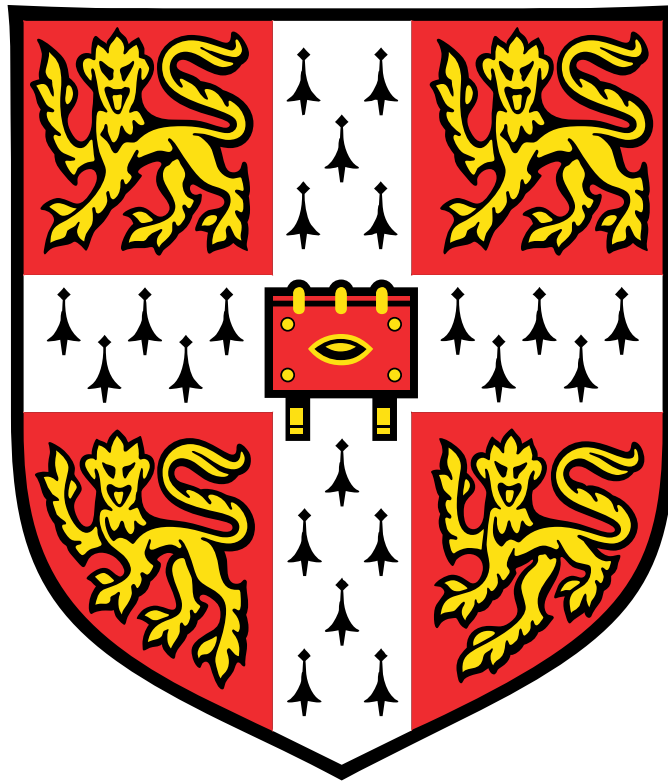


# First Year Lectures on Discrete Mathematics

Thomas Forster

September 19, 2015



# Contents

<b>1</b>	<b>Introduction</b>	<b>7</b>
1.1	Some puzzles to get you started . . . . .	8
<b>2</b>	<b>Read this first!</b>	<b>13</b>
2.1	Test . . . . .	13
2.1.1	The Existential Other . . . . .	13
2.1.2	These are things you will need . . . . .	14
2.1.3	Things you are not going to need and which we won't cover	15
2.1.4	Things you mightn't need . . . . .	15
2.2	Philosophical Introduction: the Pædagogical Difficulties . . . . .	15
2.3	The Type-Token distinction . . . . .	18
2.4	Copies . . . . .	19
2.4.1	Buddhas . . . . .	19
2.4.2	Minis . . . . .	20
2.4.3	Sets . . . . .	20
2.5	The Use-Mention Distinction . . . . .	21
2.5.1	Haddocks' Eyes . . . . .	21
2.5.2	Some good advice . . . . .	22
2.5.3	'Think' . . . . .	22
2.5.4	Ramsey for Breakfast . . . . .	22
2.5.5	The Deaf Judge . . . . .	22
2.5.6	Fun on a train . . . . .	23
2.6	Intension and Extension . . . . .	24
2.7	Semantic Optimisation and the Principle of Charity . . . . .	25
2.7.1	Overloading . . . . .	26
2.8	Fault-tolerant pattern-matching . . . . .	26
2.8.1	Overinterpretation . . . . .	27
2.8.2	Scope ambiguities . . . . .	28
2.9	Howlers of Overinterpretation . . . . .	29
<b>3</b>	<b>Sets and relations</b>	<b>35</b>
3.1	Sets for Discrete Mathematics . . . . .	37
3.1.1	Representing Sets Graphically . . . . .	37
3.1.2	Notating Sets . . . . .	39

3.1.3	Curly Brackets . . . . .	47
3.2	Relations and Functions . . . . .	49
3.2.1	Relations . . . . .	49
3.2.2	Composition and inverse . . . . .	50
3.2.3	Digraphs and matrices for relations-in-extension . . . . .	51
3.2.4	Other properties of relations . . . . .	52
3.2.5	Equivalence relations . . . . .	54
3.2.6	Partial orders . . . . .	57
3.2.7	Products of orders . . . . .	62
3.2.8	Functions . . . . .	65
3.2.9	Some exercises . . . . .	70
3.3	Cardinals . . . . .	71
3.4	Recursive Datatypes . . . . .	75
3.4.1	Induction: revision . . . . .	75
3.4.2	Definition . . . . .	78
3.4.3	Structural induction . . . . .	79
3.4.4	Generalise from $\mathbb{N}$ . . . . .	79
3.4.5	An Induction Exercise Concerning Evaluation . . . . .	80
3.4.6	Well-founded induction . . . . .	82
3.5	Operations on Cardinals, and Curry-Howard . . . . .	91
3.5.1	Natural bijections and Elementary Cardinal Arithmetic . . . . .	92
3.5.2	Cantor's Theorem . . . . .	96
3.5.3	Inclusion-Exclusion . . . . .	97
<b>4</b>	<b>Some Elementary Number Theory</b>	<b>101</b>
4.1	Different bases . . . . .	101
4.2	Euclid's Algorithm . . . . .	102
4.3	Modular Arithmetic . . . . .	103
4.3.1	Euler's theorem . . . . .	104
4.4	The RSA algorithm . . . . .	106
<b>5</b>	<b>Graph theory</b>	<b>109</b>
5.1	Menger's theorem . . . . .	110
5.2	Euler's Theorem on graphs . . . . .	112
<b>6</b>	<b>A Bit of Game Theory</b>	<b>115</b>
6.1	Bimatrix games . . . . .	120
6.1.1	Symmetrical Bimatrix Games . . . . .	122
<b>7</b>	<b>More Exercises</b>	<b>123</b>
<b>8</b>	<b>Answers to Exercises</b>	<b>135</b>

**9 Discussion answers to old tripos questions 149****Health warning**

The notes that follow started off as *my* notes for lecturing from when I was lecturing DM at Queen Mary, and in making them available to my supervisees I offer no guarantees. Word has reached me that Cambridge 1a CS students from other colleges refer to these notes, so I have tidied them up a bit. Notification of typos, etc, suggestions for improvement, etc, will be received with thanks.



# Chapter 1

## Introduction

Warning! Discrete Mathematics is a ragbag of tricks. It doesn't really have a unifying theme, being defined by what it excludes rather than what it contains: it's that part of first-year university mathematics that isn't *continuous*, that *isn't* the stuff that used to be called "calculus"—differentiation and integration. However, on the whole, what gets put into a course like this is not so much a body of knowledge and skills bound together by some internal logic (even negative logic) of its own, but rather the background mathematics that the lecturer thinks that the well-equipped computer science students have to have in their knapsacks. Quite what you need in your knapsack depends to a certain extent on what epoch you are going to live and work in. Nowadays you are less likely to need familiarity with different ways of representing numbers (binary, HEX, octal, decimal) than you would have done thirty years ago, but you are more likely to need to know about cryptography. Some topics which in some sense "ought" to be in a discrete maths course tend to get hived off into other courses; finite state machines often get treated separately (as they were in Cambridge until recently) and my notes on them are still in a separate file.

So this is a course on those bits of background mathematics that don't involve integration and differentiation, and which I think might be useful to you: it isn't supposed to have a consistent theme beyond that, so don't worry if you can't find one. One rather nice side-effect of this is that there is no obviously best book either, and you can do a lot worse than follow the habit I have had for many years of looking in the second-hand books section of charity shops and buying anything that looks like a book on first-year university mathematics. There are lots of such books (because lots of different communities need to do first-year mathematics: engineers, students doing psychology, science, economics, computer science, medicine . . . ) and in places like that they can be quite cheap. There is of course always the danger that if you buy three of them you end up with three different systems of notation, and it has to be admitted that this is a pain. On the other hand, this pain is nothing more than the fact that there are lots of different and pairwise incompatible notations, and that is something—sadly—you are going to have to get used to!

In fact the single most important lesson for you to learn from this course is confidence in manipulating the mathematical symbols you will need later. We will banish mathsangst.

You should now read (or reread!) ‘Alice in Wonderland’ and ‘Through the Looking Glass and what Alice found there’, preferably the edition [4] with Martin Gardner’s annotations, entitled ‘The Annotated Alice’. Lewis Carroll was one of the nineteenth century writers who started the process that led later to the mathematisation of logic that led to modern mathematical logic and computer science. In fact, while we are about it, anything else by Martin Gardner that comes your way should be snapped up and devoured.

The chief difficulty that students have with Discrete Mathematics is the lack of theorems, a lack of *deliverables*. The real lessons you will take away from this course is a not a knapsack full of theorems, but a new way of thinking about the materials. This lack of deliverables can be very disconcerting, and it often has the effect that students can be quite lost and not realise it. There is a difference between—on the one hand—thinking “Yes, I feel comfortable with this stuff: it looks OK” and—on the other—genuinely understanding it in the sense of being able to apply it to any purposes of yours that might crop up. If my experience of teaching this stuff is anything to go by there seems to be a very strong tendency to mistake the first for the second. The danger then is that once you realise that you hadn’t, after all, understood the first three weeks of material, you suddenly find yourself three weeks behind and stuff is still coming at you at the same rate as before. The way to combat this tendency is to make sure you know what you are letting yourself in for, and know how it differs from things you have got embroiled in in the past.

## 1.1 Some puzzles to get you started

Don’t look down on puzzles:

*A logical theory may be tested by its capacity for dealing with puzzles, and It is a wholesome plan, in thinking about logic, to stock the mind with as many puzzles as possible, since these serve much the same purpose as is served by experiments in physical science.*

Bertrand Russell

**EXERCISE 1.** *A box is full of hats. All but three are red, all but three are blue, all but three are brown, all but three are white. How many hats are there in the box?*

**EXERCISE 2.** *The main safe at the bank is secured with three locks, A, B and C. Any two of the three system managers can cooperate to open it. How many keys must each manager have?*



**EXERCISE 3.** *A storekeeper has nine bags of cement, all but one of which weigh precisely 50kg, and the odd one out is light. He has a balance which he can use to compare weights. How can he identify the rogue bag in only three weighings? Can he still do it if he doesn't know if the rogue bag is light?*

**EXERCISE 4.** *A father, a mother, a father-in-law, a mother-in-law, a husband, a wife, a daughter-in-law, a son-in-law, a niece, a nephew, a brother, a sister, an uncle and an aunt all went on holiday. There were only four people! How can this be?*<sup>1</sup>

**EXERCISE 5.** *There were five delegates, A, B, C, D and E at a recent summit.*

*B and C spoke English, but changed (when D joined them) to Spanish,  
this being the only language they all had in common;  
The only language A, B and E had in common was French;  
The only language C and E had in common was Italian;  
Three delegates could speak Portuguese;  
The most common language was Spanish;  
One delegate spoke all five languages, one spoke only four, one spoke only  
three, one spoke only two and the last one spoke only one.*

*Which languages did each delegate speak?*

**EXERCISE 6.** *People from Bingo always lie and people from Bongo always tell the truth.*

- *If you meet three people from these two places there is a single question you can ask all three of them and deduce from the answers who comes from where. What might it be?*
- *If you meet two people, one from each of the two places (but you don't know which is which) there is a single question you can ask either one of them (you are allowed to ask only one of them!) and the answer will tell you which is which. What is it?*

**EXERCISE 7.**

*Brothers and sisters have I none  
This man's father is my father's son*

*To whom is the speaker referring?*

**EXERCISE 8.** *You are told that every card that you are about to see has a number on one side and a letter on the other. You are then shown four cards lying flat, and on the uppermost faces you see*

---

<sup>1</sup>I think you have to assume that the aunt is an aunt in virtue of being an aunt of another member of the party, that the father is a father of another member of the party, and so on.

E K 4 7

*It is alleged that any card with a vowel on one side has an even number on the other. Which of these cards do you have to turn over to check this allegation?*

**EXERCISE 9.** *A bag contains a certain number of black balls and a certain number of white balls. (The exact number doesn't matter). You repeatedly do the following. Put your hand in the bag and remove two balls at random: if they are both white, you put one of them back and discard the other; if one is black and the other is white, you put the black ball back in the bag and discard the white ball; if they are both black, you discard them both and put into the bag a random number of white balls from an inexhaustible supply that just happens to be handy.*

*What happens in the long run?*

**EXERCISE 10.**

	3	8						
	1	6		4		9	7	
4		7	1					6
		2	8		7			5
	5			1			8	
8			4			2		
7		5			1	8		4
	4	3		5		7	1	
						6		

**EXERCISE 11.** *Hilary and Jocelyn are married. One evening they invite Alex and Chris (also married) to dinner, and there is a certain amount of handshaking, tho' naturally nobody shakes hands with themselves or their spouse. Later, Jocelyn asks the other three how many hands they have shaken and gets three different answers.*

*How many hands has Hilary shaken? How many hands has Jocelyn shaken?*

*The next day Hilary and Jocelyn invite Chris and Alex again. This time they also invite Nicki and Kim. Again Jocelyn asks everyone how many hands they have shaken and again they all give different answers. How many hands has Hilary shaken this time? How many has Jocelyn shaken?*

These two are slightly more open-ended.

**EXERCISE 12.** *You are given a large number of lengths of fuse. The only thing you know about each length of fuse is that it will burn for precisely one minute. (They're all very uneven: in each length some bits burn faster than others, so you don't know that half the length will burn in half a minute or anything like that). The challenge is to use the burnings of these lengths of fuse to measure time intervals. You can obviously measure one minute, two minutes, three minutes and so on by lighting each fuse from the end of the one that's just about to go out. What other lengths can you measure?*

**EXERCISE 13.** *A Cretan says “Everything I say is false”. What can you infer?*

Those exercises might take you a little while, but they are entirely do-able even before you have done any logic. Discuss them with your friends. You might want to devote your first seminar discussion to them. Don’t give up on them: persist until you crack them!

