second hand, we select* 13 *cards from the remaining* 39*, and so on. So the solution is:*

$$\binom{52}{13} \times \binom{39}{13} \times \binom{26}{13} \times \binom{13}{13}$$

We first observe that simplifying the above solution yields:

$$\begin{aligned} & \frac{52!}{13!\ 39!} \times \frac{39!}{13!\ 26!} \times \frac{26!}{13!\ 13!} \times \frac{13!}{13!\ 0!} \\ = & \frac{52!}{13!\ 13!\ 13!\ 13!} \end{aligned}$$

This makes sense. This corresponds to every permutation of the 52 cards, but within each group of 13, we treat them as unordered.

Another aspect is that in the above mindset, the hands themselves are ordered. Otherwise, we would divide the above by 4!.

We now present the *binomial theorem*. As a clarification of terminology, a *polynomial* in n *variables*, $x_1, \ldots, x_n$ is a summation of *terms*, each of the form $c \times x_1^{c_1} \times x_2^{c_2} \times \ldots \times x_n^{c_n}$, where c is a constant integer, and each c_i is a constant non-negative integer. A *monomial* is a polynomial that has one term only, and a *binomial* is a polynomial that has two terms only. The binomial theorem identifies the terms of $(x+y)^n$, where x, y are variables, and $n \in \mathbb{N} = \{1, 2, \ldots\}$.

Claim 32 (Binomial theorem)**.** *For $n \in \mathbb{N}$,*

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$$

For example,

$$\begin{aligned}(a-b)^3 &= \binom{3}{0}a^0(-b)^3 + \binom{3}{1}a^1(-b)^2 + \binom{3}{2}a^2(-b)^1 + \binom{3}{3}a^3(-b)^0 \\ &= -b^3 + 3ab^2 - 3a^2b + a^3\end{aligned}$$

Proof. By induction on n. For the base case, the left hand side of the equation is $x+y$. The right hand side is $\binom{1}{0}x^0y^1 + \binom{1}{1}x^1y^0 = x+y$.

For the step:

$$\begin{aligned}(x+y)^n &= (x+y)(x+y)^{n-1} \\ &= (x+y)\sum_{i=0}^{n-1}\binom{n-1}{i}x^i y^{n-1-i} \\ &= (x+y)\sum_{i=1}^{n}\binom{n-1}{i-1}x^{i-1}y^{n-i} \\ &= \sum_{i=1}^{n}\binom{n-1}{i-1}x^i y^{n-i} + \sum_{i=1}^{n}\binom{n-1}{i-1}x^{i-1}y^{n-i+1} \\ &= \sum_{i=1}^{n}\binom{n-1}{i-1}x^i y^{n-i} + \sum_{i=0}^{n-1}\binom{n-1}{i}x^i y^{n-i} \\ &= \binom{n-1}{0}x^0y^n + \left(\sum_{i=1}^{n-1}\left(\binom{n-1}{i-1} + \binom{n-1}{i}\right)x^i y^{n-i}\right) + \binom{n-1}{n-1}x^n y^0 \\ &= \binom{n}{0}x^0y^n + \left(\sum_{i=1}^{n-1}\left(\binom{n-1}{i-1} + \binom{n-1}{i}\right)x^i y^{n-i}\right) + \binom{n}{n}x^n y^0\end{aligned}$$

And, we have:

$$\begin{aligned}\binom{n-1}{i-1} + \binom{n-1}{i} &= \frac{(n-1)!}{(i-1)!\ (n-i)!} + \frac{(n-1)!}{(n-1-i)!\ i!} \\ &= \frac{(n-1)!}{(i-1)!\ (n-i-1)!}\left(\frac{1}{n-i} + \frac{1}{i}\right) \\ &= \frac{(n-1)!}{(i-1)!\ (n-i-1)!}\left(\frac{n}{(n-i)\ i}\right) \\ &= \frac{n!}{(n-i)!\ i!} = \binom{n}{i}\end{aligned}$$

□

Thus, the coefficients are given exactly by the combinations. An example of an application of the binomial theorem is expressed by the following claim.

Claim 33. *Given a finite set S of $n \in \mathbb{N}$ members, the number of subsets of S, i.e., the cardinality of $\mathscr{P}(S)$, is 2^n.*

Proof. We ask how many subsets of size $0, 1, \ldots, n$ the set S has. And these correspond exactly to unordered selection of items from S. That is, S has $\binom{n}{0} = 1$ subset of size 0, $\binom{n}{1} = n$ subsets of size 1, …, $\binom{n}{n} = 1$ subset of size n. Thus, the total number of its subsets is:

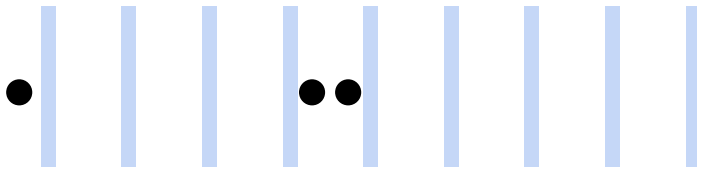
$$\begin{aligned}&\sum_{i=0}^{n} \binom{n}{i} \\ &= \sum_{i=0}^{n} \binom{n}{i} 1^i 1^{n-i} \\ &= (1+1)^n = 2^n\end{aligned}$$

□

As a final disussion point about combinations, before we introduce the notion of multichoose below, we revisit Example 4. Recall that that was an example of unordered selection with replacement: we seek the number of ways in which three officers can be chosen from a pool of 10, where an individual is allowed to occupy more than one officer position.

