



MAT1804: Mathematics for Computing

COURSE NOTES

Luke Collins*

luke.collins@um.edu.mt ◦ lc.mt

Last updated: 11 Nov 2024 (Preliminary Version)

Contents

	Practical Matters	3
<div style="border: 1px solid black; padding: 2px; display: inline-block; margin-bottom: 5px;">Lecture 1 8 Oct 2024</div>	1 Propositional Logic	5
	1.1 Propositions	5
	1.2 Connectives	6
	1.3 Well-Formed Formulæ	11
	1.4 Truth Tables	16
	2 Set Theory	22
	2.1 Standard Sets	22
<div style="border: 1px solid black; padding: 2px; display: inline-block; margin-bottom: 5px;">Lecture 2 9 Oct 2024</div>	2.2 Subsets, Intervals and Set Comprehension	23
	2.3 Set Operations	26
	2.4 Predicate Logic	33
	3 Proofs	36
<div style="border: 1px solid black; padding: 2px; display: inline-block; margin-bottom: 5px;">Lecture 3 14 Oct 2024</div>	3.1 Types of Proof	38
<div style="border: 1px solid black; padding: 2px; display: inline-block; margin-bottom: 5px;">Lecture 4 21 Oct 2024</div>	3.2 $\sqrt{2}$ is irrational	40
	3.3 There are infinitely many primes	44
<div style="border: 1px solid black; padding: 2px; display: inline-block; margin-bottom: 5px;">Lecture 5 4 Nov 2024</div>	3.4 Proof by Induction	47
	3.4.1 Base Cases different from Zero	50
	3.4.2 Strong Induction	50
<div style="border: 1px solid black; padding: 2px; display: inline-block; margin-bottom: 5px;">Lecture 6 11 Nov 2024</div>	3.5 Discussion: Recursion and the Fibonacci Numbers	55
	4 Relations and Functions	62
	4.1 Functions	63

* Current address: Room 713, Department of Mathematics, UCL, 25 Gordon Street, London, UK

A Solutions to Exercises	66
Bibliography	90
Index	91

Practical Matters

My name is Luke Collins, and this year I will be teaching you this study-unit, *Mathematics for Computing*. The primary goal behind this course is to endow you with the necessary mathematical tools and language to be able to pursue the study of computer science and related fields at undergraduate level.

Lectures. This course consists of fifteen two-hour long lectures, which will be held on Mondays at 14:00–16:00 (GMT+02:00). Most of these will be [online](#) since I live in London, but we will be meeting in person on the following dates:

- Tuesday, 8th October 2024, 13:00–15:00 (GMT+02:00), (Lecture)
Hall D1, Gateway Building, Msida Campus
- Wednesday, 9th October 2024, 18:00–20:00 (GMT+02:00), (Lecture)
M401, Maths and Physics Building, Msida Campus

We will also meet again in person for some lectures and tutorials around Christmas time, on the following dates:

- Monday, 16th December 2024, 16:00–18:00 (GMT+01:00), (Lecture)
MP405, Maths and Physics Building, Msida Campus
- Tuesday, 17th December 2023, 13:00–15:00 (GMT+01:00), (Lecture)
MP401, Maths and Physics Building, Msida Campus
- Wednesday, 18th December 2023, 14:00–16:00 (GMT+01:00), (Tutorial)
MP401, Maths and Physics Building, Msida Campus
- Thursday, 19th December 2023, 14:00–16:00 (GMT+01:00), (Lecture)
(Venue TBA)

Preliminaries. Any topics listed under the MATSEC intermediate pure mathematics syllabus are considered obvious throughout this course. You can find the syllabus [here](#), and if you need to go over anything to refresh your memory, I recommend Serge Lang’s books, [here](#) and [here](#).

Lecture notes. I will be updating this PDF document throughout the term, adding the material we cover in each lecture as we go along. Look at the front page (or footer of each page) to check the date and ensure you have the latest version.

The official reference texts for this course are [1] and [2].

Exercises. It is important to work through all the exercises provided, not only to reinforce what you have learned, but to also garner sufficient instincts for what is to come. It is not enough to be able to do the exercises—by the end of them, you should

be able to do similar exercises *easily*, almost without thinking. This way, when we go on to more advanced topics, your focus will be entirely on the new material, and you will not sacrifice any of your brain’s “processing power” to understand more basic steps. When an exercise is annotated with a ☕ symbol, this is instructing you to pour yourself a cup of tea and dedicate some time to think about the problem, it might be harder than the others.

Course outline. The course content is divided into the following chapters. Note that they are not equal in size nor in scope.

- | | |
|------------------------|----------------------------|
| 1. Propositional Logic | 4. Relations and functions |
| 2. Set theory | 5. Linear algebra |
| 3. Proofs | 6. Graph theory |

Weekend assignments. Throughout the term, I will be giving you three *weekend assignments*; i.e., short worksheets containing a few questions on what we would be covering around that time. This will force you to interact with the course material throughout the term, not just before the final exam, and will serve as feedback for me to gauge the level of the class as a whole, and for you to get some “official” feedback on your mathematical abilities.

- **Weekend Assignment 1** (1–3 November, 2024).
This assignment will be on logic, set theory and a bit of proofs.
- **Weekend Assignment 2** (29 November–1 December, 2024).
This assignment will primarily be on proofs (especially induction), relations, and functions, but might also feature some material from the first two chapters.
- **Weekend Assignment 3** (3–5 January, 2025).
This assignment will primarily focus on linear algebra and graph theory, but might also feature material from previous chapters.

Resources. On VLE, I’ve provided you with a sample weekend assignment, to give you a feel for what to expect before you get one of the real ones. I’ve also provided three sample exam papers, as well as four real past papers, all of which have corresponding solutions. Only last year’s papers contain any questions on linear algebra, since I didn’t manage to cover that topic in time last year. Naturally I will provide you with some more exam-style questions on linear algebra so you know what to expect for your exam.

If you have any questions about the course, don’t hesitate to contact me via email on luke.collins@um.edu.mt, or talk to me after one of my lectures.

1. Propositional Logic

✠ JMJ ✠

Lecture 1
8 Oct 2024

Logic is the foundational language of mathematics. It tells us how to construct statements, how to deduce statements from others, and what happens when we combine them in different ways.

Propositions

A proposition, or statement, is a meaningful sentence which is decidedly **true** or **false**. Examples of statements include:

“Today is a rainy day”, “ $1 + 1 = 5$ ”, and “ $2^{82\,589\,933} - 1$ is prime”,

whereas examples of non-statements are

“What time is it?”, “Edam cheese”, “73”, or “This statement is false”.²

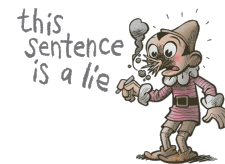
In propositional logic, a statement is taken in its entirety, usually represented by a single Greek letter (such as φ or ψ), and we only concern ourselves with whether or not it is true or false, rather than the individual components making up the statement. If a statement’s truth depends on a variable, we instead call it a *predicate*. For instance, “ x is prime” is a predicate, which we might call $\varphi(x)$, to show that it depends on the variable x . If we substitute a specific value for x , say $x = 2$, we then get the statement $\varphi(2)$, i.e., “2 is prime”.

We will discuss predicates in more detail later on, focusing only on propositions for now. This is called *propositional* or *zeroth order logic*. When we deal with predicates, we graduate to what’s called *predicate* or *first order logic*.

For what we study here, it is not important how we are able to determine the *truth-value* of a statement (i.e., whether it is true or false); we only care that it can be done. In practice, we might require very different techniques in order to do so, depending on the nature of the statement (e.g., we would use different techniques for checking whether or not “Today is a rainy day” is true, than we would for checking “ $1 + 1 = 5$ ”). Our goal is to study what happens when we combine statements together, developing a calculus which allows us to discover things about the truth-values of a compound proposition, assuming we know the truth-values of its individual component propositions.

²This is an interesting one. Why is it not a statement? Well, statements must be either true or false; so let us suppose that it is true. We immediately see the contradiction that arises: it claims itself to be false, so it cannot be true. Suppose therefore that it is false. In this case, it makes a claim which is true—contradicting that it should be false. Thus we cannot say that the statement is true, nor that it is false.

This special statement is an instance of what’s called *The Liar’s Paradox*, and the reason it is problematic is because it is talking about itself: it is *self-referential*. There are many self-referential objects in mathematics, and they need to be dealt with extra carefully, in order to avoid paradoxes like this one.



Connectives

Towards this goal, we now introduce the following *connectives* which allow us to construct compound propositions from simpler ones.

Definition 1.1 (Negation). Let φ be a statement. Then the *negation* of φ is another statement, denoted $\neg\varphi$ (read: “not φ ”), which is defined to be true precisely when φ is false, and vice-versa.

Examples 1.2. (i) If φ is the statement “The moon is made of cheese”, then $\neg\varphi$ is the statement “The moon is not made of cheese”.

(ii) If ψ is “ $1 + 1 = 2$ ”, then $\neg\psi$ is “ $1 + 1 \neq 2$ ”.

(iii) If ξ is “ $3 < 5$ ”, then $\neg\xi$ is “ $3 \geq 5$ ”.

We can summarise the behaviour of negation by tabulating all possibilities for φ , namely, the only two we care about: true or false. This is called a *truth table*.

φ	$\neg\varphi$
true	false
false	true

Table 1: Truth table for $\neg\varphi$

Definition 1.3 (Conjunction). Let φ and ψ be statements. Then the *conjunction* of φ and ψ is another statement, denoted $\varphi \wedge \psi$ (read: “ φ and ψ ”), which is defined to be true precisely when φ and ψ are both true, and false otherwise.

Example 1.4. If φ is the statement “Boris went to Eton” and ψ is the statement “Boris went to Oxford”, then $\varphi \wedge \psi$ is “Boris went to Eton and Boris went to Oxford”.

In order to construct a truth table for $\varphi \wedge \psi$, this time we require four rows, since the two possibilities for φ each in turn have two corresponding possibilities for ψ .

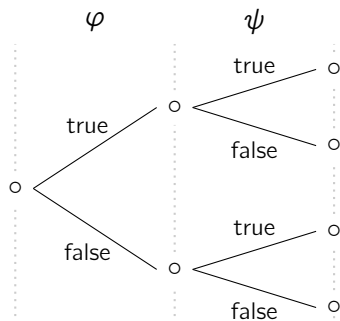


Figure 1: Possibilities double for φ and ψ

φ	ψ	$\varphi \wedge \psi$
true	true	true
true	false	false
false	true	false
false	false	false

Table 2: Truth table for $\varphi \wedge \psi$

Definition 1.5 (Disjunction). Let φ and ψ be statements. Then the *disjunction* of φ and ψ is another statement, denoted $\varphi \vee \psi$ (read: “ φ or ψ ”), which is defined to be true precisely when at least one of φ or ψ is true, and false otherwise.

Remark 1.6 (Exclusive v.s. Inclusive ‘or’). In ordinary English, the word ‘or’ is often interpreted as an *exclusive* or; that is, it may carry an implicit meaning of “only one” (as in “you can have normal chips *or* sweet potato chips with your burger”). This is not the case in mathematical usage, where ‘ $\varphi \vee \psi$ ’ should be interpreted to mean that φ holds, or ψ holds, or both do. If we mean to use an exclusive ‘or’, we should say something extra to indicate that (like “... but not both”).

Example 1.7. If φ is the statement “It is rainy today” and ψ is the statement “It will be rainy tomorrow”, then $\varphi \vee \psi$ is the statement “It is rainy today or it will be rainy tomorrow (or both)”.

As with conjunction, the truth table for disjunction requires four rows, since it is a *binary* connective (i.e., a connective involving two statements φ and ψ) as opposed to negation which is a *unary* connective (i.e., a connective involving only one statement).

φ	ψ	$\varphi \vee \psi$
true	true	true
true	false	true
false	true	true
false	false	false

Table 3: Truth table for $\varphi \vee \psi$

Definition 1.8 (Material Implication). Let φ and ψ be statements. Then the *material implication* of φ and ψ is another statement, denoted $\varphi \rightarrow \psi$ (read: “ φ implies ψ ”), which is defined to be true, except when φ is true yet ψ is false, in which case it is defined to be false.

φ	ψ	$\varphi \rightarrow \psi$
true	true	true
true	false	false
false	true	true
false	false	true

Table 4: Truth table for $\varphi \rightarrow \psi$

Remark 1.9 (Material Implication as a Promise). The material implication $\varphi \rightarrow \psi$ is equivalent to the statement “If φ , then ψ ”. It is best understood as a promise: $\varphi \rightarrow \psi$

is ‘promising’ that ψ will be true if φ is. So, for example, if φ is “You come to class” and ψ is “You get a free croissant”, then $\varphi \rightarrow \psi$ is the promise “If you come to class, you get a free croissant”.

If I, your lecturer, were to make such a promise, in what case would I be breaking it? If you don’t come to class, (i.e., φ is false), then you didn’t keep your end of the bargain, so whether or not you get a free croissant, the promise was kept (and so $\varphi \rightarrow \psi$ is true). If you come to class and get your croissant, the promise is also kept. The only instance in which the promise is broken is if you *do* come to class (φ is true), but don’t get a free croissant (ψ is false).

Remark 1.10 (Equivalent Phrases). There are many common phrases in English which are equivalent to “If φ , then ψ ”, it’s worth listing a few of them:

- | | |
|--|--|
| (i) φ implies ψ ; | (iv) ψ when φ ; |
| (ii) φ only if ψ ; | (v) ψ if φ ; |
| (iii) φ is a sufficient condition for ψ ; | (vi) ψ is a necessary condition for φ . |

Remark 1.11 (Implication \neq Causation). In ordinary English usage, “implies” or “if . . . then . . .” tends to be understood to indicate a degree of causation. So if I say φ implies ψ I would usually mean that φ had something to do with ψ (e.g., “if you had not fallen asleep then you would have got more out of this lecture”). In mathematical usage this does not need to be the case (although it usually is the case for most useful statements). So if we say $\varphi \rightarrow \psi$, we simply mean that whenever φ is true ψ is also true. So “If Paris is the capital of France then the Thames flows through London” is a true statement, despite the fact that there is obviously no connection between these two facts. Similarly, “If Malta is on Mars then Versailles is on Venus” is also a true statement (because, since the ‘ φ ’ in this case is never true, it actually does not matter what we say afterwards—the statement $\varphi \rightarrow \psi$ will still be true. Such a statement is, however, completely useless). A statement like this, where the ‘ φ ’ is never true, is said to be *vacuously* true.

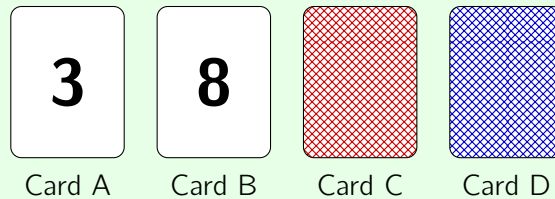
Remark 1.12 (\rightarrow is not symmetric). Of the three binary connectives we’ve seen so far, $\varphi \wedge \psi$, $\varphi \vee \psi$ and $\varphi \rightarrow \psi$, the latter is the only one which isn’t symmetric; i.e., it makes a difference which comes first: $\varphi \rightarrow \psi$ and $\psi \rightarrow \varphi$ are not the same statement. (We will address this in more detail later on).

Definition 1.13 (Converse). Consider the implication $\varphi \rightarrow \psi$. The implication with the statements swapped, i.e., $\psi \rightarrow \varphi$, is called the *converse* of $\varphi \rightarrow \psi$.



Activity 1.14 (Wason selection task, 1966).

Part 1. Consider the following set of four cards, each of which has a number on one side, and a colour on the other.



State which card(s) you must necessarily turn over in order to verify the truth of the following statement:

“If a card shows an even number on one face, then the other face must be red.”

Part 2. Consider the Maltese law that

“If you drink alcohol, you must be over 17 years old.”

Now suppose you own an establishment which serves alcohol, and you see the following four people:

- A. Someone drinking orange juice, whose age you don't know.
- B. Someone drinking vodka, whose age you don't know.
- C. Someone over 17 years old, with a drink you can't identify.
- D. Someone not over 17 years old, with a drink you can't identify.

Which of them do you examine to ensure that the law is being respected?

Part 3. Did you spot a connection between the two puzzles? Take a look at the Wikipedia article for the “Wason selection task” to check your answers.

Definition 1.15 (Biconditional). Let φ and ψ be statements. Then the *biconditional* of φ and ψ is another statement, denoted $\varphi \leftrightarrow \psi$ (read: “ φ if and only if ψ ”), which is defined to be true when φ and ψ have the same truth-value, and false otherwise.

As the symbol suggests, the biconditional of φ and ψ ensures that both $\varphi \rightarrow \psi$ and $\psi \rightarrow \varphi$ are true. In fact, it is equivalent to the statement $(\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$.

Remark 1.16 (Equivalence). If $\varphi \leftrightarrow \psi$ is true, then it essentially means that φ and ψ are equivalent statements. For instance, suppose φ is “I exercise” and ψ is “I ride my bike”. If the only way that I exercise is by riding my bike, and not engaging in other

φ	ψ	$\varphi \leftrightarrow \psi$
true	true	true
true	false	false
false	true	false
false	false	true

Table 5: Truth table for $\varphi \leftrightarrow \psi$

activities, then the statement $\varphi \rightarrow \psi$ (i.e., exercise \rightarrow bike) is true. This does not exclude me from riding my bike for other purposes, however.

If, in addition, I declare that I *only* use my bike for the purpose of exercise, and nothing else, in other words, $\psi \rightarrow \varphi$ (i.e., bike \rightarrow exercise), then combining the two pieces of information we have that $\varphi \leftrightarrow \psi$ is true.

Therefore, since the biconditional is true, the two statements “I exercise” and “I ride my bike” have become equivalent to each other.

Example 1.17 (Pythagoras’ theorem). Consider the following pair of statements:

- φ : The triangle contains a right-angle
- ψ : The triangle’s sides lengths satisfy the equation $a^2 + b^2 = c^2$

Pythagoras’ theorem states that $\varphi \rightarrow \psi$. The converse of Pythagoras’ theorem turns out to also be true, i.e., if a triangle’s side lengths satisfy the equation $a^2 + b^2 = c^2$, then it must have a right angle. Thus, since both are true, $\varphi \leftrightarrow \psi$ is true, and φ and ψ are equivalent statements.



Figure 2: Pythagoras

Here is a truth-table summarising the five connectives we’ve seen in this section.

φ	ψ	$\neg\varphi$	$\varphi \wedge \psi$	$\varphi \vee \psi$	$\varphi \rightarrow \psi$	$\varphi \leftrightarrow \psi$
true	true	false	true	true	true	true
true	false	false	false	true	false	false
false	true	true	false	true	true	false
false	false	true	false	false	true	true

Table 6: Truth table for the five connectives, $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$

Well-Formed Formulæ

So far we have seen the five simple propositions

$$\neg\varphi, \quad \varphi \wedge \psi, \quad \varphi \vee \psi, \quad \varphi \rightarrow \psi, \quad \varphi \leftrightarrow \psi.$$

But we can build other complex propositions, called *well-formed formulæ*, by applying the following rules.

Definition 1.18 (Well-formed formulæ). A proposition is called a *well-formed formula* (or wff) if it is constructed with the following set of rules:

- (i) Any atomic proposition is a wff.
- (ii) If Φ is a wff, then $\neg\Phi$ is also a wff.

If Φ and Ψ are wff's, then:

- (iii) $(\Phi \wedge \Psi)$ is also a wff;
- (iv) $(\Phi \vee \Psi)$ is also a wff;
- (v) $(\Phi \rightarrow \Psi)$ is also a wff;
- (vi) $(\Phi \leftrightarrow \Psi)$ is also a wff.

Unless constructed using only (i)-(vi) above, then any combination of symbols and connectives isn't a well-formed formula.

Example 1.19. $\varphi \wedge \psi\neg$, $\varphi\neg\psi$ and $\psi \wedge \wedge\varphi$ are not wffs.

Example 1.20. $\neg((\varphi \wedge \psi) \vee (\varphi \vee \xi))$ is a wff. Indeed,

- (1) φ , ψ and ξ are wff's by (i).
- (2) $(\varphi \wedge \psi)$ is a wff by (iii) and (1) above.
- (3) $(\varphi \vee \xi)$ is a wff by (iv) and (1) above.
- (4) $((\varphi \wedge \psi) \vee (\varphi \vee \xi))$ is a wff by (iv) and (2), (3) above.
- (5) Finally, $\neg((\varphi \wedge \psi) \vee (\varphi \vee \xi))$ is a wff by (ii) and (5) above. □

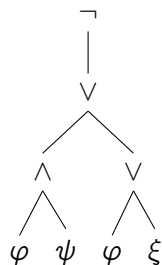


Figure 3: Syntax tree for the well-formed formula $\neg((\varphi \wedge \psi) \vee (\varphi \vee \xi))$

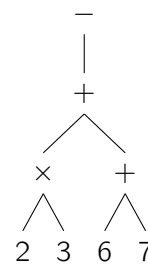


Figure 4: Syntax tree for the arithmetical expression $\neg((2 \times 3) + (6 + 7))$

This example should give you a feel as to how you should think of the way these expressions are built up. Indeed, it is helpful to mentally visualise a syntax tree for the expression (see figures 3 and 4), just as we do when we have arithmetical expressions such as

$$-((2 \times 3) + (6 + 7)).$$

In order to avoid using a large amount of brackets, we introduce the idea of relative precedence. For instance, in arithmetic, $1 + 2 \times 3$ is unambiguously interpreted as $1 + (2 \times 3)$.

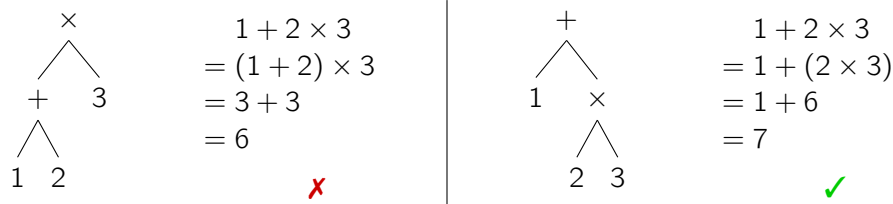


Figure 5: Two possible interpretations for $1 + 2 \times 3$. Using the established rules of precedence, we pick the one on the right.

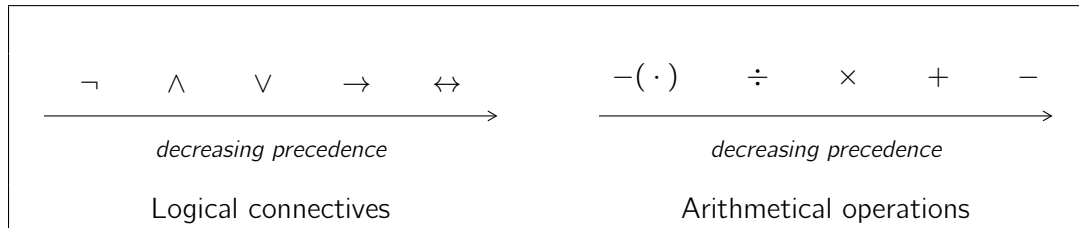


Figure 6: Rules of precedence for both logic and arithmetic operators, where $-(\cdot)$ denotes the unary (i.e., prefix) minus operator

We say that multiplication takes *precedence* over addition—i.e., without brackets we carry out multiplication before addition. The operators with higher precedence can be seen as if surrounded by brackets. Thus,

$$-1 + 2 \times 3 - 5 + 6 \quad \text{means} \quad (((-1) + (2 \times 3)) - 5) + 6,$$

and similarly

$$\varphi \wedge \psi \rightarrow \varphi \vee \psi \quad \text{means} \quad ((\varphi \wedge \psi) \rightarrow (\varphi \vee \psi)).$$

Similarly, $\neg\varphi \rightarrow \psi \wedge \xi \leftrightarrow \pi$ means $((\neg\varphi) \rightarrow (\psi \wedge \xi)) \leftrightarrow \pi$. Although we can reduce brackets to a minimum, we usually like to use brackets to distinguish between \wedge and \vee , and between \rightarrow and \leftrightarrow . Therefore, we would usually write $\varphi \vee (\psi \wedge \xi)$, even if $\varphi \vee \psi \wedge \xi$ would do. Similarly, we write $\varphi \leftrightarrow (\psi \rightarrow \xi)$ when $\varphi \leftrightarrow \psi \rightarrow \xi$ would do.

An issue we have yet to address is how to interpret unbracketed expressions with more than one use of the same operator, such as $\varphi \wedge \psi \wedge \xi$. Should this be interpreted as $(\varphi \wedge \psi) \wedge \xi$ or as $\varphi \wedge (\psi \wedge \xi)$? Later on, we will prove that the two expressions are logically equivalent. However, syntactically, the expressions are different (i.e., their trees are different), and we thus have to decide which expression we mean when we leave out the brackets. Furthermore, such an equivalence does not hold for all operators.

In arithmetic, for instance, $(1 - 2) - 3$ is not equal to $1 - (2 - 3)$. Usually, when we write $1 - 2 - 3$, we mean $(1 - 2) - 3$. This is called *left associativity*. An operator $*$ is said to be *right associative* when $x * y * z$ is to be interpreted as $x * (y * z)$. Conjunction and disjunction are left associative, while implication and biconditional are right associative. Therefore, using precedence and associativity, we could write $\varphi \wedge \psi \wedge \xi \rightarrow \pi \rightarrow \zeta$ instead of $((\varphi \wedge \psi) \wedge \xi) \rightarrow (\pi \rightarrow \zeta)$.

Exercise 1.21. 1. Which of the following are statements?

- | | |
|---|-------------------------------------|
| a) Knights always tell the truth. | b) Topological graph theory. |
| c) Is it raining outside? | d) $1 + 2 \neq 3$. |
| e) Jurassic Park is better than Jurassic World. | |
| f) Let's go to the theatre on Wednesday. | |
| g) Do you like ice cream? | h) The Earth is an oblate spheroid. |
| i) Is this a statement? | j) Engineers don't know any maths. |
| k) This is a false statement. | l) This is a statement. |

2. Deduce the negation of the following statements.

- | | |
|---|--------------------------------------|
| a) Knights always tell the truth. | b) $1 < 2$. |
| c) My cat can fly. | d) There are infinitely many primes. |
| e) Wallace and Gromit went to the moon. | f) Imaginary numbers don't exist! |


3. Consider the following four statements.

$$\begin{array}{ll} p := \text{"Pam is going"} & q := \text{"Quincy is going"} \\ r := \text{"Richard is going"} & s := \text{"Sara is going"} \end{array}$$

Express the following as propositions in terms of p , q , r and s .