If you disposed of all those with no sweat try this one:

**EXERCISE 14.** *You and I are going to play a game. There is an infinite line of beads stretching out in both directions. Each bead has a bead immediately to the left of it and another immediately to the right. A **round** of the game is a move of mine followed by a move of yours. I move first, and my move is always to point at a bead. All the beads look the same: they are not numbered or anything like that. I may point to any bead I have not already indicated. You then have to give the bead a label, which is one of the letters **a–z**. The only restriction on your moves is that whenever you are called upon to put a label on the neighbour of a bead that already has a label, the new label must be the appropriate neighbour of the bead already labelled, respecting alphabetical order: the predecessor if the new bead is to the left of the old bead, and the successor if the new bead is to the right. For example, suppose you have labelled a bead with ‘**p**’; then if I point at the bead immediately to the right of it you have to label that bead ‘**q**’; were I to point to the bead immediately to the left of it you would have to label it ‘**o**’. If you have labelled a bead ‘**z**’ then you would be in terminal trouble were I to point at the bead immediately to the right of it; if you have labelled a bead ‘**a**’ then you would be in terminal trouble if I then point at the bead immediately to the left of it. We decide in advance how many rounds we are going to play. I win if you ever violate the condition on alphabetic ordering of labels. You win if you don’t lose.*

Clearly you are going to win the one-round version, and it’s easy for you to win the two-round version. The game is going to last for five rounds. How do you plan your play? How do you feel about playing six rounds?

**EXERCISE 15.** *Have a look at <http://brainden.com/crossing-river.htm>*

It may surprise you (and it would probably surprise most people) to be told that all these puzzles are mathematical, even tho’s they don’t involve any numerical calculation . . . . Welcome to Discrete Mathematics!



## Chapter 2

# Read this first!

I am not going to expose you to any new Mathematics in this chapter, but that doesn't mean you should skip it. Read it first, to prepare you for what is to come. I am a great believer in *Naming the Devil*: philosophers have argued for a long time about the relation between thought and language but we do all agree that many things become easier to see and recognise once you have a name for them<sup>1</sup>. In the next few sections I shall be introducing you to some terminology. You won't have to prove anything using it, but it will help you once you come to proving other things, and it will help you get your bearings.

### 2.1 Test

This test is not in any sense compulsory, but if you have a crack at it the feedback you get might be extremely useful to you. Send me your submissions either by email (I accept WORD, pdf, ps, dvi and plaintext—no zips please) or fax.

#### 2.1.1 The Existential Other

Many of my students ask me how to write an exam answer. Robert Craft asked Stravinsky whom he wrote for; Stravinsky replied “For myself and the Hypothetical Other”. That should be the audience for which you write your exam answers, and explanations. Who is your Hypothetical Other?

There are many approaches to this, but one that will help you in practising to write answers is to write an answer in the form of an explanation for a suspicious person of at least normal intelligence. If you have an annoying younger sibling

---

<sup>1</sup>In [12] Oliver Sacks wrote “Muscular Dystrophy . . . was never seen until Duchenne described it in the 1850's. By 1860, after his original description, many hundreds of cases had been recognised and described, so much so that Charcot said “How come that a disease so common, so widespread, and so recognisable at a glance—a disease that has doubtless always existed—how come that it is only recognised now? Why did we need M. Duchenne to open our eyes?”

who won't take anything on trust, then write it for them. Or it could be your supervision partner who slept in and missed the supervision at which you learnt these cool things that you now have to explain to them. The key idea is to write *for an audience*. The point of having an audience in mind is that—when you wonder “shall I put this in? Shall I leave that out?”—your knowledge of the audience tells you which way to jump.

Bearing this in mind will help you write answers to these questions which might enable me to get a clear picture of what you understand and what you don't.

### 2.1.2 These are things you will need

#### EXERCISE 16.

1. Factorise  $x^2 - y^2$ .
2. What is the sum of the first  $n$  natural numbers?
3. If you toss a coin and roll a die<sup>2</sup> how many different results can you get? How about two coins and two dice? How about four dice? Make explicit to yourself the way you calculated these answers.
4. How many ways are there of arranging  $n$  things in a row? Can you explain why?
5. The expression ‘ $\binom{n}{r}$ ’; what does it mean, and what is its value?
6. What is a function? Explain injective and surjective. Let  $A = \{a, b\}$ ;  $B = \{1, 2, 3\}$ ; What are the members of  $A \times B$ ? of  $B \times A$ ? Identify these members (to your annoying younger sibling). How many functions are there from  $A$  to  $B$ ? From  $B$  to  $A$ ? Identify these functions (to your annoying younger sibling)
7. What is a prime number?
8. (a)  $x^{(y^z)}$ : is this the same as  $(x^y)^z$ ? Can you simplify either of these further?  
(b) What is  $x^0$ ? Do you remember why?
9. We will also assume you know about matrix multiplication, tho' not much will hang on it.

Multiply the matrix

$$\begin{pmatrix} 1 & 2 & 0 \\ 2 & 1 & 3 \\ 0 & 3 & 1 \end{pmatrix}$$

---

<sup>2</sup>Yes, ‘die’ is the singular of ‘dice’!

by the matrix

$$\begin{pmatrix} 2 & 1 & 1 \\ 0 & 1 & 3 \\ 1 & 0 & 1 \end{pmatrix}$$

explaining the steps.

Much if not all of this will be explained below

### 2.1.3 Things you are not going to need and which we won't cover

Complex numbers, truth tables ...

### 2.1.4 Things you mightn't need

Some of the following you won't need directly in 1a DM. However you will need them for other courses, and if you haven't got these under control it might be an early sign of trouble ahead not just in DM but also in the other courses for which you will need them.

- Sums of Arithmetic Progressions, sums of Geometric Progressions,
- Consider the power series

$$1 + x + x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 + 13x^7 \dots$$

where the coefficient of ' $x^n$ ' is the  $n$ th Fibonacci number. Do you know how to sum it?

- Expansion of  $(1 + x)^n$ ;

## 2.2 Philosophical Introduction: the Pædagogical Difficulties

It might seem odd to kick off a file of course materials on Discrete Mathematics with a section that has a title like this, but there is a reason. Some proofs just are hard, and people experience difficulty accordingly. But there are bottlenecks where people experience difficulties with the underlying concepts, and particularly with the notation.

The hard part of doing discrete maths isn't learning the proofs of the theorems. By and large the proofs are not particularly difficult at this level—though they can appear daunting. The hard part is making a certain kind of mental jump. Once you have made this jump, everything is easy. Let me explain.

Mathematicians often complain that lay people think that mathematics is about numbers. It isn't, and they are right to complain. Not just because it's a mistake, but because it's a mistake that throws people off the scent. Mathematics is a process of formalisation and abstraction that can be applied to all sorts of things, not just numbers. It just so happens that the only bits of mathematics that the average lay person encounters is mathematics as applied to *numerosity*, which is where numbers come from. In fact we can apply mathematical methods to all sorts of other ideas. (Geometry, for example).

### Variables and Things

In applying mathematical methods to a topic we find that we take a number of steps. One of them is summarised in a famous remark of the twentieth century philosopher W.V.Quine: "To be is to be the value of a variable". You are probably quite happy if I say

*"Let  $x$  be a number between 1 and 1000; divide it by 2 ..."*

or (if you are old enough to have done geometry at school)

*"Let  $ABC$  be a triangle; extend the side  $AB$  ..."*

In contrast you are almost certainly not happy if I say

*"Let  $R$  be a binary relation on a set  $X$ ; compose it with its inverse"*.

Why is this? It is because numbers (and perhaps triangles) are mathematical objects in your way of thinking, whereas relations aren't. And what has this got to do with being the value of a variable? Quine's criterion for a species of object to be a *mathematical* object (in the way that numbers—or perhaps triangles—are) is that variables can range over mathematical objects. From your point of view, the utility of the observations of Quine's is that it enables you to tell which things you are comfortable thinking of mathematically.

Computer Scientists in their slang make the distinction (from the point of view of a programming language) between **first class objects** and the rest. First class objects are the kinds of things that the variables of the language can take as values. Typically, for a programming language, numbers like integers are floating-point reals will be first-class objects but operations on those numbers will not.

This distinction between first-class objects and the rest is echoed in ordinary language (well, in all the ordinary languages known to me, at least) by the difference between nouns and verbs.

Expand on this; burble nominalisation.

Let us take a live example, one that bothers many beginners in discrete mathematics. Relations are not mathematical objects for most people. ("Let  $R$  be a binary relation on a set  $X$ ...") In consequence many people are not happy about being asked to perform operations on relations. The problem is not that they are unacquainted with the fact that—for example—the uncle-of relation is the composition of the brother-of relation with the parent-of relation.



This is, after all, something you can explain easily to any foreigner who asks you what the word ‘uncle’ means! The problem is that they don’t know that this fact *is a fact about composition of relations*. This is because they don’t think of relations as being the kind of things you perform operations on, and that in turn is because they don’t think of relations as **things** at all!

You are quite happy applying operations to numbers. The conceptual leap you have to make here is to be willing to apply operations to relations. Although thinking of them as things (rather than as relations between things) and then thinking of them as the substrates of operations are two steps rather than one, it’s probably best to think of them as two parts of a single move.

But relations are only one example of entities that you are now going to have to think of mathematically. Others are sets, functions and graphs.

This business of manufacturing new kinds of thing for us to think about and do things to has been much discussed by philosophers ever since the days of the Ancient Greeks. I first encountered the word for this process—“hypostasis” when I was a philosophy student. But it’s not just philosophy students who need to think about it—as you can see!

### Null objects

Another sign that a species of object (number, set, line ...) has become a mathematical object for you is when you are happy about degenerate or *null* objects of that species. You may remember being told in school that the discovery that zero was a number was a very important one. An analogous discovery you will be making here is that the empty set is a set. (Perhaps this is the same discovery, since numbers like 1,2,3, ... (though not 1.5, 5/3,  $\pi$  ...) are answers to questions about how many elements there are in a set. “0” is the answer to “How many things are there in the empty set?”.) If you think that the empty set “isn’t there” it’s because you don’t think that sets have any existence beyond the existence of their members. Contrast this with the relaxed feeling you have about an empty folder or file in a directory on your computer (as it might be `Things_I_learnt_from_Twitter.xls`). Files and folders on your computer are things that, for you, are unproblematic in a way that makes it possible for you to think of empty ones. You are happy to perform operations on them, after all... reading them, writing to them, copying them .... To that extent you are thinking of them as mathematical objects: the ability to be relaxed about the empty set is one of the things you will acquire when you start thinking of sets as mathematical objects. (The grin remains after the cat has gone.)

We build formulæ by taking conjunctions or disjunctions of collections of formulæ. What is the conjunction of the empty set of formulæ? The disjunction of the empty set of formulæ? Never mind about the answer to this *just* yet (though we will soon); for the moment I am trying to impress you with (i) the novel idea that the question is a sensible one and (ii) that accepting the fact that it is a sensible question is part of thinking of sets as mathematical objects, which in turn is part of doing discrete maths.

Integrate this last para into

(My Ph.D. thesis has the shortest title on record: “N.F.” A title is a string of the preceding para

characters. So the shortest possible title is the empty string of characters. Note that having the empty string as your title is not the same as having no title!) TTBA “untitled”.) When we get on to languages and automata you will have to distinguish between the empty language (the language that has no formulæ in it) and the language whose sole formula is the empty string!!

### Envoi

I’ve inflicted on you this brief digression on Philosophy and Foundations because every student, in mastering the skills and ideas of Computer Science, has to go through a hugely speeded-up version of the journey that Mathematics and Philosophy went through in dreaming up these objects in the first place.

## 2.3 The Type-Token distinction

The terminology ‘type-token’ is due to the remarkable nineteenth century American philosopher Charles Sanders Peirce. (You may have heard the tautology  $((A \longrightarrow B) \longrightarrow A) \longrightarrow A$  referred to as *Peirce’s Law*). The two ideas of token and type are connected by the relation “is an instance of”. Tokens are instances of types.

It’s the distinction we reach for in situations like the following

- (i) “I wrote a *book* last year”
- (ii) “I bought two **books** today”

In (ii) the two things I bought were physical objects, but the thing I wrote in (i) was an abstract entity. What I wrote was a *type*. The things I bought today with which I shall curl up tonight are *tokens*. This important distinction is missable because we typically use the same word for both the type and the token.

- A best seller is a book large numbers of whose *tokens* have been sold. There is a certain amount of puzzlement in copyright law about ownership of tokens of a work versus ownership of the type. James Hewitt owns the copyright in Diana’s letters to him but not the letters themselves. (Or is it the other way round? Either way the man’s a bounder.)
- I remember being very puzzled when I was first told about printing. I was told that each piece of type could only be used once. Once for each book, in the sense of once for each print run Not once for each *copy* of a book. The copies from any one print run are all tokens of a type.
- I read somewhere that “...next to Mary Woollstonecroft was buried Shelley’s heart, *wrapped in one of his poems*.” To be a bit more precise, it was wrapped in a *token* of one of his poems.
- You have to write an essay of 5000 words. That is 5000 word tokens. On the other hand, there are 5000 words used in this course material that come from latin. Those are word types.

- Grelling’s paradox: a **heterological** word is one that is not true of itself. ‘long’ is heterological: it is not a *long* word. ‘English’ is not heterological but *homological*, for it is an English word. Notice that it is word *types* not word *tokens* that are heterological (or homological!) It doesn’t make any sense to ask whether or not ‘italicised’ is heterological. Only word *tokens* can be italicised!
- What is the difference between “unreadable” and “illegible”? A book (type) is unreadable if it is so badly written that one cannot force oneself to read it. A book (token) is illegible if it is so defaced or damaged that one cannot decipher the (tokens of) words on the page.
- We must not forget the difference between a program (type) and the tokens of it that run on various machines.
- Genes try to maximise the number of tokens of themselves in circulation. We attribute the intention to the gene *type* because it is not the action of any *one* token that invites this mentalistic metaphor, but the action of them all together. However it is the number of *tokens* that the type appears to be trying to maximise.