One way to think about this, which results in re-posing the question as one about combinations, is the following. Each officer position is an identical

"ball." Each of the 10 candidates is a "bin." We ask in how many ways we can have the 10 bins contain the 3 balls, such that each bin contains between 0 and 3 balls. To visualize the bins, we can think of 9 partitions, which results in 10 bins. For example, the following picture depicts the 9 partitions which result in 10 bins, with the first bin containing one ball, and the fifth bin containing the other two. This would be one of the ways in which the bins can contain the balls.



To further converge towards a way of counting the different possibilities, the balls-and-bins situation in the above picture can be thought of as a bit-string, i.e., string of 0's and 1's. For example, the scenario above is the bit-string 011110011111. And what we are asking is: how many bit-strings of length 12 do we have that contain exactly three 0's?

The answer to that question is a simple combination: we pick three of the 12 bit positions to be a 0. That is, the solution is:

$$\binom{12}{3} = \frac{12 \times 11 \times 10}{3 \times 2} = 220$$

Multichoose The above example illustrates *multichoose*: unordered selection with replacement. k-out-of-n multichoose is represented as:

$$\left(\!\binom{n}{k}\!\right)$$

And it turns out that there is a simple formula for it based on combination:

$$\left(\!\binom{n}{k}\!\right) = \binom{n+k-1}{k}$$

In Example 4, $n = 10$, $k = 3$, and so $\left(\!\binom{10}{3}\!\right) = \binom{10+3-1}{3} = \binom{12}{3}$.

Example 19. *We have decided to add* 5 *dashes of powdered spice to a dish. We have available to us bags of* 9 *different powdered spices. How many ways are there to select those* 5 *dashes from the* 9*?*

This is unordered selection with replacement, because we assume that we have a limitless amount of each spice available, or at least a sufficient amount of each of the 9 *spices for* 5 *dashes. Thus, the solution is:*

$$\left(\!\binom{9}{5}\!\right) = \binom{9+5-1}{5}$$

Example 20. *In a large basket, we have a medley of apples, oranges and pears. We reach in and pick* 4 *pieces of fruit. How many different possibilities do we have of sets of the* 4 *pieces of fruit?*

The solution is:

$$\left(\!\binom{3}{4}\!\right) = \binom{3+4-1}{4} = \binom{6}{4} = 15$$

The above example illustrates an important point about multichoose. In k-out-of-n multichoose, it is certainly possible that $k > n$. This makes sense, because it is selection with replacement. Therefore, even though we have only $n < k$ distinct items, we can pick more than n items because the items are replenished, i.e., it is with replacement. This is different from, for example, combinations and permutations. In both those cases, for k-out-of-n, it must be the case that $k \leq n$. In those cases, the selection is without replacement.

Principle of inclusion-exclusion We begin with an example question: among 100 students, 75 take a math course, 50 take a physics course, and 45 take both. How many take at least one of those two courses?

The principle of *inclusion-exclusion* is useful is answering questions such as these. It is based in the following observations, and their corresponding generalizations. For finite sets, it is true that:

$$|A \cup B| = |A| + |B| - |A \cap B|$$
$$|A \cup B \cup C| = |A| + |B| + |C| - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$$

Example 21. *Among* 100 *students,* 75 *take a math course,* 50 *take a physics course, and* 45 *take both. How many take at least one of those two courses?*

Let M *be the set each of whom takes a math course, and* P *that takes the physics course. We seek* $|M \cup P|$*. And by the formula above, it is* $75 + 50 - 45 = 80$*.*

And therefore, the number that take neither is $100 - 80 = 20$*.*

Discrete Probability

We now introduce *probability*, which captures the notion of the likelihood that an event may occur. We begin with the notion of an *experiment* which is something we conduct or happens, and has one or more *outcomes*. Each outcome in the context of an experiment is called an *elementary event*. A *sample space* is a set of elementary events.

For example, our experiment may be a toss of a two-sided coin, which has one of two possible outcomes, heads or tails. We could associate the symbol H with the elementary event that is the former, and T with the elementary event that is the latter. The set $\{H, T\}$, then, is a sample space. Similarly, we may associate the toss of a 6-sided die with the sample space $\{1, 2, \ldots, 6\}$, where each of its members represents the elementary event that the die lands on that number.

Note: in this course, we deal with space spaces that are finite, and therefore countable, only. Some of the following notions rely on this assumption.

An *event* is a subset of a sample space. For example, given the sample space $\{HH, HT, TH, TT\}$, that is the set of elementary events associated with tossing two coins, the subset $\{HH, HT, TH\}$ is an event; it is the event that we get at least one heads. A sample space is a subset of itself, and is therefore an event, which we can call the *certain event*. The emptyset, $\emptyset$, is the *null event*. Given a sample space S and two events $A, B \subseteq S$, we say that the events A and B are *mutually exclusive* if $A \cap B = \emptyset$. E.g., in tossing two coins, the event that we get no tails, $\{HH\}$, is mutually exclusive from the event that the first toss is a tails, $\{TH, TT\}$. We can think of each elementary event $s \in S$ as an event $\{s\}$; the elementary events are mutually exclusive from one another.

Probability A *probability distribution*, Pr, is a function from the powerset of a sample space S to the real numbers $\mathbb{R}$ that satisfies the following axioms, which are called the *probability axioms*.

1. $\Pr\{A\} \geq 0$ for every event $A \subseteq S$.

2. $\Pr\{S\} = 1$. (This is why we call S the certain event.)