- Pam is not going.
- Pam is going, but Quincy is not.
- If Pam is going, then so is Quincy.
- Pam is going if Quincy is.
- Pam is going only if Quincy is.
- Pam is going if and only if Quincy is.
- Neither Pam nor Quincy is going.

- h) Pam and Quincy are not both going.
 i) Either Pam is not going or Quincy is not going.
 j) Pam is not going if Quincy is.
 k) Either Pam is going, or Richard and Quincy are going.
 l) If Pam is going, then both Richard and Quincy are going.
 m) Pam is staying, but Richard and Quincy are going.
 n) If Richard is going, then if Pam is staying, Quincy is going.
 o) If neither Richard nor Quincy is going, then Pam is going.
 p) Richard is going only if Pam and Quincy are staying.
 q) Richard and Quincy are going, although Pam and Sara are staying.
 r) If either Richard or Quincy is going, then Pam is going and Sara is staying.
 s) Richard and Quincy are going if and only if either Pam or Sara is going.
 t) If Sara is going, then either Richard or Pam is going, and if Sara is not going, then both Pam and Quincy are going.
4. For each of the following, give two possible syntax trees (there may be more possible), together with the corresponding implied bracketing; one of them being the correct interpretation, and highlight which is which.
- a) $\varphi \wedge \psi \rightarrow \varphi$ b) $\varphi \leftrightarrow \neg\psi \vee \xi$ c) $\varphi \vee \psi \wedge \xi \wedge \pi \rightarrow \neg\varphi$
 d) $\varphi \rightarrow \psi \rightarrow \xi \leftrightarrow \psi \wedge \varphi \rightarrow \xi$ e) $\neg\varphi \vee \psi \leftrightarrow \varphi \rightarrow \xi$

-  5. On an island called *The Island of Knights and Knaves*, certain inhabitants called *knights* always tell the truth, and other inhabitants called *knaves* always lie.

Every inhabitant on this island is either a knight or a knave.




- a) You, a tourist, arrive on the island and are greeted by three people, A , B and C . You ask A : “Are you a knight or a knave?”. He answers, but you don’t hear him. B proceeds to say “ A said that he is a knave”. C promptly interrupts: “Don’t believe B , he is lying!”. What are B and C ?
- b) Suppose instead of asking A whether he is a knight or a knave, you ask “How many knights are among you?”. Again you don’t hear his answer, and B says: “ A said that there is one knight among us.” Then C again claims that “ B is lying!”. Now what are B and C ?

- c) In this problem, there are only two people, A and B , each of which whom is either a knight or a knave. A makes the following statement: "At least one of us is a knave." What are A and B ?
- d) Suppose A says "I am a knave or B is a knight". What are A and B ?
- e) Suppose A says "I am a knave or $2+2 = 5$ ". What do you conclude?
- f) Again we have three people, A , B and C , each of whom is either a knight or a knave. The following discourse ensues:

A : All of us are knaves.

B : Exactly one of us is a knight.

What are A , B and C ?

-  6. When Alice entered the Forest of Forgetfulness, she did not forget *everything*; only certain things. She often forgot her name, and most likely the day of the week.

Now, the Lion and the Unicorn were frequent visitors of the forest. These two are strange creatures: the lion lies on Mondays, Tuesdays and Wednesdays and tells the truth on the other days of the week. The Unicorn, on the other hand lies on Thursdays, Fridays and Saturdays, but tells the truth on other days of the week.



- a) One day Alice met the Lion and the Unicorn resting under a tree. The following discourse ensued:

Lion : Yesterday was one of my lying days.

Unicorn : Yesterday was one of my lying days too.

Alice, who was a very bright girl, was able to deduce the day of the week. What day was it?

- b) On another occasion Alice met the lion alone. He made the following statements: "I lied yesterday", "I will lie again two days after tomorrow". What day of the week is it?
- c) On what days of the week is it possible for the Lion to make the following two statements: "I lied yesterday", "I will lie again tomorrow".
- d) On what days of the week is it possible for the lion to say "I lied yesterday and I will lie again tomorrow".

[Warning: The answer is *not* the same as the previous problem.]

Truth Tables

We've already seen truth tables which tell us the truth-values of the simple propositions

$$\neg\varphi, \quad \varphi \wedge \psi, \quad \varphi \vee \psi, \quad \varphi \rightarrow \psi, \quad \varphi \leftrightarrow \psi.$$

We can similarly construct a truth table for any wff.

In general, the number of rows in a truth table is determined by the number of atomic propositions in the formula or formulæ to be considered. If there is only one atomic proposition, then there are only two possibilities: the statement it stands for can either be true or false, hence the table will have two rows.

If there are two atomic propositions, then as we've already seen, there are four possible combinations of truth and falsity and consequently the table has four rows. In general, if the number of atomic propositions is n , the number of rows is 2^n . Thus if a formula contains three different atomic propositions, its truth table has $2^3 = 8$ rows, and so on.

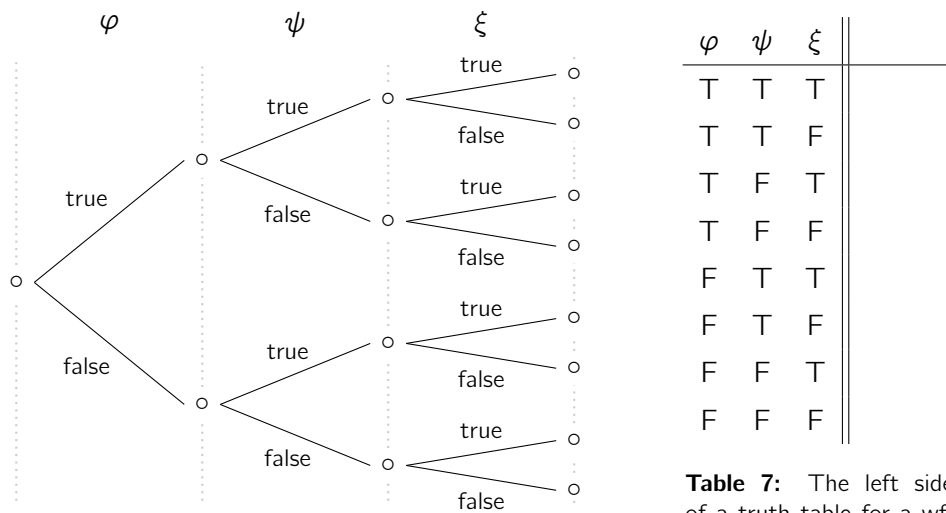


Figure 7: 8 possibilities with three atomic propositions φ , ψ and ξ

Table 7: The left side of a truth table for a wff containing three atomic propositions, φ , ψ and ξ

To set up a truth table for a formula, write the formula at the upper right side of the table and list the atomic propositions it contains in alphabetical order to the left. If there are n of them, write beneath the rightmost of them a column of 2^n alternating T's and F's, beginning with T. Then, under the next letter to the left (if any remain), write another column of 2^n T's and F's, again beginning with T, but alternating every two rows. Repeat this procedure, moving again to the left and doubling the alternation interval each time, until each letter has a column of T's and F's beneath it. If, for example, the formula contains three atomic propositions, φ , ψ , and ξ , the left side of the the table should resemble [table 7](#).

Then on the right-hand side of the table, write, *under each operator* in order of precedence (i.e., from the “low-hanging fruit” of the syntax tree, going upwards), the resulting truth-value in each case. Once you’ve filled in the final column (which corresponds to the root of the syntax tree), circle it, since this represents the truth-value of the whole expression.

Worked Example 1.22. Let’s start with something easy, say, the truth table for $\neg\neg\varphi$.

φ	$\neg\neg\varphi$
T	T
F	F

Table 8: Truth table for $\neg\neg\varphi$

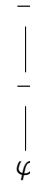


Figure 8: Syntax tree of $\neg\neg\varphi$

The table has two rows, since there is only one atomic proposition. The negation sign to the immediate left of φ is the first operator we come across when “climbing” the syntax tree, this reverses the values of φ in each row, and the negation sign to its left (which is the root of the tree) reverses them again, so that $\neg\neg\varphi$ has the same truth value as φ in every situation.

Remark 1.23 (Involution). When performing an operation (logical or otherwise), we say it is an *involution*, or *involutionary*, if doing it twice is equivalent to having done nothing at all. Thus, negation is involutory since $\neg\neg\varphi$ is equivalent to φ . Similarly in arithmetic, the minus prefix is an involution, since $-(-x)$ is the same as x . Rotation by 180° is also an involution, as is pressing the mute button on a TV remote control.

Worked Example 1.24. We construct the truth table for $\neg\varphi \vee \psi$.

φ	ψ	$\neg\varphi \vee \psi$
T	T	T
T	F	F
F	T	T
F	F	T

Table 9: Truth table for $\neg\varphi \vee \psi$

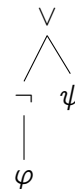


Figure 9: Syntax tree of $\neg\varphi \vee \psi$

Here we begin by computing the negation $\neg\varphi$, simply flipping the value of φ in each row. Then, we compare these negated values with the value of ψ in that row, computing their disjunction in the column below the \vee . This is the final result, so we circle it.

Remark 1.25. It is not necessary to present the syntax tree when computing truth tables, we provide them here just for explanatory purposes.

Definition 1.26 (Tautologies and Contradiction). If a proposition is always true, no matter the truth-value of its atomic propositions, then it is said to be a *tautology*. Similarly, if a proposition is always false, it is said to be a *contradiction*.

We can tell whether a proposition is a tautology from its truth table, since its final column will be entirely full of T's. Similarly, the final column of a contradiction will consist entirely of F's.

Remark 1.27. Saying that two propositions φ and ψ are equivalent to each other is the same as saying that $\varphi \leftrightarrow \psi$ is a tautology.

Worked Example 1.28. Let us give two more examples of truth tables.

(i) $(\varphi \vee \psi) \wedge \neg(\varphi \wedge \psi)$

φ	ψ	$(\varphi \vee \psi) \wedge \neg(\varphi \wedge \psi)$		
T	T	T	F	T
T	F	T	T	F
F	T	T	T	F
F	F	F	F	F

Table 10: Truth table of $(\varphi \vee \psi) \wedge \neg(\varphi \wedge \psi)$

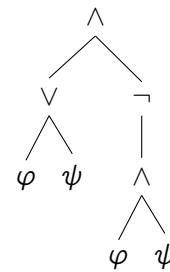


Figure 10: Syntax tree

(ii) $(\varphi \wedge \psi) \wedge \xi \leftrightarrow \varphi \wedge (\psi \wedge \xi)$

φ	ψ	ξ	$(\varphi \wedge \psi) \wedge \xi \leftrightarrow \varphi \wedge (\psi \wedge \xi)$				
T	T	T	T	T	T	T	T
T	T	F	T	F	T	F	F
T	F	T	F	F	T	F	F
T	F	F	F	F	T	F	F
F	T	T	F	F	T	F	T
F	T	F	F	F	T	F	F
F	F	T	F	F	T	F	F
F	F	F	F	F	T	F	F

Table 11: Truth table of $(\varphi \wedge \psi) \wedge \xi \leftrightarrow \varphi \wedge (\psi \wedge \xi)$

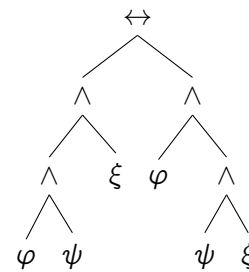


Figure 11: Syntax tree

Notice that this is an example of a tautology. In particular, this truth table shows the logical equivalence of the syntactically distinct statements $(\varphi \wedge \psi) \wedge \xi$ and $\varphi \wedge (\psi \wedge \xi)$ which we alluded to when discussing left- and right-associativity.

Exercise 1.29. 1. Construct truth tables for the following propositions. Say which of these are tautologies and contradictions.

- | | |
|--|--|
| a) $(\varphi \rightarrow \psi) \rightarrow (\psi \rightarrow \varphi)$ | b) $\varphi \wedge \psi \rightarrow \varphi \vee \psi$ |
| c) $\varphi \wedge \neg\varphi$ | d) $\varphi \vee (\psi \wedge \xi) \rightarrow (\varphi \vee \psi) \wedge \xi$ |
| e) $\varphi \vee (\psi \rightarrow \xi) \rightarrow \xi$ | f) $\neg\varphi \vee \neg\psi \rightarrow \varphi \vee \psi$ |


2. The following are important tautologies in propositional logic. Prove them using truth-tables, and explain in words why each of them is true, giving real-world examples to aid your explanation.

- | | |
|---|--------------------------------------|
| a) $\varphi \vee \neg\varphi$ | (Law of the Excluded Middle) |
| b) $\neg\neg\varphi \leftrightarrow \varphi$ | (Negation Involution) |
| c) $\neg(\varphi \rightarrow \psi) \leftrightarrow (\varphi \wedge \neg\psi)$ | (Negated Implication) |
| d) $\text{false} \rightarrow \varphi$ | (Principle of Explosion) |
| e) $\varphi \rightarrow \text{true}$ | (Principle of Absolute Truth) |
| f) $\varphi \wedge \psi \rightarrow \varphi$ | (Conjunction Elimination) |
| g) $\varphi \rightarrow \varphi \vee \psi$ | (Disjunction Introduction) |
| h) $(\varphi \rightarrow \psi) \wedge (\psi \rightarrow \xi) \rightarrow (\varphi \rightarrow \xi)$ | (Law of Syllogism) |
| i) $(\varphi \rightarrow \psi) \leftrightarrow (\neg\psi \rightarrow \neg\varphi)$ | (Law of Contrapositive) |
| j) $\varphi \vee (\psi \wedge \xi) \leftrightarrow (\varphi \vee \psi) \wedge (\varphi \vee \xi)$ | (\vee distributes over \wedge) |
| k) $\varphi \wedge (\psi \vee \xi) \leftrightarrow (\varphi \wedge \psi) \vee (\varphi \wedge \xi)$ | (\wedge distributes over \vee) |
| l) $\neg(\varphi \vee \psi) \leftrightarrow \neg\varphi \wedge \neg\psi$ | (De Morgan's Law for \vee) |
| m) $\neg(\varphi \wedge \psi) \leftrightarrow \neg\varphi \vee \neg\psi$ | (De Morgan's Law for \wedge) |

3. (Universal Logic Operator). Define a new logical operator \diamond by

$$(\varphi \diamond \psi) \leftrightarrow \neg\varphi \wedge \neg\psi.$$

- Construct a truth table for $\varphi \diamond \psi$.
- Show that $\neg\varphi \leftrightarrow \varphi \diamond \varphi$ and that $\varphi \wedge \psi \leftrightarrow (\varphi \diamond \varphi) \diamond (\psi \diamond \psi)$.
- Find a way of expressing $\varphi \vee \psi$ and $\varphi \rightarrow \psi$ using only the \diamond operator.

 4. (How computers add using logic). Define a new logical operator \oplus by

$$(\varphi \oplus \psi) \leftrightarrow \neg(\varphi \leftrightarrow \psi).$$

- Construct a truth table for $\varphi \oplus \psi$.
- Prove that $\varphi \oplus \psi \leftrightarrow (\varphi \wedge \neg\psi) \vee (\neg\varphi \wedge \psi)$.

- c) **Figure 12** depicts a digital circuit known as a *binary half-adder* which performs binary addition in a computer’s CPU. In a computer, **true** is represented by the value 1, and **false** is represented by the value 0. The addition of binary bits works using *carries*, as shown in **table 12**.

A	B	sum	carry
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

Table 12: Binary Addition

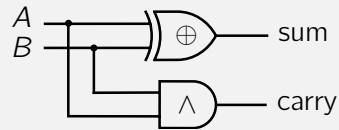


Figure 12: Binary Half-Adder

Express the sum and carry in **figure 12** as two propositions in terms of A and B , using the \oplus and \wedge operators. Hence, via truth-tables or otherwise, verify that the circuit behaves as desired by considering the different possible values (0 or 1) of A and B .

- d) A *binary full-adder* is a circuit which performs binary addition, but accepts a carry-in as well, which we shall denote by C_{in} , effectively adding three numbers together.

A	B	C_{in}	S	C_{out}
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

Table 13: Addition with C_{in}

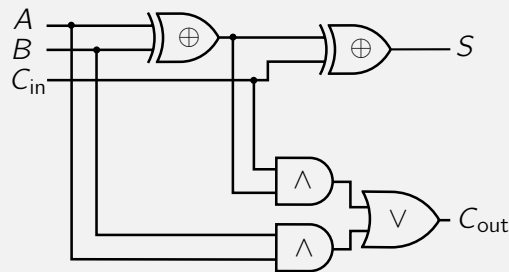


Figure 13: Binary Full-Adder

Let $S(A, B, C_{in})$ denote the sum output of the full binary-adder given inputs A , B and C_{in} , and similarly let $C(A, B, C_{in})$ denote the carry-out.³ Translate these into two propositions using the \oplus , \wedge and \vee operators by referring to the circuit in **figure 13**. Hence via truth-tables or otherwise, verify that the circuit behaves as desired.

- e) Full-binary adders may be connected in series to achieve what is known as a *ripple-carry adder*. This is how computers add numbers together!

Suppose we are working with 4-bit numbers, that is, binary numbers which are four digits long. To be able to refer to each digit, we will give each one a label by writing the entire 4-bit number as $A_4A_3A_2A_1$. So for example, if the number is 1010, then $A_4 = 1$, $A_3 = 0$, $A_2 = 1$ and $A_1 = 0$. Two 4-bit numbers $A_4A_3A_2A_1$ and $B_4B_3B_2B_1$ can be added together by using the following 4-bit ripple-carry adder:

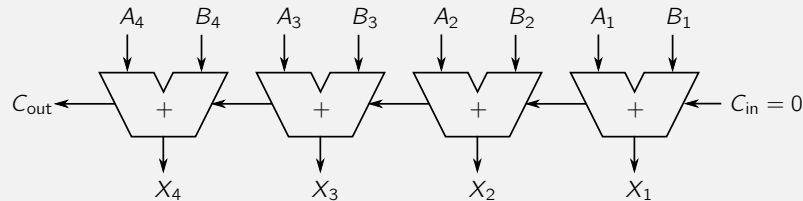


Figure 14: Ripple-carry adder, made up of four full-binary adders

The result is then the 4-bit number $X_4X_3X_2X_1$. This fact may seem like it came out of nowhere, but think of how similar it is to when we add two numbers normally. We start from the right, adding the last two digits of the numbers, and then pass any carries to the next column of digits, and so on until we are done. This is what is being done here, simply in binary, and by a circuit. Note that we start with a carry of zero, as we would when adding two numbers normally.

Express the digits X_1 , X_2 , X_3 and X_4 as propositions, using the two operators $S(A, B, C_{in})$ and $C(A, B, C_{in})$ we described before. Hence, by referring to [table 13](#) as the truth-table for these logical operators, work out $6 + 7$ in binary, given that 6 is 0110, and 7 is 0111.

³Note that these are regular logical operators which take three propositions as inputs instead of the usual one or two (such as \neg , \vee , \wedge , etc.).

2. Set Theory

A set is a *collection of distinct “objects”*. In particular, the defining characteristic of a set is the idea of *membership*—an object x is either a member of a set S , or not. We write $x \in S$ for “ x is an element of the set S ” (or x is in S), and similarly $y \notin S$ for the negation “ y is not an element of S ”. Sets may be defined by listing their elements between curly brackets, e.g.,

$$A = \{1, 2, 3, 4, 5\}$$

defines the set A whose elements are 1, 2, 3, 4 and 5. We have $1 \in A$, but $0 \notin A$ (for example). It is conventional to use capital letters for sets.

Standard Sets

Some of the important sets which we encounter are:

- The **empty set**, denoted by the symbol \emptyset , is the set such that

$$x \notin \emptyset \text{ for all } x.$$

- The set of **natural numbers**, denoted by the symbol \mathbb{N} , is the infinite set containing all positive whole numbers and zero:

$$\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}.$$

- The set of **integers**, denoted by the symbol \mathbb{Z} (for the German *zählen*, meaning *counting*), is the infinite set containing the positive whole numbers, the negative whole numbers and zero:

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}.$$

- The set of **rational numbers**, denoted by the symbol \mathbb{Q} (for *quotient*), is the set of all numbers which can be expressed as a ratio of two integers. For example, this set contains the numbers $\frac{1}{2}$, $\frac{22}{7}$, $-\frac{1}{3}$, 0 and 5 ($= \frac{5}{1}$).
- The set of **real numbers**, denoted by the symbol \mathbb{R} , contains all of the rational numbers, together with all the numbers which have infinitely many digits after the decimal point. Some of these are rational (e.g. $\frac{1}{3} = 0.333\dots$ and $\frac{1}{7} = 0.142857142\dots$), but others are *irrational*, that is, not rational (e.g. $\sqrt{2} = 1.41421\dots$, $\pi = 3.14159\dots$ and $e = 2.7182818\dots$).

It is not easy to see that some numbers are irrational. Later we will see a proof of the fact that $\sqrt{2}$ is irrational.

Subsets, Intervals and Set Comprehension

Notice that each of the sets we defined (\emptyset , \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R}) contains all the elements of the previous one. When a set B contains all the elements of A , or more formally, if

$$\text{For all } x, x \in A \rightarrow x \in B,$$

we say A is a *subset* of B and write $A \subseteq B$. For example, take the sets $A = \{1, 2, 3\}$ and $B = \{1, 2, 3, 4\}$, then $A \subseteq B$. We can visualise the two sets in what is often called a *Venn diagram*.

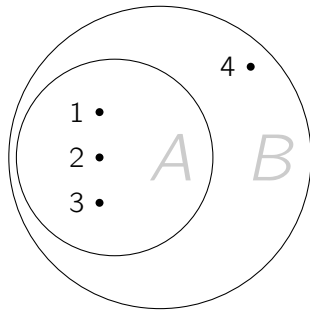


Figure 15: Venn Diagram for $A \subseteq B$

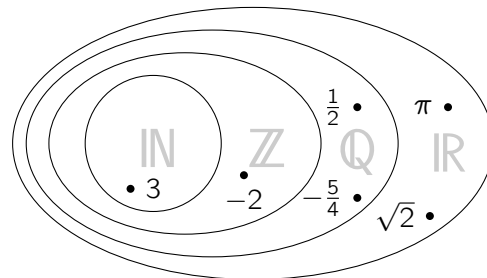


Figure 16: Venn Diagram for $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$

Remark 2.1. Note that by this definition, every set S is a subset of itself. Also note that it is not necessarily the case that for two given sets, one set is a subset of the other or vice-versa; for example if $C = \{2, 4, 6, 8\}$, we neither have $A \subseteq C$ nor $C \subseteq A$.⁴

If A contains every element of B , and B contains every element of A , that is, if both $A \subseteq B$ and $B \subseteq A$, we say that A is *equal to* B , written $A = B$. Equivalently, $A = B$ is the same as saying that for all x , $x \in A \leftrightarrow x \in B$. Observe that

$$\emptyset \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$$

but none of these are equal. In particular, by proving that $\sqrt{2} \in \mathbb{R}$ but $\sqrt{2} \notin \mathbb{Q}$, we will see that $\mathbb{Q} \neq \mathbb{R}$.

Remark 2.2. Do not confuse the two relations \in and \subseteq . Make sure you understand why each of the following are true.

- (i) $4 \in \{1, 2, 3, 4\}$ but $4 \notin \{1, 2, 3\}$
- (ii) $\{1, 2, 3\} \notin \{1, 2, 3, 4\}$ but $\{1, 2, 3\} \subseteq \{1, 2, 3, 4\}$
- (iii) $\{1\} \in \{\{1\}, \{1, 2\}, \{1, 2, 3\}\}$ but $\{1\} \not\subseteq \{\{1\}, \{1, 2\}, \{1, 2, 3\}\}$
- (iv) $\{1, 2\} \in \{1, 2, \{1, 2\}\}$ and $\{1, 2\} \subseteq \{1, 2, \{1, 2\}\}$

⁴Unlike the similar looking relation " \leq " for real numbers, where it *must* be the case that $x \leq y$ or $y \leq x$. Because of this, \subseteq is called a *partial order*, and \leq is called a *total order*.

Notation. An important group of notations we introduce are the subsets of real numbers called the **real intervals**:

- $[a, b]$ is the set of $x \in \mathbb{R}$ such that $a \leq x \leq b$
- $[a, b)$ or $[a, b[$ is the set of $x \in \mathbb{R}$ such that $a \leq x < b$
- $(a, b]$ or $]a, b]$ is the set of $x \in \mathbb{R}$ such that $a < x \leq b$
- (a, b) or $]a, b[$ is the set of $x \in \mathbb{R}$ such that $a < x < b$
- $[a, \infty)$ or $[a, \infty[$ is the set of $x \in \mathbb{R}$ such that $a \leq x$
- (a, ∞) or $]a, \infty[$ is the set of $x \in \mathbb{R}$ such that $a < x$
- $(-\infty, b]$ or $] - \infty, b]$ is the set of $x \in \mathbb{R}$ such that $x \leq b$
- $(-\infty, b)$ or $] - \infty, b[$ is the set of $x \in \mathbb{R}$ such that $x < b$

So for example, if x is a real number such that $1 \leq x \leq 2$, then $x \in [1, 2]$. If moreover, $x \neq 2$, then $x \in [1, 2)$. If y is a positive real number, then $y \in (0, \infty)$, whereas if y is a non-negative real number, then $y \in [0, \infty)$.

Exercise 2.3. 1. Consider the sets $A = \{1, 2, 3\}$, $B = \{2, 4, 6, 8\}$, $C = \{-1, 0, 1\}$ and $D = \{\sqrt{2}, e, \pi\}$. For each of the following, say whether they are true and false.

- | | | |
|--------------------------------|-------------------------------------|------------------------------------|
| a) $1 \in A$ | b) $\{1, 2\} \in A$ | c) $4 \notin A$ |
| d) $A \subseteq B$ | e) $A = C$ | f) $C \subseteq C$ |
| g) $D \subseteq \mathbb{Q}$ | h) $C \subseteq \mathbb{Z}$ | i) $\sqrt{2} \subseteq \mathbb{R}$ |
| j) $[-1, 2] \subseteq [-2, 2)$ | k) $(-3, 3) \subseteq [-3, \infty)$ | |

✠ JMJ ✠

Lecture 2
9 Oct 2024

Notation (Set Comprehension). Here we introduce an alternative notation to describe sets, instead of explicitly listing their elements. Suppose we want to describe the set of even numbers, E . Since there are infinitely many, in our current notation, we are forced to use ellipses (...) and let the reader deduce what the set contains:

$$E = \{\dots, -4, -2, 0, 2, 4, \dots\}.$$

There is a level of ambiguity with this notation however. Alternatively, using set comprehension, we write this as

$$E = \{2n : n \in \mathbb{Z}\},$$

where the colon is read “*such that*”. The whole expression is read as “ $E =$ the set of all things of the form $2n$, such that $n \in \mathbb{Z}$ ”; in other words, E is the set of even numbers. In general, the notation

$$X = \{x \in S : \varphi(x)\}$$

defines the set of all things “ x ” in S which satisfy the predicate $\varphi(x)$. For example, the set of prime numbers can be written as

$$P = \{n \in \mathbb{N} : n \text{ is prime}\}$$

or as

$$P = \{n : n \in \mathbb{N} \text{ and } n \text{ is prime}\}.$$

In general, there are many ways to express the same set using comprehension.