## 2.4 Copies

### 2.4.1 Buddhas

It is told that the Buddha could perform miracles. But—like Jesus—he felt they were vulgar and ostentatious, and they displeased him.

A merchant in a city of India carves a piece of sandalwood into a bowl. He places it at the top of some bamboo stalks which are high and very slippery, and declares that he will give the bowl to anyone who can get it down. Some heretical teachers try, but in vain. They attempt to bribe the merchant to say they had succeeded. The merchant refuses, and a minor disciple of the Buddha arrives. (His name is not mentioned except in this connection). The disciple rises through the air, flies six times round the bowl, then picks it up and delivers it to the merchant. When the Buddha hears the story he expels the disciple from the order for his frivolity.

But that didn’t stop him from performing them himself when forced into a corner. In *Siete Noches* [1] (from which the above paragraph is taken) J. L. Borges proceeds to tell the following story, of a miracle of *courtesy*. The Buddha has to cross a desert at noon. The Gods, from their thirty-three heavens, each send him down a parasol. The Buddha does not want to slight any of the Gods, so he turns himself into thirty-three Buddhas. Each God sees a Buddha protected by a parasol he sent.<sup>3</sup>

<sup>3</sup>As is usual with Borges, one does not know whether he has a source for this story in the literature, or whether he made it up. And—again, as usual—it doesn’t matter.

Apparently he did this routinely whenever he was visiting a city with several gates, at each of which people would be waiting to greet him. He would make as many copies of himself as necessary to be able to appear at all the gates simultaneously, and thereby not disappoint anyone.

### 2.4.2 Minis

Q: How many elephants can you fit in a mini?

A: Four: two in the front and two in the back.

Q: How many giraffes can you fit in a mini?

A: None: it's full of elephants.

Q: How can you tell when there are elephants in the fridge?

A: Footprints in the butter.

Q: How can you tell when there are *two* elephants in the fridge?

A: You can hear them giggling when the light goes out.

Q: How can you tell when there are *three* elephants in the fridge?

A: You have difficulty closing the fridge door.

Q: How can you tell when there are *four* elephants in the fridge?

A: There's a mini parked outside.

### 2.4.3 Sets

If  $A$  is a set with three members and  $B$  is a set with four members, how many ordered pairs can you make whose first component is in  $A$  and whose second component is in  $B$ ?

Weeeell . . . you pick up a member of  $A$  and you pair it with a member of  $B$  . . . that leaves two things in  $A$  so you can do it again . . . . The answer must be three!

Wrong! Once you have picked up a member of  $A$  and put it into an ordered pair—it's still there!

One would tend not to use the word *token* in this connection. One would be more likely to use a word like *copy*. One makes lots of copies of the members of  $A$ . Just as the Buddha made lots of copies of himself rather than lots of *tokens* of himself. I suppose you could say that the various tokens of a type are copies of each other.

It is possible to do a lot of rigorous analysis of this distinction, and a lot of refinements suggest themselves. However, in the culture into which you are moving the distinction is a piece of background slang useful for keeping your thoughts on an even keel, rather than something central you have to get absolutely straight. In particular we will need it later (see page 91) when making sense of ideas like *disjoint union*.

## 2.5 The Use-Mention Distinction

We must distinguish words from the things they name: the word ‘butterfly’ is not a butterfly. The distinction between the word and the insect is known as the “use-mention” distinction. The word ‘butterfly’ has nine letters and no wings; a butterfly has two wings and no letters. The last sentence *uses* the word ‘butterfly’ and the one before that *mentions* it. Hence the expression ‘use-mention distinction’.

### 2.5.1 Haddocks’ Eyes

As so often the standard example is from [2].

[...] The name of the song is called ‘Haddock’s eyes’.”

“Oh, that’s the name of the song is it”, said Alice, trying to feel interested.

“No, you don’t understand,” the Knight said, looking a little vexed.

“That’s what the name is *called*. The name really is ‘*The agèd, agèd man*’.”

“Then I ought to have said, ‘That’s what the *song* is called’?” Alice corrected herself.

“No you oughtn’t: that’s quite another thing! The *song* is called ‘*Ways and means*’, but that’s only what it is *called*, you know!”

“Well, what *is* the song, then?” said Alice, who was by this time completely bewildered.

“I was coming to that,” the Knight said. “The song really is ‘*A-sitting on a Gate*’ and the tune’s my own invention”.

The situation is somewhat complicated by the dual use of single quotation marks. They are used both as a variant of ordinary double quotation marks for speech-within-speech (to improve legibility)—as in “Then I ought to have said, ‘That’s what the *song* is called’?”—and also to make names of words or strings of words—‘The agèd, agèd man’.. Even so, it does seem clear that the White Knight has got it wrong. At the very least if the name of the song really *is* “The agèd agèd man” (as he says) then clearly Alice was right to say that was what the song was called. Granted, it might have more names than just that one—‘Ways and means’ for example—but that was no reason for him to tell her she had got it wrong. And again, if his last utterance is to be true he should leave the single quotation marks off the title, or—failing that (as Martin Gardner points out in [4])—burst into song. These infelicities must be deliberate (Carroll does not make elementary mistakes like that), and one wonders whether or not the White Knight realises he is getting it wrong ... is he an old fool and nothing more? Or is he a paid-up party to a conspiracy to make the reader’s reading experience a nightmare? The Alice books are one long nightmare, and perhaps not just for Alice.

### 2.5.2 Some good advice

Q: Why should you never fall in love with a tennis player?

A: Because ‘love’ means ‘nothing’ to them.

### 2.5.3 ‘Think’

“If I were asked to put my advice to a young man in one word, Prestwick, do you know what that word would be?”

“No” said Sir Prestwick.

“ ‘Think’, Prestwick, ‘Think’ ”.

“I don’t know, R.V. ‘Detail’?”

“No, Prestwick, ‘Think’.”

“Er, ‘Courage’?”

“No! ‘Think’!”

“I give up, R.V., ‘Boldness’?”

“For heaven’s sake, Prestwick, what is the matter with you? ‘Think’!”

“ ‘Integrity’? ‘Loyalty’? ‘Leadership’?”

“ ‘Think’, Prestwick! ‘Think’, ‘Think’, ‘Think’ ‘Think’!”

Michael Frayn: *The Tin Men*. Frayn has a degree in Philosophy.

### 2.5.4 Ramsey for Breakfast

In the following example F.P. Ramsey<sup>4</sup> uses the use-mention distinction to generate something very close to paradox: the child’s last utterance is an example of what used to be called a “self-refuting” utterance: whenever this utterance is made, it is not expressing a truth.

**PARENT:** Say ‘breakfast’.

**CHILD:** Can’t.

**PARENT:** What can’t you say?

**CHILD:** Can’t say ‘breakfast’.

### 2.5.5 The Deaf Judge

**JUDGE** (*to*

**PRISONER**): Do you have anything to say before I pass sentence?

**PRISONER:** Nothing

**JUDGE** (*to*

---

<sup>4</sup>You will be hearing more of this chap.

COUNSEL : Did your Client say anything?

COUNSEL: ‘Nothing’ my Lord.

JUDGE: Funny, I could have sworn I saw his lips move. . .

### 2.5.6 Fun on a train

The use-mention distinction is a rich source of jokes. One of my favourites is the joke about the compartment in the commuter train, where the passengers have travelled together so often that they have long since all told all the jokes they know, and have been reduced to the extremity of numbering the jokes and reciting the numbers instead. In most versions of this story, an outsider arrives and attempts to join in the fun by announcing “*Fifty-six!*” which is met with a leaden silence, and he is tactfully told “It’s not the joke, it’s the way you tell it”. In another version he then tries “*Forty-two!*” and the train is convulsed with laughter. Apparently that was one they hadn’t heard before.<sup>5</sup>

Notice that bus “numbers” are typically numerals not numbers. Not long ago, needing a number 7 bus to go home, I hopped on a bus that had the string ‘007’ on the front. It turned out to be an entirely different route! Maybe this confusion in people’s minds is one reason why this service is now to be discontinued.<sup>6</sup>

A good text to read on the use-mention distinction is the first six paragraphs (that is, up to about p. 37) of Quine’s [11].

Related to the use-mention distinction is the error of attributing powers of an object to representations of that object. I tend to think that this is a use-mention confusion. But perhaps it’s a deliberate device, and not a confusion at all. So do we want to stop people attributing to representations powers that strictly belong to the things being represented? Wouldn’t that spoil a lot of fun? Perhaps, but on the other hand it might help us understand the fun better. There was once a famous English stand-up comic by the name of *Les Dawson* who (did mother-in-law jokes but also) had a routine which involved playing the piano *very badly*. I think Les Dawson must in fact have been quite a good pianist: if you want a sharp act that involves playing the piano as badly as he seemed to be playing it you really have to know what you are doing<sup>7</sup>. The moral is that perhaps you only experience the full *frisson* to be had from use-mention confusion once you understand the use-mention distinction properly.

We make a fuss of this distinction because we should always be clear about the difference between a thing and its representation. Thus, for example, we distinguish between numerals and the numbers that they represent. If we write numbers in various bases (Hex, binary, octal . . .) the numbers stay the same,

<sup>5</sup>For sophisticates: this is a joke about *dereferencing*.

<sup>6</sup>But it’s obvious anyway that bus numbers are not numbers but rather strings. Otherwise how could we have a bus with a “number” like ‘7A’?

<sup>7</sup>Wikipædia confirms this: apparently he was an accomplished pianist.

but the numerals we associate with each number change. Thus the numerals ‘XI’, ‘B’, ‘11’, ‘13’, ‘1011’ all represent the same number.<sup>8</sup>

## 2.6 Intension and Extension

The intension-extension distinction is an informal device but it is a standard one which we will need at several places. We speak of **functions-in-intension** and **functions-in-extension** and in general of **relations-in-intension** and **relations-in-extension**. There are also ‘intensions’ and ‘extensions’ as nouns in their own right.

Consider two properties of being *human* and being a *featherless biped*—a creature with two legs and no feathers. There is a perfectly good sense in which these concepts are the same (or can be taken to be, for the sake of argument: one can tell that this illustration dates from before the time when the West had encountered Australia with its kangaroos!), but there is another perfectly good sense in which they are different. We name these two senses by saying that ‘human’ and ‘featherless biped’ are the same property in extension but are different properties in intension.

A more modern and more topical illustration is as follows. A piece of code that needs to call another function can do it in either of two ways. If the function being called is going to be called often, on a restricted range of arguments, and is hard to compute, then the obvious thing to do is compute the set of values in advance and store them in a look-up table in line in the code. On the other hand if the function to be called is not going to be called very often, and the set of arguments on which it is to be called cannot be determined in advance, and if there is an easy algorithm available to compute it, then the obvious strategy is to write code for that algorithm and call it when needed. In the first case the embedded subordinate function is represented as a function-in-extension, and in the second case as a function-in-intension.

Functions-in-extension are sometimes called the **graphs** of the corresponding functions-in-intension: the graph of a function  $f$  is  $\{\langle x, y \rangle : x = f(y)\}$ . One cannot begin to answer exercise 37 unless one realises that the question must be, “How many binary relations-*in-extension* are there on a set with  $n$  elements?” (There is no answer to “how many binary relations-in-intension ...?” Explain to the Hypothetical Other why this is so.)

It turns up nowadays in the connection with the idea of evaluation. In recent times there has been increasingly the idea that intensions are the sort of things one *evaluates* and that the things to which they evaluate are extensions. Propositions evaluate to truth-values. Truth-values (**true** and **false**) are propositions-in-extension.

We do need both. Some operations are more easily understood on relations-in-intension than relations-in-extension (composition for example) Ditto ancestral

---

<sup>8</sup>Miniexercise: What is that number, and under which systems do those numerals represent it?



## 2.7 Semantic Optimisation and the Principle of Charity

When a politician says “We have found evidence of weapons-of-mass-destruction programme-related activities”, you immediately infer that that have *not* found weapons of mass destruction (whatever they are). Why do you draw this inference?

Well, it’s *so* much easier to say “We have found weapons of mass destruction” than it is to say “We have found evidence of weapons-of-mass-destruction-related programme-related activities” that the only conceivable reason for the politician to say the second is that he won’t be able to get away with asserting the first. After all, why say something longer and less informative when you can say something shorter and more informative? We here, doing a course in discrete mathematics, will tend to see this as a principle about maximising the amount of information you convey while minimising the amount of energy you expend in conveying it. We will be doing a teeny weeny bit of optimisation theory (in chapter 6) but only a very teeny-weeny bit (just enough for you to develop a taste for it) and certainly not enough to come to grips with all the complexities of human communication. But it’s not a bad idea to think of ourselves as generally trying to minimise the effort involved in conveying whatever information it is that we want to convey.

Quine used the phrase “The Principle of Charity” for the assumption one makes that the people one is listening to are trying to minimise effort in this way. It’s a useful principle, in that by charitably assuming that they are not being unnecessarily verbose it enables one to squeeze a lot more information out of one’s interlocutors’ utterances than one otherwise might, but it’s dangerous. Let’s look at this more closely.