3. For pairwise mutually exclusive events $A_1, \ldots, A_n$,

$$\Pr\{A_1 \cup A_2 \cup \ldots \cup A_n\} = \Pr\{A_1\} + \Pr\{A_2\} + \ldots + \Pr\{A_n\}$$

Note: we choose to write $\Pr\{\cdot\}$ rather than $\Pr(\cdot)$, i.e., with the customary round backets that we use for functions, merely to emphasize that while $\Pr\{\cdot\}$ is a function, it is a function that happens to be a probability distribution.

We call $\Pr\{A\}$ the *probability* of the event A. For example, suppose we associate the sample space $S = \{1, 2, \ldots, 6\}$ with the roll of a 6-sided die. And suppose $\Pr\{1\} = \Pr\{2\} = \ldots = \Pr\{5\} = 1/10$, and $\Pr\{6\} = 1/2$. Then, such a Pr can be a probability distribution. (We need to assert, in addition, that Axiom 3 is satisfied.)

A probability distribution is said to be *discrete* if it is defined over a sample space that is countable. As our note above says, in this course, we deal with finite, and therefore countable, sample spaces only. Thus, all probability distributions with which we deal are discrete. In a discrete probability distribution over a sample space S, for an event $A \subseteq S$:

$$\Pr\{A\} = \sum_{s \in A} \Pr\{s\}$$

Given the above probability axioms, we can establish a number of claims for a discrete probability distribution, Pr.

Claim 34. *$Pr\{\emptyset\} = 0$.*

Proof. Assume otherwise for the purpose of contradiction, i.e., assume $\Pr\{\emptyset\} > 0$. We observe that if S is the sample space, then $S \cap \emptyset = \emptyset$, that is, S and $\emptyset$ are mutually exclusive. Therefore, $\Pr\{S \cup \emptyset\} = \Pr\{S\} = \Pr\{S\} + \Pr\{\emptyset\} > 1$, a contradiction to the axiom $\Pr\{S\} = 1$. □

Claim 35. *If $A \subseteq S$ is an event, then $Pr\{\overline{A}\} = 1 - Pr\{A\}$.*

Proof. $\overline{A} = S \setminus A$. And $\overline{A} \cap A = \emptyset$. Therefore, $\Pr\{\overline{A} \cup A\} = \Pr\{S\} = 1 = \Pr\{\overline{A}\} + \Pr\{A\} \implies \Pr\{\overline{A}\} = 1 - \Pr\{A\}$. □

The above claim can be useful in intuiting the probability of an event by considering its complement. For example, for the events associated with the

toss of two coins, suppose each of the elementary events HH, HT, TH, TT has equal probability of $1/4$. Then, $\Pr\{\text{at least one heads}\} = 1 - \Pr\{\text{no heads}\} = 1 - \Pr\{TT\} = 1 - 1/4 = 3/4$.

Claim 36. *For events A, B with $A \subseteq B$, it is true that $Pr\{A\} \leq Pr\{B\}$.*

Proof. $B \supseteq A \implies B = A \cup (B \setminus A) \implies \Pr\{B\} = \Pr\{A\} + \Pr\{B \setminus A\} \implies \Pr\{B\} \geq \Pr\{A\}$. □

Claim 37. *$Pr\{A \cup B\} = Pr\{A\} + Pr\{B\} - Pr\{A \cap B\}$.*

Proof.

$$
\begin{aligned}
& A = (A \setminus (A \cap B)) \cup (A \cap B) \\
\implies & \Pr\{A\} = \Pr\{A \setminus (A \cap B)\} + \Pr\{A \cap B\}
\end{aligned}
$$

$$
\begin{aligned}
& B = (B \setminus (A \cap B)) \cup (A \cap B) \\
\implies & \Pr\{B\} = \Pr\{B \setminus (A \cap B)\} + \Pr\{A \cap B\}
\end{aligned}
$$

$$
\begin{aligned}
\implies & \Pr\{A\} + \Pr\{B\} - \Pr\{A \cap B\} = \\
& \Pr\{A \setminus (A \cap B)\} + \Pr\{B \setminus (A \cap B)\} + \Pr\{A \cap B\} = \\
& \Pr\{A \cup B\}
\end{aligned}
$$

□

A corollary to the above claim is: $\Pr\{A \cup B\} \leq \Pr\{A\} + \Pr\{B\}$.

Uniform probability distribution Given a sample space $S = \{s_1, \ldots, s_n\}$, if $\Pr\{s_1\} = \ldots = \Pr\{s_n\}$, we call such a Pr a uniform probability distribution. Given such a uniform distribution over a sample space S, and an event $A \subseteq S$, we have a relatively simple formula for $\Pr\{A\}$:

$$\Pr\{A\} = \frac{|A|}{|S|}$$

Example 22. *Suppose we toss three coins, with each outcome equally likely. What is the probability that we have at least two heads?*

If S is the same space, then $|S| = 2^3$. The event A mentioned above occurs when we have either (i) exactly two heads, or, (ii) all three are heads. The number of ways in which (ii) can happen is 1. The number of ways in which (i) can happen is $\binom{3}{2}$. So:

$$Pr\{A\} = \frac{\binom{3}{2} + 1}{2^3} = \frac{1}{2}$$

Example 23. *We have a basketful of apples, oranges, pears and peaches. We reach in and take two pieces of fruit in a manner that every multiset of two pieces of fruit is equally likely. What is the probability that we end up with two different kinds of fruit?*

Let A be the event that we end up with two different kinds of fruit. Then, $Pr\{A\} = 1 - Pr\{\overline{A}\}$, where $\overline{A}$ is the event that we end up with two of the same kind of fruit. The number of ways in which $\overline{A}$ can happen is 4, because we have 4 different kinds of fruit.