Examples 2.4. We give some examples of set comprehension.

$$\begin{aligned} \{n^2 : n \in \mathbb{N}\} &= \{0, 1, 4, 9, 16, \dots\} \\ \{5n : n \in \mathbb{Z}\} &= \{\dots, -5, 0, 5, 10, \dots\} \\ \{x \in \mathbb{R} : 1 \leq x \leq 2\} &= [1, 2] \\ \{x \in \mathbb{Q} : x + 2 = 1\} &= \{-1\} \\ \{x \in \mathbb{N} : x + 2 = 1\} &= \emptyset \\ \{2x : x \in \mathbb{R}\} &= \mathbb{R} \\ \{x \in \mathbb{R} : x > 0\} &= (0, \infty) \\ \{a/b : a, b \in \mathbb{Z} \text{ and } b \neq 0\} &= \mathbb{Q} \end{aligned}$$

Exercise 2.5. 1. Express the following sets by listing their elements. E.g., the set $\{2x+6y : x, y \in \mathbb{N}\}$ can be written as $\{0, 2, 6, 8, 10, 12, 14, 16, \dots\}$.

- | | |
|---|--|
| a) $\{4n + 1 : n \in \mathbb{Z}\}$ | b) $\{7n - 2 : n \in \mathbb{Z}\}$ |
| c) $\{n^2 : n \in \mathbb{Z}\}$ | d) $\{n \in \mathbb{Z} : -5 < n \leq 5\}$ |
| e) $\{n \in \mathbb{N} : -5 \leq n < 5\}$ | f) $\{x \in \mathbb{R} : x^2 = 5\}$ |
| g) $\{x \in \mathbb{Z} : x^2 = 3\}$ | h) $\{x \in \mathbb{R} : x^2 = 3 \text{ or } x^2 = 4\}$ |
| i) $\{q \in \mathbb{Q} : q = \frac{1}{1+n} \text{ and } n \in \mathbb{N}\}$ | j) $\{(a, b) : a \in \mathbb{N} \text{ and } b \in \mathbb{Z}\}$ |
| k) $\{5a + 2b : a, b \in \mathbb{Z}\}$ | l) $\{\{a, b\} : a \in \mathbb{N} \text{ and } b \in \{0, 1\}\}$ |

2. Write each of the following sets using set comprehension notation.

- | | |
|--|--|
| a) $\{10, 11, 12, 13, 14, 15, 16\}$ | b) $\{3, 5, 7, 9, 11, 13\}$ |
| c) $\{2, 4, 8, 16, 32, 64, \dots\}$ | d) $\{1, 9, 25, 49, 81, 121, \dots\}$ |
| e) $\{\dots, -14, -7, 0, 7, 14, \dots\}$ | f) $\{\dots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \dots\}$ |
| g) $\{\dots, -1, 3, 7, 11, 15, \dots\}$ | h) $\{\emptyset, \{0\}, \{0, 1\}, \{0, 1, 2\}, \dots\}$ |
| i) $\{\dots, -\frac{2\pi}{3}, -\frac{\pi}{3}, 0, \frac{\pi}{3}, \frac{2\pi}{3}, \dots\}$ | j) $\{1, 2, 3, 5, 6, 7, 9, 10, 11, \dots\}$ |
| ☺ k) $\{1, 1.1, 1.11, 1.111, \dots\}$ | ☺ l) $\{3, \{3\}, \{\{3\}\}, \{\{\{3\}\}\}, \dots\}$ |

Set Operations

Now, let us define some set operations, that is, ways to combine sets to create new sets.

Definitions 2.6. Suppose A and B are two sets. Then

- (i) The *union of A and B* , denoted $A \cup B$, is the set defined by the property

$$x \in A \vee x \in B \leftrightarrow x \in A \cup B.$$

- (ii) The *intersection of A and B* , denoted $A \cap B$, is the set defined by the property

$$x \in A \wedge x \in B \leftrightarrow x \in A \cap B.$$

- (iii) The *difference between A and B* , denoted $A \setminus B$, is the set defined by the property

$$x \in A \wedge x \notin B \leftrightarrow x \in A \setminus B.$$

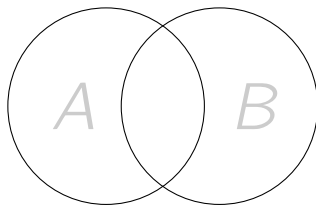


Figure 17: $A \cup B$

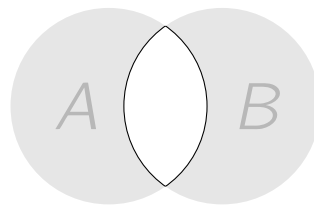


Figure 18: $A \cap B$

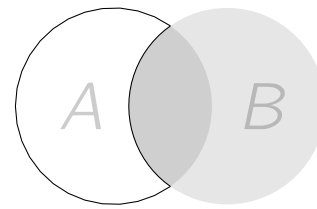


Figure 19: $A \setminus B$

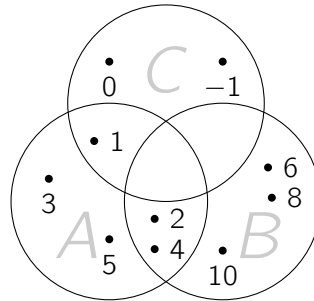


Figure 20: Sets in [Examples 2.7](#)

Examples 2.7. If $A = \{1, 2, 3, 4, 5\}$, $B = \{2, 4, 6, 8, 10\}$ and $C = \{-1, 0, 1\}$, then

$$A \cup B = \{1, 2, 3, 4, 5, 6, 8, 10\}$$

$$A \cap B = \{2, 4\}$$

$$A \setminus B = \{1, 3, 5\}$$

$$(A \cup B) \cap C = \{1, 2, 3, 4, 5, 6, 8, 10\} \cap \{-1, 0, 1\} = \{1\}$$

$$A \cup (B \cap C) = \{1, 2, 3, 4, 5\} \cup \emptyset = \{1, 2, 3, 4, 5\} = A$$

Notice that for any element x of A or B , we can summarise whether it is in $A \cup B$, $A \cap B$ or $A \setminus B$ using a table listing the four possible cases, as in [table 14](#). Indeed, it should

is it in A ?	is it in B ?	is it in $A \cup B$?	is it in $A \cap B$?	is it in $A \setminus B$?
✓	✓	✓	✓	✗
✓	✗	✓	✗	✓
✗	✓	✓	✗	✗
✗	✗	✗	✗	✗

Table 14: Table summarising behaviour for $A \cup B$, $A \cap B$ and $A \setminus B$

be clear that this is just a truth table, where instead of atomic propositions φ and ψ , this time we have the propositions $x \in A$ and $x \in B$ determining the truth/falsity of $x \in A \cup B$, $x \in A \cap B$ or $x \in A \setminus B$ (see [table 15](#)).

$x \in A$	$x \in B$	$x \in A \cup B$	$x \in A \cap B$	$x \in A \setminus B$
T	T	T	T	F
T	F	T	F	T
F	T	T	F	F
F	F	F	F	F

Table 15: Truth tables for $A \cup B$, $A \cap B$ and $A \setminus B$ in familiar format

We see that \cup and \cap behave identically to \vee and \wedge respectively, whereas \setminus is equivalent to a negated implication (i.e., $x \in A \setminus B \leftrightarrow \neg(x \in A \rightarrow x \in B)$). This is because of the definition of $A \setminus B$, indeed, one can check by truth table that $\neg(\varphi \rightarrow \psi) \leftrightarrow \varphi \wedge \neg\psi$.

One can easily prove various properties about these operators, most of them are very intuitive and follow immediately from the properties of the corresponding zeroth-order logic operators or (\vee), and (\wedge), and not (\neg).

Worked Example 2.8. We prove, using a truth table, that for any three sets A , B and C , we have $(A \cap B) \cap C = A \cap (B \cap C)$.

Indeed, this is the same as checking that for any x , the proposition $x \in (A \cap B) \cap C \leftrightarrow x \in A \cap (B \cap C)$ is a tautology. Using the rules above, we can construct a truth table to check whether this is a tautology, which we do in [table 16](#).

Remark 2.9. It is not difficult to actually construct the truth table, what we've done here is basically the same as in [worked example 1.28\(ii\)](#). The important thing is that you understand *why* constructing this truth table establishes that the two sets $A \cap (B \cap C)$ and $(A \cap B) \cap C$ are the same: the table shows that, depending on all

$x \in A$	$x \in B$	$x \in C$	$x \in (A \cap B) \cap C \leftrightarrow x \in A \cap (B \cap C)$					
T	T	T	T	T	T	T	T	
T	T	F	T	F	T	F	F	
T	F	T	F	F	T	F	F	
T	F	F	F	F	T	F	F	
F	T	T	F	F	T	F	T	
F	T	F	F	F	T	F	F	
F	F	T	F	F	T	F	F	
F	F	F	F	F	T	F	F	

Table 16: Truth table to prove that $A \cap (B \cap C) = (A \cap B) \cap C$

possible cases of whether or not any given element x is in A , B or C , then x will be in $A \cap (B \cap C)$ precisely when it is in $(A \cap B) \cap C$, and vice-versa. Thus, these two sets must consist of precisely the same elements, establishing their equality. Think of this truth table in terms of [table 14](#) if it makes things clearer.

You should also be capable of drawing a Venn diagram which shows that the region corresponding to $(A \cap B) \cap C$ is the same as $A \cap (B \cap C)$, as in [figure 21](#).

Worked Example 2.10. Let's give another example. Let's prove that for any set A , we have $A \setminus A = \emptyset$.

Thus, we need to prove that for any x , $x \in A \setminus A \leftrightarrow x \in \emptyset$. Recall that $x \in \emptyset$ is, by definition of \emptyset , always false, and that the behaviour of \setminus is summarised in [table 15](#). As can be seen in [table 17](#), $x \in A \setminus A \leftrightarrow x \in \emptyset$ is indeed a tautology, thus $A \setminus A = \emptyset$

$x \in A$	$x \in A \setminus A \leftrightarrow x \in \emptyset$		
T	F	T	F
F	F	T	F

Table 17: Truth table to prove that $A \setminus A = \emptyset$

for any set A .

Worked Example 2.11. Let's give one more example for good measure. We prove that for any two sets A and B , we have $A \setminus (A \setminus B) \subseteq A \cap B$.

This time, since it's \subseteq instead of $=$, we need to check (by definition of \subseteq) that if $x \in A \setminus (A \setminus B)$, then $x \in A \cap B$, i.e., that the proposition $x \in A \setminus (A \setminus B) \rightarrow x \in A \cap B$ is tautological. As we can see by [table 18](#), $x \in A \setminus (A \setminus B) \rightarrow x \in A \cap B$ is a tautology, therefore $A \setminus (A \setminus B) \subseteq A \cap B$.

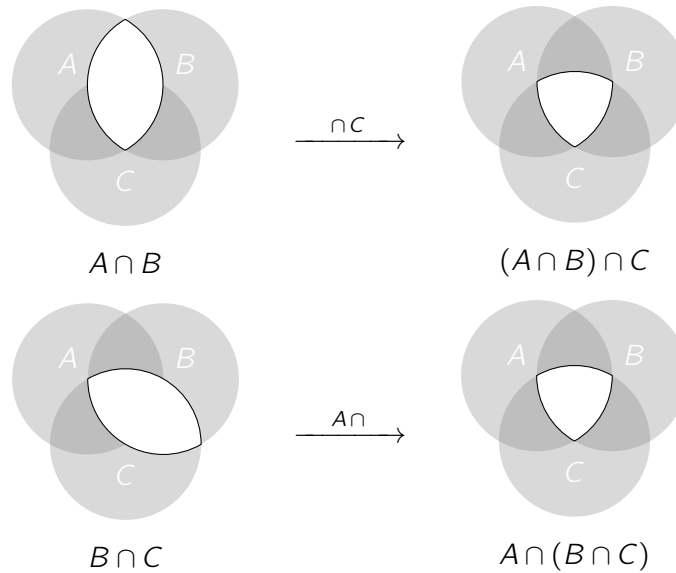


Figure 21: Venn Diagrams showing that $(A \cap B) \cap C$ and $A \cap (B \cap C)$ are the same set

$x \in A$	$x \in B$	$x \in A \setminus (A \setminus B) \rightarrow x \in A \cap B$			
T	T	T	F	T	T
T	F	F	T	T	F
F	T	F	F	T	F
F	F	F	F	T	F

Table 18: Truth table to prove that $A \setminus (A \setminus B) \subseteq A \cap B$

Below we give a reasonably comprehensive list of common properties concerning the operations we've introduced so far. They can all be proved using truth tables.

Proposition 2.12 (Union, Intersection, Difference Properties). *Let A, B and C be sets. Then*

- (i) $A \cup (B \cap C) = (A \cup B) \cap C$
- (ii) $A \cap (B \cup C) = (A \cap B) \cup C$
- (iii) $A \cup B = B \cup A$
- (iv) $A \cap B = B \cap A$
- (v) $A \cup \emptyset = A$
- (vi) $A \cap \emptyset = \emptyset$
- (vii) $A \cup A = A \cap A = A$
- (viii) $A \setminus \emptyset = A$
- (ix) $A \setminus A = \emptyset$
- (x) $A \setminus (A \setminus B) = A \cap B$
- (xi) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
- (xii) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
- (xiii) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- (xiv) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Other useful laws are known as the complement laws, where we assume that we have some all-encompassing *universal set* Ω . This allows us to have what can be thought

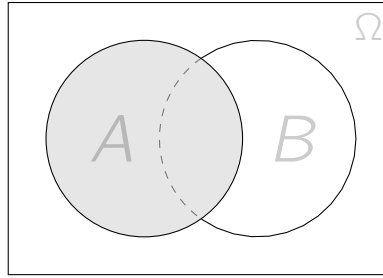


Figure 22: \bar{A}

of as the set theoretic analogue to negation (\neg), just as \cap and \cup are clearly analogues of \wedge and \vee . The complement of A is just $\Omega \setminus A$, i.e., “everything except for what’s in the set A ”, where the term “everything” here is always within the confines of the universal set.

Proposition 2.13 (Complement Laws). *If Ω is a set, $A, B, C \subseteq \Omega$ and the notation \bar{S} denotes $\Omega \setminus S$ for any set S , then*

- (i) $\overline{A \cup B} = \bar{A} \cap \bar{B}$
- (ii) $\overline{A \cap B} = \bar{A} \cup \bar{B}$
- (iii) $A \cup \bar{A} = \Omega$
- (iv) $A \cap \bar{A} = \emptyset$
- (v) $\overline{\Omega} = \emptyset$
- (vi) $\overline{\emptyset} = \Omega$
- (vii) If $A \subseteq B$, then $\bar{B} \subseteq \bar{A}$
- (viii) $\overline{\bar{A}} = A$
- (ix) $A \setminus B = A \cap \bar{B}$
- (x) $\overline{A \setminus B} = \bar{A} \cup B$
- (xi) $\bar{A} \setminus \bar{B} = B \setminus A$

Proof. We give a proof of (i), and leave the rest as an exercise.

For (i), we need to show that $\overline{A \cup B} = \bar{A} \cap \bar{B}$, i.e., $\Omega \setminus (A \cup B) = (\Omega \setminus A) \cap (\Omega \setminus B)$. Since all relevant sets are subsets of Ω , we have that “ $x \in \Omega$ ” is true in all cases. Table 19 shows that we have the required tautology. □

$x \in A$	$x \in B$	$x \in \Omega \setminus (A \cup B) \leftrightarrow x \in (\Omega \setminus A) \cap (\Omega \setminus B)$								
T	T	T	F	T	T	T	F	F	T	F
T	F	T	F	T	T	T	F	F	T	T
F	T	T	F	T	T	T	T	F	T	F
F	F	T	T	F	T	T	T	T	T	T

Table 19: Truth table to prove that $\overline{A \cup B} = \bar{A} \cap \bar{B}$

Remark 2.14. Even though $\Omega \setminus A$ is a composite operation on the set A (in the sense that it is made up of Ω and \setminus), it is faster, when constructing a truth table, to think

of “ $\Omega \setminus$ ” as a single operator on a given set, because it behaves identically to \neg (see [table 20](#)).

$x \in A$	$x \in \Omega \setminus A$
T	F
F	T

Table 20: Truth tables for $\Omega \setminus A$

Worked Example 2.15. Let’s give one last example to demonstrate the observation above, we’ll prove (vii) from [proposition 2.13](#). Let’s translate this into a proposition with logic symbols. We need to show that if $A \subseteq B$, then $\bar{B} \subseteq \bar{A}$, i.e., $A \subseteq B \rightarrow (\Omega \setminus B \subseteq \Omega \setminus A)$, i.e., $(x \in A \rightarrow x \in B) \rightarrow (x \in \Omega \setminus B \rightarrow x \in \Omega \setminus A)$. The required

$x \in A$	$x \in B$	$(x \in A \rightarrow x \in B) \rightarrow (x \in \Omega \setminus B \rightarrow x \in \Omega \setminus A)$	\mathbf{T}	F	T	F
T	T	T	T	F	T	F
T	F	F	T	T	F	F
F	T	T	T	F	T	T
F	F	T	T	T	T	T

Table 21: Truth table to prove [proposition 2.13\(vii\)](#)

truth table can be seen in [table 21](#).

We’ll conclude this section with the notion of a power set.

Definition 2.16. Given a set A , the *power set of A* is the set

$$\{A : A \subseteq X\}$$

of all subsets of X and is denoted by $\wp X$.

Example 2.17. For example,

$$\wp\{1, 2, 3\} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

and

$$\begin{aligned} \wp\wp\{1, 2\} = & \{\emptyset, \{\emptyset\}, \{\{1\}\}, \{\{2\}\}, \{\{1, 2\}\}, \{\emptyset, \{1\}\}, \{\emptyset, \{2\}\}, \\ & \{\emptyset, \{1, 2\}\}, \{\{1\}, \{2\}\}, \{\{1\}, \{1, 2\}\}, \{\{2\}, \{1, 2\}\}, \\ & \{\emptyset, \{1\}, \{2\}\}, \{\emptyset, \{1\}, \{1, 2\}\}, \{\emptyset, \{2\}, \{1, 2\}\}, \\ & \{\{1\}, \{2\}, \{1, 2\}\}, \{\emptyset, \{1\}, \{2\}, \{1, 2\}\} \end{aligned}$$

Notice that $B \subseteq A$ if and only if $B \in \wp A$, and $A \not\subseteq \wp A \not\subseteq \wp\wp A$, etc.

Exercise 2.18. 1. Consider the sets $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$, $B = \{2, 4, 6, 8, 10, 12, 14\}$, and $C = \{2, 3, 6, 9\}$. Determine:

- | | | |
|------------------------|--|--------------------|
| a) $A \cup B$ | b) $A \cap B$ | c) $B \cup C$ |
| d) $A \setminus C$ | e) $B \cap C$ | f) $B \setminus A$ |
| g) $A \setminus B$ | h) $A \cap C$ | i) $C \setminus B$ |
| j) $C \cup (B \cap A)$ | k) $(A \setminus B) \cup (B \setminus C) \cup (C \setminus A)$ | |
| l) $\wp(A \cap C)$ | | |

2. Let $X = \{4, 7, 2, 1\}$, $Y = \{4, 6, 12, 7, 3\}$ and $Z = \{0, 1, 2\}$. Determine:

- | | | |
|--|------------------------|---|
| a) $X \cup Y$ | b) $X \setminus Y$ | c) $(X \setminus Y) \cup (Y \setminus X)$ |
| d) $X \cap Y \cap Z$ | e) $X \cup (Y \cap Z)$ | f) $(X \cup Y) \cap Z$ |
| g) $X \setminus (Y \setminus (Z \setminus X))$ | | |

3. Let A , B and C be sets. Draw Venn diagrams and shade the appropriate regions to illustrate the following.

- | | | |
|--|---------------------------------|---------------------------------|
| a) A | b) $B \setminus A$ | c) $(A \setminus B) \cap C$ |
| d) $(A \cup B) \setminus C$ | e) $A \cup (B \cap C)$ | f) $(A \cup B) \cap (A \cup C)$ |
| g) $A \cap (B \cup C)$ | h) $(A \cap B) \cup (A \cap C)$ | |
| i) Based on (e) and (f), is $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$? | | |
| j) Based on (g) and (h), is $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$? | | |

4. Prove the facts in [proposition 2.12](#) using truth tables.

5. Prove the facts in [proposition 2.13](#) using truth tables.

6. Prove the following propositions about sets.

- | | |
|---|---|
| a) $A \cap B = \emptyset \leftrightarrow B \setminus A = B$ | b) $A \subseteq B \leftrightarrow A \cap B = A$ |
| c) $A \subseteq B \leftrightarrow A \setminus B = \emptyset$ | d) $A \setminus (A \setminus B) \subseteq B$ |
| e) If $A \subseteq C$, $B \subseteq C$ and $C \setminus A \subseteq B$, then $C = A \cup B$ | |

Predicate Logic

A *predicate* captures the idea of a proposition with “holes”. For instance, consider the propositions:

- (i) 4 is an even number,
- (ii) 8 is an even number,
- (iii) 5 is an even number.

We can identify these as different instances of the predicate

$$\varphi(x) = \text{“}x \text{ is an even number”},$$

where x is a “hole” we plug things into; we call x a *variable*. Indeed, we would write (i) as $\varphi(4)$, (ii) as $\varphi(8)$ and (iii) as $\varphi(5)$. Notice that for different values of x , the predicate is sometimes true, and sometimes false. The distinction between a proposition and a predicate is that a proposition has no variables; for instance, “Today is a Monday” is a proposition, whereas “ x is a Monday” is a predicate.

Sometimes we deal with statements like “there is at least one x such that $\varphi(x)$ is true” or “for every x , $\varphi(x)$ is false”. In such statements, x is usually understood to be a member of some set.

This leads us to introduce two new kinds of statements.

Definition 2.19 (Universally quantified statement). Let $\varphi(x)$ be a predicate, and let X be a set. Then the universal statement $\forall x \in X, \varphi(x)$ (read: “for all $x \in X$, $\varphi(x)$ ”) is the statement defined to be true so long as $\varphi(x)$ holds for each $x \in X$, and false otherwise.

For example, if $\varphi(n)$ is “ n can be factorised into a product of prime numbers”, then $\forall n \in \mathbf{IN}, \varphi(n)$ is the statement “for all $n \in \mathbf{IN}$, n can be factorised into a product of prime numbers”; or, more succinctly, “all natural numbers can be factorised into a product of prime numbers”.

Remark 2.20 ($\forall = \wedge$). A universally quantified statement is equivalent to (possibly infinitely many) \wedge ’s chained together. In the example we gave about primes, we can think of it as $\varphi(0) \wedge \varphi(1) \wedge \varphi(2) \wedge \varphi(3) \wedge \dots$.

Definition 2.21 (Existentially quantified statement). Let $\varphi(x)$ be a predicate, and let X be a set. Then the existential statement $\exists x \in X: \varphi(x)$ (read: “there exists $x \in X$ such that $\varphi(x)$ ”) is the statement defined to be true so long as $\varphi(x)$ holds for at least one $x \in X$, and false otherwise.

Example 2.22. If $\varphi(n)$ is “ n is the sum of three squares” and $S = \{n \in \mathbf{IN} : 1 \leq n \leq 15\}$, then $\exists n \in S : \varphi(n)$ is a true statement (since, e.g., $14 = 1^2 + 2^2 + 3^2$).

Remark 2.23 ($\exists = \vee$). An existentially quantified statement is equivalent to (possibly infinitely many) \vee 's chained together. In the example we gave, we can think of it as $\varphi(1) \vee \varphi(2) \vee \varphi(3) \vee \cdots \vee \varphi(15)$.

Remark 2.24 (Dummy Variables). When a predicate is quantified, i.e., when one of \forall or \exists is placed in front of a predicate $\varphi(x)$, the result is no longer a predicate, but becomes a proposition. This is because there is no longer a variable which can be substituted for. For example, if $\varphi(x)$ is “I rolled an x on the dice” where $x \in D = \{1, 2, 3, 4, 5, 6\}$, then we can substitute a value for x in $\varphi(x)$ (e.g., $\varphi(4)$ is “I rolled a 4 on the dice”), but

$$\begin{aligned} \exists x \in D : \varphi(x) \text{ is } & \varphi(1) \vee \varphi(2) \vee \varphi(3) \vee \varphi(4) \vee \varphi(5) \vee \varphi(6), \\ \text{i.e., I rolled a 1 or I rolled a 2 or, } & \dots, \text{ or I rolled a 6,} \end{aligned}$$

which contains no variable. In this context, x is called a *dummy variable*, because it appears in the notation $\forall x \in D, \varphi(x)$ but there isn't actually a variable there.

This is analogous to how $\int_1^{10} \frac{dt}{t}$ and $\sum_{i=1}^{10} i^2$ are both numbers, even though they look like they contain variables.

Negation of Quantified Statements. Suppose I make the universal statement “All the cars in the world are red”. In order to disprove my claim, all you need to do is to prove the existence of a car that is not red.

In other words, if C is the set of cars in the world, then

$$\neg(\forall c \in C, c \text{ is red}) \quad \leftrightarrow \quad \exists c \in C : \neg(c \text{ is red}).$$

And in general, we have the rules

$$\begin{aligned} \neg\forall x \in X, \varphi(x) & \leftrightarrow \exists x \in X : \neg\varphi(x) \\ \neg\exists x \in X, \varphi(x) & \leftrightarrow \forall x \in X : \neg\varphi(x) \end{aligned}$$

Example 2.25. The negation of $\forall x \in \mathbb{R}, x^2 \geq 0$ is $\exists x \in \mathbb{R} : x^2 < 0$.

Remark 2.26. Recall that we have seen the following tautologies about negated statements:

$$\begin{aligned} \neg(\neg\varphi) & \leftrightarrow \varphi & \neg(\varphi \wedge \psi) & \leftrightarrow \neg\varphi \vee \neg\psi & \neg(\varphi \vee \psi) & \leftrightarrow \neg\varphi \wedge \neg\psi \\ \neg(\varphi \rightarrow \psi) & \leftrightarrow \varphi \wedge \neg\psi \end{aligned}$$

They do come in handy when negating quantified statements.