Suppose I hear you say

We have found evidence of weapons-of-mass-destruction programme-related activities. (1)

Now you *could* have said

We have found weapons of mass destruction. (2)

Naturally I will of course put two and two together and infer that you were not in a position to say (2), and therefore that you have *not* found weapons of mass destruction. However, you should notice that (1) emphatically does *not* imply that

We have *not* found weapons of mass destruction. (3)

After all, had you been lucky enough to have found weapons of mass destruction then you have most assuredly found evidence of weapons-of-mass-destruction programme-related activities: the best possible evidence indeed. So what is going on?

What’s going on is that (1) does not imply (3), but that (4) does!

We have chosen to say “We have found evidence of weapons-of-mass-destruction programme-related activities” instead of “We have found weapons of mass destruction ”. (4)

Notice that (1) and (4) are not the same!

Now the detailed ways in which this optimisation principle is applied in ordinary speech do not concern us here—beyond one very simple consideration. I want you to understand this optimisation palaver well enough to know when you are tempted to apply it, and to lay off. The formal languages we use in mathematics and computer science are languages of the sort where this kind of subtle reverse-engineering of interlocutors’ intentions is a hindrance not a help. Everything is to be taken literally.

### 2.7.1 Overloading

Not quite the same as ambiguity.

+ on reals and on natural numbers are different operations. They look sort-of similar, because they obey some of the same rules, so there is a temptation to think are the same thing—and certainly to use the same symbol for them. A symbol used in this way is said to be **overloaded**, and it’s not quite the same as the symbol being **ambiguous** because there is a connection of meaning between the two uses which there might not be when a symbol is being used ambiguously.

Overloading is a way of being thrifty in our use of notation. The drawback is that it gets us into the habit of expecting ambiguities even in settings where there is none. This leads us to . . .

## 2.8 Fault-tolerant pattern-matching

My brother-in-law once heard someone on the bus say “My mood swings keep changing.” He—like you or I on hearing the story—knew at once that what the speaker was trying to say was that they suffer from mood swings!

This is an example of something we do all the time. There are things out there is the world that we need to recognise, for good or ill. Things we might want to eat or to mate with, things that might want to eat us. We need to be able to spot these things, and we need to be able to spot them even if they imperfectly presented to us on account of the signal to noise ratio being less than it should be. We need to be able to match the patterns that we see in the outside world to the template in our heads, and because real signals are noisy, we need to be tolerant of faults and noise. hence the expression *fault-tolerant pattern matching*

Reinterpreting silly utterances like this so that they make sense is something that we are incredibly good at. And by ‘incredibly good’ I mean that this is one of the things we can do *vastly* better than computers do (in contrast to the things like multiplying 100-digit numbers in our head, which computers can do

polymorphism?

very much better than we can). In fact we are so good at it that nobody has yet quite worked out how we do it, though there is a vast literature on it, falling under the heading of what people in linguistics call “pragmatics”. Interesting though that literature is I am mentioning it here only to draw your attention to the fact that learning to do this sort of thing *better* is precisely what we are *not* going to do. I want you to recognise this skill, and know when you are using it, in order not to use it *at all*!

Fault-tolerant pattern matching is very useful in everyday life but absolutely no use at all in the lower reaches of computer science. It is all too easy for fault-tolerant pattern matching to turn into *overenthusiastic* pattern matching—otherwise known as *syncretism*: the error of making spurious connections between ideas. A rather alarming finding in the early days of experiments on sensory deprivation was that people who are put in sensory deprivation tanks start hallucinating: their receptors expect to be getting stimuli, and when they don’t, they wind up their sensitivity until they start getting positives. Since they are in a sensory deprivation chamber, those positives are one and all spurious ... we have been *overinterpreting*.

### 2.8.1 Overinterpretation

Why on earth might we *not* want to use it?? Well, one of the differences between the use of symbols in mathematics (e.g. in programming languages) and the use of symbols in everyday language is that in maths we use symbols formally and rigidly and we suffer for it if we don’t. If you write a bit of code with a grammatical error in it the O/S will reject it: “Go away and try again.” One of the reasons why we design mathematical language (and programming languages) in this po-faced fault-intolerant way is that that is the easiest way to do it. Difficult though it is to switch off the error-correcting pattern-matching software that we have in our heads, it is much more difficult still to discover how it works and thereby emulate it on a machine—which is what we would have to do if we were to have a mathematical or programming language that is fault-tolerant and yet completely unambiguous. In fact this enterprise is generally regarded as so difficult as to be not worth even attempting. There may even be some deep philosophical reason why it is impossible even in principle: I don’t know.

Switching off our fault-tolerant pattern-matching is difficult for a variety of reasons. Since it comes naturally to us, and we expend no effort in doing it, it requires a fair amount of self-awareness even to realise that we *are* doing it. Another reason is that one feels that to refrain from sympathetically reinterpreting what we find being said to us or displayed to us is unwelcoming, insensitive, autistic and somehow not fully human. Be that as it may, you have to switch all this stuff off all the same. Tough!

So we all need some help in realising that we do it. I’ve collected in section 2.9 a few examples that have come my way. I’m hoping that you might find them instructive.

### 2.8.2 Scope ambiguities

Years ago when I was about ten a friend of my parents produced a German quotation, and got it wrong. (I was a horrid child, and I blush to recall the episode). I corrected him, and he snapped “All right, everybody isn’t the son of a German Professor”) (My father was Professor of German at University College London at the time). Quick as a flash I replied “What you mean is ‘Not everybody is the son of a professor of German’.”

I was quite right. (Let’s overlook the German professor/professor of German bit). He said that Everybody Isn’t the son of a professor of German. That’s not true. Plenty of people are; I am, for one. What he meant was “Not everybody is ...”. It’s the difference between “ $(\forall x)(\neg \dots)$ ” and “ $\neg(\forall x)(\dots)$ ”—the difference is real, and it matters.

The difference is called a matter of **scope**. ‘Scope’? The point is that in “ $(\forall x)(\neg \dots)$ ” the “scope” of the ‘ $\forall x$ ’ is the whole formula, whereas in “ $\neg(\forall x)(\dots)$ ” it isn’t.

For you, the moral of this story is that you have to identify with the annoying ten-year old rather than with the adult that he annoyed: it’s the annoying 10-year-old that is your rôle model here!

It is a curious fact that humans using ordinary language can be very casual about getting the bits of the sentence they are constructing in the right order so that each bit has the right scope. We often say things that we don’t literally mean. (“Everybody isn’t the son of ...” when we mean “Not everybody is ...”) On the receiving end, when trying to read things like  $(\forall x)(\exists y)(x \text{ loves } y)$  and  $(\exists y)(\forall x)(x \text{ loves } y)$ , people often get into tangles because they try to resolve their uncertainty about the scope of the quantifiers by looking at the overall meaning of the sentence rather than by just checking to see which order they are in!

**EXERCISE 17.** Match up the formulæ on the left with their English equivalents on the right.

- |  |  |
|--|--|
| (i) $(\forall x)(\exists y)(x \text{ loves } y)$   | (a) Everyone loves someone               |
| (ii) $(\forall y)(\exists x)(x \text{ loves } y)$  | (b) There is someone everyone loves      |
| (iii) $(\exists y)(\forall x)(x \text{ loves } y)$ | (c) There is someone that loves everyone |
| (iv) $(\exists x)(\forall y)(x \text{ loves } y)$  | (d) Everyone is loved by someone         |

In the real world people make mistakes and say things that aren’t exactly what they mean ( “Everybody isn’t the son of a german professor”) so listeners have to get quite good at spotting these errors and correcting them. So good, in fact, that we don’t notice we do it. In mathematics (and, in particular, with programming languages) errors of the kind we are so skillful at correcting are never tolerated, so there is no need to have lots of clever software to detect and correct them. The fault-tolerant pattern-matching skill is no longer an asset and its deployment merely distracts us from the task of reading the formula in question. The result is that when we encounter a formula with nasty alternations of quantifiers and tricky scoping, such as the Pumping Lemma from

Languages-and-Automata, we think “This looks ghastly; it can’t be what he means. Life isn’t that bad: let’s reach for the rescoping software” whereas what we should be doing is just trying to read it as it is. Sadly life—or at any rate the Pumping Lemma—really is that bad! The Pumping Lemma is less than completely straightforward to read even with the best of intentions (it has more quantifiers in it than we are used to) and attempting to read it without first switching off your rescoping software is a sure recipe for disaster.

## 2.9 Howlers of Overinterpretation

$\lambda x.\lambda y.2$

What is  $\lambda x.\lambda y.2$ ? Overinterpretation will probably make you think this should simplify to 2; it doesn’t. It really just is the function whose constant value is the function whose constant value is 2. What happens if you apply this function to 3? It’s actually idiotically simple. It’s the result of applying to 3 the function whose constant value is the function whose constant value is 2. And please do not make the mistake of thinking that the function with constant value 2 (the one that returns 2 whatever it is given as argument) is the same as the number 2. There is an important difference between a pint of Guinness and the magic Guinness glass (given by the Leprichaun to the Irishman who released him from a bottle wherein he’d been trapped since the Bronze Age) that automatically refills itself with Guinness every time anyone drinks from it. This difference is not *quite* the same as the difference between 2 and  $\lambda x.2$  but it might help to remind you of that difference.

We do need to distinguish between an object and the unary functions whose constant value is that object. However I don’t want to think about a nullary function (a function with no input) whose [constant] value is  $x$ : that would start to sound too much like mediaeval theology. Nevertheless you might need to think about this kind of thing in the years to come.

### The square of a relation

What is the square of the  $<$  relation on  $\mathbb{N}$ ? Well, one thing it ain’t is  $\{\langle x, y \rangle : x^2 < y^2\}$ , which is the answer one of my students gave once. You get into this mess if you forget what the square of a relation is, and fault-tolerantly match to something you do know, such as squaring of numbers.

Actually it’s a perfect example of the kind of mess you can get into if—before taking on board the idea of overinterpretation—you *free-associate* rather than actually *think*. You have to learn how not to overinterpret—and to be *born again* as a mathmo/compsci—before it is safe to free-associate like this.

## The power set of the empty set

The empty set is the set with no elements. We write it as ' $\emptyset$ ' or occasionally as ' $\{\}$ '. I say *the* empty set because there is in fact only *one* empty set. There is the criterion of identity for sets: two sets are the same set if they have the same members. (Not true for multisets or lists for example). So what is the power set of the empty set? Let's take this question slowly, in stages, and answer it carefully by reading *entirely literally* all the definitions we need to refer to. Recall that the power set,  $\mathcal{P}(X)$ , of a set  $X$  is the set of all subsets of  $X$ .  $Y$  is a subset of  $X$  (written ' $Y \subseteq X$ ') if everything that is in  $Y$  is in  $X$ . So in order to devise the power set of the empty set we are going to open up a bag and put into it everything we can find that is a subset of the empty set.

**Q: So what are the subsets of  $\emptyset$ ?**

Were you about to say "none"? If you were about to say that, then I want to smack your wrist. *Obviously* the empty set is a subset of itself—just look at the definition!! So why did you leave it out? Because it didn't sound like a sensible answer. Why didn't it sound like a sensible answer? Because somewhere in your mind is the unspoken assumption that if I ask you for the something-or-others of  $X$ , you should come up with something new. "He can't be wanting me to mention  $X$  co's he already knows *that*." But recall the definition of 'subset of':  $x \subseteq y$  holds precisely when everything that is in  $x$  is also in  $y$ . So every set is (trivially) a subset of itself. So in particular the empty set is a subset of itself.

Very well, we are agreed there is one subset of  $\emptyset$ , namely  $\emptyset$  itself. Also, by extensionality, it is the *only* subset. (That bit, at least, is unproblematic.)

**Q: OK, So what is the power set of the emptyset?**

Were you about to say  $\emptyset$ ? If so I'm going to smack your wrist yet *again*. You were probably thinking something like "...the empty set is  $\{\}$  so the set containing the empty set must be  $\{\{\}\}$  and the curly brackets can't be doing anything so that must be the same as  $\{\}$ ". This mistake arises from your overinterpretation of data that you feel to be suspect, namely  $\{\{\}\}$ . But if you are careful, you will see that it isn't suspect at all, and it won't be hard to explain this to yourself. The set that contains all the subsets of the empty set has as one of its members (its sole member as it happens) the empty set. So it isn't empty! So it *can't* be the same as the empty set, by extensionality!

So the mistake of thinking that  $\mathcal{P}(\emptyset) = \emptyset$  arises from thinking that the expression ' $\{\emptyset\}$ ' is a bit of suspect data to which you need to apply your fault-tolerant pattern-matching software. The idea that ' $\{\emptyset\}$ ' is a bit of suspect data is a separate mistake that deserves an analysis of its own. The trap is the trap of thinking that because the empty set *has nothing inside it* then it *actually isn't there at all*. Why do you think this? Because you are not happy with the idea of a set being *empty*. But—I put it to you—there is nothing any odder about the idea of an empty *set* than there is about the idea of an empty *folder*,

or an empty *file*. It's no odder than the idea that zero is an integer. "How many strawberries have you got in that punnet?" "None, sadly!". Once you are thinking about sets properly this difficulty goes away.

### The power set of $\{1, 2, 3\}$

I once had a student who, when asked in an exam to write down all the subsets of  $\{1, 2, 3\}$ , supplied only  $\{1, 2\}$ ,  $\{1, 3\}$  and  $\{2, 3\}$ . My guess is that

- She omitted  $\{1, 2, 3\}$  on the grounds that 'subset' probably meant 'proper subset'. We saw this mistake earlier; where?
- She omitted the singleton subsets because she was probably thinking something like "why would anyone want to write down ' $\{1\}$ '? That's silly. Anyone writing that down probably really means '1', and that isn't a set, so I can leave it out".
- She left out the empty set because she didn't think it was there. We've seen this too.