All that remains is for us to intuit the size of the same space, call it S, which is all possible multisets of size 2. Our situation corresponds to unordered selection with replacement, and so:

$$\begin{aligned} Pr\{A\} = 1 - Pr\{\overline{A}\} = 1 - \frac{|\overline{A}|}{|S|} = 1 - \frac{4}{\left(\!\binom{4}{2}\!\right)} \\ = 1 - \frac{4}{\binom{4+2-1}{2}} = 1 - \frac{4}{10} = \frac{3}{5} \end{aligned}$$

It is somewhat interesting to sanity-check the solution in the above example by changing the number of different kinds of fruit in the basket, call it d. The example considers the case that $d = 4$. The following table gives us the

probability of picking two different pieces of fruit for different values of d.

d	$\Pr\{A\} = 1 - \frac{d}{\left(\!\binom{d}{2}\!\right)}$
1	$1 - \frac{1}{\binom{1+2-1}{2}} = 1 - \frac{1}{1} = 0$
2	$1 - \frac{2}{\binom{2+2-1}{2}} = 1 - \frac{2}{3} = 1/3$
3	$1 - \frac{3}{\binom{3+2-1}{2}} = 1 - \frac{3}{6} = 1/2$
4	$1 - \frac{4}{\binom{4+2-1}{2}} = 1 - \frac{4}{10} = 3/5$
5	$1 - \frac{5}{\binom{5+2-1}{2}} = 1 - \frac{5}{15} = 2/3$
6	$1 - \frac{6}{\binom{6+2-1}{2}} = 1 - \frac{6}{21} = 5/7$
7	$1 - \frac{7}{\binom{7+2-1}{2}} = 1 - \frac{7}{28} = 3/4$

The table suggests that as the number of kinds of fruit increases in the basket, the probability of picking two different kinds of fruit increases. This of course appeals to the common sense.

Conditional probability and independence Conditional probability addresses situations that we already have some prior knowledge about some outcomes. Consider the following game, which is from a TV show called "Let's Make a Deal."

There are three curtains, numbered 1, 2 and 3. Behind one of them is a desirable prize. Behind the other two, there is nothing. The game goes as follows. You are first asked to pick one of the curtains. The host then draws back one of the other curtains that does not contain the prize; we know that there is at least one. The host them gives you the opportunity to change your choice to the other curtain that remains closed.

Should we change our choice? Is it rational to do so?

We can pose this as a problem of intuiting the probability of winning if we switch our choice, given our *a priori* knowledge that the curtain that the host

drew back does not contain the prize. If this probability is higher than 1/3, we should switch; otherwise, there is no rational reason to switch. The value 1/3 comes from our assumption that initially, we have a uniform distribution, i.e., the probability that the prize is behind any one of the curtains is 1/3.

The above problem is called "The Monty Hall problem," after the host of the game show. We revisit it after our discussions on conditional probability. A simpler example is: suppose we toss two coins, with every elementary event equally likely, and you know that one of them lands heads. So that is our *a priori* knowledge. What is the probability that both land heads?

The fact that one of the coins lands heads eliminates the event TT, that both land tails. So, the only possible events are HH, HT, TH. And therefore, the conditional probability in question is 1/3.

The conditional probability of an event A given that an event B occurs, i.e., $\Pr\{B\} \neq 0$, read as "the probability of A given B" is:

$$\Pr\{A \mid B\} = \frac{\Pr\{A \cap B\}}{\Pr\{B\}}$$

One way to understand the above formula is that we normalize the probability that both A and B occur by the probability that B occurs. For example, for our coin toss example above, A is the event that both coins land heads, and B is the event that one of them lands heads. And we have:

$$\Pr\{A \mid B\} = \frac{\Pr\{A \cap B\}}{\Pr\{B\}} = \frac{\Pr\{A\}}{\Pr\{B\}} = \frac{1/4}{3/4} = \frac{1}{3}$$

We exploited the fact that $A \cap B = A$, because $A \subseteq B$.

We say that events A and B are said to be *independent* if $\Pr\{A \cap B\} = \Pr\{A\}\Pr\{B\}$. This is equivalent, if $\Pr\{B\} \neq 0$, to: $\Pr\{A \mid B\} = \Pr\{A\}$.

Example 24. *Suppose we toss a coin once and then again, in a manner that every elementary event, HH, TT, HT, TH, is equally likely. Let A be the event that the first toss lands heads. And B be the event that the two*

tosses land differently. Are the events A and B independent?

We compare $Pr\{A\}$ with $Pr\{A \mid B\}$.

$$Pr\{A\} = 1/2$$
$$Pr\{A \mid B\} = \frac{Pr\{A \cap B\}}{Pr\{B\}} = \frac{Pr\{HT\}}{Pr\{HT, TH\}} = \frac{1/4}{2/4} = \frac{1}{2}$$

Thus, the events A and B are indeed independent.

Example 25. *You have a coin that you fear may be biased. That is, it lands heads with some probability $p \in (0, 1)$, and tails with probability $1 - p$. You do not know what p is, except that it is neither 0 nor 1. Devise a way to get a fair coin toss.*

Consider the following approach. We repeatedly toss the coin twice till the two outcomes are different. Then we adopt the first of the two tosses as our result.

Why does this work? With every two tosses, we have the sample space $S = \{HH, HT, TH, TT\}$. And we observe that $Pr\{HT\} = Pr\{TH\} = p(1 - p)$. That is, we have the same probability for the two events that correspond to different outcomes for the two tosses.