Example 2.27. The negation of “For all $x, y \in \mathbb{R}$, if $x - y < 2$, then $f(x) - f(y) < 4$ ” becomes “there exist $x, y \in \mathbb{R}$ such that $x - y < 2$ but $f(x) - f(y) \geq 4$ ”.

Remark 2.28. (i) Sometimes we write things like $\forall x, y, z \in \mathbb{R}, \varphi(x, y, z)$. Instead of $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, \forall z \in \mathbb{R}, \varphi(x, y, z)$.

(ii) We also write things like $\forall \epsilon > 0$ rather than $\forall \epsilon \in (0, \infty)$. In general, we tend to assume a variable introduced by an inequality like this is a real number (as opposed to an integer or rational number greater than 0).

(iii) The order of quantifiers matters! Let M be the set of men, and W be the set of women. Let $\varphi(m, w)$ be the statement “ m and w will be happy together”. The statements $\forall m \in M, \exists w \in W : \varphi(m, w)$ and $\exists w \in W : \forall m \in M, \varphi(m, w)$ mean different things. In the first one, since m is introduced before w , then w may depend on m (i.e., w may be different for different m ’s). In the second one, w is introduced before m , so we are talking about the same woman for each man!

This is analogous to how we can do things like:

```
for(i=0; i<10; i++)
    for(j=i, j<10; j++)
        printf("%d", i+j);
```

Notice that the second for-loop depends on a variable introduced by the first one; we cannot swap the for-loops.

Exercise 2.29. 1. a) What is the difference between a proposition and a predicate?

b) Explain the difference between the statements

$$\forall n \in \mathbb{N}, \exists m \in \mathbb{N} : n < m \quad \text{and} \quad \exists m \in \mathbb{N} : \forall n \in \mathbb{N}, n < m.$$

Which of the two is correct?

c) Let the predicate φ be “ $n(n+1) \leq 30$ ”. Write out $\forall n \in \{n \in \mathbb{N} : n \leq 5\}, \varphi(n)$ as a proposition, and determine whether it is true.

2. Negate the following statements.

a) $\forall x > 1, x^2 > x$

b) $\exists x, y > 0 : x + y < 2\sqrt{xy}$

c) $\forall a \in \mathbb{N}, \exists b \in \mathbb{N} : a^2 = b$

d) $\forall n \in \mathbb{N}, \exists a, b, c, d \in \mathbb{N} : n = a^2 + b^2 + c^2 + d^2$

e) $\forall a, b, c \in \mathbb{R}, \exists x_1, x_2 \in \mathbb{R} : ax_1^2 + bx_1 + c = ax_2^2 + bx_2 + c = 0.$

f) $\forall \epsilon > 0, \exists N \in \mathbb{N} : \forall n \geq N, a - \epsilon < a_n < a + \epsilon$

g) $\forall \epsilon > 0, \exists \delta > 0 : |x - x_0| < \delta \rightarrow |f(x) - f(x_0)| < \epsilon.$

h) $\exists x \in A : \forall y \in B, \exists z \in C : x + y + z = 3\sqrt[3]{xyz}$

3. Proofs

✠ JMJ ✠

Lecture 3
14 Oct 2024

The day-to-day job of mathematicians (such as myself) is to come up with proofs for mathematical statements, all of which can essentially be formulated using the symbols we've learned over the last two chapters.

Even though the symbols of logic and set theory are essential to “speak” the language of mathematics, we tend to prefer writing things like “every even number $N \geq 4$ can be expressed as the sum of two primes”, as opposed to

$$\forall N \in \mathbf{IN}, \text{even}(N) \wedge (N \geq 4) \rightarrow \exists p, q \in \mathbf{IN} : \text{prime}(p) \wedge \text{prime}(q) \wedge (N = p + q).$$

We feel confident of the fact that, if necessary, we can encode every single mathematical theorem in terms of these symbols, so that mathematics is based on a rock solid, formal, logical foundation. But insisting on using them exclusively is a bit like insisting we only program a computer using 1s and 0s, namely, it is a bit limiting.

Take for instance, the fundamental theorem of calculus (i.e., the fact that integration and differentiation are opposites): for any differentiable function f defined on $[a, b]$, we have

$$\int_a^b f'(x) dx = f(b) - f(a).$$

If we wanted to, we could encode this high-level statement in terms of logical symbols, and give a proof using only logical symbols. In fact, there are many online projects dedicated to doing precisely so, you can find one of them [here](#). Every step is justified by something you can click on, and you can keep clicking till you end up at the very “bottom”, down with the axioms of propositional and predicate logic.

Optional Discussion: How are logic and set theory enough?

A natural question which might come to you at this stage is—“but how can we encode integrals as sets or propositions, aren't they an entirely separate type of ‘object’?”. Indeed, take a simpler proposition which we've seen already: $1 + 1 = 2$. Here we're using the symbol $=$ which we've defined in terms of \subseteq , but what about '1', '2', and $+$? Are these different ‘objects’ to sets and propositions?

In formal mathematics, the answer is actually no—we try to encode everything using sets—and when we say everything, we mean *everything*. There are very important reasons for this: we like to think that all mathematical statements live in the same axiomatic system (usually called the [ZF\(C\) universe](#)), this way, all of mathematics is built on only 9 axioms of set theory. For instance, take the natural numbers,

$$\mathbf{IN} = \{0, 1, 2, 3, 4, \dots\}.$$

What are these numbers exactly? Can we think of them as being “constructed”

from a more basic kind of object? The answer is yes, and in mathematics, we choose sets to be our building blocks for everything else.

What are numbers exactly? Formally, we define the set \mathbf{IN} as the *closure* of the set $\{\emptyset\}$ under the successor operation $x \mapsto x \cup \{x\}$. This means that \mathbf{IN} is the smallest set containing \emptyset , together with any other set(s) which can be obtained by repeatedly applying the operation $x \mapsto x \cup \{x\}$. The successor of each natural number represents the next natural number in the usual order, so identifying 0 with the empty set, we have

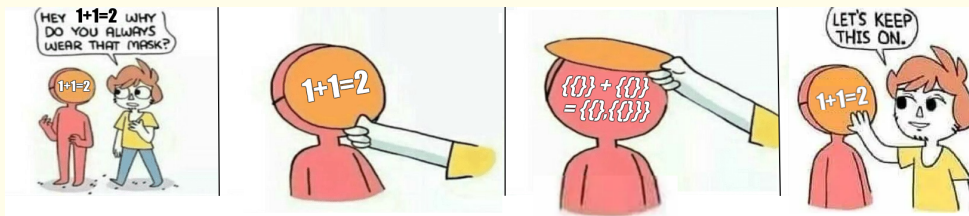
$$\begin{aligned} 0 &= \emptyset \\ 1 &= 0 \cup \{0\} = \emptyset \cup \{0\} = \{0\} = \{\emptyset\} \\ 2 &= 1 \cup \{1\} = \{0, 1\} = \{\emptyset, \{\emptyset\}\} \\ 3 &= 2 \cup \{2\} = \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\ 4 &= 3 \cup \{3\} = \{0, 1, 2, 3\}, \end{aligned}$$

and so on. In general, each natural number k ends up being structurally represented as the set of all its predecessors:

$$k = \{0, 1, 2, \dots, k - 1\}.$$

There is nothing inherently special about this way of encoding \mathbf{IN} . This is just one of many ways to construct a set which captures the behaviour of \mathbf{IN} , namely, a set where we have

- a least element 0, (i.e., \emptyset), and
- a way to always “add 1” (i.e., the successor operation $x \mapsto x \cup \{x\}$).



When encoded this way, the natural numbers are called [von Neumann ordinals](#). The two properties above capture entirely the essence of the natural numbers, and by constructing an object which behaves this way, we showed that it is possible to encode \mathbf{IN} with sets alone, and we don't need to think of numbers as autonomous “objects” in their own right.^a One can define a notion of “addition” and “multiplication” and so on, all in terms of the underlying set representations, and prove things like $1 + 1 = 2$ (refer to the “meme” above). But of course in

practice, we still think of the natural numbers as usual, only now safer in the knowledge that they are built on a more fundamental idea which we understand well. Similarly, we can construct \mathbb{Z} , \mathbb{Q} and \mathbb{R} in terms of sets alone, but we will not get into that here.

^aThis is analogous to how any photo, video or text on a computer is just 1s and 0s at the lowest level, but we still don't think about them in terms of 1's and 0's!

Types of Proof

Direct Proof. A direct (or deductive) proof of a statement ω begins from some previously proven statement α , and demonstrates step by step, that $\alpha \rightarrow \beta$, then that $\beta \rightarrow \gamma$, and so on, obtaining the chain of implications

$$\alpha \rightarrow \beta \rightarrow \gamma \rightarrow \cdots \rightarrow \omega.$$

To prove a conditional statement $\varphi \rightarrow \psi$, we assume that φ is true, and continue as above to show that ψ is true.

Proof by Contrapositive. In order to prove $\varphi \rightarrow \psi$, assume that ψ is false and show that this implies φ is also false. This will be a proof of $\neg\psi \rightarrow \neg\varphi$, which is logically equivalent to $\varphi \rightarrow \psi$.

Proof by Contradiction. To prove a statement φ , assume that it is false, and deduce from this assumption a false statement, i.e., prove that $\neg\varphi \rightarrow \text{false}$. This is logically equivalent to φ .

To prove a conditional statement $\varphi \rightarrow \psi$ by contradiction, assume that $\neg(\varphi \rightarrow \psi)$, i.e., assume that $\neg\varphi \wedge \psi$, and show that you get a contradiction.

Examples 3.1. Let us give a proof of each kind for two simple statements.

(i) If $x^2 - 3x + 2 < 0$, then $x > 0$.

Direct Proof. We have

$$\begin{aligned} x^2 - 3x + 2 < 0 &\implies 3x > 2 + x^2 && (+ 3x \text{ both sides}) \\ &\implies 3x > 2 && (\text{since } x^2 \geq 0) \\ &\implies x > 2/3 && (\div 3 \text{ both sides}) \\ &\implies x > 0. && \square \end{aligned}$$

Proof by Contrapositive.

$$\begin{aligned} x \leq 0 &\implies x - 1 < 0 \wedge x - 2 < 0 \\ &\implies (x - 1)(x - 2) > 0 && (a, b < 0 \implies ab > 0) \\ &\implies x^2 - 3x - 2 \geq 0. && \square \end{aligned}$$

Proof by Contradiction. Suppose that $x^2 - 3x + 2 < 0$, and (for contradiction) that $x \leq 0$. Then

$$x^2 < 3x - 2 \implies x^2 < -2 \quad (\text{since } x \leq 0 \implies 3x \leq 0),$$

which is impossible. □

(ii) For any two positive real numbers x and y , $\frac{x}{y} + \frac{y}{x} \geq 2$.

Direct Proof. Let x and y be two positive real numbers. Then

$$\begin{aligned} \frac{x}{y} + \frac{y}{x} &= \frac{x^2 + y^2}{xy} \\ &= \frac{x^2 + y^2 - 2xy + 2xy}{xy} \\ &= \frac{(x - y)^2}{xy} + 2 \geq 2, \quad \left(\frac{(x-y)^2}{xy} \geq 0 \text{ since } x, y > 0\right) \end{aligned}$$

which completes the proof. □

We can't really give a contrapositive proof of this statement, since it isn't a conditional (if... then...) statement.

Proof by contradiction. Let x and y be two positive real numbers, and assume (for contradiction) that

$$\begin{aligned} \frac{x}{y} + \frac{y}{x} < 2 &\implies \frac{x^2 + y^2}{xy} < 2 \\ &\implies x^2 + y^2 < 2xy \quad (\text{since } xy > 0) \\ &\implies (x - y)^2 < 0, \end{aligned}$$

which is nonsense. □

Example 3.2. Let us prove the following biconditional statement.

$$x = 2 \quad \text{if and only if} \quad x^3 + x = 2(x^2 + 1).$$

Since this is a biconditional statement (\Leftrightarrow), we need to prove two conditional statements, namely, the both directions (\Rightarrow and \Leftarrow). We will give a direct proof for both.

Proof. (\Rightarrow). This is the easy direction, we simply need to show that assuming $x = 2$, the equation on the right is true. Indeed,

$$\begin{aligned} \text{LHS} &= x^3 + x = 2^3 + 2 = 8 + 2 = 10 \\ \text{RHS} &= 2(x^2 + 1) = 2(2^2 + 1) = 2 \cdot 5 = 10, \end{aligned}$$

and thus LHS = RHS, as required.

(\Leftarrow). For this direction, we need to show that if the equation holds, it must follow that x is 2. Essentially, we need to solve the equation.

$$\begin{aligned}
 & x^3 + x = 2(x^2 + 1) \\
 \implies & x^3 - 2x^2 + x - 2 = 0 \\
 \implies & x^2(x - 2) + (x - 2) = 0 \\
 \implies & (x - 2)[x^2 + 1] = 0 \\
 \implies & x - 2 = 0 \quad \text{or} \quad x^2 + 1 = 0 \quad (\text{since } \mathbb{R} \text{ is an integral domain}^5) \\
 \implies & x = 2 \quad \text{or} \quad x^2 = -1 \\
 \implies & x = 2 \quad \text{or} \quad \text{false} \quad (\text{squares are always } \geq 0) \\
 \implies & x = 2, \quad (\varphi \vee \text{false} \rightarrow \varphi)
 \end{aligned}$$

which completes the proof. □

Remark 3.3 (\Leftarrow but \Rightarrow ?). Don't be confused about the direction of the arrows in the second part of the proof, the argument is still in the right direction, i.e., we started from $x^3 + x = 2(x^2 + 1)$ and concluded that $x = 2$:

$$x = 2 \Leftarrow \dots \Leftarrow x^3 - 2x^2 + x - 2 = 0 \Leftarrow x^3 + x = 2(x^2 + 1).$$

$\sqrt{2}$ is irrational

Let us give a few more examples. But first, we need to give some definitions.

Definition 3.4 (Divides). We say that an integer a *divides* another integer b , written $a \mid b$, if there exists an integer d such that $b = ad$. We also say that a is a *factor* of b , that b is a *multiple* of a , or that b is *divisible* by a .

We say that a number is *even* if it is divisible by 2, and we say it is *odd* otherwise. It can be shown (by induction, which we will cover shortly) that odd numbers are precisely those numbers which can be written in the form $2k + 1$ for some integer k .

Example Theorem 3.5. *The sum of two even numbers is even.*

Proof. Suppose a and b are two even numbers. Then they are divisible by 2, i.e., $a = 2k$ and $b = 2\ell$ for appropriate integers k and ℓ . But their sum is then

$$a + b = 2k + 2\ell = 2(k + \ell),$$

which is clearly divisible by two. □

⁵An *integral domain* is a fancy name for a structure where if the product of two things is zero, then one of them must be zero. This is not always the case, e.g., for matrices, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, so a product of two non-zero matrices can be the zero matrix.

More generally, we have the following.

Example Theorem 3.6. *Let $n, a, b \in \mathbb{Z}$. If $n \mid a$ and $n \mid b$, then $n \mid (a + b)$.*

Proof. If $n \mid a$, then $a = nk$ for some $k \in \mathbb{Z}$, and similarly, if $n \mid b$, then $b = n\ell$ for some $\ell \in \mathbb{Z}$. Thus

$$a + b = nk + n\ell = n(k + \ell),$$

which is clearly divisible by n . □

Activity 3.7 (You try!). Show that the sum of any five consecutive integers is divisible by 5.

Remark 3.8 (Theorem vs Proposition vs Lemma). We've been using the term *theorem* so far, this is essentially another word for a true statement or true proposition. When reading mathematics, if something is labelled as a theorem, it is probably an important statement. By contrast, a *proposition* (when the term appears in mathematical literature) tends to be less important, and a *lemma* is usually just used as a stepping stone to something more important.

Logically speaking, they all mean the same thing, namely, “a true statement”—you can think of it as being similar to the difference in a novel between the protagonist, a secondary character and a character that appears only once over a couple of pages.

Lemma 3.9. *Suppose $n \in \mathbb{Z}$. If n^2 is even, then n is even.*

Proof. We prove this by contrapositive: if n is *not even*, then n^2 is *not even*, i.e., if n is odd, then n^2 is odd. Indeed, if n is odd, then we can write it as $2k + 1$ for some k . But then

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

i.e., n^2 is of the form $2m + 1$ for some integer m , which shows that n^2 is odd. □

Remark 3.10. Try to get a feel as to why it makes sense to prove this by contrapositive. It's easier to make an assumption about n , and then see what happens to n^2 , than going in the other direction.

✠ JMJ ✠

Lecture 4
21 Oct 2024



Now let's address the title of this section—the fact that $\sqrt{2}$ is irrational. It is not easy to convince students that there are irrational numbers. The ancient Greeks, in particular, the Pythagoreans, believed that numbers were either *whole* (i.e., integers) or *parts of a whole* (i.e., rationals). This seems perfectly reasonable. Pythagoras is famous for his theorem relating the lengths of sides in a right-angled triangle,⁶ and

⁶Although there is evidence which suggests that the theorem was known to the Babylonians before Pythagoras.

perhaps the simplest case we can consider is when the legs of the right-angled triangle are both equal to 1.

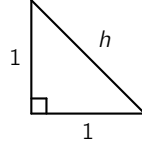


Figure 23: Right-angled triangle with legs of unit length

By Pythagoras' theorem, we get that the hypotenuse h must satisfy $h^2 = 1^2 + 1^2$, from which one easily obtains $h = \sqrt{2}$. Naturally, since numbers are either whole or parts of a whole, there must be a way to express

$$\sqrt{2} = \frac{a}{b}$$

for some integers $a, b \in \mathbb{Z}$, right? That's what the Pythagoreans believed.

Let us prove that this is impossible.⁷ We will do this by contradiction; that is, we will assume that there *exist* integers a and b such that $\sqrt{2} = \frac{a}{b}$, and show that this assumption leads us to an absurd conclusion. Before we proceed with the proof, we just need to make the following observation.

Definition 3.11 (HCF). The *highest common factor* of two integers a and b (not both zero), denoted by $\text{hcf}(a, b)$, is the largest integer d such that $d \mid a$ and $d \mid b$. Two integers a and b are said to be *relatively prime* or *coprime* if $\text{hcf}(a, b) = 1$.

Lemma 3.12. A number $x \in \mathbb{R}$ is rational if and only if we can express it as $x = \frac{a}{b}$ with $a, b \in \mathbb{Z}$ coprime.

The important part here is that a and b are coprime. E.g., $\frac{28}{6}$ is a rational number, and indeed we can write it as $\frac{14}{3}$ where we have that $\text{hcf}(14, 3) = 1$.

Proof. (\Leftarrow). This direction is obvious. If $x \in \mathbb{R}$ can be expressed as $\frac{a}{b}$ with a, b coprime, then in particular it can be expressed as $\frac{a}{b}$, so by definition it is rational.

(\Rightarrow). Suppose $x \in \mathbb{R}$ is rational. Then by definition, we may write it as $x = \frac{c}{d}$ for appropriate $c, d \in \mathbb{Z}$. Now if $\text{hcf}(c, d) = 1$, we are done, so suppose $\text{hcf}(c, d) = t \neq 1$. This means we can write $c = ta$ and $d = tb$ for appropriate $a, b \in \mathbb{Z}$, and so $x = \frac{ta}{tb} = \frac{a}{b}$. Now, if we show that $\text{hcf}(a, b) = 1$, we will be done, since we've expressed $x = \frac{a}{b}$. Indeed, suppose (for contradiction) that it is not, i.e., $\text{hcf}(a, b) = r \neq 1$. This means that $a = ru$ and $b = rv$ for some $u, v \in \mathbb{Z}$. But this in turn implies that $c = tru$ and $d = trv$, i.e., that $tr \mid c$ and $tr \mid d$. But since $r \neq 1$, then $tr > t$, which contradicts the fact that t is the highest common factor of c and d . \square

⁷If you wish, you can watch a YouTube version of this proof [here](#).

Now we are ready to give the proof.

Proof that $\sqrt{2}$ is irrational. Suppose (for contradiction) that $\sqrt{2}$ is rational, i.e., that we may write $\sqrt{2} = \frac{a}{b}$, where by [lemma 3.12](#) we may assume that $\text{hcf}(a, b) = 1$.

$$\sqrt{2} = \frac{a}{b} \implies 2 = \left(\frac{a}{b}\right)^2 \implies 2 = \frac{a^2}{b^2} \implies a^2 = 2b^2.$$

In particular, this means that a^2 is even, which by [lemma 3.9](#), means a is even. But since a is even, then $a = 2n$ for some $n \in \mathbb{Z}$, which means

$$a^2 = 2b^2 \implies (2n)^2 = 2b^2 \implies 4n^2 = 2b^2 \implies 2n^2 = b^2.$$

This similarly gives us that b^2 is even, which again by [lemma 3.9](#) means that b is also even. Therefore a and b are both divisible by 2. But we chose a and b so that they have no common divisors, so this is a contradiction. \square

Remark 3.13 (👤). It is said that one of the disciples of Pythagoras, *Hippasos of Metapontion*, presented an argument to Pythagoras that $\sqrt{2}$ is irrational. He was so outraged by this proof that he had Hippasos killed by throwing him to the sea!

Remark 3.14 (What's the point?). Okay, so there is no rational number which, when squared, gives 2. But why do we expand our number system from \mathbb{Q} to \mathbb{R} to incorporate $\sqrt{2}$ (and many other numbers)? Why should we accept that there is a “real” number whose square root is 2? After all, there is no real number such that $r^2 = -1$, so why aren't we on Pythagoras' side of the argument?

The issue with \mathbb{Q} is essentially that it has “holes”, and it is because of these holes that we need the real numbers. The holes are not as gaping and obvious to spot as they are in a set like \mathbb{Z} ; indeed, between any two rationals p and q , there is another rational (an easy one would be $\frac{p+q}{2}$), so the holes aren't something we can immediately visualise. To detect them, it's best to consider something like the plot in [figure 24](#). If we only worked with rational numbers, then this graph *doesn't intersect the x-axis*,

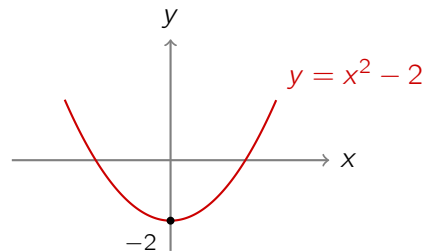


Figure 24: A plot of the parabola $y = x^2 - 2$

since the intercepts are at $x = \pm\sqrt{2}$, which aren't rational numbers. We can get

rational numbers very close to $\sqrt{2}$, e.g., by taking the first few digits of the decimal representation of $\sqrt{2} \approx 1.41421356237$. This is rational because it equals

$$\frac{141\,421\,356\,237}{100\,000\,000\,000},$$

but it is not exactly $\sqrt{2}$. It is because of the discomfort of these situations (and others where these holes cause problems) that we choose to work with a larger number system where these holes are “filled in”, namely, the real numbers.

There are infinitely many primes

A classical theorem, which dates back to Euclid in 300 BC, is the fact that there are infinitely many prime numbers.

Definition 3.15 (Prime). We say that an integer $p \geq 2$ is *prime* if its only divisors are ± 1 and $\pm p$.

We will need to assume the following fact, which we will prove later (by induction).

Theorem 3.16. *Every integer $n \geq 2$ is prime or a product of primes.*

Theorem 3.17. *There are infinitely many primes.*

Euclid's proof. For contradiction, suppose there are finitely many primes, and let p_1, \dots, p_n denote all of them. Define $N := 1 + \prod_{i=1}^n p_i$. Clearly $N \geq 2$, and it is not prime since it is larger than each p_i , but it is neither a product of primes since if $p_i \mid N$, then by [example theorem 3.6](#), $p_i \mid (N - \prod_{i=1}^n p_i) = 1$ which is impossible. This contradicts [theorem 3.16](#). \square

Remark 3.18. Certain proofs are very elegant and succinct, but it's difficult to see how one can come up with them. For instance, a well known proof of the fact that $\pi < \frac{22}{7}$ (where $\frac{22}{7}$ is typically used as an approximation of π) is to observe that

$$0 < \int_0^1 \frac{x^4(1-x^4)}{1+x^2} dx = \frac{22}{7} - \pi,$$


where it is clear that the integral is positive since it represents the area between 0 and 1 bounded by the curve $y = \frac{x^4(1-x^4)}{1+x^2}$, which is clearly positive for all inputs x .

- Exercise 3.19.** 1. a) Show that the sum of two odd numbers is even.
 b) Show that the product of two odd numbers is odd.
 c) Show that if ab is even, then at least one of a and b must be even.
 d) Show that a is odd if and only if a^3 is odd.

2. Prove that for every integer x , $x + 4$ is odd if and only if $x + 7$ is even.
3. If $x, y > 0$, show that $(\frac{1}{x} + \frac{1}{y})(x + y) \geq 4$.
4. Show that if n is not divisible by 2, then it is not divisible by 4.
5. Prove that if you add the squares of three consecutive numbers and then subtract two, you always get a multiple of 3.
6. Show that if x is irrational, then $\sqrt[3]{x}$ is also irrational.
7. Show that $k(k + 1)$ is even for every integer k .
8. Prove that for every integer x , if x is odd then there exists an integer y such that $x^2 = 8y + 1$.
9. Throughout this question, you may use the fact that any integer can be expressed as either $3k$, $3k + 1$ or $3k + 2$ for some $k \in \mathbb{Z}$.
 - a) Show that a square can never be two more than a multiple of 3. Hence, deduce that the number $\underbrace{10 \cdots 01}_{n \text{ zeroes}}$ is not a square for any n .
 - b) Show that if n^2 is a multiple of 3, then so is n .
 - c) Show that $\sqrt{3}$ is irrational.
 - d) Hence, show that $\frac{2+5\sqrt{3}}{1+\sqrt{3}}$ is irrational.
 - e) At what stage would the proof fail if you would try to prove that $\sqrt{4}$ is irrational?
10. Show that the product of any four consecutive integers is a multiple of eight.
11. Let $x \geq 0$ be a real number. Show that $x < \epsilon$ for any $\epsilon > 0$ if and only if $x = 0$.
12. Prove that for all integers a and m , if a and m are the lengths of the sides of a right-angled triangle and $m + 1$ is the length of the hypotenuse, then a is an odd integer.
13. Throughout this question, you may assume *Bézout's lemma*: that for any $a, b \in \mathbb{Z}$, there exist $s, t \in \mathbb{Z}$ such that $\text{hcf}(a, b) = sa + tb$.
 - a) Show that for all non-zero $a, b, k \in \mathbb{Z}$, $k \text{hcf}(a, b) = \text{hcf}(ka, kb)$.
 - b) Define $\text{hcf}(a_1, \dots, a_k)$ in the obvious way, i.e., as the largest number d such that $d \mid a_1, \dots$, and $d \mid a_k$ for all k . Show that $\text{hcf}(a, b, c) = \text{hcf}(\text{hcf}(a, b), c)$ and that $\text{hcf}(a, b, c, d) = \text{hcf}(\text{hcf}(a, b, c), d)$.