### Affirming the consequent

Years ago I was teaching elementary Logic to a class of first-year law students, and I showed them this syllogism:

"If George is guilty he'll be reluctant to answer questions; George is reluctant to answer questions. Therefore George is guilty."

Then I asked them: Is this argument valid? A lot of them said 'yes'.

We all know that an obvious reason—the first reason that comes to mind—why someone might be reluctant to answer questions is that they might have something to hide. And that something might be their guilt. So if they are reluctant to answer questions you become suspicious at once. Things are definitely not looking good for George. Is he guilty? Yeah—string him up!

But what has this got to do with the question my first-years were actually being asked? Nothing whatever. They were given a premiss of the form  $P \longrightarrow Q$ , and another premiss  $Q$ . Can one deduce  $P$  from this? Clearly not. Thinking that you can is the fallacy of *affirming the consequent*.

There are various subtle reasons for us to commit this fallacy, and we haven't got space to discuss them here. The question before the students in this case was not: do the premisses (in conjunction with background information) give evidence for the conclusion? The question is whether or not the inference from the premisses to the conclusion is logically valid. And that it clearly isn't. The mistake my students were making was in misreading the question, and specifically in misreading it as a question to which their usual fault-tolerant pattern-matching software would give them a swift answer.

$A \times \emptyset$

What is  $A \times \emptyset$ ? Do the sensible thing: try to form ordered pairs whose first components are in  $A$  and whose second components are in  $\emptyset$ . So you pick up a member of  $A$  to put into your *chase* (that's the thing printers hold in their hand and put bits of type in when setting something up in type) and then you reach for a member of  $\emptyset$ . Ouch!

It is possible to get into a tangle by trying to find the correct description of the set of *defective* ordered pairs: things that ought to be ordered pairs but are defective in that altho' they have a first component in  $A$  they somehow lack a second component.  $A \times \emptyset$  is the obvious place to put these discards and offcuts. You might well think that such a discard-or-offcut is just a member of  $A$ , and conclude that  $A \times \emptyset$  is  $A$ .

There are no ordered pairs whose first component is in  $A$  and whose second component is in  $\emptyset$ : any attempt to assemble one fails. A long way of saying this is to say that the set of all such pairs—namely  $A \times \emptyset$ —is  $\emptyset$ , and that of course is the correct answer.

The discards and offcuts never actually get as far as existing (they are the discards and offcuts—after all—from the things that are being brought into existence) so you are not obliged to find anywhere to put them. So you shouldn't be surprised that obvious place to think to put them—namely  $A \times \emptyset$ —should turn out to be empty!

### Is the Identity Relation a Function?

*“Well, functions give you back values when you feed them arguments. The identity relation obviously doesn't do anything so it can't be a function!”*

Is that what you were thinking? Shame on you! *Of course* the identity relation is a function. Look at the definition of a function: each argument is related to one and only one value. The identity relation relates each thing to one and only one thing, namely itself! Duh!

### Is the Identity Relation a Partial Order?

Lots of people say: ‘no’! They think that because it doesn't order things then it can't be a partial order. However, if you read the definitions you will see that it is.

### Can a Relation be both Symmetrical and Antisymmetrical?

*“Well, obviously not, because the words sound as if the conditions are mutually contradictory. On the other hand, why would they be asking me if it was that easy? Er ... is this a multiple choice question ...? Will I be penalised for guessing? ... Can I ask a friend?”*



How about just answering the question? It might be quicker!

Suppose  $R$  is both symmetrical and antisymmetrical. Then, whenever  $x$  is related to  $y$  by  $R$ ,  $y$  is related to  $x$  by  $R$ —by symmetry. But if  $x$  is related to  $y$  and  $y$  to  $x$ , then  $x = y$  by antisymmetry. So if  $x$  is related to  $y$ ,  $x = y$ . So  $R$  must be a subset of the identity relation. So perhaps the identity relation itself might be both symmetrical and antisymmetrical, and so indeed it turns out.

And that is about all you can say!

### Is the Empty Relation Transitive?

I have had students get in a tangle over the question whether or not the empty relation is transitive<sup>9</sup>. Or over the question of whether or not the relation  $\{(1, 2)\}$  is transitive. It's the same tangle. The tangle is this: for a relation to be transitive, it's necessary for it to contain the ordered pair  $\langle x, z \rangle$  whenever it contains the ordered pairs  $\langle x, y \rangle$  and  $\langle y, z \rangle$ . "But what if it doesn't contain any ordered pair?" they wail. Or "What if it contains an ordered pair  $\langle x, y \rangle$  but no pair  $\langle y, z \rangle$ ?" This is overinterpretation. Nobody said it in order to be transitive it had to contain an ordered pair  $\langle x, y \rangle$  or had to contain pairs  $\langle x, y \rangle$  and  $\langle y, z \rangle$ . Merely that **if** it contained pairs  $\langle x, y \rangle$  and  $\langle y, z \rangle$  **then** it would have to contain the ordered pair  $\langle x, z \rangle$ . If it doesn't satisfy the antecedent of the conditional then the condition is trivially satisfied. It's mechanical to check that the empty relation and the relation  $\{(1, 2)\}$  are transitive. Ian Stewart's example *If you pick a guinea pig up by its tail its eyes fall out*—is true. Conditionals whose antecedents are false are vacuously true: in the nature of things these conditionals are unlikely to be *useful* but that doesn't make the *false*.

Haven't defined conditional  
or antecedent

You only get into a tangle if you try to be too clever, and overinterpret.

### Coda

If you get these questions wrong it's almost certainly not because you are ignorant or stupid, but because you are approaching them the wrong way.

---

<sup>9</sup>See section 3.2.4 if you do not yet know what *transitive* means



## Chapter 3

# Sets and relations

That was an introductory pep talk. Now we start on some mathematics!

Sets are extensions. Two sets with the same members have the same set. One could say that sets are properties-in-extension. The properties *human* and *featherless biped* are true of the same things but are not the same property). Lists and multisets are extensional too, but we have to be careful about how we express this fact. The lists  $[1; 3]$  and  $[3; 1]$  have the same members but are not the same lists. For two lists to be the same list they not only have to have the same elements but have to have them in the same *slots*. For two multisets to be the same multiset it is necessary not only that they have the same members but that they have them with the same multiplicity.

which way round to write  
relational composition, and  
which way round to write  
pairs in functions

	ordered	not ordered
repetitions allowed	lists	multisets
no repetitions	wellorderings	sets

### Multisets in brief

The two most natural examples of things-that-we-want-to-think-of-as multisets are (i) the set of roots of a polynomial; and (ii) the set of factors of a natural number. The equation  $x^2 - 3x + 2 = 0$  has two solutions, 1 and 2. That is to say, the set of its solutions is  $\{1, 2\}$ . The equation  $x^2 - 2x + 1$  has two solutions, but they are both 1, so the set of its solutions is the set  $\{1\}$ . But thinking of the collection of answers as a *set* conceals the fact that (in some sense!) there are *two* roots, which just happen to be the same. A better way of presenting the same information would be to say that that the collection of roots is the *multiset*  $\{1, 1\}$ . What this means of course is that the appropriate datatype for the collection of solutions of  $x^2 - 3x + 2 = 0$  is *multiset* not *set*. What about the set of prime factors of 60? That is the multiset  $\{2, 2, 3, 5\}$ . Notice that the collection of roots-of-a-polynomial, or of prime-factors-of-a-natural-number is

always best thought of as a multiset rather than as a set, even if every member has multiplicity one! The multiset  $\{1, 2\}$  is not the same object as the set  $\{1, 2\}$ , any more than the list  $[1]$  is the same as the set  $\{1\}$ .

We will not be much concerned with multisets in the remainder of this course, and the only natural examples of multisets we are going to see here appeared in the last paragraph. However, they are a useful data structure and you should not forget about them entirely. My chief reason for mentioning them here is to bring out into the open the range of different datatypes that may come your way the better to understand what is going on. When you say that  $x^2 - 4x + 4$  has two roots, the extensional data object whose cardinality is two is a multiset not a set. You need to always be clear about what you are dealing with.

### Pure Set Theory

There is a discipline of Pure Set theory, that studies sets that can only have other sets as members, but mostly we will be interested only in sets whose members are things other than sets, and which are therefore of more immediate interest. Sets of numbers, or sets of ordered pairs, or sets of matrices, or sets of sets of matrices. Generally we are not likely to be interested in sets-of-sets-of<sup>*n*</sup> things for *n* more than about two.

While we are about it, there is a distinction Pure Set Theorists make which won't much concern us here. Some sets are *paradoxical*—such as the set of all sets that are not members of themselves. If you think about this you will tie yourself in a knot. Is it a member of itself or not? If it is, it isn't, and if it isn't it is!! Clearly it can't exist—but then I shouldn't have been talking about the **set** of all sets that aren't members of themselves. Set theorists tend to use the word **proper class** for dodgy collections like this one. This is because they use the word **class** in a noncommittal way to cover not only collections that are OK (which means the vast majority of them) but also the dangerous collections like the collection of all sets that aren't members of themselves. A proper class is a thing that's a bit like a set except that it's not allowed to be a member of anything—that's because it's not really there! We also talk of **families** and **collections** when we want to be noncommittal. That explains why when we are considering a class that cannot be a set (like the collection  $\{x : x \notin x\}$  we have just considered) we call it a *proper* class. It's just like calling a subset a *proper* subset, a usage you will have met earlier.

I am giving the paradoxes very short shrift in this course material. They are very titillating, and although they do have connections with things you need to understand (Cantor's theorem and proofs of uncountability and—later on—the unsolvability of the halting problem) they are of little direct relevance and they will most assuredly do your head in should you spend any time on them. There is a theory that the ability to lose sleep over the paradoxes is what distinguishes *homo sapiens* from other species of the genus *homo*, but you shouldn't make that a reason to study them. After all, if you're reading this, the chances are that you are already known to be human.

## 3.1 Sets for Discrete Mathematics

There are hardly any theorems in set theory that we need to know, and, of those that we are going to prove, one of them (Cantor's theorem) is very easy. (In fact, one of the things that disconcerts 1a students is that there are no tangible *deliverables* in 1a DM) What is going to take up most of our time is the task of coming to grips with the notation, which is not designed to make it easy for new entrants to feel at home! The other theorem that I'm going to prove (the Inclusion-Exclusion Principle in section 3.5.3) isn't really very hard either, but if one tries to prove it properly one has to absorb a lot of notation, which makes working through it a very useful discipline. That's the peak, and the rising ground starts here.

$V$  is the universal set, and  $\emptyset$  is the empty set. Another thing all set-theoretic notations have in common is curly brackets. The simplest of the many notations we have uses curly brackets in connection with commas: thus  $\{1, 2, 4\}$  is the set whose members are 1, 2 and 4.

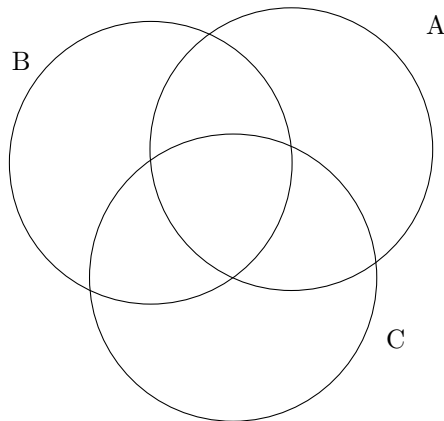
Please note: **these curly brackets are not mere punctuation**, as '(' and ')' are in English. They are part of the grammar. '{' and '}' cannot be replaced by '(' and ')' to make things easier to read. And they cannot be omitted without changing the meaning. Remember the discussion of the power set of the empty set on page 30.

There is no standard notation for lists and multisets, though some programming languages (ML for example) use square brackets for lists with semicolons as delimiters. Thus  $[1; 2; 4]$  is the list whose elements are 1, 2 and 4 *in that order*. (Why did I say *elements* of the list  $[1; 2; 4]$  but *members* of the set  $\{1, 2, 4\}$ ? I'm not sure: I don't think there is any significance to it.)

### 3.1.1 Representing Sets Graphically

Need some pictures

You have probably encountered Venn diagrams. These are a useful way of illustrating equalities and inequalities between unions, intersections and complements of sets.  $A \cup B \cup C = \overline{\overline{A} \cap \overline{B} \cap \overline{C}}$  and suchlike.



Venn diagrams won't *prove* equalities and inequalities, but they can be a useful picture to draw if you are in doubt about them, and can sometimes help you visualise and think things through. Of course if you are going to use them to check an equation or inequation, you have to draw your sets properly: the circle for  $A$  must overlap with the circle for  $B$ , and neither must be included in the other, lest you appear to have a proof that  $A \subseteq B$  or *vice versa*. If you are drawing a picture to check an equation that mentions three sets  $A$ ,  $B$  and  $C$ , you will want to draw the three circles so that all eight unions/intersections/differences (why are there eight? if you don't already know this will be explained in section 3.2.8) are present, and this can in fact be done. Here we come to our first cautionary tale. You can draw *three* circles so that all unions/intersections/differences are present, but you can't draw *four*. Try it and see. The appearance of the number 3 here is to do with the fact that the surface of the paper on which you are drawing your picture has two dimensions. If you want to draw four regions for  $A$ ,  $B$ ,  $C$  and  $D$  then they can't all be *convex*. (Type 'Anthony Edwards' (or 'A.W.F. Edwards') and 'Venn diagram' into your favourite search engine. Yes, and go and look at the windows in Caius chapel.) If you want four convex regions showing all unions/intersections/differences then you have to go up a dimension. You can imagine four spheres in space intersecting in all possible ways. Although this fact is a very cute piece of discrete mathematics in its own right I am dragging it in here as an illustration to warn you about the way in which notations which are handy and attractive sometimes fail to give you the whole picture.