Example 26. *A standard pack of 52 cards includes 12 "face cards" – Queens, Kings and Jacks. Suppose you draw two cards uniformly at random from such a standard pack, and notice that the first is not a face card. What is the probability that the second is a face card?*

Let A be the event that the first is not a face card, and B be the event that the second is. We seek $Pr\{B \mid A\}$.

$$Pr\{B \mid A\} = \frac{Pr\{B \cap A\}}{Pr\{A\}} = \frac{(40 \times 12)/(52 \times 51)}{40/52}$$
$$= \frac{40 \times 12 \times 52}{52 \times 51 \times 40} = \frac{12}{51}$$

This makes sense, because once we remove a non-face card, we have a $12/51$ chance of drawing a face card. Also, the events A and B are not independent.

Because:

$$\begin{aligned} Pr\{B\} &= Pr\big\{(B \cap A) \cup \big(B \cap \overline{A}\big)\big\} \\ &= Pr\{B \cap A\} + Pr\big\{B \cap \overline{A}\big\} \\ &= \frac{40 \times 12}{52 \times 51} + \frac{12 \times 11}{52 \times 51} \\ &= \frac{12 \times (40 + 11)}{52 \times 51} \\ &= \frac{12}{52} \neq \frac{12}{51} = Pr\{B \mid A\} \end{aligned}$$

In the above example, does it make sense that $\Pr\{B\}$, the probability that the second card that is chosen, is $\frac{12}{52}$? We observe that this is the same probability that, if we choose one card uniformly at random from the pack of 52, it is a face card. What if, for example, we pick 10 cards, one after another uniformly at random, and ask what the probability is that the eighth is a face card? The answer, as per the above mindset, should still be $\frac{12}{52}$.

We argue that this does make sense based on the following reasoning. Suppose we shuffle the cards thoroughly and lay them out left to right on a table. The leftmost card then, can be seen as corresponding to our first pick, the second card from the left as our second pick, and so on. Now, if we ask what the probability is that any one of them is a face card, it is $\frac{12}{52}$. Thus, if we uniformly at random pick n cards out of the 52, and ask what the probability is that the k^{th} of those cards is a face card, for $1 \leq k \leq n$, the answer is the same, $\frac{12}{52}$.

We now articulate Bayes's theorem, which relates $\Pr\{A \mid B\}$ and $\Pr\{B \mid A\}$. It is useful, for example, when one of those probabilities is easier to intuit than the other.

Claim 38 (Bayes's theorem)**.** *Suppose* $Pr\{A\} \neq 0, Pr\{B\} \neq 0$*. Then:*

$$Pr\{A \mid B\} = \frac{Pr\{A\}Pr\{B \mid A\}}{Pr\{B\}}$$

Proof.

$$\begin{aligned}
\Pr\{A \mid B\} &= \frac{\Pr\{A \cap B\}}{\Pr\{B\}} \\
\Pr\{B \mid A\} &= \frac{\Pr\{A \cap B\}}{\Pr\{A\}} \\
\implies \Pr\{B\}\Pr\{A \mid B\} &= \Pr\{A\}\Pr\{B \mid A\} \\
\implies \Pr\{A \mid B\} &= \frac{\Pr\{A\}\Pr\{B \mid A\}}{\Pr\{B\}}
\end{aligned}$$

□

Example 27. *We revisit Example 26 and ask, instead, what $Pr\{A \mid B\}$ is, i.e., the probability that the first card we draw is not a face card, given that the second is.*

$$\begin{aligned}
Pr\{A\} &= \frac{40}{52} \\
Pr\{B\} &= \frac{12}{52} \\
Pr\{A \mid B\} &= \frac{Pr\{A\}Pr\{B \mid A\}}{Pr\{B\}} && \because \textit{Bayes} \\
&= \frac{40/52 \times 12/51}{12/52} = \frac{40 \times 12 \times 52}{52 \times 51 \times 12} \\
&= \frac{40}{51}
\end{aligned}$$

Example 28. *We address the Monty Hall problem that we introduced earlier. Recall that the problem is as follows. There are three curtains behind one of which is a prize. We initially pick a curtain, and Monty then opens one of the other curtains that does not contain the prize. He then gives us the option of switching our choice to the third curtain before he reveals behind which curtain the prize is. The question is: should we switch? Or more specifically, does our probability of winning increase by switching?*

Assume that we choose Curtain 1 initially and then Monty opens curtain 2. Consider the following two events:

- *P_1 is the event that the prize is behind Curtain 1.*

- *R_2 is the event that after we have initially chosen Curtain 1, Monty opens Curtain 2.*

Then, we are interested to know $Pr\{P_1 \mid R_2\}$. Because, if $Pr\{P_1 \mid R_2\} < 1/2$, that would be a good rationale to switch to Curtain 3.

We leverage Bayes to determine $Pr\{P_1 \mid R_2\}$. For that, we need to determine $Pr\{P_1\}, Pr\{R_2\}$ and $Pr\{R_2 \mid P_1\}$. $Pr\{P_1\} = 1/3$ because the prize is equally likely to be behind any of the three curtains. $Pr\{R_2 \mid P_1\} = 1/2$ because if the prize is behind Curtain 1, given that we have chosen Curtain 1 initially, Monty can open either Curtain 2 or 3, and we assume he picks one with equal probability.

As for $Pr\{R_2\}$, we know that it is 0 if the prize is behind Curtain 2. Also, Monty cannot open Curtain 1 as we chose it initially. So the only way the event R_2 can occur is if the prize is behind Curtain 3. And this occurs with probability $1/2$ because the prize may be behind either Curtain 1 or 3 with equal probability. So:

$$\begin{aligned} Pr\{P_1 \mid R_2\} &= \frac{Pr\{P_1\}Pr\{R_2 \mid P_2\}}{Pr\{R_2\}} \\ &= \frac{1/3 \times 1/2}{1/2} = 1/3 \end{aligned}$$

Therefore, we should switch to Curtain 3, because the probability that the prize is behind Curtain 3 is $1 - 1/3 = 2/3$.