- c) Hence, show that for all integers a and b , if $5 \mid ab$, then $5 \mid a$ or $5 \mid b$.

For questions 14 and 15, it may be useful to remember the fact that $ax^2 + bx + c$ has rational roots \Leftrightarrow it can be factorised as $(px + q)(rx + s)$ where p, q, r, s are integers \Leftrightarrow the discriminant $\Delta = b^2 - 4ac$ is a square number.

14. Consider the quadratic $p(x) = 2x^2 - 5x + a$, where a is an integer. Suppose p can be factorised over the integers (i.e., p has rational roots).
- Suppose k is an integer. Show that $4k^2 - 25$ not divisible by 8.
 - Prove that $(n + 5)(n - 5)$ is divisible by 8 if and only if n is odd.
 - Show that a has the form $-\frac{1}{8}(n + 5)(n - 5)$ where n is odd.
 - Obtain a factorisation of $p(x)$ in terms of n .
-  15. Let a/b be a rational number different from 1. Show that a/b plus its reciprocal b/a can never equal an integer.

16. Show that it is possible to have irrational^{irrational} = rational.
[Hint: consider $\sqrt{2}^{\sqrt{2}}$.]

17. If a, b, c, d are in arithmetic progression, show that $\frac{a^2 - d^2}{b^2 - c^2} = 3$.

18. Prove that for all real numbers x and y , $x^4 + x^2y + 4y^2 \geq 5x^2y$.

19. Show that, to square a number ending in 5, you can just remove the 5, multiply the remaining number by one more than itself, and stick 25 on the end. E.g.,

$$65^2 \rightarrow (6 \times 7) \text{ } \frown \text{ } 25 = 4225$$

$$495^2 \rightarrow (49 \times 50) \text{ } \frown \text{ } 25 = 245025$$

20. a) (Cauchy–Schwarz Inequality). For any real numbers a, b, x, y , show that

$$(ax + by)^2 \leq (a^2 + b^2)(x^2 + y^2).$$

- b) Deduce that that $a + b \leq \sqrt{2}\sqrt{a^2 + b^2}$. Hence or otherwise, deduce that for any $x, y > 0$,

$$\sqrt{\frac{x}{x+y}} + \sqrt{\frac{y}{x+y}} \leq \sqrt{2}.$$

Is this bound sharp? (i.e., is there an assignment of x and y for which we have equality instead of \leq ?)

Proof by Induction

Induction is a powerful tool we use to prove statements about natural numbers $(0, 1, 2, 3, \dots)$, or for discrete structure more generally.

The idea behind it can be understood by considering the so-called *domino effect*. Consider an infinite line of dominoes. We wish to prove that all the dominoes will fall, and we do this as follows:

- (1) Prove that the first one will fall.
- (2) Prove that for any n , if the n th domino falls, then the $(n + 1)$ st domino falls.

Suppose we manage to prove both (1) and (2). By (1), we know that the first domino falls. But then by (2), the second one falls also. But now we can use (2) again to conclude that the third domino falls. And the fourth. And the fifth. This can continue indefinitely, thus proving that all the dominoes fall.

Let us transfer this to a mathematical context. Suppose we wish to prove that a statement $\varphi(n)$ is true for every natural number n . We can do this by:

- (1) Proving that $\varphi(n)$ is true for the case $n = 0$, i.e., proving that $\varphi(0)$ is true. This is called the *base case*.
- (2) Assume that $\varphi(n)$ is true (we call this the *inductive hypothesis*, IH). Based on this assumption, prove that $\varphi(n + 1)$ is true. This is called the *inductive step*.

Example 3.20. Let us prove a very popular formula by induction. The sum of the first n positive integers:

$$1 + 2 + \cdots + n = \frac{n}{2}(n + 1).$$

Let the formula above be the statement $\varphi(n)$. Clear $\varphi(0)$ is true, because the left-hand side is $\sum_{k=1}^0 k = 0 = \frac{0}{2}(0 + 1)$, which equals the right-hand side. So the base case is done.

Next we assume $\varphi(n)$ is true, i.e. that $1 + 2 + \cdots + n = \frac{n}{2}(n + 1)$. This is the inductive hypothesis.

Now can we prove $\varphi(n + 1)$? We have:

$$\begin{aligned} 1 + 2 + \cdots + n + (n + 1) &= \frac{n}{2}(n + 1) + (n + 1) && \text{(by the IH)} \\ &= (n + 1)\left(\frac{n}{2} + 1\right) \\ &= \frac{n+1}{2}(n + 2) \\ &= \frac{n+1}{2}((n + 1) + 1), \end{aligned}$$

in other words, we have that $\varphi(n + 1)$ is true! This concludes the proof. □

Make sure you understand this proof, in that it achieves both (1) and (2). Understand *why* we are allowed to use $\varphi(n)$ in the inductive step.

✠ JMJ ✠

Lecture 5
4 Nov 2024

Example 3.21. We show that the number $4^n + 2$ is always divisible by 3.

We let $\varphi(n) \leftrightarrow (\exists \alpha \in \mathbb{N} : 4^n + 2 = 3\alpha)$, because this is what it means to be divisible by 3.

For $\varphi(0)$, we have $4^0 + 2 = 1 + 2 = 3 = 3(1)$, so we take $\alpha = 1$ and this completes the base case.

Now assume $\varphi(n)$ holds, i.e. $4^n + 2 = 3\alpha$ for some $\alpha \in \mathbb{N}$. Can we show $\varphi(n+1)$?

$$\begin{aligned} 4^{n+1} + 2 &= 4(4^n) + 2 \\ &= 4(4^n + 2 - 2) + 2 \\ &= 4(3\alpha - 2) + 2 \quad (\text{by IH}) \\ &= 12\alpha - 8 + 2 \\ &= 12\alpha - 6 \\ &= 3(4\alpha - 2) \\ &= 3\beta \quad \text{where } \beta = (4\alpha - 2) \in \mathbb{N} \end{aligned}$$

i.e. $\varphi(n+1)$ is true. □

Remark 3.22. It's more common to assume $\varphi(n-1)$ and prove $\varphi(n)$, rather than what we've been doing. This is obviously equivalent, but stylistically it is preferable. Let's give an example where we prove things this way.

Example 3.23. How about an example with matrices. If $\mathbf{A} = \begin{pmatrix} 3 & 1 \\ 0 & 2 \end{pmatrix}$, then the matrix power \mathbf{A}^n is given by

$$\mathbf{A}^n = \begin{pmatrix} 3^n & 3^n - 2^n \\ 0 & 2^n \end{pmatrix}.$$

Proof. By induction on n . For the base case, $\mathbf{A}^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 3^0 & 3^0 - 2^0 \\ 0 & 2^0 \end{pmatrix}$, so the statement holds when $n = 0$. Now when $n \geq 1$,

$$\begin{aligned} \mathbf{A}^n &= \mathbf{A}^{n-1} \mathbf{A} \\ &= \begin{pmatrix} 3^{n-1} & 3^{n-1} - 2^{n-1} \\ 0 & 2^{n-1} \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 0 & 2 \end{pmatrix} \quad (\text{by the IH}) \\ &= \begin{pmatrix} 3^{n-1}(3) + 0 & 3^{n-1} + 2(3^{n-1} - 2^{n-1}) \\ 0 & 2^{n-1}(2) \end{pmatrix} \\ &= \begin{pmatrix} 3^n & 3^{n-1} + 2(3^{n-1}) - 2^n \\ 0 & 2^{k+1} \end{pmatrix} \\ &= \begin{pmatrix} 3^n & 3^{n-1}(1+2) - 2^n \\ 0 & 2^{k+1} \end{pmatrix} = \begin{pmatrix} 3^n & 3^n - 2^n \\ 0 & 2^n \end{pmatrix}, \end{aligned}$$

as required. □

Notice that in the last example, we do not explicitly define a predicate $\varphi(n)$, nor do we actually state the inductive hypothesis. This is typically how one presents an inductive argument, since the predicate is always simply a copy of the result we wish to prove, as is the inductive hypothesis (simply with $n - 1$ instead of n). It suffices to open the proof with the phrase “by induction on n ”, the reader will be familiar with the structure of the proof.

The general strategy for the inductive step is to try and “break down” the object we are working with into an analogous object of a “lesser kind”, plus something else which elevates it to the object under consideration (e.g., the matrix \mathbf{A}^n into $\mathbf{A}^{n-1}\mathbf{A}^1$, or a sum $\sum_{k=1}^n f(k)$ into $\sum_{k=1}^{n-1} f(k) + f(n)$). This allows one to apply the inductive hypothesis. Thus, one deduces that induction would not be very useful when it is very difficult, or impossible, to relate what $\varphi(n - 1)$ says with what $\varphi(n)$ says. Let us give an example with series, which emphasises this strategy of breaking the $\varphi(n)$ case down into the $\varphi(n - 1)$ case “plus other stuff”.

Example 3.24. We prove that $\sum_{k=n}^{2n} k(k + 2) = \frac{n}{6}(n + 1)(14n + 19)$.

Proof. For the base case, we have $\sum_{k=0}^0 k(k + 2) = 0 = \frac{0}{6}(0 + 1)(14(0) + 19)$, so the statement holds.⁸ Now when $n \geq 1$,

$$\begin{aligned} & \sum_{k=n}^{2n} k(k + 2) \\ &= \underbrace{\sum_{k=n-1}^{2(n-1)} k(k + 2)}_{\text{the } \varphi(n-1) \text{ case}} - \underbrace{\sum_{k=n-1}^{n-1} k(k + 2) + \sum_{k=2(n-1)+1}^{2(n-1)+2} k(k + 2)}_{\text{“other stuff”}} \\ &= \frac{n-1}{6}n(14(n-1) + 19) - (n-1)(n+1) + (2n-1)(2n+1) + 2n(2n+2) \quad (\text{by IH}) \\ &= \frac{1}{6}(14n^3 + 33n^2 + 19n) \quad 9 \\ &= \frac{n}{6}(n+1)(14n+19), \end{aligned}$$

as required. □

⁸Sometimes, in cases where the $n = 0$ feels a bit vacuous, we prove the $n = 1$ case instead. Technically, if one does this and excludes the zero case, this proves the result for $n \geq 1$, and not for all $n \in \mathbb{N}$. But it’s fine usually, because the reason we consider $n = 1$ in the first place is because $n = 0$ is not interesting. In this case, $n = 1$ gives $\sum_{k=1}^2 k(k + 2) = 1(1 + 2) + 2(2 + 2) = 11 = \frac{1}{6} \cdot 2 \cdot 33 = \frac{1}{6}(1 + 1)(14 + 19)$, so the case $n = 1$ holds. At least it feels like we’ve actually proved something!

⁹Even though this cubic might seem like a headache to factorise (factor theorem, etc.), remember that we know what this should equal if the result is true; it should be $\frac{n}{6}(n + 1)(14n + 19)$ —so we can use this fact to make an “educated guess” about the factors.

Base Cases different from Zero

If we want to prove a statement, not for all natural numbers, but only for all numbers n greater than or equal to a certain number a , then the proof by induction consists of the following:

- (1) Proving that $\varphi(a)$ is true,
- (2) Assuming that $\varphi(n - 1)$ is true for some $n > a$, prove that $\varphi(n)$ is true.

Example 3.25. Let's show that $3^n < n!$ for all $n \geq 7$.

Proof. By induction on n . When $n = 7$, we have $3^n = 3^7 = 2187 < 5040 = 7!$, which establishes the base case.

For $n > 7$, we have

$$3^n = 3 \cdot 3^{n-1} \stackrel{\text{IH}}{<} 3 \cdot (n-1)! < n(n-1)! = n!,$$

which completes the proof. □

Example 3.26. Suppose Bertu sells imqaret in boxes of 4 or 5 pieces, exclusively. Then we can buy precisely any whole number $N \geq 12$ of imqaret. (In other words, any number $N \geq 12$ can be written as a sum of 4's and 5's.)

Proof. By induction on N . When $N = 12$, then $N = 4 + 4 + 4$, which completes the base case. Now consider $N > 12$. If, by the inductive hypothesis, $N - 1$ has a solution involving at least one 4, then we can change it to a 5 and the proof is done.

Thus, suppose $N - 1$ is written only using 5's. Then $N - 1$ is a multiple of 5, so it is at least 15, thus it contains at least three 5's. But replacing $5 + 5 + 5$ with $4 + 4 + 4 + 4$ increases the sum by 1. □

Strong Induction

In a previous lecture we mentioned that we would prove [theorem 3.16](#) using induction. This states that any integer $n \geq 2$ is prime, or can be expressed as a product of primes. Let's try and prove it now.

Attempted Proof of Theorem 3.16. Clearly 2 is prime, so that completes the base case.

Now for $n > 2$, if n is prime, we would be done, so suppose n is not prime, i.e., n has a divisor d in the range $1 < d < n$. Thus we can write $n = da$ for some $a \in \mathbb{N}$.

By the IH $n - 1$ is prime or a product of primes. Now what...? ☒

We get stuck here because knowing something about the factorisation of $n-1$ doesn't really help with the factorisation of n . On the other hand, if we could apply the IH to the numbers a and d , then that might be helpful. Can we do this?

If we go back to the intuition with dominoes, it makes sense that we can. If we make the following change:

- (1) Prove that the first one will fall.
- (2) Prove that for any n , if **all dominoes before the n th one fall**, then the n th domino falls.

All we've done here is said that all the dominoes before the current one fell, as opposed to *just* the previous one, which corresponds to the following mathematical formulation:

- (1) Proving that $\varphi(0)$ is true (or an appropriate base case),
- (2) Assuming that $\varphi(k)$ is true for all $k < n$, prove that $\varphi(n)$ is true.

Using this new principle, we can finally prove [theorem 3.16](#).

Proof of theorem 3.16. Clearly 2 is prime, so that completes the base case.

Now for $n > 2$, if n is prime, we would be done, so suppose n is not prime, i.e., n has a divisor d in the range $1 < d < n$. Thus we can write $n = da$ for some $a \in \mathbb{N}$.

By the IH, since a and d are both $< n$, then they are both either prime or a product of primes. Write $a = p_1 \cdots p_r$ (where $r = 1$ if a is prime, and $r > 1$ if it is a product of primes), and similarly $d = q_1 \cdots q_s$, where p_i, q_i are all prime. But then $n = p_1 \cdots p_r q_1 \cdots q_s$, so we have written n as a product of primes. \square

Exercise 3.27. 1. Prove the following by induction for all $n \geq 1$.

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

b) $1 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$

c) For any $x \in \mathbb{R}$, $x + x^2 + \cdots + x^n = \frac{x^{n+1} - x}{x - 1}$.

d) $\sum_{k=1}^n \frac{k^2 + k + 1}{k^2 + k} = \frac{n(n+2)}{n+1}$ e) $\sum_{k=3}^{3n} \frac{1}{4k^2 - 1} = \frac{3n-2}{30n+5}$

2. Prove the following by induction.

a) $\sum_{k=1}^n \frac{k!}{(k-2)!} = \frac{n}{3}(n^2 - 1)$

b) $\sum_{k=2n}^{4n} k^2 = \frac{n}{3}(2n+1)(28n+1)$

$$\begin{aligned} \text{c) } \prod_{k=2}^n \left(1 - \frac{1}{k}\right) &= \frac{1}{n} & \text{d) } 1 \cdot 1! + \cdots + n \cdot n! &= (n+1)! - 1 \\ \text{e) } \sum_{k=2}^n \frac{1}{\sqrt{k-1} + \sqrt{k}} &= \sqrt{n} - 1 \end{aligned}$$

3. Use induction to show that de Morgan's laws generalise to any finite number of sets,

$$\overline{\bigcap_{k=1}^n A_k} = \bigcup_{k=1}^n \bar{A}_k \quad \text{and} \quad \overline{\bigcup_{k=1}^n A_k} = \bigcap_{k=1}^n \bar{A}_k.$$

4. Let A be a set of n elements. Show, using induction, that

- A has 2^n possible subsets, including \emptyset .
- A has $n(n-1)/2$ possible subsets of size 2.

5. (A mathematical joke). Since we saw in [example 3.20](#) that

$$1 + 2 + \cdots + n = \frac{\frac{n}{2} \cdot \frac{n+1}{2}}{\frac{1}{2}},$$

we have

$$\sin(1) + \sin(2) + \cdots + \sin(n) = \frac{\sin\left(\frac{n}{2}\right) \cdot \sin\left(\frac{n+1}{2}\right)}{\sin\left(\frac{1}{2}\right)}.$$

Proof. Take the sine of everything. □

Why is the joke funny? (Or if it didn't make you laugh, what is wrong with the "proof"?) Prove that the second statement is actually true by induction.

6. Prove the following by induction.

- $7^n + 11$ is a multiple of 6
- $23^n + 43$ is a multiple of 11
- $2^{n+2} + 3^{2n-1}$ is divisible by 7
- $3^n + 7^{n-1} + 8$ is divisible by 12
- $n^2 + 5n - 2$ is even
- $3n^2 + 15n - 15$ is odd
- 19 divides $2^{2n+1}(3^{n+2}) + 5^{2n+1}(2^{n+2})$

7. Prove that for $n \in \mathbb{N}$,

$$\frac{(1 + \sqrt{5})^n + (1 - \sqrt{5})^n}{2^{n-1}}$$

is even.

8. Bernoulli's inequality states that for any real number $x > -1$ and any positive integer $n > 1$,

$$(1 + x)^n > 1 + nx.$$

Prove this result by induction on n .

9. Prove the following by induction.

a) $2n + 4 \leq 2^{n+2}$

b) $(2n)! < (2^n n!)^2$

c) $\frac{1}{2}(a^n + b^n) \geq \frac{1}{2^n}(a + b)^n$

d) $2! \cdot 4! \cdots (2n)! \geq [(n + 1)!]^n$


10. Show that $1 + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} < 2\sqrt{n}$.


11. Show that for real $a, b, c \geq 1$, we have $4(1 + abc) \geq (1 + a)(1 + b)(1 + c)$.
[Hint: Prove more generally that $2^{n-1}(1 + \prod_{k=1}^n a_k) \geq \prod_{k=1}^n (1 + a_k)$.]

12. Prove, using ordinary induction, that the principle of strong induction holds.

13. Prove that $\sqrt{\underbrace{2 + \sqrt{2 + \sqrt{2 + \cdots + \sqrt{2}}}}_{n \text{ 2's}}} = 2 \cos\left(\frac{\pi}{2^{n+1}}\right)$.

14. Prove that for all $n \geq 3$, the sum of the interior angles of a regular polygon with n vertices is $180^\circ(n - 2)$.

-  15. (Powers of 5). Prove that for all $n \in \mathbb{N}$, the number 5^n can always be expressed as a sum of two squares.

-  16. (Catalan Numbers). A sequence of open and closed brackets is said to be *balanced* if each open bracket can be matched with a closed bracket. For example,

$$((())) \quad ()() \quad ()(())(())$$

are balanced, whereas $)()$, $(())$ and $((()))(())$ are not. If we have n pairs of open/closed brackets, the *Catalan number* C_n is the number of distinct balanced arrangements of the $2n$ brackets. For example, $C_3 = 5$, since the only possibilities are $()()()$, $((()))$, $()(())$, $(())()$, and $((()))$.

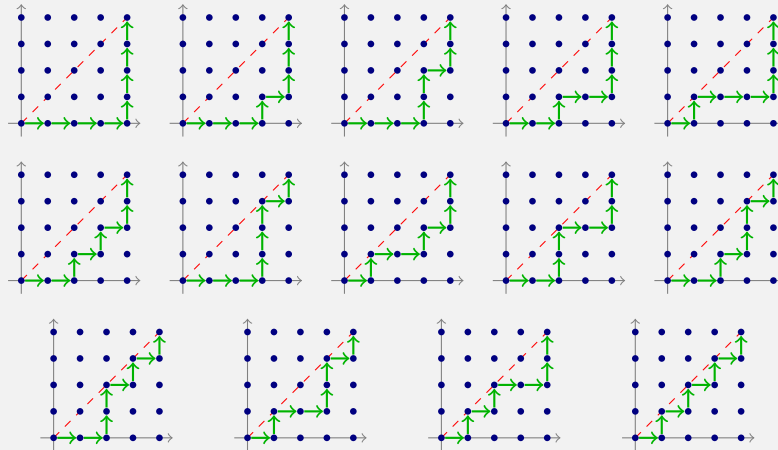
- a) Show that in general, $C_{n+1} = C_n C_0 + C_{n-1} C_1 + \cdots + C_0 C_n$, where $C_0 = 1$ by convention.

- b) (Optional if you don't know much calculus). Show that C_n is the coefficient of x^n in the Maclaurin series expansion of the function $f(x) = (1 - \sqrt{1 - 4x})/2$. [Hint: Consider $(\sum_{n=0}^{\infty} C_n x^n)^2$.]

Hence, deduce that $C_n = \frac{1}{n+1} \binom{2n}{n}$.

c) Show that C_n is the number of *monotonic paths* from $(0, 0)$ to (n, n) in \mathbb{N}^2 which do not go above the diagonal. A monotonic path is one which goes only rightwards or upwards.

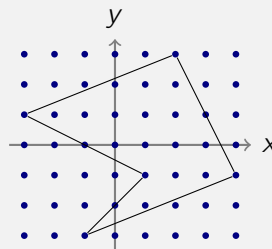
Here is an illustration for the case $n = 4$:



These are all such paths from $(0, 0)$ to $(4, 4)$, so $C_4 = 14$.

☺☺☺ 17. (Pick’s Theorem). Consider the points in the plane with whole number coordinates (this is called \mathbb{Z}^2). A *simple polygon* is a polygon whose edges do not intersect each other.

Show that the area of a simple polygon with vertices at integer coordinates is $i + \frac{1}{2}b - 1$, where i is the number of points contained entirely within the polygon, and b is the number of points that lie on the boundary of the polygon (i.e., on some edge).



In the example above, there are $i = 15$ points inside the polygon, and $b = 8$ on the boundary. Thus the area is $A = 15 + \frac{1}{2}(8) - 1 = 18$.

Discussion: Recursion and the Fibonacci Numbers

✠ JMJ ✠

Lecture 6
11 Nov 2024

A very important result, which goes hand-in-hand with induction, is the idea of definition by recursion. This idea is essential in mathematics and computer science, the idea of a function “using itself” in a definition.

Let us motivate this with an example, before we state the theorem. Recall that $N! = N \cdot (N - 1) \cdot \dots \cdot 2 \cdot 1$. An alternative way to define this is the following: suppose we want to find $5!$, *but we already know what $4!$ is*. How can we use this information? Well if we already know what $4!$ is, we can just multiply this by 5 and we get $5!$ —in general, we have that $N! = N \cdot (N - 1)!$. We could use this to define factorial differently—let $\text{fac}(N)$ denote our “newly” defined factorial.

If we define $\text{fac}(N) = N \cdot \text{fac}(N - 1)$, this almost works. Indeed, if we try to evaluate $5!$ this way, we do

$$\begin{aligned} \text{fac}(5) &= 5 \cdot \text{fac}(4) \\ &= 5 \cdot 4 \cdot \text{fac}(3) \\ &= 5 \cdot 4 \cdot 3 \cdot \text{fac}(2) \\ &= 5 \cdot 4 \cdot 3 \cdot 2 \cdot \text{fac}(1) \\ &= 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \cdot \text{fac}(0) && (*) \\ &= 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \cdot 0 \cdot \text{fac}(-1) \\ &\vdots \end{aligned}$$

Something seems to have gone wrong here. The “unrolling” of the fac ’s seems to have worked, because we did get the product $5 \cdot \dots \cdot 1$ appearing, but this will keep on going forever. We need some mechanism which stops this infinite expansion. If we instead say $\text{fac}(0) = 1$, then we would actually stop at the line (*). This is called the *base case*. Familiar?

So we define

$$\text{fac}(N) = \begin{cases} 1 & \text{if } N = 0 \\ N \cdot \text{fac}(N - 1) & \text{otherwise.} \end{cases}$$

And this works! Apart from being nicely succinct (without having to use informal notions such as \dots), this gives us a way to write an elegant algorithm for computing $N!$:

```

1: function fac(N)
2:   if N = 0 then
3:     | return 1
4:   else
5:     | return N * fac(N - 1)

```

But is this always allowed? Can we similarly define a function, say,

$$f(N) = \begin{cases} 1 & \text{if } N = 0 \\ N f(N + 1) & \text{otherwise?} \end{cases}$$

Try to work out $f(5)$. It's not hard to see why this definition is problematic. Thus, we need to see precisely *when* we are allowed to do this. Indeed, notice that $\text{fac}(N)$ made use of N , and of *the value of* $\text{fac}(N - 1)$. In other words, in defining $f(N)$, if we only allow $f(N - 1)$ to appear (and possibly N), then the definition should be fine.

This is what the following theorem guarantees.

Theorem 3.28 (Definition by Recursion). *Suppose X is a set, let $x \in X$ and let $g: \mathbb{N} \times X \rightarrow X$ be a total function. Then there exists a unique total function $f: \mathbb{N} \rightarrow X$ such that*

$$f(N) = \begin{cases} x & \text{if } N = 0 \\ g(N, f(N - 1)) & \text{otherwise.} \end{cases}$$

Don't worry too much about the wording here, we haven't even rigorously defined the term "function" yet (although we will in the next lecture), just think of it the way you're used to from sixth form. All this theorem is telling us is that we are allowed to have $f(N - 1)$ appearing in the definition of f (and only that), and this will determine a unique, valid function from \mathbb{N} to X . We will not prove it here, since it is a bit technical (although not difficult). You probably guessed it, but the proof is by induction!

For $N!$, the function $g: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ we need to take $g(N, t) = Nt$.

This theorem can be generalised so that we have any number of base cases.