While we are about it there is another reason why you shouldn't think of Venn diagrams as the be-all and end-all of Set theory. Venn diagrams are no good for representing more than two levels of sets. One can indicate a point  $c$  inside a region called  $C$  but one cannot indicate members of  $c$ —should  $c$  be a set in its own right—nor can one indicate things that  $C$  is a member of. This is a grave limitation on Venn diagrams as ways of illustrating facts in set theory.

Examples of important constructs using three levels which therefore cannot be represented:  $\bigcap X$ ,  $\bigcup X$ ,  $\mathcal{P}(X)$ .

Where are these defined?

Moral: Venn diagrams are fine, but don't allow the comfortable feelings you have about them to constrain your imagination when it comes to sets.

Notice that I have just—quite automatically—exploited a common convention that we use a lower case letter (in this case 'c') for a variable to range over elements of a set denoted by the corresponding uppercase variable (in this case 'C'). Some people use a convention that if we are to have a third level—things that  $C$  is to be a member of—we use a calligraphic font:  $\mathcal{C}$ .

### 3.1.2 Notating Sets

I said above 'The simplest notation ...' but as I said there there are actually two quite different ways of notating sets. The system of the previous paragraph takes notations for the individual members of a set, puts them in a row, and places curly brackets round them. The result is a notation for the set whose members we have listed. The other notation for sets also uses curly brackets, but doesn't mention the members explicitly in the way we have just seen: instead it mentions them indirectly (in a way that assembler programmers might recognise as bearing a haunting similarity to *indirect addressing*). The notation

$$\{x : F\}$$

denotes the set of all things satisfying the condition  $F$  that we find after the colon. Thus

$$\{x : x = 2 \vee x = 4\}$$

denotes the set of all things that are equal to 2 or to 4—so we could have written it as

$$\{2, 4\}$$

Similarly

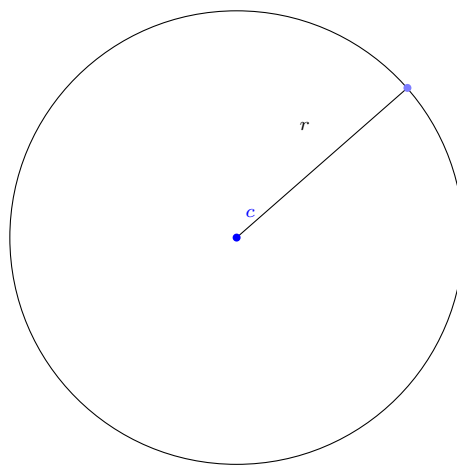
$$\{x : x \in A \vee x \in B\}$$

has a shorter notation too, and one that you know:  $A \cup B$ . This indirect notation, using variables, enables us to write down notations for infinite sets—in contrast to the first notation (curly brackets plus commas), which obviously enables us to point to finite sets only.

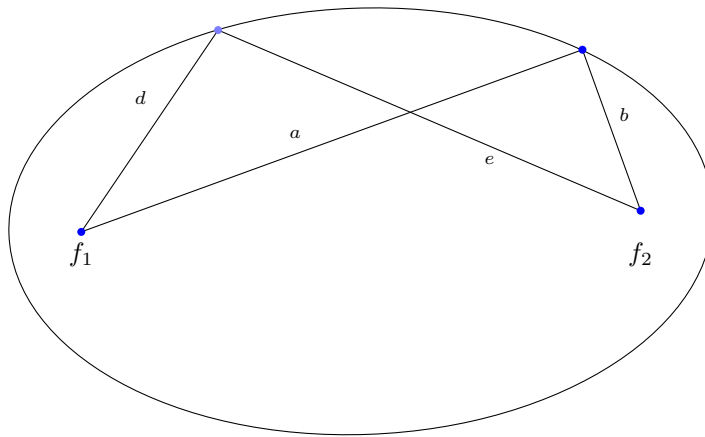
See 47 Some people write ' $\{x|F\}$ ' for the set of things that are  $F$ . The vertical bar has uses already—we will write ' $|x|$ ' for the number of things in the set  $x$ , and ' $|x|$ ' for the absolute value of a complex number  $x$ , and all these are uses you will most certainly encounter (there is a third use: some people write ' $f|X$ ' for the restriction of the function  $f$  to the set  $X$ , though this is probably an attempt to write ' $f \upharpoonright X$ ' when they haven't got the ' $\upharpoonright$ ' sign) and we don't want to introduce further confusion by giving it a fourth use. I shall adhere to the alternative notation that uses a colon:  $\{x : F(x)\}$  as above. However you should be warned that many people prefer the notation with the vertical bar.

A banality to check that you are happy with:  $A = \{x : x \in A\}$ .

**EXERCISE 18.** *A circle is the set of points in the plane (that's  $\mathbb{R}^2$  for the moment) that are a fixed distance from the centre. Write down a set abstract denoting a circle. It will have two free variables in it (“parameters”). (It is customary to write  $d(x, y)$  for the distance between points  $x$  and  $y$ .)*







An ellipse is the set of points in the plane the sum of whose distances from two points (the foci— $f_1$  and  $f_2$  in the picture) is a constant. (In the picture above  $a + b = c + d$ ). Write down a set abstract denoting an ellipse. It will have three free variables in it (“parameters”).

degrees of freedom?

**EXERCISE 19.** A parabola is the set of points the sum of whose distances from a given point and a given line is a constant. Write down a set abstract denoting a parabola.

need lots more exercises here

### Variables and binders

Some people make explicit the presence inside  $F$  of the variable that is to the left of the semicolon, the business variable (or *eigenvariable* if you want a fancy name for it). Thus you might see ‘ $\{x : F(x)\}$ ’ or (since some people don’t) ‘ $\{x : F\}$ ’. Both of these are shorthand for set abstractions. In the first case you are being told that the variable ‘ $x$ ’ really does appear inside the expression that  $F$  represents, and in the second case you aren’t being told this. But usually you will be given the formula in full rather than a shorthand for it.

Several subtleties arise at this point.

1. (Vacuous quantification and abstraction)

What does ‘ $\{x : A\}$ ’ mean, if the variable ‘ $x$ ’ does not appear in  $A$  at all? Well, it means either the empty set or the universe, depending on what  $A$  is. After all, if  $x$  is not mentioned by  $A$ , the yes/no answer to “Is  $x$  in the set?” does not depend on  $x$ ; they’re either all in, or none.

2. (alpha-conversion). There is no difference between  $\{x : F(x)\}$  and  $\{y : F(y)\}$ . Those of you who have done a bit of logic will recognise this as the same phenomenon that  $(\forall x)(F(x))$  and  $(\forall y)(F(y))$  are in some sense the same formula. You may feel that this is a slight bug in the design of our language: it makes distinctions that we don’t need. We will find the same phenomenon arising in lambda calculus, and there there is a known alternative which does not have this bug: combinator logic. There is no space to discuss these matters here. Sufficient unto the day is the evil thereof.

There is a connection here with two other ideas which are probably new to you with this course. Quantifiers and  $\lambda$ -terms. You can take a formula with an ‘ $x$ ’ free in it (such as ‘ $x > 3$ ’) and prefix it by a quantifier, like ‘ $\forall$ ’ or ‘ $\exists$ ’. Or you can take a term with ‘ $x$ ’ free in it (such as ‘ $x + 5$ ’) and prefix it with ‘ $\lambda x$ ’. This gives you expressions like  $\{x : x > 3\}$  or  $(\forall x)(x > 3)$  or  $\lambda x.(x + 5)$  in which the variable ‘ $x$ ’ is no longer free. So the curly-brackets-in-pairs, the quantifiers, and the letter  $\lambda$  are all called **binders**. Often having a word enables you to keep track of the connection of ideas.

Ooops, I mentioned  $\lambda$ -calculus there before telling you what it is.  $\lambda x.F(x)$  is the function that, when given  $x$ , returns  $F(x)$ . (You may have seen the notation ‘ $x \mapsto F(x)$ ’ too.) When we apply a function  $\lambda x.\dots$  to an argument  $a$  we knock the ‘ $\lambda x$ ’ off the front and replace all the ‘ $x$ ’s in the dots by ‘ $a$ ’s. Thus  $\lambda x.x^2$  applied to 2 evaluates to 4.

Some exercises here

Have a look at section 2.9.

Say something about reduction.

$\beta$ -

Of course the thing to the right of the dot might be another lambda term. I shall also adhere to the universal practice of writing ‘ $\lambda xy.(\dots)$ ’ for ‘ $\lambda x.(\lambda y.(\dots))$ ’. Lambda calculus is a great improvement on the old system, under which people would write things like ‘ $y = F(x)$ ’ and ‘ $y = x^2$ ’, relying on an implicit convention that—where ‘ $x$ ’ and ‘ $y$ ’ are the only two variables used—then  $y$  is the output (the vertical axis used to be called “ordinate”) and  $x$  is the input (the horizontal axis used to be called “abscissa”). This convention—and others like it—have served us quite well, but in the information technology age, when one increasingly wants machines to do a lot of the formula manipulations that used to be done by humans, it turns out that lambda notation and notations related to it are more useful. Another reason for using lambda calculus rather than the assumption that  $x$  is an input and  $y$  an output is that life is simpler and syntax is easier to describe if all variables are equivalent in the sense that they don’t come equipped with baggage. We want  $(\forall x)(\Phi)$  to mean the same as  $(\forall y)(\Phi)$  and we want this interchangeability to apply across the board. We will see more of  $\lambda$ -calculus in section 3.5.

**Sumset, Power set etc**

We will now briefly go over some notations that you are probably familiar with, just in case you aren't! You know what ' $\subseteq$ ' means. Care to guess what ' $\supseteq$ ' means? (It's pronounced 'superset'.)

There are other notations along these lines that you will need to know if you do not know them already.

Seen these b4 somewhere

Sumset:  $\bigcup x := \{y : (\exists z)(y \in z \wedge z \in x)\}$ ; and  
Intersection  $\bigcap x := \{y : (\forall z)(z \in x \longrightarrow y \in z)\}$ .

$\mathcal{P}(x)$  is the **power set** of  $x$ :  $\{y : y \subseteq x\}$ .

Set difference:  $x \setminus y$  is the set of things that are in  $x$  but not in  $y$ .

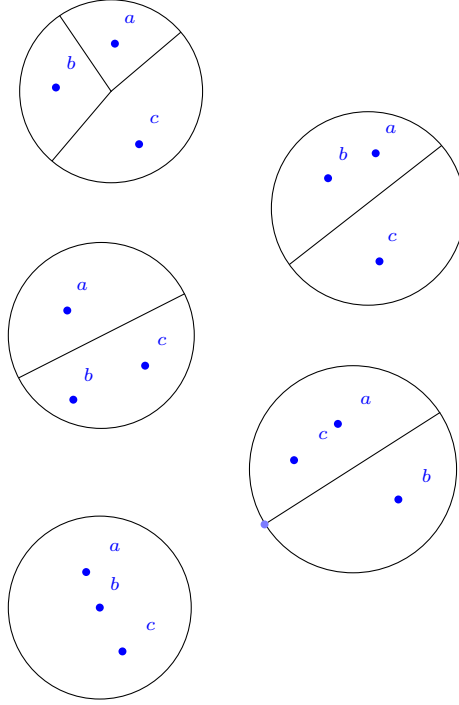
The symmetric difference:  $x \Delta y$ , of  $x$  and  $y$ , is the set of things in one or the other but not both:  $(x \setminus y) \cup (y \setminus x)$ . This is sometimes written 'XOR'.

**DEFINITION 1.** A **partition** of a set  $x$  is a family  $\Pi$  of pairwise disjoint nonempty subsets of  $x$  that collectively exhaust  $x$ . The nonempty subsets comprising the partition are called **pieces**. If  $\Pi_1$  and  $\Pi_2$  are partitions of  $x$ , we say that  $\Pi_1$  **refines**  $\Pi_2$  if every piece of  $\Pi_1$  is a subset of a piece of  $\Pi_2$ . (Do not confuse this capital ' $\Pi$ ' with the capital ' $\Pi$ ' used to denote the product of all numbers in a set.)

**EXERCISE 20.** Which of the sets in the left column are partitions, and of which sets in the right column are they partitions?

- |  |                      |
|--|----------------------|
| (i) $\{\{1\}, \{2, 3\}, \{1, 2\}\}$          | (a) $\{1, 2, 3\}$    |
| (ii) $\{\{1\}, \{2, 4\}, \{3\}\}$            | (b) $\{1, 2, 3\}$    |
| (iii) $\{\{1, 2\}, \{2, 4\}, \{3\}\}$        | (c) $\{1, 2, 3, 4\}$ |
| (iv) $\{\{1, 3\}, \{2, 4\}\}$                | (d) $\{1, 2, 3, 4\}$ |
| (v) $\{\{1\}, \{3\}, \{2, 4\}\}$             | (e) $\{1, 2, 3, 4\}$ |
| (vi) $\{\{1\}, \emptyset, \{3\}, \{2, 4\}\}$ | (f) $\{1, 2, 3, 4\}$ |

**EXERCISE 21.** List all partitions of  $\{a, b, c\}$ . (You might find it helpful to draw a picture of each — a kind of Venn Diagram.)



Need to rotate the diameter in one of these to correct the duplication.