Example 29. *Suppose we have two coins, one of which is fair, and the other always comes up heads. Suppose we pick one of those coins uniformly at random and toss it three times, and it so happens that it comes up heads all of the three times. What is the probability that we happened to pick the coin that always comes up heads?*

Let A be the event that we pick the coin that always comes up heads. Let B be the event that all three tosses of the chosen coin come up heads. We seek $Pr\{A \mid B\}$.

We leverage Bayes, for which we need to know $Pr\{A\}, Pr\{B\}$ and $Pr\{B \mid A\}$.

$Pr\{A\} = 1/2$, and $Pr\{B \mid A\} = 1$. To determine $Pr\{B\}$, we observe:

$$\begin{aligned} Pr\{B\} &= Pr\{B \cap A\} + Pr\{B \cap \overline{A}\} \\ &= Pr\{A\}Pr\{B \mid A\} + Pr\{\overline{A}\}Pr\{B \mid \overline{A}\} \\ &= 1/2 \times 1 + 1/2 \times 1/8 \\ &= 9/16 \end{aligned}$$

So our solution:

$$\frac{Pr\{A\}Pr\{B \mid A\}}{Pr\{B\}} = \frac{1/2 \times 1}{9/16} = \frac{8}{9}$$

We expect that the more tosses we make that are all heads, the higher the probability that we have chosen the biased coin. Of course, if we see even one tails, we immediately know that we have chosen the fair coin.

Expectation We conclude our discussions on discrete probability with the notion of expectation, or the expected value of a discrete random variable.

Given a sample space S over which we specify a probability distribution, Pr, a *discrete random variable* X is a function from the sample space to a real number, $X : S \to \mathbb{R}$.

For example, suppose we toss a coin thrice, and I am to lose \$2 for every tails, and win \$10 for every heads. Then, we can specify a discrete random variable, call it W, which is my total winnings. The sample space is $\{H, T\} \times \{H, T\} \times \{H, T\}$. The range of W is $\{-6, 6, 18, 30\}$.

As we deal with only discrete random variables in this course, we drop the qualifier "discrete," henceforth. Given a random variable X, we define the event $X = x$ to be the set $\{s \in S \mid X(s) = x\}$. In our above example, the event $W = 18$ is $\{THH, HTH, HHT\}$. And then:

$$\Pr\{X = x\} = \sum_{s \in S : X(s) = x} \Pr\{s\}$$

In our above example, if the coin is fair, then $\Pr\{W = 18\} = 3/8$.

The *expected value*, *expectation* or *mean* of a random variable $X : S \to \mathbb{R}$ is

denoted $E[X]$, and defined as:

$$\begin{aligned} E[X] &= \sum_{x \in \mathbb{R}} x \cdot \Pr\{X = x\} \\ &= \sum_{s \in \mathbb{S}} X(s) \cdot \Pr\{s\} \end{aligned}$$

As the formula suggests, the expectation of X is a weighted average, where each of the values X can take is weighted by the probability with which X takes that value.

For example, in our above coin-toss game, the expectation of the random variable W, assuming that the coin is fair, is:

$$\begin{aligned} E[W] &= -6 \times \frac{1}{8} + 6 \times \frac{3}{8} + 18 \times \frac{3}{8} + 30 \times \frac{1}{8} \\ &= \frac{1}{8}(-6 + 18 + 54 + 30) = 12 \end{aligned}$$

The idea behind the expected value is exactly what we associate with the term "expectation." That is, if we play the coin-toss game, we expect to win \$12. And interesting observation is that the expectation is not necessarily one of the values that the random variable can take. That is, in our above example, there is no situation in which we actually win \$12, as our winning from playing the game once is one of $-6, 6, 18$ or 30.

Example 30. *We toss a fair 6-sided die whose faces are numbered* $1, \ldots, 6$. *What is the expectation of the toss?*

If T is a random variable that is the value the die lands, we have:

$$E[T] = \frac{1}{6}(1 + 2 + \ldots + 6) = \frac{21}{6} = 3.5$$

The expectation can be used to make decisions that we can argue are rational. Consider the following example.

Example 31. *You need to put in \$15 upfront to play the following game. We toss a fair coin twice. You earn \$4 for every tails and \$10 for every heads. Would you play this game?*

One way to rationally answer this question is to define an appropriate random variable and compute its expected value. Let X be a random variable that is

our earnings after the two tosses. If $E[X] \geq 15$, we agree to play the game. If not, we do not play the game.

We observe:

$$E[X] = 8 \times \frac{1}{4} + 14 \times \frac{1}{2} + 20 \times \frac{1}{4} = 14$$

So, if we play the game in the above example, we expect to lose money. This is exactly the kind of set up we see in Casinos. It is not quite true that "the house always wins." Rather, if we play a game in the Casino, we expect to lose money. Of course, we may win as well, and the house may lose. But the expectation captures the long-term trend. That is, provided the Casino is able to stay in business long enough and has sufficiently many visitors, it is highly likely to make a profit. Of course, if the odds are too skewed in favour of the house, no one would visit.

In the above example, we can ask what the probability is that we win more than \$15 so we do not lose money. And the answer is of course that the only way is if we land both heads, which happens with probability 1/4 only.

Example 32. *We revisit Example 25, in which we are given a biased coin, which lands heads with probability $p \in (0, 1)$, and tails with probability $1 - p$. Our algorithm to ensure a fair coin toss is: repeatedly toss the coin twice till we see two different results. Choose the first of the two as the result of our fair coin toss.*

As we discuss there, this works because $Pr\{HT\} = Pr\{TH\}$. However, a concern may be the number of times we may have to repeatedly toss the coin before we finally have a result for our fair coin toss. How many could it be?