Theorem 3.29 (General Definition by Recursion). *Let X be a set, let $x_0, \dots, x_r \in X$, and let $g: X^{r+1} \times \mathbb{N} \rightarrow X$ be a function. Then there exists a unique function $f: \mathbb{N} \rightarrow X$ such that*

$$f(N) = \begin{cases} x_N & \text{if } 0 \leq N \leq r, \\ g(f(N - r), f(N - r + 1), \dots, f(N - 2), f(N - 1), N) & \text{otherwise.} \end{cases}$$

This looks a bit complicated, so let us give an example to clarify. The Fibonacci sequence, named after Leonardo Bonacci of Pisa (1170–1270 A.D.), is defined as follows.

$$F_n = \begin{cases} 0 & \text{if } n = 0 \\ 1 & \text{if } n = 1 \\ F_{n-1} + F_{n-2} & \text{otherwise.} \end{cases}$$

Here we have $r = 1$ in [theorem 3.29](#) with $X = \mathbb{N}$, so our definition must match the form

$$f(N) = \begin{cases} x_0 & \text{if } N = 0 \\ x_1 & \text{if } N = 1 \\ g(f(N-1), f(N-2), N) & \text{otherwise} \end{cases}$$

if we are allowed to define it. The base cases are clearly compatible. But what about the last case? Is it a function of the form $g(f(N-2), f(N-1), N)$? Yes! It simply does not make use of the variable N , but it makes use of “what it’s allowed to”, namely the values of F_N for the previous two natural numbers.

Activity 3.30. Show, using induction, that the n th Fibonacci number is given by the formula

$$F_n = \frac{1}{\sqrt{5}} \left(\varphi^n - \frac{1}{(-\varphi)^n} \right),$$

where $\varphi = \frac{1+\sqrt{5}}{2}$ is an important number called the *Golden Ratio*.

Remark 3.31. If you are interested in the formal details of induction and recursion (and they are very interesting), it turns out you can do induction and recursion on any set which can be ordered (i.e., a ranked poset), not just the natural numbers. Such structures include programming languages: you can prove things about programming languages using induction (e.g. type safety, normalisation, etc.).

But this falls out of the scope of this course. However, if you are interested, for the mathematical side, I suggest looking at the Recursion Theorem in chapter 3 of [5]. For the computer science side, I suggest investing in a copy of the famous “*Wizard book*” ([10]).

Exercise 3.32. 1. Prove the following properties of the Fibonacci sequence by induction.

- | | |
|---|--|
| a) $F_n < 2^n$ | b) $F_n \geq \left(\frac{3}{2}\right)^{n-2}$ |
| c) $\sum_{k=1}^n (F_k)^2 = F_n F_{n+1}$ | d) $\sum_{k=1}^n F_k = F_{n+2} - 1$ |
| e) $F_{n-1} F_{n+1} = F_n^2 + (-1)^n$ | |

☞ 2. Suppose you toss a fair coin n times. Show that the probability that you get at least 2 successive heads is $1 - F_{n+2}/2^n$.

3. A *derangement* of $1, 2, \dots, N$ is an arrangement of the numbers such that no number i is in the i th position. For example, 4321 and 21534 are derangements, but 54321 is not, because 3 appears in the 3rd position.

The number of derangements of the numbers $1, \dots, N$ is denoted by $!N$.

☞ a) Explain why

$$!N = \begin{cases} 1 & \text{if } N = 0 \\ 0 & \text{if } N = 1 \\ (N - 1)[!(N - 1) + !(N - 2)] & \text{otherwise,} \end{cases}$$

using combinatorial reasoning.

b) Prove, using induction, that $!N = N!(\frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^N \frac{1}{N!})$.

c) Deduce that $!N \approx N!/e$.

d) 15 people in an office organise a “Secret Santa” for Christmas, where they each write their names on a piece of paper, place them in a hat, and subsequently each person picks one from the hat.

If someone gets their own name, they have to do the whole process again. What is the probability that they have to do the process N times?

Remark 3.33 (Mathematician vs Programmer). As a mathematician, I don't worry too much about computation. But it's important to realise that even though it is quite elegant, the following algorithm, which can be inferred from the way we defined Fibonacci numbers, is quite bad.

```

1: function fib( $N$ )
2:   if  $N < 2$  then
3:     return  $N$ 
4:   else
5:     return fib( $N - 1$ ) + fib( $N - 2$ )
    
```

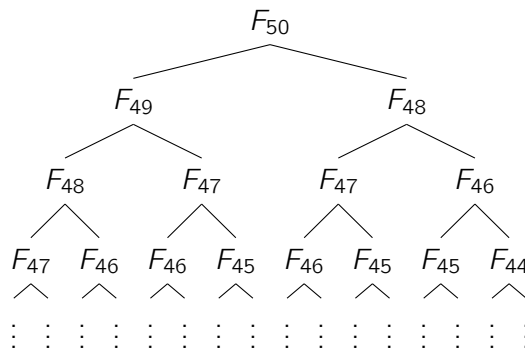


Figure 25: Recursive function calls for the $\Theta(\varphi^N)$ Fibonacci algorithm

Notice that when computing, say, F_{50} using this algorithm, many redundant calls are

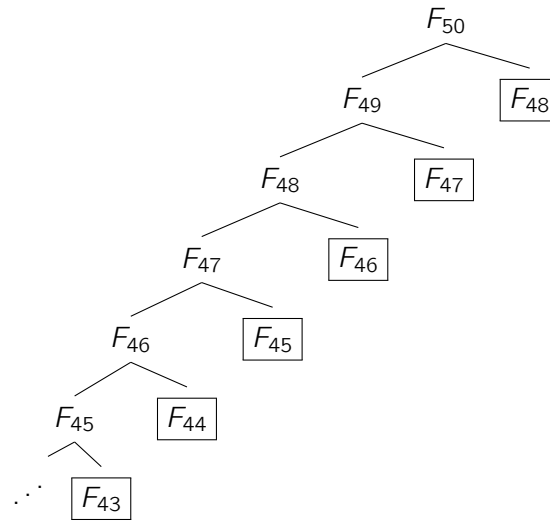


Figure 26: Recursive function calls for the Fibonacci algorithm with caching. The boxed function calls are efficient since we just need to fetch them from the cache.

being made. For instance, we will wastefully compute F_{48} twice, and in turn this will produce two evaluation trees which are identical and needlessly repeat computations. Similarly we end up working out F_{47} three times, F_{46} four times, and so on. Refer to [figure 25](#).

What we can do is *cache* the value once it has been computed, so we never work out a Fibonacci number if it's already been worked out. Here is the updated algorithm which does the caching:

```

1: fibs_done ← array full of  $N$  zeros
2: function fib( $N$ )
3:   if  $N < 2$  then
4:     | return  $N$ 
5:   else if fibs_done[ $N$ ]  $\neq 0$  then
6:     | return fibs_done[ $N$ ]
7:   else
8:     | ans ← fib( $N - 1$ ) + fib( $N - 2$ )
9:     | fibs_done[ $N$ ] ← ans
10:  | return ans

```

This time, we only make a recursive function call once per Fibonacci call! Look at the two recursive call trees in [figures 25](#) and [26](#) to get a better understanding.

So as a takeaway from this example, when designing an algorithm, always consider how you can speed things up by saving previously computed terms. This ties into a broader principle of algorithm design, known as *dynamic programming*. I'm sure you'll

cover this in some other relevant study-unit.

It's worth mentioning that in this case, there is actually a simple non-recursive solution (which actually doesn't require storing N previous values). The idea is to keep only the previous two terms, and work iteratively, rather than recursively.

Here it is:

```

1: function fib( $N$ )
2:   previous  $\leftarrow$  0
3:   current  $\leftarrow$  1
4:   for  $N - 1$  times do
5:     new  $\leftarrow$  previous + current
6:     previous  $\leftarrow$  current
7:     current  $\leftarrow$  new
8:   return current

```

This method is quite natural to formulate, but had we started with it, we would have deprived ourselves of the exploration of recursion, which wouldn't have been very fun. Moreover, there are other algorithms whose recursive formulation is very elegant, and cannot easily be transformed into an iterative implementation.

Exercise 3.34 (Binomial Coefficients). The number $\binom{n}{k}$ is the number of subsets of size k , of a set of size n . In other words,

$$\binom{n}{k} = \#\{X \in \mathcal{P}\{1, \dots, n\} : \#X = k\}.$$
¹⁰

For example, $\binom{5}{3} = 10$ since there are 10 subsets of $\{1, 2, 3, 4, 5\}$ with size 3,

$$\#\left\{ \begin{array}{l} \{1, 2, 3\}, \{1, 2, 4\}, \{1, 2, 5\}, \{1, 3, 4\}, \{1, 3, 5\}, \\ \{1, 4, 5\}, \{2, 3, 4\}, \{2, 3, 5\}, \{2, 4, 5\}, \{3, 4, 5\} \end{array} \right\} = 10.$$

a) Explain why for $n \geq 0$ and $0 \leq k \leq n$,

$$\binom{n}{k} = \begin{cases} 1 & \text{if } k = 0 \text{ or } n = k \\ \binom{n-1}{k-1} + \binom{n-1}{k} & \text{otherwise.} \end{cases}$$

b) Hence, using a programming language of your choice, write a recursive function `binom(n,k)` which computes the number $\binom{n}{k}$.

¹⁰For a finite set A , the notation $\#A$ denotes the *size* or *cardinality* of A , i.e., how many elements it contains.

- c) Write a function called `pascal(n)` which prints on screen Pascal's triangle up to row n . Pascal's triangle is a triangular array where the k th position in the n th row is $\binom{n}{k}$.

The output should look like this:

$\binom{0}{0}$		1			
$\binom{1}{0}$	$\binom{1}{1}$	1 1			
$\binom{2}{0}$	$\binom{2}{1}$	$\binom{2}{2}$	1 2 1		
$\binom{3}{0}$	$\binom{3}{1}$	$\binom{3}{2}$	$\binom{3}{3}$	1 3 3 1	
$\binom{4}{0}$	$\binom{4}{1}$	$\binom{4}{2}$	$\binom{4}{3}$	$\binom{4}{4}$	1 4 6 4 1

Pascal's triangle up to row 4 Desired output of `pascal(4)`

- d) Your program will probably take a very long time to print out `pascal(50)`. Improve the implementation of `binom(n,k)` using caching, and try again to output `pascal(50)`.
- e) Show using induction that

$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-(k-1))}{k!}.$$


Hence write an iterative implementation of `binom(n,k)`.

- f) (The Binomial theorem). Prove that for any $x \in \mathbb{R}$ and $n \in \mathbb{N}$,

$$(1+x)^n = \sum_{k=0}^n \binom{n}{k} x^k.$$

- g) Write a function which takes as input an integer n , and prints on screen the expansion of $(1+x)^n$. For instance, when $n = 10$, the function should output

$$x^{10} + 10x^9 + 45x^8 + 120x^7 + 210x^6 + 252x^5 + 210x^4 + 120x^3 + 45x^2 + 10x + 1$$

-  h) Prove the following relationship between Fibonacci numbers and binomial coefficients:

$$F_{n+1} = \sum_{k=0}^{n/2} \binom{n-k}{k}.$$

4. Relations and Functions

Relations are one of the most fundamental objects in mathematics and computing, and a distinguished kind of relation is certainly the most important: the function.

Definition 4.1 (Input-output pair). Given two elements $a \in A$ and $b \in B$ from the two sets A and B , the set $\{\{a\}, \{a, b\}\} \in \wp\wp(A \cup B)$ is called an *input-output pair*, which we will denote by $\langle\langle a, b \rangle\rangle$. In this case, we call a the *input* and b the *output* of the pair, respectively.

It is a simple exercise in the definition of set equality to verify that input-output pairs have the property that $\langle\langle a, b \rangle\rangle = \langle\langle c, d \rangle\rangle$ if and only if $a = c$ and $b = d$. In other words, unlike sets, input-output pairs satisfy $\langle\langle a, b \rangle\rangle \neq \langle\langle b, a \rangle\rangle$ unless $a = b$.

The set of all input-output pairs with inputs in the set A and outputs in the set B will be denoted by $A * B$, that is,

$$A * B := \{x \in \wp\wp(A \cup B) : \exists a \in A, \exists b \in B : x = \langle\langle a, b \rangle\rangle\}.$$

Example 4.2. If $A = \{1, 2, 3\}$ and $B = \{a, b\}$, then

$$A * B = \{\langle\langle 1, a \rangle\rangle, \langle\langle 1, b \rangle\rangle, \langle\langle 2, a \rangle\rangle, \langle\langle 2, b \rangle\rangle, \langle\langle 3, a \rangle\rangle, \langle\langle 3, b \rangle\rangle\}.$$

Definition 4.3 (Relation). Let A, B be two sets. A (*binary*) *relation* from A to B is any subset R of $A * B$. If $\langle\langle a, b \rangle\rangle \in R$, we say a and b are *related* by R and write $a R b$.

Sometimes we use special symbols instead of letters for relations. For example, \leq is a relation from \mathbb{R} to \mathbb{R} , and $x \leq y \iff \langle\langle x, y \rangle\rangle \in \leq$, where $\leq \subseteq \mathbb{R} * \mathbb{R}$.

Example 4.4. Consider the sets $A = \{1, \dots, 6\}$ and $B = \{odd, even, prime\}$. We can define the relation $\sim \subseteq A * B$ which relates the numbers in A to the words in B which describe them. For example $1 \sim odd$ and $2 \sim prime$, but $4 \not\sim prime$ (that is, $\langle\langle 4, prime \rangle\rangle \notin \sim$). Visually, we can think of the relation as a subset of all possible ‘arrows’ from elements in the set A to those of the set B (as in [figure 27](#)).

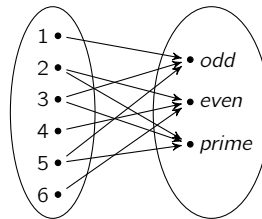


Figure 27: The relation $\sim \subseteq A * B$

Definition 4.5 (Domain and codomain). If R is a relation from the set A to the set B , then the set A is called the *domain* of R , which we denote by $\text{dom}(R)$, and the set B is called the *codomain* of R , which we denote by $\text{cod}(R)$.

Functions

A function is basically a special kind of relation.

Definition 4.6 (Function). A *function* is a relation f from a set A to a set B such that

$$\forall a \in A, \forall b, b' \in B, \langle\langle a, b \rangle\rangle \in f \wedge \langle\langle a, b' \rangle\rangle \in f \implies b = b'.$$

In words, a function from A to B is a set of input-output pairs such that for any element $a \in A$ in the domain, there is at most one input-output pair $\langle\langle a, b \rangle\rangle \in f$. (Indeed, the condition is saying that if $\langle\langle a, b \rangle\rangle$ and $\langle\langle a, b' \rangle\rangle$ are both in f , then b and b' must be the same, so that “two” input-output pairs are actually the same one.)

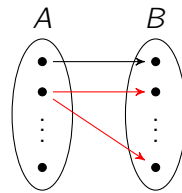


Figure 28: A function cannot relate an element in A to more than one in B

If for $a \in A$ there exists an input-output pair $\langle\langle a, b \rangle\rangle \in f$, then we write $f(a) = b$. Moreover, we interpret the notation ‘ $f(a)$ ’ alone to stand for the unique $b \in B$ to which a is related by f .

Example 4.7. If we have the sets $A = \{1, 2, 3, 4, 5\}$, $B = \{10, 20, 30, 40\}$ and then define $f = \{\langle\langle 1, 20 \rangle\rangle, \langle\langle 2, 20 \rangle\rangle, \langle\langle 3, 10 \rangle\rangle, \langle\langle 5, 40 \rangle\rangle\}$, then f is a function from A to B (see [figure 29](#)). Moreover, $f(1) = 20$, and $f(3)$ is the value 10. In this case, $f(4)$ does not exist.

Remark 4.8. The notation $f(a)$ only makes sense for functions. Indeed, the relation \sim from [example 4.4](#) is not functional, since some elements in A are related to more than one $b \in B$ (and therefore not *at most* one as in [definition 4.6](#)). So for example, since both $2 \sim \text{even}$ and $2 \sim \text{prime}$, we cannot make sense of $f(2)$, since it could either be referring to *even* or *prime* (where f is representing \sim).

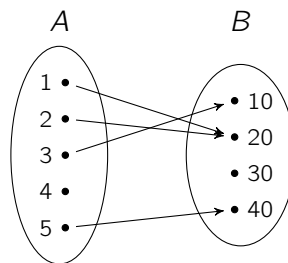


Figure 29: A depiction of the function $f: A \rightarrow B$ from [example 4.7](#).

Another example: recall that a square root of a number $x \in \mathbb{R}$ is some number $y \in \mathbb{R}$ such that $y^2 = x$. Recall also that for $x > 0$, there are always two possible square roots of x , one positive, the other negative. By convention, we use the symbol \sqrt{x} to denote the positive root of x . If we do not assume such a convention, and write for example, $\sqrt{4} = \pm 2$ instead, then if we write $\sqrt{4}$ alone, it is not clear which of $+2$ or -2 this notation is referring to. This way, $x \mapsto \sqrt{x}$ is a function.

To show that a function f has domain A and codomain B , we sometimes write f in “full” as $f: A \rightarrow B$ (where the arrow is indicative of the phrase “from A to B ”). A function $f: A \rightarrow B$ is said to be *total* if for all $a \in A$, there exists some $b \in B$ such that $f(a) = b$. In other words, a function f is total if every a in the domain has a

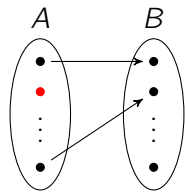


Figure 30: A total function cannot leave an element in A unrelated to any element in B

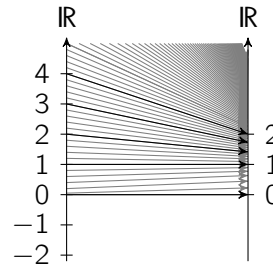


Figure 31: A visualisation of the square root function $f: \mathbb{R} \rightarrow \mathbb{R}$ where $f(x) = \sqrt{x}$.

pair in f (unlike in the example we just gave, where $4 \in A$ had no input-output pair in f , see [figures 29](#) and [30](#)). To show that f is a total function with domain A and codomain B , we denote it by writing $f: A \rightarrow B$ instead of $f: A \rightarrow B$. If a function is not total, i.e., if there is at least one $a \in A$ with no existing input-output pair in f , then we say f is *partial*.

Definition 4.9 (Domain restriction). Let $f: A \rightarrow B$ be a function, and let $A' \subseteq A$. Then we define the function $(f \upharpoonright A'): A' \rightarrow B$, read f *restricted to* A' , by

$$f \upharpoonright A' := \{\langle a, b \rangle \in f : a \in A'\},$$

or equivalently,

$$(f \upharpoonright A')(a) := f(a)$$

for $a \in A'$.

Example 4.10. If $f: A \rightarrow B$ is the same as in [example 4.7](#), and $A' = \{1, 2, 3\} \subseteq A$, then $f \upharpoonright A' = \{\langle 1, 20 \rangle, \langle 2, 20 \rangle, \langle 3, 10 \rangle\}$ (see [figure 32](#)). Similarly, $f \upharpoonright \{1, 2, 3, 5\} = f$, but $f \upharpoonright \{1, 2, 3, 5\}$ is total, unlike f , which is partial.

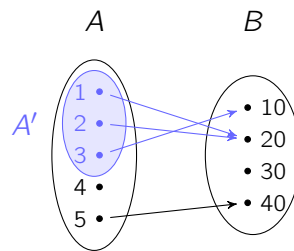


Figure 32: An example of domain restriction. The blue arrows comprise the function $f \upharpoonright A'$, where $A' \subseteq A$.

A. Solutions to Exercises

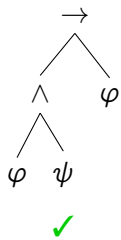
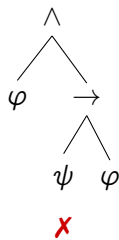
Exercise 1.21

1. (a), (d), (e), (h), (j), (l) are statements, the rest are not. Notice that (k) is an instance of the liar’s paradox.
2.
 - a) Knights do not always tell the truth, or equivalently, Knights sometimes lie
 - b) $1 \geq 2$
 - c) My cat cannot fly
 - d) There are not finitely many primes, or equivalently, There are finitely many primes
 - e) Wallace and Gromit didn’t go to the moon, or equivalently, Wallace didn’t go to the moon or Gromit didn’t go to the moon (or both).
 - f) Imaginary numbers do exist!
3.

a) $\neg p$	b) $p \wedge \neg q$
c) $p \rightarrow q$	d) $q \rightarrow p$
e) $p \rightarrow q$	f) $p \leftrightarrow q$
g) $\neg p \wedge \neg q$	h) $\neg(p \wedge q)$
i) $\neg p \vee \neg q$	j) $q \rightarrow \neg p$
k) $p \vee (r \wedge q)$	l) $p \rightarrow (r \wedge q)$
m) $\neg p \wedge r \wedge q$	n) $r \rightarrow \neg p \rightarrow q$
o) $\neg(r \vee q) \rightarrow p$	p) $r \rightarrow \neg p \wedge \neg q$
q) $r \wedge q \wedge \neg p \wedge \neg s$	r) $r \vee q \rightarrow p \wedge \neg s$
s) $r \wedge q \leftrightarrow p \vee s$	t) $(s \rightarrow r \vee p) \wedge (\neg s \rightarrow p \wedge q)$

4. As mentioned in the question, there are many possible syntax trees for some of these. Here we give one possible (wrong) one, the right one, and the corresponding expressions with brackets.

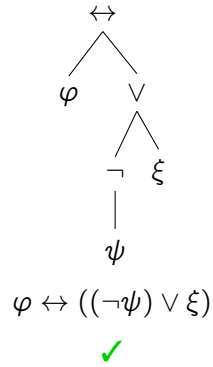
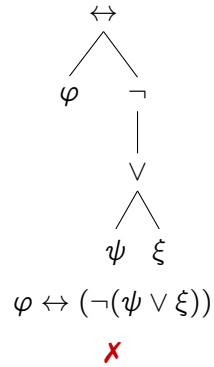
a) $\varphi \wedge \psi \rightarrow \varphi$



X: $\varphi \wedge (\psi \rightarrow \varphi)$

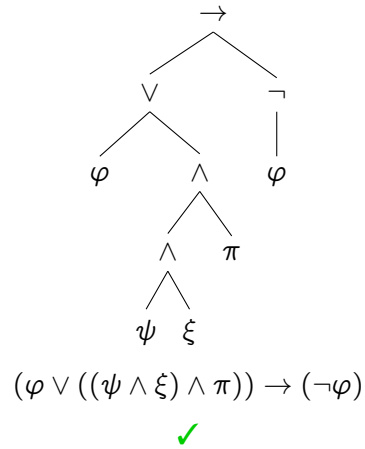
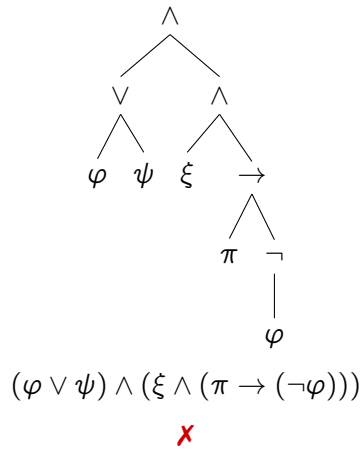
✓: $(\varphi \wedge \psi) \rightarrow \varphi$

b) $\varphi \leftrightarrow \neg\psi \vee \xi$

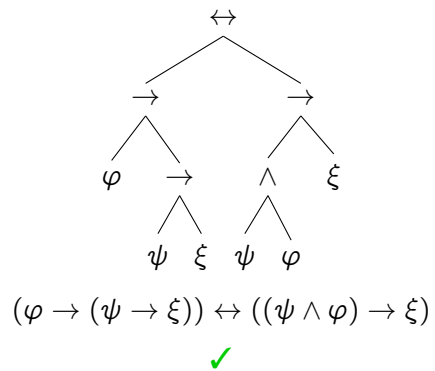
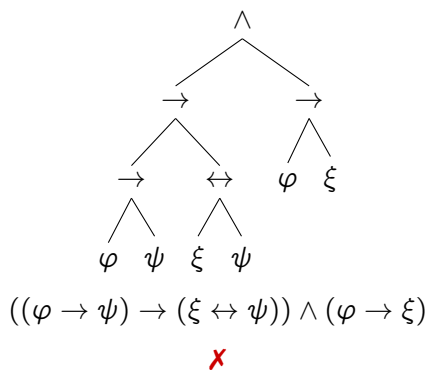


c) $\varphi \vee \psi \wedge \xi \wedge \pi \rightarrow \neg\varphi$

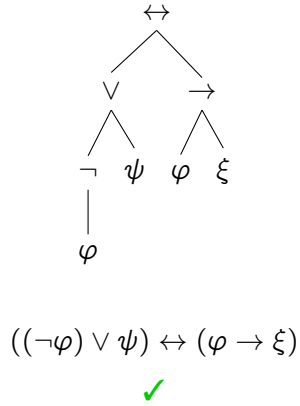
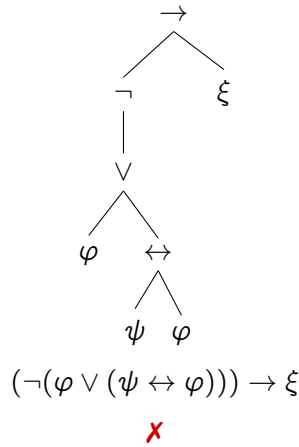
[Hint: remember that \wedge is left associative!]



d) $\varphi \rightarrow \psi \rightarrow \xi \leftrightarrow \psi \wedge \varphi \rightarrow \xi$



e) $\neg\varphi \vee \psi \leftrightarrow \varphi \rightarrow \xi$



5. a) We consider separate cases. Suppose what B said is true, i.e., that A said “I am a knave”. But what this translates to is “I am a liar”, which is none other than the liar’s paradox which we’ve encountered before. Hence what B said cannot be true, and hence B is a knave. This makes what C said correct, and hence C is a knight.
- b) The answer is the same as part (a), but the reasoning is a bit different. The first thing to realise is that similar to part (a), B and C must be of opposite types since they are contradicting each other. So of these two, one is a knight and the other is a knave. Now, if A were a knight, then there would be two knights present, and he would not have lied and said there was only one. On the other hand, if A were a knave, then it would be true that there is one knight present, but being a knave he could not have made a true statement. Therefore A could not have said that there was one knight among them. So B falsely reported A ’s statement, and thus B is a knave and C is a knight.
- c) Suppose A were a knave. Then the statement “At least one of us is a knave” would be false (since knaves make false statements); and hence they would both be knights. Thus, if A were a knave he would also have to be a knight, which is impossible. Therefore A is not a knave, he is a knight. Hence his statement must be true, so at least one of them really is a knave. Since A is a knight, then B must be the knave. So A is a knight and B is a knave.
- d) This problem utilises an (inclusive) “or” statement. With the truth-table in mind, suppose that A is a knave. If he is a knave, then his statement is immediately true (since the first part of the or-statement is true) and therefore he cannot have said it. Hence he must be a knight. Now since he is a knight, we know that his statement must be true. So at least one

of these is true: (1) A is a knave, (2) B is a knight. Since possibility (1) cannot be, then (2) must be correct, and hence A and B are both knights.