### Restricted variables

We must now brave the jungle of enhancements of the curly bracket notation! Often instead of writing things like

$$\{x : x \in A \wedge \Phi\}$$

(where  $\Phi$  is some condition or other) we move the membership part of the condition to the left of the colon thus:

$$\{x \in A : \Phi\}$$

For example, where  $A = \mathbb{N}$  and  $\Phi$  is  $(\exists y)(x = 2 \cdot y)$ : instead of writing

$$\{x : x \in \mathbb{N} \wedge (\exists y)(x = 2 \cdot y)\} \quad (3.1)$$

we can write

$$\{x \in \mathbb{N} : (\exists y)(x = 2 \cdot y)\} \quad (1)$$

which means exactly the same thing. The difference is merely one of emphasis: the second notation suggests somehow that the natural numbers is a kind of

context or environment for what happens after the colon. And, yes—in case you were wondering—this last thing is, indeed, the same as

$$\mathbb{N} \cap \{x : (\exists y)(x = 2 \cdot y)\} \quad (2)$$

There is a similar notation for the quantifiers: often one writes ‘ $(\forall n \in \mathbb{N})(\dots)$ ’ instead of ‘ $(\forall n)(n \in \mathbb{N} \longrightarrow \dots)$ ’ and ‘ $(\exists n \in \mathbb{N})(\dots)$ ’ instead of ‘ $(\exists n)(n \in \mathbb{N} \wedge \dots)$ ’ and here, too, there is a suggestion that  $\mathbb{N}$  is a kind of environment or local universe or context. We can use the same notational device in connection with  $\lambda$ -terms too. Thus,  $\lambda x \in X. \{x\}$  is the function that sends members of  $X$  to their singletons. This function will reappear in the proof of Cantor’s theorem in section 3.5.2.

“guarded” quantification

### Index sets

We can even write formulæ (1) and (2) as

$$\{2y : y \in \mathbb{N}\} \quad (3.2)$$

This is possible because there is a convention that allows us to write

$$\{f(y) : y \in X\}$$

to mean the set of values of the function  $f$  for arguments in  $X$ , and  $\{2y : y \in \mathbb{N}\}$  is just a special case of this.

Now, if  $\{f(y) : y \in X\}$  is a set, so is

$$\bigcup \{f(y) : y \in X\}$$

and this is sometimes written

$$\bigcup_{y \in X} f(y)$$

You will even see things like

$$\{\pm n : \Phi(n)\} \quad (\otimes)$$

There are more casual notations to be seen, but I won’t expose you to them. The general idea at this stage is: do not be casual; you shouldn’t use slang until you have learned to talk proper!

exhumed material here...

$f : \mathbb{N} \longrightarrow \{0, 1\}$  should really be a boolean, a proposition, so we can write  $\{f : (f : \mathbb{N} \longrightarrow \{0, 1\}) \wedge \Phi(f)\}$ .

One of my colleagues used the expression

$$\{f : \mathbb{N} \longrightarrow \{0, 1\} \mid (\forall n \in \mathbb{N})(f(n) \leq f(n+1))\}$$

Moving a boolean rather than a set-membership to the left is a bit more complicated.....

**EXERCISE 22.** Give two set abstracts for the set of natural numbers that are perfect squares, one using the existential quantifier  $\exists$  and the other using the trick introduced in this section of moving some information to the left of the colon

While on the subject of functions, a last notational point. In most mathematical usage the terminology ‘ $f(x)$ ’ is overloaded: it can denote either the value that the function  $f$  allocates to the argument  $x$  or the set of values that  $f$  gives to the arguments in the set  $x$ . Normally this overloading does not cause any confusion, because typically it is clear from the context which is meant.  $f(\pi)$  is clearly a number and  $f(\mathbb{R})$  a set of numbers. The give-away here is in the style of letter used for the argument. As you can probably guess by now, I am a purist who doesn’t like relying on contextual cues in this way, it prolongs our bad habit of fault-tolerant pattern-matching, and it can be avoided—because there is a notation that disambiguates these two styles of functional application without using information about the variable.  $f^{\text{“}x}$  is the set of values that  $f$  allocates to the arguments in the set  $x$ :

$$f^{\text{“}x} = \{f(y) : y \in x\}$$

and  $f(x)$  will continue<sup>1</sup> to be the value that  $f$  assigns to the argument  $x$ . This double apostrophe notation is used for relations as well:  $R^{\text{“}X}$  is

$$\{y : (\exists x \in X)(R(y, x))\}.$$

This is why it’s OK to write ‘ $f^{-1}^{\text{“}X}$ ’ for  $\{y : f(y) \in X\}$  even though  $f^{-1}$  might not be a function. (You might not yet know what  $R^{-1}$  is, so you might like to review this section after section 3.2.2.) Some people write  $x.R$  for  $R^{\text{“}\{x\}}$ . My first thought is that they should be shot, but there are excuses.

Can use abbr in restricted contexts

For us the commonest use of this notation is in settings like “ $f^{\text{“}X} \subseteq X$ ”, which says that  $x$  is **closed under**  $f$ . Of course we can talk about sets being closed under  $n$ -ary functions with  $n > 1$ , and if  $g$  is an  $n$ -ary function (“a function of  $n$  variables”), then  $g^{\text{“}(X^n) \subseteq X$ .

work these last two paragraphs in carefully

We have to use this move-to-the left trick to have a sensible notation for  $A \times B$  as a set abstract. The usual answer is

$$A \times B =: \{\langle x, y \rangle : x \in A \wedge y \in B\}$$

although both

$$\{u : (\exists x \in A)(\exists y \in B)(u = \langle x, y \rangle)\}$$

and

$$\{u : \mathbf{fst}(u) \in A \wedge \mathbf{snd}(u) \in B\}$$

are of course correct too.

### 3.1.3 Curly Brackets

this section in prop-  
it's newly copied in

The following expression turned up in an example sheet. Or was it a tripos question(?) I forget. Anyway, it's a(n admittedly fairly extreme) example of the kind of notation you are going to have to be happy reading.

$$\{2z \in \mathbb{N} \mid z \leq 5 \wedge 20/z \in \{w \in \mathbb{N} \mid w \leq z\}\} \quad (3.1)$$

The person who put this question together was using it to try to make a number of points. In this commentary I'll be trying to make those points for him/her.

The first point is that the curly bracket symbol is used in various distinct but related ways. We write things like ' $\{a, b\}$ ' to denote the set that has 1 and 2 in it but nothing else. Let us call this the **primary** use of curly brackets. But we also use them in expressions like

$$\{x \mid \Phi\} \quad (3.2)$$

In this usage the ' $x$ ' is a *variable*, and the expression denotes the set containing precisely those things that satisfy  $\Phi$ , that being the thing after the vertical bar. Just a brief check, before we go on: make sure you are happy that  $\{1, 2\}$  is the same set as  $\{x \mid x = 1 \vee x = 2\}$ . see page 39.

(Notice *en passant* that some people—such as your humble correspondent—will use a colon instead of a vertical line after the variable in expressions like 3.2 above. Sadly there are lots of overlapping notations. I prefer the colon to the vertical bar because we also use the vertical bar to mean “cardinal of”. Thus  $|\{1, 2\}| = 2$ . I think my way causes less confusion. You should be prepared to see both notations used.)

Notice that in formula 3.1 the thing between the left ' $\{$ ' and the ' $\mid$ ' isn't just a naked variable as it was in formula 3.2. This exploits two conventions which we must explain. We often write

$$\{x \mid x \in A \wedge \Psi\} \quad (3.3)$$

as

$$\{x \in A \mid \Psi\} \quad (3.4)$$

This looks perverse, but there is reason to it. We use it in situations where one feels that the set  $A$  provides a *context*. For example the expression  $\{x \mid x^2 < 26\}$  denotes the set of all numbers whose square is less than 26. We might be interested in the set of all *real* numbers whose square is less than 26, in which case one would write

$$\{x \mid x^2 < 26 \wedge x \in \mathbb{R}\} \quad (3.5)$$

---

<sup>1</sup>You need to be warned that the ambiguous use of the “ $f(A)$ ” notation to mean both  $f(A)$  and  $f“A$  is widespread and you should expect to see it. Whether or not you propose to use it yourself is a matter between you and your conscience; i shall not pry.

or one might be interested in the set of all natural numbers whose square is less than 26, in which case one would write

$$\{x \mid x^2 < 26 \wedge x \in \mathbb{N}\} \quad (3.6)$$

but—because in circumstances like this one usually is thinking of  $\mathbb{R}$  or  $\mathbb{N}$  as a *universe of discourse*, the place where it is happening—one would write these as

$$\{x \in \mathbb{R} \mid x^2 < 26\} \quad (3.7)$$

and

$$\{x \in \mathbb{N} \mid x^2 < 26\} \quad (3.8)$$

Before you go any further check your understanding by writing out—in primary notation—what the set in formula 3.8 is. (I won't ask you to write out what the set from formula 3.7 is because it's infinite!)

But what we have before us in formula 3.1 is an example of a further liberalisation of this last step. This liberalisation will allow us to write things like

$$\{x^3 \in \mathbb{N} \mid x^2 < 26\} \quad (3.9)$$

You cannot deduce from what has gone before what this expression is used to mean, but you might be able to guess. What it denotes is the set that you get from the set denoted by formula 3.8, and replacing every number in that set by its cube.

We are now in a position to attack formula 3.1.

The last point the questionmaster was trying to get across is that  $w \in \{x : \phi(x)\}$  is the same as  $\phi(w)$ . Being a member of the set of all green things is just the same as being a green thing. Or rather, since the example is  $20/z \in \{w \in \mathbb{N} \mid w \leq z\}$  the point is that being a member of the set of green slimy things is the same as being green and slimy. This formula is just the same as

$$20/z \in \mathbb{N} \wedge 20/z \leq z \quad (3.10)$$

This will simplify formula 3.1 to

$$\{2z \in \mathbb{N} \mid z \leq 5 \wedge 20/z \in \mathbb{N} \wedge 20/z \leq z\} \quad (3.11)$$

So we ascertain what

$$\{z \in \mathbb{N} \mid z \leq 5 \wedge 20/z \in \mathbb{N} \wedge 20/z \leq z\} \quad (3.12)$$

is and then multiply everything in it by 2. A simple case analysis shows that the only natural number  $z$  below 5 such that  $20/z \leq z$  is 5. So the set of 3.12 is  $\{5\}$ . (Not 5 itself! That's another point the questionmaster was trying to make!)

Finally multiply everything in  $\{5\}$  by 2 to obtain  $\{10\}$ .



## 3.2 Relations and Functions

Relations-in-extension and functions-in-extension are sets of tuples. What is a tuple? An  $n$ -tuple is just a list of length  $n$ .<sup>2</sup>

For the rest of this section we are going to think of relations generally as relations-in-extension: sets of tuples. Quite a lot of what we are going to do makes sense when done to relations-in-intension as well, but the default will be that all relations under discussion are relations-in-extension.

The  $n$ -tuples that will be most important to us are those where  $n = 2$ . We call these tuples **ordered pairs**. An ordered pair has two different—we used the word *slot* earlier. If  $p$  is a pair, we can write  $\text{fst}(p)$  and  $\text{snd}(p)$  for the first and second components of  $p$  (the things in the first and second slots of  $p$ ). We will also write ‘ $\vec{x}$ ’ for the  $n$ -tuple ‘ $\langle x_1 \dots x_n \rangle$ ’. This is because I write ordered pairs, triples, and so on with angle brackets:  $\langle x, y \rangle$ . However, the world being the deeply flawed place it is, you will find people using round brackets for this, and writing the ordered pair of  $x$  and  $y$  as ‘ $(x, y)$ ’. I avoid it because this notation is used for several other things already, but not everybody feels like me, and you must not panic when you see it notated differently.

- $(x, y)$  might be the open interval  $\{z \in \mathbb{R} : x < z < y\}$ .  
While we are about it  $[x, y]$  is (in the same tradition) the closed interval  $\{z \in \mathbb{R} : x \leq z \leq y\}$ , and  $(x, y]$  is (in the same tradition) the half-open interval  $\{z \in \mathbb{R} : x < z \leq y\}$ , and  $[x, y)$  similarly.
- $(x, y)$  might also be the permutation that swaps  $x$  and  $y$  and fixes everything else.
- $(x, y)$  is also the Highest Common Factor of  $x$  and  $y$ .

All this is in small print because mostly you don’t really need it: it’s here only to put things in context. However when we come to chapter 4 you will encounter the usage  $(x, y)$  for the highest common factor of  $x$  and  $y$ .

### 3.2.1 Relations

The **arity** of a function or a relation is the number of arguments it is supposed to have. It is a significant but generally unremarked fact that one can do most of mathematics without ever having to consider relations of arity greater than 2. Relations of arity two are **binary**.

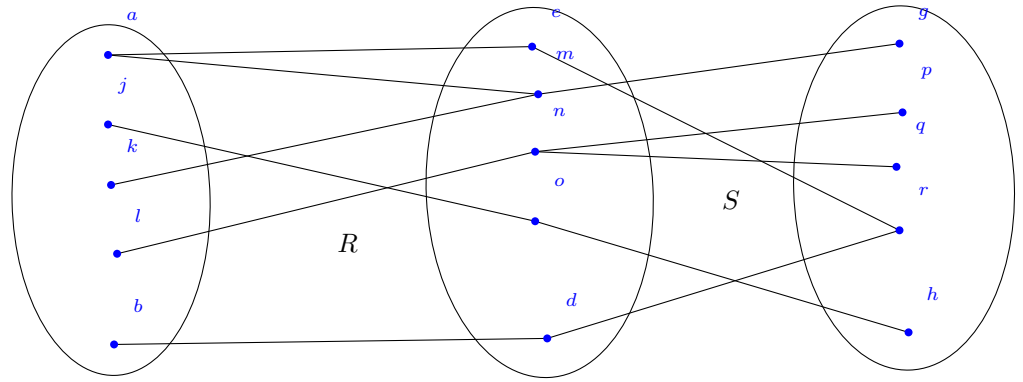
We write  $R(x, y)$  to mean that  $x$  and  $y$  are related by  $R$ . Sometimes we write it as  $xRy$  instead. This is **infix** notation. Infix notation is universally used with order relations. We always write ‘ $x \leq y$ ’ rather than ‘ $\leq (x, y)$ ’, though there is no significance to this. I respect this tradition, but I tend not to use infix notation otherwise. One reason for this is that there is not way of writing ternary etc relations as infix!