Of course, in the worst-case, we may never stop – we may get so unlucky that both consecutive coin tosses always have the same result. But what if we ask how many consecutive pair of tosses we expect to have to make before we are able to stop?

Let T be the corresponding random variable. We can intuit $E[T]$ from our definition of expectation. We observe that T takes on values in $\mathbb{N}$, i.e., $1, 2, \ldots$ That is, we may stop after the first pair of coin tosses, or the second, and so on. The only reason we engage in a second pair of coin tosses is that we got the same results for both tosses in the first pair. The probability with which

we get the same result in a pair of tosses is $p^2 + (1-p)^2$, i.e., both tails or heads, with each event being mutually exclusive.

So we have the following for $E[T]$, with explanations for the lines with equation numbers following.

$$\begin{aligned}
E[T] &= 1 \times 2p(1-p) + \\
&\quad 2 \times \left[p^2 + (1-p)^2\right] \times 2p(1-p) + \\
&\quad 3 \times \left[p^2 + (1-p)^2\right]^2 \times 2p(1-p) + \\
&\quad 4 \times \left[p^2 + (1-p)^2\right]^3 \times 2p(1-p) + \\
&\quad \ldots \\
&= \sum_{i=1}^{\infty} i \times \left[p^2 + (1-p)^2\right]^{i-1} \times 2p(1-p) \\
&= 2p(1-p) \sum_{i=1}^{\infty} i \times \left[p^2 + (1-p)^2\right]^{i-1} \\
&= 2p(1-p) \sum_{i=1}^{\infty} \sum_{j=i}^{\infty} \left[p^2 + (1-p)^2\right]^{j-1} \qquad (4.1) \\
&= 2p(1-p) \sum_{i=1}^{\infty} \frac{\left[p^2 + (1-p)^2\right]^{i-1}}{1 - \left[p^2 + (1-p)^2\right]} \qquad (4.2) \\
&= \frac{2p(1-p)}{1 - \left[p^2 + (1-p)^2\right]} \sum_{i=1}^{\infty} \left[p^2 + (1-p)^2\right]^{i-1} \\
&= \frac{2p(1-p)}{\left[1 - (p^2 + (1-p)^2)\right]^2} \qquad (4.3) \\
&= \frac{2p(1-p)}{\left[2p(1-p)\right]^2} \qquad (4.4) \\
&= \frac{1}{2p(1-p)}
\end{aligned}$$

Explanations: for clarify, adopt $a = p^2 + (1-p)^2$.

(4.1) We seek $1 \times a^0 + 2 \times a^1 + 3 \times a^2 + 4 \times a^3 + \ldots$ We rewrite this as $(a^0 + a^1 + a^2 + a^3 + \ldots) + (a^1 + a^2 + a^3 + \ldots) + (a^2 + a^3 + \ldots) + \ldots$ This is exactly what the double summation expresses.

(4.2) The inner summation is what is called a *geometric series*. It is of the form $a^{i-1} + a^i + a^{i+1} + a^{i+2} + \ldots$ We can intuit what that summation is as follows:

$$\begin{aligned} S &= a^{i-1} + a^i + a^{i+1} + a^{i+2} + \ldots \\ aS &= a^i + a^{i+1} + a^{i+2} + \ldots \end{aligned}$$

$$\begin{aligned} S - aS &= a^{i-1} \\ \Longrightarrow S &= \frac{a^{i-1}}{1-a} \end{aligned}$$

(4.3) We again have a geometric series, except that the first term in the summation is $a^0 = 1$.

(4.4) $1 - [p^2 + (1-p)^2] = 2p(1-p)$. We can intuit this by looking at the binomial expansion of $[p + (1-p)]^2$, or simply by observing that $2p(1-p) = \Pr\{HT, TH\} = 1 - \Pr\{HH, TT\} = 1 - \left[p^2 + (1-p)^2\right]$.

As an example, suppose $p = 1/2$, that is, the coin is fair. Then, the number of pairs of tosses we expect to have to make before we have a result for our fair coin toss is: $\frac{1}{2p(1-p)} = 2$.

If the coin is more skewed, e.g., $p = 1/8$, then the expected number of pairs of tosses is $\frac{1}{2\times 1/8\times 7/8} = \frac{32}{7}$, which is between 4 and 5. It makes sense that our expected number of pairs of tosses increases as the coin gets more skewed. We get the minimum when the coin is fair, i.e., 2 pairs of tosses only.

In Example 32 above, we could have saved ourselves a whole lot of work on the math if we had been a bit more creative with the random variable we defined, paired with some additional observations about the expected value of random variables.

The first observation is the so-called *linearity of expectation*: if X, Y are random variables, then $E[X + Y] = E[X] + E[Y]$. The second is about so-called *indicator random variables*. An indicator random variable is a random variable which takes one of two values only: 0 or 1. Then, if X is an indicator random variable, $E[X] = \Pr\{X = 1\}$.

To prove the linearity of expectation, we recall that a random variable is a function, and rely on how we define addition for functions. We restrict

ourselves to functions whose codomain is the real numbers. Given functions $f\colon A \to \mathbb{R}, g\colon A \to \mathbb{R}$, we define the function $(f+g)\colon A \to \mathbb{R}$ as $(f+g)(a) = f(a) + g(a)$.