- e) The only valid conclusion here is that the author of this problem is not a knight! The fact is that neither a knave nor a knight could have made such a statement.
- f) To begin with, A must be a knave, for if he were a knight, then what he says must be true and therefore he himself must be a knave, which contradicts the fact that knights are truthful. Thus his statement is false, meaning that there is at least one knight among them. Now suppose B were a knave, then A and B would both be knaves, so C would be a knight (we have established that there is at least one knight among them). This would mean that there is exactly one knight among them, hence B 's statement would be true. We would thus have the impossibility of a knave making a true statement. Therefore B must be a knight.

So we know that A is a knave, and B is a knight, hence his statement is true and there is exactly one knight among them. Thus C must also be a knave. Therefore the solution is that A and C are knaves, and B is a knight.

6. a) The only days a lion can say "I lied yesterday" are Mondays and Thursdays. The only day the Unicorn can say "I lied yesterday" are Thursdays and Sundays. Therefore the only day they can both say it is on Thursday.
- b) The lion's first statement implies that it is a Monday or a Thursday. The second statement implies that it is not Thursday. Hence it is Monday.
- c) On no day of the week is this possible! Only on Mondays and Thursdays could he make the first statement, only on Wednesdays and Sundays could he make the second. So there is no day he could say both.
- d) This is a very different situation! It illustrates the difference between making two statements separately and making one which is the conjunction (\wedge) of the two. Given the statement $a \wedge b$, it follows that both a and b are true separately; but if $a \wedge b$ is false, it only follows that at least one is false.

Now the only day of the week it could be true that the lion lied yesterday and will lie again tomorrow is Tuesday (this is the only day which occurs between the lion's lying days). So the day that the lion said that couldn't be Tuesday, for on Tuesdays the statement is true, but the lion doesn't make true statements on Tuesdays. Therefore it is not Tuesday. Therefore the day must be either Monday or Wednesday.

Exercise 1.29

1. a)

φ	ψ	$(\varphi \rightarrow \psi) \rightarrow (\psi \rightarrow \varphi)$		
T	T	T	T	T
T	F	F	T	T
F	T	T	F	F
F	F	T	T	T

b) This one is a tautology.

φ	ψ	$\varphi \wedge \psi \rightarrow \varphi \vee \psi$		
T	T	T	T	T
T	F	F	T	T
F	T	F	T	T
F	F	F	T	F

c) This one is a contradiction.

φ	$\varphi \wedge \neg \varphi$	
T	F	F
F	F	T

d)

φ	ψ	ξ	$\varphi \vee (\psi \wedge \xi) \rightarrow (\varphi \vee \psi) \wedge \xi$				
T	T	T	T	T	T	T	T
T	T	F	T	F	F	T	F
T	F	T	T	F	T	T	T
T	F	F	T	F	F	T	F
F	T	T	T	T	T	T	T
F	T	F	F	F	T	T	F
F	F	T	F	F	T	F	F
F	F	F	F	F	T	F	F

e)

φ	ψ	ξ	$\varphi \vee (\psi \rightarrow \xi) \rightarrow \xi$		
T	T	T	T	T	T
T	T	F	T	F	F
T	F	T	T	T	T
T	F	F	T	T	F
F	T	T	T	T	T
F	T	F	F	F	T
F	F	T	T	T	T
F	F	F	T	T	F

f)

φ	ψ	$\neg \varphi \vee \neg \psi \rightarrow \varphi \vee \psi$			
T	T	F	F	T	T
T	F	F	T	T	T
F	T	T	T	T	T
F	F	T	T	F	F

2. You can use the tool <https://lc.mt/tt> to generate truth tables and check your answers. Here’s an explanation, together with a “real world” example for (h). The law of syllogism is saying that if φ implies ψ and ψ implies ξ , then φ implies ξ . For instance, if φ is “It rains”, ψ is “the grass gets wet” and ξ is “the grass grows”, then the law of syllogism allows us to deduce, from “If it rains the grass gets wet” and “If the grass gets wet, then it grows” that “If it rains, the grass grows”.

3. a)

φ	ψ	$\varphi \diamond \psi$	
φ	ψ	$\neg \varphi \wedge \neg \psi$	
T	T	F	F
T	F	F	F
F	T	T	F
F	F	T	T

- b) These proofs can either be done via truth-tables, or by applying known tautologies:

$$\begin{aligned} \varphi \diamond \varphi &\leftrightarrow \neg \varphi \wedge \neg \varphi \leftrightarrow \neg \varphi \\ (\varphi \diamond \varphi) \diamond (\psi \diamond \psi) &\leftrightarrow \neg(\varphi \diamond \varphi) \wedge \neg(\psi \diamond \psi) \\ &\leftrightarrow \neg(\neg \varphi) \wedge \neg(\neg \psi) \\ &\leftrightarrow \varphi \wedge \psi \end{aligned}$$

Make sure you understood which law was used for each \leftrightarrow .

c) We have:

$$\begin{aligned} \varphi \vee \psi &\leftrightarrow \neg\neg(\varphi \vee \psi) \\ &\leftrightarrow \neg(\neg\varphi \vee \neg\psi) \\ &\leftrightarrow \neg(\varphi \diamond \psi) \\ &\leftrightarrow (\varphi \diamond \psi) \diamond (\varphi \diamond \psi), \end{aligned}$$

$$\begin{aligned} \varphi \rightarrow \psi &\leftrightarrow \neg\varphi \vee \psi \\ &\leftrightarrow \neg(\neg\neg\varphi \wedge \neg\psi) \\ &\leftrightarrow \neg(\neg\varphi \diamond \psi) \\ &\leftrightarrow \neg((\varphi \diamond \varphi) \diamond \psi) \\ &\leftrightarrow ((\varphi \diamond \varphi) \diamond \psi) \diamond ((\varphi \diamond \varphi) \diamond \psi), \end{aligned}$$

4. a)

φ	ψ	$\varphi \oplus \psi$	$\neg(\varphi \leftrightarrow \psi)$
T	T	F	T
T	F	T	F
F	T	T	F
F	F	F	T

b) We use known tautologies (although doing a truth-table and comparing with 4(a) is fine too).

$$\begin{aligned} (\varphi \oplus \psi) &\leftrightarrow \neg(\varphi \leftrightarrow \psi) \\ &\leftrightarrow \neg((\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)) \\ &\leftrightarrow \neg((\neg\varphi \vee \psi) \wedge (\neg\psi \vee \varphi)) \\ &\leftrightarrow \neg(\neg\varphi \vee \psi) \vee \neg(\neg\psi \vee \varphi) \\ &\leftrightarrow (\neg\neg\varphi \wedge \neg\psi) \vee (\neg\neg\psi \wedge \neg\varphi) \\ &\leftrightarrow (\varphi \wedge \neg\psi) \vee (\psi \wedge \neg\varphi) \\ &\leftrightarrow (\varphi \wedge \neg\psi) \vee (\neg\varphi \wedge \psi) \end{aligned}$$

c) The sum is $A \oplus B$, the carry is $A \wedge B$. The circuit behaves as desired:

A	B	$A \oplus B$	$A \wedge B$
T	T	F	T
F	T	T	F
T	F	T	F
T	T	F	F

Substituting T with 1 and F with 0, we get precisely the table for binary addition.

$$\begin{aligned} \text{d) } S(A, B, C_{in}) &\leftrightarrow (A \oplus B) \oplus C_{in} \\ C(A, B, C_{in}) &\leftrightarrow (A \wedge B) \vee ((A \oplus B) \wedge C_{in}) \end{aligned}$$

The circuit behaves as desired:

			$S(A, B, C_{in})$		$C(A, B, C_{in})$			
A	B	C_{in}	$(A \oplus B) \oplus C_{in}$	$(A \wedge B) \vee ((A \oplus B) \wedge C_{in})$				
T	T	T	F	T	T	T	F	F
T	T	F	F	F	T	T	F	F
T	F	T	T	F	F	T	T	T
T	F	F	T	T	F	F	T	F
F	T	T	T	F	F	T	T	T
F	T	F	T	T	F	F	T	F
F	F	T	F	T	F	F	F	F
F	F	F	F	F	F	F	F	F

Substituting T with 1 and F with 0, we get precisely the table for binary addition of three variables.

$$\begin{aligned} \text{e) } X_1 &= S(A_1, B_1, 0) \\ X_2 &= S(A_2, B_2, C(A_1, B_1, 0)) \\ X_3 &= S(A_3, B_3, C(A_2, B_2, C(A_1, B_1, 0))) \\ X_4 &= S(A_4, B_4, C(A_3, B_3, C(A_2, B_2, C(A_1, B_1, 0)))) \end{aligned}$$

Suppose the digits of $6 + 7$ have binary representation $X_4X_3X_2X_1$. Using the formulæ above with $A_4A_3A_2A_1 = 0110$ and $B_4B_3B_2B_1 = 0111$, we have:

$$\begin{aligned} X_1 &= S(A_1, B_1, 0) \\ &= S(0, 1, 0) = 1 \\ X_2 &= S(A_2, B_2, C(A_1, B_1, 0)) \\ &= S(1, 1, C(0, 1, 0)) \end{aligned}$$

$$\begin{aligned}
 &= S(1, 1, 0) = 0 \\
 X_3 &= S(A_3, B_3, C(A_2, B_2, C(A_1, B_1, 0))) \\
 &= S(1, 1, C(1, 1, C(0, 1, 0))) \\
 &= S(1, 1, C(1, 1, 0)) \\
 &= S(1, 1, 1) = 1 \\
 X_4 &= S(A_4, B_4, C(A_3, B_3, C(A_2, B_2, C(A_1, B_1, 0)))) \\
 &= S(0, 0, C(1, 1, C(1, 1, C(0, 1, 0)))) \\
 &= S(0, 0, C(1, 1, C(1, 1, 0))) \\
 &= S(0, 0, C(1, 1, 1)) \\
 &= S(0, 0, 1) = 1
 \end{aligned}$$

Therefore $6 + 7 = X_4X_3X_2X_1 = 1101$, which represents 13 in binary.

Exercise 2.3

1. a) true b) false (\subseteq , not \in) c) true
 d) false e) false f) true
 g) false h) true i) false (\in not \subseteq)
 j) false ($2 \in [-1, 2]$ but $2 \notin [-2, 2]$) k) true

Exercise 2.5

1. a) $\{\dots, -7, -3, 1, 5, 9, 13, \dots\}$ b) $\{\dots, -16, -9, -2, 5, 12, 19, \dots\}$
 c) $\{0, 1, 4, 9, 16, 25, 36, \dots\}$ d) $\{-4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$
 e) $\{0, 1, 2, 3, 4\}$ f) $\{-\sqrt{5}, \sqrt{5}\}$
 g) $\{\} = \emptyset$ h) $\{-2, -\sqrt{3}, \sqrt{3}, 2\}$
 i) $\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \dots\}$ j) $\left\{ \begin{array}{l} \dots, (0, -1), (0, 0), (0, 1), (0, 2), \dots \\ \dots, (1, -1), (1, 0), (1, 1), (1, 2), \dots \\ \dots, (2, -1), (2, 0), (2, 1), (2, 2), \dots \\ \vdots \end{array} \right\}$

k) $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\} = \mathbb{Z}$
 Explanation: Suppose $X, Y \in \mathbb{Z}$. If we can find two integers a_1 and b_1 such that $Xa_1 + Yb_1 = 1$, then $Xa + Yb$ takes on all values of \mathbb{Z} for different $a, b \in \mathbb{Z}$.

Indeed, suppose we want $Xa + Yb$ to be equal to some $n \in \mathbb{Z}$ of our choice. Then we plug in $a = a_1n$ and $b = b_1n$, since this gives $X(a_1n) + Y(b_1n) = Xa_1n + Yb_1n = n(Xa_1 + Yb_1) = n(1) = n$.

So all we need to do here is show that we can find $a_1, b_1 \in \mathbb{Z}$ such that $5a_1 + 2b_1 = 1$ (which shouldn't be hard).

l) $\{\{0\}, \{1, 0\}, \{1\}, \{2, 0\}, \{2, 1\}, \{3, 0\}, \dots\}$

Note that $\{0, 0\} = \{0\}$, since we don't care about repetition in sets.

2. There are various different ways one can express the same set using set comprehension. Here only one way is given.

a) $\{n \in \mathbb{N} : 10 \leq n \leq 16\}$

b) $\{2n + 3 : n \in \mathbb{N} \text{ and } n \leq 5\}$

c) $\{2^n : n \in \mathbb{N} \text{ and } n \geq 1\}$

d) $\{m^2 : m = 2n + 1 \text{ and } n \in \mathbb{N}\}$

e) $\{7n : n \in \mathbb{Z}\}$

f) $\{2^n : n \in \mathbb{Z}\}$

g) $\{4n + 3 : n \in \mathbb{Z}\}$

h) $\{\{m \in \mathbb{N} : m \leq n\} : n \in \mathbb{Z}\}$

i) $\{\frac{\pi^n}{3} : n \in \mathbb{Z}\}$

j) $\{m \in \mathbb{N} : m/4 \notin \mathbb{N}\}$

k) $\{\frac{10}{9}(1 - 10^{-n}) : n \in \mathbb{N}\}$

Explanation: 10^n is the number 1 followed by n zeros. Subtracting 1, we get $10^n - 1$ which is then the number made up of n nines. Dividing this number by 9 to get $\frac{1}{9}(10^n - 1)$, we obtain the number made up of n ones. Now for this number to be in our set, we want a decimal point to appear after the first digit. Thus we must divide by 10, $n - 1$ times, to get the number $\frac{1}{10^{n-1}} \times \frac{1}{9}(10^n - 1)$, which simplifies to $\frac{10}{9}(1 - 10^{-n})$.

l) This one is quite hard, here is the solution:

$$\{x : \text{for all sets } H, \text{ if } 3 \in H \text{ and for every } z \in H \text{ we have } \{z\} \in H, \text{ then } x \in H\}.$$

In logical symbols,

$$\{x : \forall H((3 \in H \wedge \forall z(z \in H \rightarrow \{z\} \in H)) \rightarrow x \in H)\}.$$

Let's break it down. Let's say a set H is "3-hungry" if it contains 3, and if for each $z \in H$, we have $\{z\} \in H$ too. Since a 3-hungry set contains 3, it will therefore contain $\{3\}$, and consequently also $\{\{3\}\}$, and so on. So any 3-hungry set will be a superset of the set we want to express (let's call it T). Now define

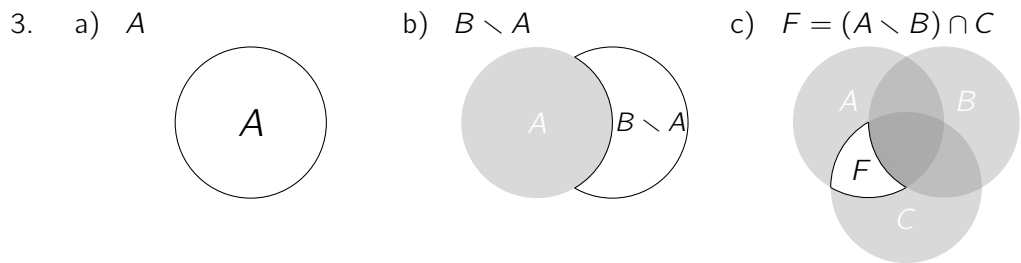
$$S = \{x : x \text{ is in every 3-hungry set}\}.$$

Clearly T is 3-hungry by definition, so $S \subseteq T$. But also every element of T is contained in every 3-hungry set, so $T \subseteq S$. Thus $S = T$, and notice that S is the same set which we have defined above (with less scary notation).

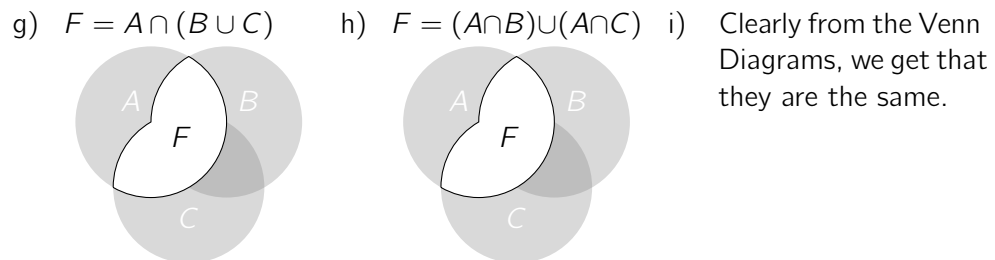
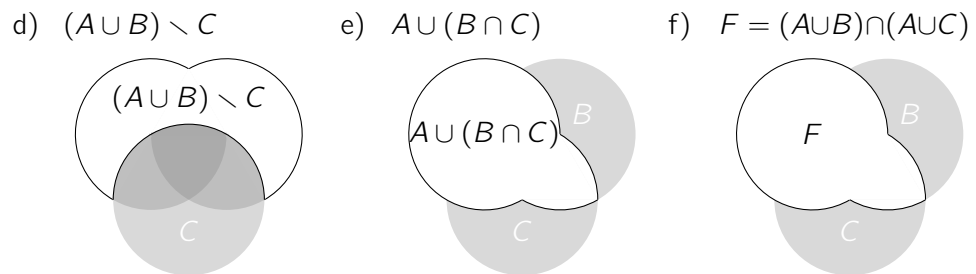
Exercise 2.18

1. a) $\{1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 14\}$ b) $\{2, 4, 6, 8\}$
 c) $\{2, 3, 4, 6, 8, 9, 10, 12, 14\}$ d) $\{1, 4, 5, 7, 8\}$
 e) $\{2, 6\}$ f) $\{10, 12, 14\}$
 g) $\{1, 3, 5, 7\}$ h) $\{2, 3, 6\}$
 i) $\{3, 9\}$ j) $\{2, 3, 4, 6, 8, 9\}$
 k) $\{1, 3, 4, 5, 7, 8, 9, 10, 12, 14\}$ l) $\{\emptyset, \{2\}, \{3\}, \{6\}, \{2, 3\}, \{2, 6\}, \{3, 6\}, \{2, 3, 6\}\}$

2. a) $\{1, 2, 3, 4, 6, 7, 12\}$ b) $\{1, 2\}$
 c) $\{1, 2, 3, 6, 12\}$ d) \emptyset
 e) $\{1, 2, 4, 7\}$ f) $\{1, 2\}$
 g) $\{1, 2\}$



in the set not in the set



j) Clearly from the Venn Diagrams, we get that they are the same.

Throughout questions 4–6, you may use the tool <https://lc.mt/tt> to generate truth tables and check your answers. Make sure you know how to translate a statements about sets into the appropriate proposition, as in [worked example 2.15](#) for instance.

Exercise 2.29

1. a) A proposition is decidedly either true or false, and doesn't have any variables. On the other hand, the truth-value of a predicate may depend on variables which occur within it. We may apply the quantifiers \forall, \exists to predicates which specify the values which the variables in the predicate may take on. If all the variables of a predicate are quantified, then it becomes a proposition (since all variables are accounted for). In this case, we say there are no *free variables*.

For example, consider the predicate $\varphi(x, y)$ defined by “ x or y is an even number”. Then

$$\begin{aligned} \forall x \in \mathbf{IN}, \varphi(x, y) &\leftrightarrow \bigwedge_{x \in \mathbf{IN}} \varphi(x, y) \\ &\leftrightarrow \varphi(1, y) \wedge \varphi(2, y) \wedge \cdots \end{aligned}$$

is a predicate but not a proposition, since even though we have quantified x (we said $x \in \mathbf{IN}$), we still haven't specified the values of y , thus y is a *free variable* in the predicate. But if we consider

$$\begin{aligned} \forall x \in \mathbf{IN}, \forall y \in \mathbf{IN}, \varphi(x, y) \\ &\leftrightarrow \bigwedge_{x \in \mathbf{IN}} \bigwedge_{y \in \mathbf{IN}} \varphi(x, y) \\ &\leftrightarrow (\varphi(1, 1) \wedge \varphi(1, 2) \wedge \varphi(1, 3) \wedge \cdots) \\ &\quad \wedge (\varphi(2, 1) \wedge \varphi(2, 2) \wedge \varphi(2, 3) \wedge \cdots) \\ &\quad \wedge (\varphi(3, 1) \wedge \varphi(3, 2) \wedge \varphi(3, 3) \wedge \cdots) \\ &\quad \wedge \cdots \end{aligned}$$

this is a predicate containing infinitely many \wedge 's just as before, but we know what all of them are, without any variables appearing. Thus it is also a proposition—in fact, we can say that it is false. Since we have \wedge 's, if at least one of them is false, then the whole proposition is false. Indeed, $\varphi(1, 1)$ is false, so the whole proposition is false.

- b) The first predicate says that the m may be different for different values of n , the second says that m is fixed and works for all n . The first one is true, the second one is false.
- c) Note that $\forall n \in \{n \in \mathbf{IN} : n \leq 5\}, \varphi(n)$ is a proposition, because it is a predicate whose variables are all quantified. Thus we may write it out

explicitly as

$$\begin{aligned} & \varphi(1) \wedge \varphi(2) \wedge \varphi(3) \wedge \varphi(4) \wedge \varphi(5) \\ & \leftrightarrow (2 \leq 30) \wedge (6 \leq 30) \wedge (12 \leq 30) \wedge (20 \leq 30) \wedge (30 \leq 30), \end{aligned}$$

thus we see that the proposition is true.

2. a) $\exists x > 1 : x^2 \leq x$
- b) $\forall x, y > 0, x + y \geq 2\sqrt{xy}$
- c) $\exists a \in \mathbb{N} : \forall b \in \mathbb{N}, a^2 \neq b$
- d) $\exists n \in \mathbb{N} : \forall a, b, c, d \in \mathbb{N}, n \neq a^2 + b^2 + c^2 + d^2$
- e) $\exists a, b, c \in \mathbb{R} : \forall x_1, x_2 \in \mathbb{R}, 0 \neq ax_1^2 + bx_1 + c \neq ax_2^2 + bx_2 + c \neq 0$.
Note that $\neg(a = b = c) \leftrightarrow a \neq b \neq c \neq a$. Why do you think we need the extra $\neq a$ at the end?
- f) $\exists \epsilon > 0 : \forall N \in \mathbb{N}, \exists n \geq N : a - \epsilon \geq a_n \vee a_n \geq a + \epsilon$
- g) $\exists \epsilon > 0 : \forall \delta > 0, |x - x_0| < \delta \wedge |f(x) - f(x_0)| \geq \epsilon$
- h) $\forall x \in A, \exists y \in B : \forall z \in C, x + y + z \neq 3\sqrt[3]{xyz}$

Hints for Exercise 3.19

1. The proofs here should be similar to [example theorem 3.5](#), except for (c) which is easiest to do by contrapositive, as is the reverse direction of (d), similar to [lemma 3.9](#).
2. Straightforward direct proof.
3. This should be quite similar to [examples 3.1\(ii\)](#), either method should work. For a direct proof, rewrite the LHS as $\frac{1}{xy}((x - y)^2 + 4xy)$.
4. Use the contrapositive.
5. Straightforward direct proof.
6. Contradiction or contrapositive both work. For contradiction, show that if $\sqrt[3]{x}$ is rational (i.e., not irrational), then you can express x as a rational number too.
7. Use the fact that every integer is either odd or even, and consider both cases for k separately.
8. Direct proof: if x is odd, then x^2 is $(2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1$ for some k , and $k(k + 1)$ is even by the previous problem, so we can write it as $2y$ and get $4(2y) + 1 = 8y + 1$.

9. a) Consider the three cases separately, square them and see that the squares are of the form $3k$ or $3k + 1$ (but never $3k + 2$).
- Also, $10 \cdots 01 = 9 \cdots 9 + 2 = 3(3 \cdots 3) + 2$, which is 2 more than a multiple of 3, so it cannot be a square.
- b) Basically identical to [lemma 3.9](#).
- c) Identical to the proof that $\sqrt{2}$ is irrational.
- d) By contrapositive or contradiction, you can show that if the given number is rational, it implies that $\sqrt{3}$ is rational: $\frac{2+5\sqrt{3}}{1+\sqrt{3}} = \frac{a}{b} \implies \sqrt{3} = \frac{2b-a}{a-5b}$.
- e) It fails because we cannot have an analogue of [lemma 3.9](#), i.e., it's not always true that if n^2 is a multiple of 4, then n is (e.g., if $n = 6$, then $n^2 = 36$ is a multiple of 4, but $n = 6$ isn't).
10. Among four consecutive integers, precisely one of them is a multiple of four, and another one of them is even.
- For a more rigorous argument, write $a - 1, a, a + 1, a + 2$. If a is even (say $a = 2k$), then this product is $4k(k + 1)(2k + 1)(2k - 1)$. Moreover, one of k and $k + 1$ must be even. Proceed similarly in the case that a is odd.
11. The \implies direction is by contradiction. If $x < \epsilon$ for any $\epsilon > 0$, and $x \neq 0$, then it follows that $x > 0$. So in particular we can take $\epsilon = x$, and we get that $x < x$, which is nonsense. The \impliedby direction is obvious.
12. By Pythagoras' theorem, we have $(m + 1)^2 = m^2 + a^2$, which becomes $a^2 = 2m + 1$, so a^2 is odd, which implies that a is odd (this part can be proven identically to [lemma 3.9](#)).
13. a) Reason about the hcf from its definition. Bézout's lemma is important here.
- b) Similar advice to (a).
- c) Proceed by contradiction: suppose $5 \mid ab$, and that $5 \nmid a$ and $5 \nmid b$. This implies that $\text{hcf}(5, a) = \text{hcf}(5, b) = 1$, and use (a) and (b) to show that $\text{hcf}(5, ab) = \text{hcf}(5, a) \text{hcf}(5, b) = 1$, which contradicts that ab is divisible by 5.
14. a) Observe that $4k^2 - 25 = 2(2k^2 - 13) + 1$, i.e., it is an odd number, so it cannot be divisible by 8.
- b) If n is odd, we can write it as $2k + 1$ for some k . Plug this in to $(n + 5)(n - 5)$ and expand, the result should be clearly divisible by 8 (show this by factorising 8 out of it, and recall that $k(k + 1)$ is even).

For the converse, show that if n is even (i.e., put $n = 2k$) we end up with something not divisible by 8 (part (a) should help here).

- c) By standard facts about quadratic equations, this happens if and only if the discriminant $\Delta = n^2$ for some n . If we work out Δ , we get $25 - 8a$. If this equals n^2 , we get $a = -(n + 5)(n - 5)/8$.
- d) Staring at $2x^2 - 5x - \frac{1}{8}(n + 5)(n - 5) = \frac{1}{8}(16x^2 - 40x + (5 + n)(5 - n))$ for long enough, we see it factorises as $\frac{1}{8}(4x - 5 + n)(4x - 5 - n)$.
15. If $\frac{a}{b} + \frac{b}{a} = \frac{a^2 + b^2}{ab} = k$, then $a^2 - kab + b^2 = 0$. This is a quadratic in a , with discriminant $\Delta = b^2(k^2 - 4)$. Clearly we want Δ to be a square since a must be an integer (hence a rational root). Δ is a square if and only if $k^2 - 4$ is a square. Say $k^2 - 4 = \ell^2$. This rearranges to $(k - \ell)(k + \ell) = 4$. This can only happen if $k - \ell = 1$ and $k + \ell = 4$, or $k - \ell = 4$ and $k + \ell = 1$, or else $k - \ell = k + \ell = 2$. The first two cannot happen since k and ℓ are to be integers. The last one implies that $k = 2$, in other words, that the quadratic only has rational solutions for a if it is $a^2 - 2ab + b^2 = 0$. But this means $(a - b)^2 = 0$, i.e., $a = b$, and the question states that $a/b \neq 1$.
16. We don't know if $x = \sqrt{2}^{\sqrt{2}}$ is rational or irrational. If it is rational, then the proof is done. If it is not, then we know $y = \sqrt{2}$ is irrational, and that $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2}^2 = 2$, which is rational.
17. If a, b, c, d are in arithmetic progression with common difference δ , then $a^2 - d^2 = (a + d)(a - d) = (2a + 3\delta)(3\delta)$ and $b^2 - c^2 = (b + c)(b - d) = (2a + 3\delta)\delta$, and dividing completes the proof.
18. Similar to [examples 3.1\(ii\)](#), but this time it involves $(x^2 - 2y)^2$.
19. Direct proof: if a number ends in 5, then we can write it as $10a + 5$, where a is the number without the 5 on the end. Then $(10a + 5)^2 = 100a(a + 1) + 25$, which is precisely $a(a + 1)$ with a 25 added to the end.
20. a) A direct proof: If we expand $(a^2 + b^2)(x^2 + y^2) - (ax + by)^2$, we get $b^2x^2 - 2abxy + a^2y^2$, which equals $(bx - ay)^2$ and is ≥ 0 .
- b) Square rooting both sides (we can do this because both sides of the inequality are clearly positive), we get $|ax + by| \leq \sqrt{a^2 + b^2} \sqrt{x^2 + y^2}$. We can get rid of the $|\cdot|$ since if $ax + by \geq 0$, $|ax + by| = ax + by$, whereas if $ax + by < 0$, the statement of the inequality with the $|\cdot|$ removed is obviously true. Thus we have $ax + by \leq \sqrt{a^2 + b^2} \sqrt{x^2 + y^2}$.

Plugging in $x = y = 1$ gives us the first desired inequality.

For the second part, we divide both sides of the previous inequality by

$\sqrt{a^2 + b^2}$ to get

$$\frac{a}{\sqrt{a^2 + b^2}} + \frac{b}{\sqrt{a^2 + b^2}} \leq \sqrt{2},$$

and letting $a = \sqrt{x}$ and $b = \sqrt{y}$ (we can do this because x and y are positive), we get the second desired inequality.

It is sharp, since we get equality when we plug in $x = y = 1$.

Hints for Exercise 3.27

Most of the hint here are on how to deal with the inductive step, since the base case(s) are almost always straightforward, but always remember that the base case(s) are an essential part of the proof!

1. a) For the inductive step, notice that $1^2 + \dots + n^2 = 1^2 + \dots + (n-1)^2 + n^2 = \frac{n-1}{6}n(2(n-1) + 1) + n^2$ by IH, and simplify.
 - b) Similar.
 - c) Similar, this time we have $\frac{x^n - x}{x-1} + x^n$.
 - d) Similar, in Σ -notation we have $\sum_{k=1}^{n-1} \frac{k^2+k+1}{k^2+k} + \frac{n^2+n+1}{n^2+n} = \frac{(n-1)(n+1)}{n}$, and simplify.
 - e) Notice that in general, $\sum_3^{3n} = \sum_3^{3(n-1)} + \sum_{3(n-1)+1}^{3n}$, so the inductive step is $\sum_{k=3}^{3(n-1)} \frac{1}{4k^2-1} + \sum_{k=3(n-1)+1}^{3n} \frac{1}{4k^2-1} = \frac{3(n-1)-2}{30(n-1)+5} + \frac{1}{4k^2-1} + \frac{1}{4(3n-2)^2-1} + \frac{1}{4(3n-1)^2-1} + \frac{1}{4(3n)^2-1}$, and simplify.
2. a) One can simplify the statement itself by noticing that $k!/(k-2)! = k(k+1)$. The proof is similar to the problems from 1.
 - b) This one is a bit more complicated but not that much, making an observation similar to that in 1(e), we use the fact that a sum like \sum_{2n}^{4n} can be broken into $\sum_{2(n-1)}^{4(n-1)} - \sum_{2(n-1)}^{2n-1} + \sum_{4(n-1)+1}^{4n}$.
- c–e) Straightforward (remember \prod is to \times as \sum is to $+$).
3. Straightforward, use de Morgan's law on two sets as the base case, and the fact that $\bigcap_{k=1}^n A_k = (\bigcap_{k=1}^{n-1} A_k) \cap A_n$; similarly for \bigcup .
4. a) To go to the $n-1$ case, simply remove an element x from A , and apply IH to $A \setminus \{x\}$. Then observe that $\wp A$ is precisely $\wp(A \setminus \{x\})$, together with an exact copy of these sets with x added to each one.
 - b) A similar idea to the above will work, this time being careful with the sizes.

5. This is what mathematicians' sense of humour is like. Obviously this is wrong because $\sin(A + B) \neq \sin A + \sin B$ in general, and similarly the sine of the RHS is not the sine of each term in the fraction.

The proof involves some trigonometric [booklet formulæ](#) in the inductive step.

6. a) Hint: $7^n + 11 = 7(7^{n-1} + 11 - 11) + 11 = 7(7^{n-1} + 11) - 66$, and apply IH.
 b) Similar.
 c) Similar, a bit harder: $2^{n+2} + 3^{2n-1} = 2(2^{(n-1)+2} + 3^{2(n-1)-1} - 3^{2(n-1)-1}) + 3^2(3^{2(n-1)-1}) = 2(2^{(n-1)+2} + 3^{2(n-1)-1}) + 7(3^{2n-3})$, and apply IH.
 d) This one is harder, the same idea works but the proof requires multiple applications of it.
 e) Easier! Just notice that $n^2 + 5n - 2 = (n - 1)^2 + 5(n - 1) - 2 + 2n + 4$ and apply IH.
 f) Similar idea works here.
 g) Same idea as before works, keep at it.
7. Hint: $\alpha^n + \beta^n = (\alpha + \beta)(\alpha^{n-1} + \beta^{n-1}) - \alpha\beta(\alpha^{n-2} + \beta^{n-2})$.
8. Quite easy, just note that $(1+x)^n = (1+x)(1+x)^{n-1} \stackrel{\text{IH}}{>} (1+x)(1+(n-1)x) = 1 + nx + (n-1)x^2 \geq 1 + nx$.
9. a) Hint: $2n + 4 = 2(n - 1) + 4 + 2 \leq 2^{n+1} + 2 \leq 2^{n+1} + 2^{n+1} = 2^{n+2}$
 b) Hint: $(2n)! = 2n(2n - 1)(2(n - 1))! < 2n(2n - 1)(2^{n-1}(n - 1)!)^2 < (2n)^2(2^{n-1}(n - 1)!)^2 = (2^n n!)^2$.
 c) Same hint as question 7.
 d) Hint: $(2n)! = (2n)(2n - 1) \cdots (n + 2)(n + 1)! > (n + 1)(n + 1) \cdots (n + 1)(n + 1)! = (n + 1)^n(n + 1)!$.
10. After applying IH, we need to show that $2\sqrt{n-1} + \frac{1}{\sqrt{n}} < 2\sqrt{n}$. This is equivalent to $2\sqrt{n} - 2\sqrt{n-1} > \frac{1}{\sqrt{n}}$, which is true since

$$2\sqrt{n} - 2\sqrt{n-1} = \frac{2}{\sqrt{n} + \sqrt{n-1}} > \frac{2}{\sqrt{n} + \sqrt{n}} = \frac{1}{\sqrt{n}}.$$

11. The inductive step is essentially as follows:

$$2^{n-1} \left(1 + \prod_{k=1}^n a_k \right) = 2a_n 2^{n-2} \left(1 + \prod_{k=1}^{n-1} a_k \right) - 2^{n-1} (a_n - 1)$$

$$\stackrel{\text{IH}}{\geq} (a_n + a_n) \prod_{k=1}^{n-1} (1 + a_k) \geq \prod_{k=1}^n (1 + a_k).$$

12. What we need to prove here is that if

- (i) $\varphi(0)$ is true, and
- (ii) $\forall n \in \mathbb{N}, (\forall m < n, \varphi(m)) \rightarrow \varphi(n)$,

then $\forall n \in \mathbb{N}, \varphi(n)$. If we let $\psi(n) \leftrightarrow (\forall m \leq n, \varphi(m))$, then notice that $\psi(n)$ implies $\varphi(n)$, so if we show $\forall n \in \mathbb{N}, \psi(n)$, then the proof will be complete. The base case $\psi(0)$ is equivalent to $\varphi(0)$, which is true by (i).

For the inductive step, the IH $\psi(n - 1)$ combined with (ii) allows us to deduce $\psi(n)$. This completes the proof by ordinary (weak) induction. \square

13. This one is quite easy actually, since the standard (booklet) trigonometric identity $\cos(2A) = 2 \cos^2 A - 1$ implies that $2 \cos A = \pm \sqrt{2 + 2 \cos(2A)}$, and since in our case, $A \leq \frac{\pi}{2}$, then it is surely the positive root.

14. Hint: split the regular n -sided polygon into a triangle plus a polygon on $n - 1$ sides.

15. $5^n = 5 \cdot 5^{n-1} \stackrel{\text{IH}}{=} (4 + 1)(a^2 + b^2) = a^2 + b^2 + 4a^2 + 4b^2 = a^2 + 4ab + 4b^2 + b^2 - 4ab + 4a^2 = (a + 2b)^2 + (a - 2b)^2.$

16. a) If we are considering $2(n+1)$ brackets, then suppose $2(k+1)$ is the position of the closing bracket of the first bracket. Then the sequence splits into two, and looks something like this:

$$\underbrace{(\quad \dots \quad)}_{\text{length } 2k} \quad \uparrow \quad \underbrace{(\quad \dots \quad)}_{\text{length } 2(n-k)}$$

There are $C_k C_{n-k}$ possibilities to fill in the gaps, and summing over the possible values of k gives the required relation.

b) If $f(x) = \sum_{n=0}^{\infty} C_n x^n$, then

$$\begin{aligned} (f(x))^2 &= (C_0 + C_1x + C_2x^2 + \dots)^2 \\ &= C_0C_0 + (C_1C_0 + C_0C_1)x + (C_2C_0 + C_1C_1 + C_0C_2)x^2 + \dots \\ &= C_1 + C_2x + C_3x^2 + \dots \\ \implies C_0 + x(f(x))^2 &= C_0 + C_1x + C_2x^2 + \dots = f(x), \end{aligned}$$

so $1 + xf(x)^2 = f(x)$, which we can solve for $f(x)$ to obtain the desired function. Then, use the binomial theorem on the previous result to get that

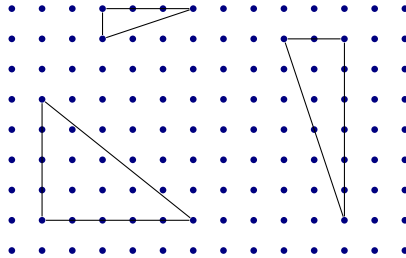
$$f(x) = \sum_{n=0}^{\infty} \binom{1/2}{n+1} \frac{(-4)^{n+1} x^n}{2},$$

and extract the coefficient of x^n from this.

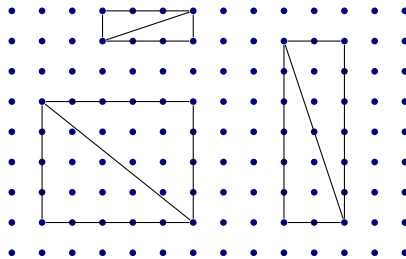
c) This is straightforward, \rightarrow corresponds to ‘(’ and \uparrow to ‘)’.

17. This is by induction on the number of sides of the polygon, with a triangle as the base case. This is one of the few examples where the base case is the tricky part!

Let’s first consider the case where the triangle has two of its sides parallel to the x - and y -axes, respectively, such as the three triangles below.



The area of such triangles is precisely half the area of the rectangles obtained when “doubling” them:



In general, if such a rectangle has base m units and height n units, then it has $i = (m - 1)(n - 1)$ and $b = 2(m + n)$. Using the fact that it has area $A = mn$, combining the equations allows us to express $A = i + \frac{1}{2}b - 1$. Thus Pick’s theorem holds for rectangles when their sides are parallel to the coordinate axes.

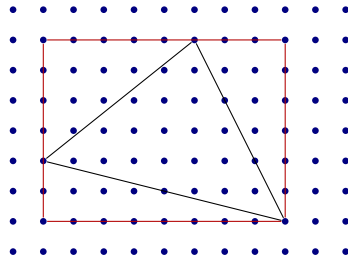
Now to go to the triangles, let m be the length of the side parallel to the x -axis, and n be the length of the side parallel to the y -axis. Then, for the triangle, $b_{\triangle} = m + n + \ell - 1$, where ℓ is the number of points on the slanted side (including both corner points). When the triangle is “doubled”, we get a rectangle with $b_{\square} = 2m + 2n$ boundary points, and $i_{\square} = 2i_{\triangle} + \ell - 2$ interior points. Thus,

$$A_{\triangle} = \frac{1}{2}A_{\square} = \frac{1}{2}(i_{\square} + \frac{1}{2}b_{\square} - 1)$$

$$\begin{aligned}
 &= \frac{1}{2}(2i_{\triangle} + \ell - 2 + m + n - 1) \\
 &= \frac{1}{2}(2i_{\triangle} + b_{\triangle} - 2) = i_{\triangle} + \frac{1}{2}b_{\triangle} - 1,
 \end{aligned}$$

which proves Pick’s theorem for these kinds of triangles.

Finally, to go to more general triangles, notice that the area of any triangle can be expressed as the difference of the area of a rectangle and three rectangles of the previous kind by “enclosing” it as in the following example.



If the area of our desired triangle is A_{\triangle} , the area of the enclosing rectangle is A_{\square} , and the three triangles around our desired triangle have areas A_1 , A_2 and A_3 respectively, then we have

$$A_{\triangle} = A_{\square} - A_1 - A_2 - A_3,$$

where we know that Pick’s theorem can be applied to calculate each area on the right-hand side of the equation.

Thus all you have to do is argue, similar to the way I did above above, that

$$b_{\square} = b_1 + b_2 + b_3 - b_{\triangle} \quad \text{and} \quad i_{\square} = i_1 + i_2 + i_3 + i_{\triangle} + b_1 + b_2 + b_3 - b_{\square} - 3,$$

and consequently use these equations to prove Pick’s theorem for any triangle.

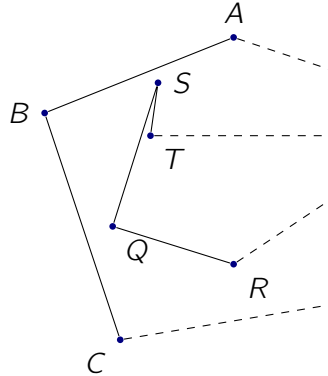
Now for the inductive step, if the number of sides is > 3 , then there are a pair of vertices of the polygon which we can join by a line that lies completely within the polygon, splitting it into two smaller polygons. We will prove this in a moment, but assuming that it is true, then by the IH we can apply Pick’s theorem to these two smaller polygons, obtaining

$$A = i_1 + \frac{1}{2}b_1 - 1 + i_2 + \frac{1}{2}b_2 - 1.$$

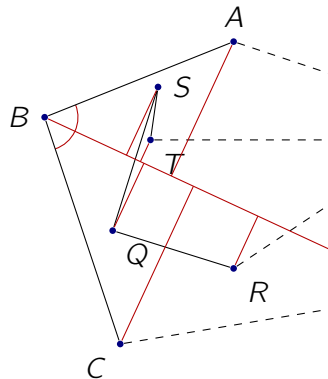
Obtain a relationship between i and b of the large polygon and the corresponding numbers for the two smaller polygons, and deduce that $A = i + \frac{1}{2}b - 1$, completing the proof.

Finally, to see that this dividing line always exists, pick a vertex of the polygon where the interior angle is smaller than 180° . Call it B , so that its neighbouring vertices are A and C , and the interior angle is \widehat{ABC} . Then there are two cases,

either the line segment AC is completely in the polygon, in which case we are done.



If not, then the polygon might look like something above, where we cannot join A to C while staying inside. In this case, draw the angle bisector of \widehat{ABC} , and connect each vertex of the polygon to it by a perpendicular line.



Then as we walk along the bisector, starting from B , the first perpendicular we come across will correspond to a point which we can join to B so that the line joining them lies completely inside the polygon. If not, it has to cross another edge of the polygon, and one of the vertices of that edge would have a perpendicular closer to B .

This finally completes the proof. Notice also that the point chosen (S in this case) is *not* necessarily the point closest to B (which in fact is T in this case).

Hints for Exercise 3.32

Note that any induction proofs involving F_n requires two base cases since we go back two steps in the inductive step.

1. a) Hint: $F_n = F_{n-1} + F_{n-2} \stackrel{\text{IH}}{<} 2^{n-1} + 2^{n-2} < 2^{n-1} + 2^{n-1} = 2^n$.

b) Hint: $F_n = F_{n-1} + F_{n-2} \geq \left(\frac{3}{2}\right)^{n-3} + \left(\frac{3}{2}\right)^{n-4} = \frac{5}{2}\left(\frac{3}{2}\right)^{n-4} > \frac{9}{4}\left(\frac{3}{2}\right)^{n-4} = \left(\frac{3}{2}\right)^{n-2}$

c) Hint: $F_n F_{n+1} = F_n(F_n + F_{n-1}) = F_n^2 + F_n F_{n-1} \stackrel{\text{IH}}{=} F_n^2 + \sum_{k=1}^{n-1} (F_k)^2$.

d) Hint: $\sum_{k=1}^n F_k \stackrel{\text{IH}}{=} F_{n+1} + F_n - 1 = F_{n+2} - 1$.

e) Hint: $F_{n-1} F_{n+1} = F_{n-1}(F_{n-1} + F_n) = F_{n-1}^2 + F_{n-1} F_n \stackrel{\text{IH}}{=} F_{n-2} F_n - (-1)^{n-1} + F_{n-1} F_n = F_n(F_{n-2} + F_{n-1}) + (-1)^n = F_n^2 + (-1)^n$

2. Let $F(n)$ denote the number of sequences of the letters in $\{H, T\}$ of length n , having *no two successive H's*. Clearly we have $F(1) = 2$ and $F(2) = 3$.

Now to build a sequence of length n with no successive H 's, you can start from one of length $n - 1$ and add a T on the end, or else start from one of length $n - 2$ and add an HT to the end. It follows that

$$F(n) = F(n - 1) + F(n - 2),$$

and since $F(1) = 2 = F_3$ and $F(2) = 3 = F_4$, it follows that $F(n) = F_{n+2}$.

Now we are interested in sequences which *do* contain at least one pair of successive H 's, this is simply the remaining ones, i.e., there are $2^n - F_{n+2}$ in number.

Hence, the probability is $(2^n - F_{n+2})/2^n$.

3. a) Hint: https://en.wikipedia.org/wiki/Derangement#Counting_derangements
 b) Straightforward.
 c) Observe that $N!/e = N!e^{-1} = N! \sum_{n=0}^{\infty} (-1)^n/n! \approx N! \sum_{n=0}^N (-1)^n/n!$.
 d) $!15/15! \approx 1/e$.

Hints for Exercise 3.34

- a) If $k = 0$, then there is only \emptyset , and if $n = k$, then the only subset is the whole set.

Otherwise, observe that any subset of size k of $\{1, \dots, n\}$ either contain n , or not. If it doesn't, then it's just a subset of $\{1, \dots, n - 1\}$, there are precisely $\binom{n-1}{k}$ of those. If it does, then it corresponds precisely to a $(k - 1)$ -subset of $\{1, \dots, n - 1\}$, with n added to it. There are therefore precisely $\binom{n-1}{k-1}$ of these.

Therefore, $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$.

- b) In Python, the program would look something like this.

```
def binom(n,k):
    if k==0 or n==k:
```

```

        return 1
    else:
        return binom(n-1,k-1) + binom(n-1,k)

```

c) Again in Python, something like:

```

def pascal(N):
    for n in range (0,N+1):
        for k in range(0,n+1):
            print(binom(n,k), end='\t')
        print()

```

d) This should print `pascal(50)` in under a second.

```

cached_binoms = {}

def binom(n,k):
    global cached_binoms
    if k==0 or n==k:
        return 1
    elif (n,k) in cached_binoms:
        return cached_binoms[(n,k)]
    else:
        ans = binom(n-1,k-1) + binom(n-1,k)
        cached_binoms[(n,k)] = ans
    return ans

```

e) Use the recurrence from (a). The implementation might look something like:

```

def binom(n,k):
    ans = 1
    for i in range(k):
        ans *= n-i
    for i in range(k):
        ans /= i+1
    return ans

```

f) By induction, straightforward, plus the recurrence from (a).

```

g) def expansion(n):
    if n>1:
        print(f'x^{n} + ',end='')
    for k in range(n-1,1,-1):
        print(f'{binom(n,k)}x^{k} + ',end='')
    print(f'{n}x + ',end='')
    print('1')

```


h) Hint: Start with the sum, and use the binomial recurrence from (a), i.e., $\binom{n-k}{k} = \binom{n-1-k}{k} + \binom{n-1-k}{k-1}$.

Bibliography

- [1] E. Lehman, F. T. Leighton, A. R. Meyer, *Mathematics for Computer Science*, MIT OpenCourseware, 2010.
- [2] R. L. Graham, D. E. Knuth, O. Patashnik, *Concrete Mathematics* (2nd ed.), Addison–Wesley, 1994.
- [3] R. M. Smullan, *First-Order Logic* (2nd ed.), Springer–Verlag, 1971.
- [4] R. M. Smullan, *What is the name of this book? The Riddle of Dracula and Other Logical Puzzles*, Prentice–Hall, 1978.
- [5] K. Hrbáček, T. Jech, *Introduction to Set Theory* (3rd ed.), Marcel Dekker Inc., 1999.
- [6] I. Hewitt, *Introduction to University Mathematics* (Michaelmas 2021), University of Oxford Course Notes, 2021.
- [7] G. Pace, *Mathematics of Discrete Structures for Computer Science*, Springer–Verlag, 2012.
- [8] J. Muscat, *Introductory Mathematics*, University of Malta Course Notes, 1999.
- [9] A. Doxiadis, *Logicomix: An Epic Search for Truth*, Bloomsbury UK, 2009.
- [10] H. Ableson, G. J. Sussman, *Structure and Interpretation of Computer Programs* (2nd ed.), MIT University Press, 1996.

Index

- $A * B$, 62
- \bar{A} , see complement laws
- \mathbb{N} , see natural numbers
- \mathbb{Q} , see rational numbers
- \mathbb{R} , see real numbers
- \mathbb{Z} , see integers
- \cap , see intersection
- $\text{cod}(f)$, see codomain
- \cup , see union
- $\text{dom}(f)$, see domain
- \emptyset , see empty set
- \exists , see existential quantifier
- \forall , see universal quantifier
- $\text{hcf}(a, b)$, see highest common factor
- \wedge , see conjunction
- \leftrightarrow , see biconditional
- $\langle\langle a, b \rangle\rangle$, see input-output pair
- \neg , see negation
- \vee , see disjunction
- \mathcal{P} , see power set
- \rightarrow , see implication
- \setminus , see set difference
- \subseteq , see subset
- $a \mid b$, see divides
- $f(a)$, 63
- $f: A \dashrightarrow B$, 64
- $f: A \rightarrow B$, 64
- $f \upharpoonright A$, see domain restriction
- 0th order logic, see propositional logic
- 1st order logic, see predicate logic
- and, see conjunction
- base case, 47
- bi-implication, see biconditional
- biconditional, 9
- binary relation, 62
- Catalan Numbers, 53
- Cauchy–Schwarz inequality, 46
- causation, 8
- codomain, 62
- complement laws, 29
- conjunction, 6
- connective, 6
- contradiction, 18, 38
- contrapositive, 38
- converse, 8
- coprime, 42
- deductive proof, 38
- direct proof, 38
- disjunction, 7
- divides, 40
- domain, 62
- domain restriction, 64
- domino effect, 47
- dummy variable, 34
- empty set, 22
- equivalence, 9
- Euclid, 44
- even, 40
- exclusive or, 7
- existential quantifier, 33
- factor, see divides
- first order logic, see predicate logic
- function, 63
- functional, 63
- greatest common divisor, see highest common factor
- highest common factor, 42
- Hippasos of Metapontion, 43
- iff, see biconditional
- IH, see inductive hypothesis
- implication, 7
- implies, see implication
- inclusive or, 7
- induction, 47

inductive hypothesis, 47
 inductive step, 47
 input-output pair, 62
 integers, 22
 integral domain, 40
 intersection, 26
 intervals, 24

 left associative, 13

 material implication, *see* implication
 multiple, *see* divides

 natural numbers, 22
 necessary condition, 8
 negation, 6
 not, *see* negation

 odd, 40
 only if, 8
 or, *see* disjunction

 partial function, 64
 Pick's theorem, 54
 power set, 31
 precedence, 12
 predicate, 33
 predicate logic, 5, 33
 prime, 44
 proposition, 5
 propositional logic, 5
 Pythagoras, 43

 rational numbers, 22
 real numbers, 22

 relation, 62
 relatively prime, *see* coprime
 right associative, 13

 set comprehension, 24
 set difference, 26
 set-builder notation, *see* set
 comprehension
 statement, 5
 strong induction, 50
 subset, 23
 sufficient condition, 8
 syntax tree, 12

 tautology, 18
 total function, 64
 truth tables, 16

 union, 26
 universal quantifier, 33
 universal set, 29

 Venn diagram, 23
 von Neumann ordinals, 37

 well-defined, *see* functional
 well-formed formula, 11
 wff, *see* well-formed formula

 xor, *see* exclusive or

 Zermelo–Fraenkel Axioms, 36
 zeroth order logic, *see* propositional
 logic
 ZFC, *see* Zermelo–Fraenkel Axioms