Claim 39. *If $X : S \to \mathbb{R}, Y : S \to \mathbb{R}$ are random variables where S is a sample space, then $E[X+Y] = E[X] + E[Y]$.*

Proof.

$$\begin{aligned}
E[X] &= \sum_{s\in\mathbb{S}} X(s)\cdot \Pr\{s\} \\
E[Y] &= \sum_{s\in\mathbb{S}} Y(s)\cdot \Pr\{s\} \\
E[X+Y] &= \sum_{s\in\mathbb{S}} (X+Y)(s)\cdot \Pr\{s\} \\
&= \sum_{s\in\mathbb{S}} (X(s)+Y(s))\cdot \Pr\{s\} \\
&= \sum_{s\in\mathbb{S}} ((X(s)\cdot \Pr\{s\}) + (Y(s)\cdot \Pr\{s\})) \\
&= \sum_{s\in\mathbb{S}} X(s)\cdot \Pr\{s\} + \sum_{s\in\mathbb{S}} Y(s)\cdot \Pr\{s\} \\
&= E[X] + E[Y]
\end{aligned}$$

□

Note that the above can be generalized to several random variables. That is:

$$E\left[\sum_{i=1}^{n} X_i\right] = \sum_{i=1}^{n} E[X_i]$$

Claim 40. *If X is an indicator random variable, i.e., takes on the value 0 or 1 only, then $E[X] = Pr\{X = 1\}$.*

Proof. As X takes on the value 0 or 1 only:

$$\begin{aligned}
E[X] &= 0\cdot \Pr\{X=0\} + 1\cdot \Pr\{X=1\} \\
&= \Pr\{X=1\}
\end{aligned}$$

□

We now return to Example 32. Consider the following alternative way of intuiting the expected number of pairs of tosses till we are able to return the result of a fair coin toss.

Suppose we carry out n pairs of such tosses. We first ask in how many we expect to have TH or HT. We then ask what n must be so that this expectation is at least 1. We proceed as follows, assuming that we carry out n pairs of tosses. Define n random variables, $X_1, \ldots, X_n$ as follows:

$$X_i = \begin{cases} 1 & \text{if the } i^{\text{th}} \text{ pair is } TH \text{ or } HT \\ 0 & \text{otherwise} \end{cases}$$

Let R be a random variable that is the number of such pairs of tosses for which we are able to return a result. Then:

$$\begin{aligned} R &= \sum_{i=1}^{n} X_i \\ \implies E[R] &= E\left[\sum_{i=1}^{n} X_i\right] \\ &= \sum_{i=1}^{n} E[X_i] \\ &= \sum_{i=1}^{n} \Pr\{X_i = 1\} \\ &= \sum_{i=1}^{n} 2p(1-p) \\ &= 2p(1-p)\sum_{i=1}^{n} 1 \\ &= 2np(1-p) \end{aligned}$$

And so,

$$E[R] \geq 1 \iff 2np(1-p) \geq 1 \iff n \geq \frac{1}{2p(1-p)}$$

The notion of an indicator random variable is related closely to the notion of a *Bernoulli trial*. A Bernoulli trial is an experiment which has one of two outcomes only: success or failure. And, if p is the probability of success in a Bernoulli trial, the expected number of trials before a success is $1/p$. This can be proved easily by leveraging an appropriately defined indicator random variable. Our experiment in Example 32 can be seen as a Bernoulli trial: success is a pair of coin tosses with different outcomes. As the probability of success is $2p(1-p)$, the expected number of trials before a success is $\frac{1}{2p(1-p)}$.

Example 33. *We revisit the situation in Example 29. We have a fair coin, and a coin that always lands heads. Suppose we pick one of the two uniformly at random, toss it, and repeat both of those steps till we get tails. What is the expected number of tosses?*

We adopt the notion of a Bernoulli trial. That is, success is when we get a tails from our randomly chosen coin. If we are able to intuit the probability of success, call it p, then $1/p$ *is the expectation we seek.*

Thus, the success event is when: (i) we choose the fair coin, and, (ii) a toss results in tails. And this probability is $1/2 \times 1/2 = 1/4$*, and therefore, our expected number of tosses is* 4.

The approach in the above example may be used to distinguish the coins. Following is another approach. We toss both coins simultaneously till one of them lands tails. We would then have immediately identified which coin is which. What is the expected number of tosses of each coin in this approach?

The expectation in this case is the same as the expected number of tosses of the fair coin till it lands tails. We can perceive this as a Bernoulli trial: we toss the fair coin, and success is that it lands tails. The probability of success, then, is $1/2$, and therefore the expectation is 2. Thus, we expect to have to toss each coin twice before we identify which is which. Thus, the total number of tosses is 4.

We conclude with an example from algorithms. Suppose you are given a set of n distinct integers, where n is odd. You are asked for an algorithm to find the median of those integers. The median is the middlemost value from

amongst the members of the set. E.g., the median of $\{-42, 17, 4, 5, 6\}$ is 5.

Consider the following randomized algorithm. We pick a number from the set, call it i, uniformly at random from amongst the n numbers. We then check whether i is indeed the median. We can do this, for example, by comparing i to every other number, and counting how many are smaller than i. The number of integers in the set that is smaller than i is $(n-1)/2$ if and only if i is the median. If we find out that i is not the median, we repeat the entire process. That is, we pick an integer uniformly at random and test it. (Of course, we may again pick i.)

This algorithm may not seem good, but it is simple, and somewhat surprisingly good in expectation. We can ask, for example, how many trials, i.e., random pick and subsequent check, we expect to make before we find the median. To answer this, we perceive a random pick as a Bernoulli trial. Success is if we picked the median. The probability of success, then, is $1/n$. Therefore, the expected number of trials before success is n.

— Mahesh Tripunitara