---

<sup>2</sup>Some programming languages—ML for example—distinguish between  $n$ -tuples and lists of length  $n$ . We won’t make this distinction, and we don’t at this stage need to go into why they do.

Relations being sets, you can do anything to relations that you can do to sets: all the boolean operations: union, intersection, set difference and so on. But there are some extra operations you can do to relations which don't arise in this way. Composition and inverse; mere *sets* do not have composition and inverse, but *sets of ordered pairs* do. And just as there are special sets (the empty set, the universal set) there are also some special relations: the identity relation. It's often written ' $\Delta_X$ ' or ' $1_X$ ' (where  $X$  is the intended domain) or even just ' $1$ '.

### 3.2.2 Composition and inverse



$x$  is related to  $y$  by  **$R$ -composed-with- $S$**  if there is a  $z$  such that  $x$  is related to  $z$  by  $R$  and  $z$  is related to  $y$  by  $S$ . In symbols

$$x R \circ S y \longleftrightarrow (\exists z)(xRz \wedge zSy)$$

So  $R \circ S$  is the composition of  $R$  with  $S$ . Often written  $R \cdot S$ . (or, in infix notation,  $R \circ S(x, y) \longleftrightarrow (\exists z)(R(x, z) \wedge S(z, y))$ )

Notice that I haven't mentioned ordered pairs here, and this definition of  $R \circ S$  works for relations-in-intension just as well as for relations-in-extension. In fact it's probably more natural to think of composition as something one does to relations-in-intension.

Lots of examples here please

**EXERCISE 23.** Write down a set abstract for the composition  $R \circ S$  of two binary relations-in-extension  $R$  and  $S$ .

Answer:  $\{\langle x, z \rangle : (\exists y)(\langle x, y \rangle \in R \wedge \langle y, z \rangle \in S)\}$ .

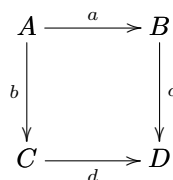
You might wonder what the composition of two ternary relations is. Don't: we won't need it. But do bear in mind that  $R \circ S$  is not in general the same as  $S \circ R$ : the sibling of your parent is probably not the parent of your sibling. Mini exercise: how is it legally possible for them to be the same?

If  $R \circ S = S \circ R$  we say that  $R$  and  $S$  **commute**. This word 'commute' is probably more usually used of functions. (see the end of section ??.)

If  $(\forall x)(f(g(x)) = g(f(x)))$  we say  $f$  and  $g$  commute.

binary operations commute

There is a style of picture which, although you will not explicitly need to know about it, you may find helpful. For example, when people say that the following diagram "commutes"



they mean that  $c \circ a = d \circ b$ .  $R \circ R$  is written  $R^2$ , and similarly  $R^{n+1}$  is  $R \circ R^n$  for all natural numbers  $n$ . Remember that 1 is the identity relation, and  $R \circ 1$  is just  $R$ , so one can think of 1 as  $R^0$ , which is pleasing. The **inverse** or **converse** of  $R$ , written ' $R^{-1}$ ', is  $\{\langle x, y \rangle : \langle y, x \rangle \in R\}$ . However, do not be misled by this exponential notation into thinking that  $R \circ R^{-1}$  is the identity.

(What can you say about  $R$  if  $R \circ R$  is the identity? On this last point see exercise 34 part (v). If you matched (v) up correctly by a process of elimination then you will have checked the correctness of your answer independently.)

### 3.2.3 Digraphs and matrices for relations-in-extension

Have a look at

[https://www.dpmms.cam.ac.uk/~tf/cam\\_only/discrete-trial-101-test.pdf](https://www.dpmms.cam.ac.uk/~tf/cam_only/discrete-trial-101-test.pdf)

It is sometimes convenient to think of a binary relation as a matrix whose entries are 1 and 0 (proxies for **true** and **false**). This has an advantage, namely that under this scheme the matrix product of the matrices for  $R$  and  $S$  is the matrix for  $R \circ S$ . (If you want the entries to be **true** and **false** (instead of their proxies of 1 and 0) you have to take multiplication to be  $\wedge$  and addition to be  $\vee$  (in your definition of matrix multiplication).

More chat here

If this is the matrix for the relation  $R \subseteq A \times B$

$R$	$b_1$	$b_2$	$b_3$
$a_1$	$T$	$T$	$F$
$a_2$	$F$	$F$	$T$
$a_3$	$T$	$F$	$T$

and this is the matrix for the relation  $S \subseteq B \times C$

$S$	$c_1$	$c_2$	$c_3$
$b_1$	$T$	$T$	$F$
$b_2$	$T$	$F$	$F$
$b_3$	$F$	$T$	$F$

then we obtain the matrix for  $R \circ S$  by matrix multiplication ...

You might like to fill in the question marks yourself ...

#### EXERCISE 24.

$R \circ S$	$c_1$	$c_2$	$c_3$
$a_1$	?	?	?
$a_2$	?	?	?
$a_3$	?	?	?

However, in principle it is not a good habit to think of binary relations as matrices in this way, because it forces one to decide on an ordering of the underlying set (after all, we have to decide on an order in which to write down the rows and columns) and this choice of an order makes this representation less general than the picture of binary relations-in-extension as sets of ordered pairs. (If you look at the table (3.2.5) of compatibility between blood groups, the suggestive distribution of crosses is suggestive only because the columns are written in the same order as the rows.)

Despite this, it can be useful at times, since it does give a nice picture of converses: the matrix of inverse/converse  $R^{-1}$  of  $R$  is the transpose of the matrix corresponding to  $R$  (so a symmetrical relation is one whose matrix is equal to its own transpose—and this is true however you order the elements of the domain) and this fact may help you break into this set of ideas.

This possibility of representing binary relations as matrices with values in  $\{0, 1\}$  or in  $\{\text{true}, \text{false}\}$  serves also to make the point that you must always be prepared to re-think the data structures that you use in writing programs. Sometimes you might want to think of relations as matrices, sometimes as digraphs, sometimes as God-knows-what. And the same goes for other data structures too; this trick of trying to think of a object that is *prima facie* of one data type as actually belonging to another is essential if you are to exploit all your algorithms fully. If you can contort your problem into a problem about graphs then you can use a graph algorithm on it; if you can contort it into a problem about matrices then you can use a matrix algorithm on it.

Most of the applications of matrices belong in what one might loosely call ‘Continuous Mathematics’ rather than Discrete Mathematics (specifically in connection with Vector Spaces) and we do not cover Vector Spaces here.

### 3.2.4 Other properties of relations

A relation  $R$  is **transitive** if  $\forall x \forall y \forall z \ R(x, y) \wedge R(y, z) \rightarrow R(x, z)$  (or, in brief,  $R^2 \subseteq R$ ). A relation  $R$  is **symmetrical** if  $\forall x \forall y (R(x, y) \longleftrightarrow R(y, x))$  or  $R =$

must define ‘digraph’ at some point.

$R^{-1}$ . Beginners often assume that symmetrical relations must be reflexive. They are wrong, as witness “rhymes with”, “conflicts with”, “can see the whites of the eyes of”, “is married to”, “is the sibling of” and so on.

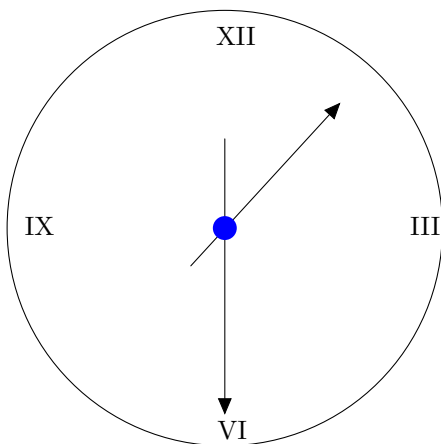
A binary relation  $R$  is **extensional** if  $(\forall x)(\forall y)(x = y \longleftrightarrow (\forall z)(R(x, z) \longleftrightarrow R(y, z)))$ . Notice that a relation can be extensional without its converse being extensional: think “square roots”. An extensional relation on a set  $X$  corresponds to an injection from  $X$  into  $\mathcal{P}(X)$ , the power set of  $X$ . For us the most important example of an extensional relation will be  $\in$ , set membership. Two sets with the same members are the same set.

A binary relation on a set  $X$  is **reflexive** if it relates every member of  $X$  to itself. (A relation is **irreflexive** if it is disjoint from the identity relation: note that irreflexive is not the same as not reflexive!) That is to say,  $R$  is reflexive iff  $(\forall x \in X)(\langle x, x \rangle \in R)$ . Notice that this means that reflexivity is not a property of a relation, but of the structure  $\langle X, R \rangle$  of which the relation is a component.

**EXERCISE 25.** Look up ‘monophyletic’. Using only the auxiliary relation “is descended from” give a definition in first-order logic of what is is for a monadic predicate of lifeforms to be monophyletic.

Finally, it may be worth making the point that not all relations are binary relations. There is a natural three-place relation of *betweenness* that relates points on a line, but this doesn’t concern us much. Of more interest (it lurks in the background in chapter 4 is the three-place relation of “later than” between hours on a clock. We cannot take this relation to be binary because if we do, it will simply turn out to be the universal relation. Every time on the clock is later than every other time if you wait long enough! However, with a three-place relation we can say “Starting at 12 o’clock we first reach 3 o’clock and then 6 o’clock” (which is true) and “Starting at 12 o’clock we first reach 6 o’clock and then 3 o’clock” (which isn’t). Or we can think of it as “starting at  $x$  and reading clockwise we encounter  $y$  first and then  $z$ ”)

**EXERCISE 26.** Consider the clockface below. Write down the graph of the three-place order relation on the four positions on the face.



**EXERCISE 27.** Show that, for all  $R, S$  and  $T$ ,

- (i)  $R \subseteq S \rightarrow R \circ T \subseteq S \circ T$ ;
- (ii)  $R \subseteq S \rightarrow T \circ R \subseteq T \circ S$ ;
- (iii)  $R \circ (S \cup T) = (R \circ S) \cup (R \circ T)$ ;
- (iv)  $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$ .

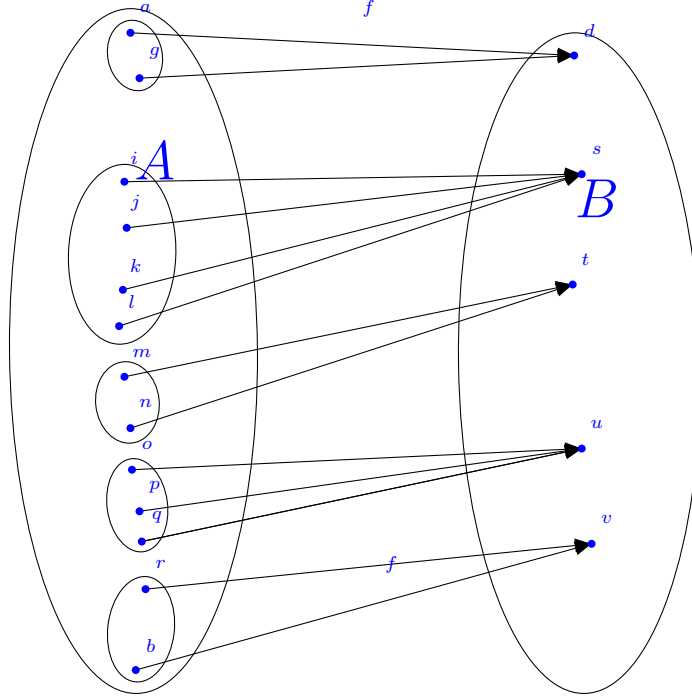
Which of the following are true?

- (i)  $R \subseteq S \rightarrow R^{-1} \subseteq S^{-1}$ ;
- (ii)  $R \subseteq S \rightarrow R^{-1} \supseteq S^{-1}$ ;
- (iii)  $R = R^{-1} \rightarrow 1 \subseteq R$ .

### 3.2.5 Equivalence relations

An **equivalence relation** is a relation that is symmetrical, transitive and reflexive. There is an important connection with the *partitions* that we met in definition 1 in section 3.1.2.

The following picture shows us some things we will want to define and describe.



Here we have a picture of a surjection  $f : A \twoheadrightarrow B$ , where  $B = \{d, s, t, u, v\}$  and  $A = \{a, g, i, k, l, m, n, o, p, q, r, b\}$ . The left-to-right arrows in the picture correspond (one-to-one) with the ordered pairs in [the graph of]  $f$ . The five things that look like parachutes falling left-to-right are examples of things often called **fibres**. Thus a fibre is a thing in the target (range, codomain, call it what you like) together with all the arrows that reach it, and the sources of the arrows which can be found bundled into an ellipse on the left. Since the function going from left-to-right is  $f$  we say that these fibres are fibres **of**  $f$ . The set of (five) ellipses on the left is a partition of  $A$ , and each ellipse is a piece (of that partition). There is an equivalence relation lurking here, and that is the relation that holds between any two members of  $A$  that belong to the same piece (ellipse). It's perhaps a wee bit laborious to write out all the ordered pairs in this relation, co's there are quite a few of them. How many, exactly? We don't seem to have used the letter ' $E$ ' in this picture, so we can use it to denote this equivalence relation. (The letter  $E$  is often used to denote an equivalence relation.) Finally we say that  $f$  is a **classifier** for  $E$ , by which we mean that  $(\forall xy)(f(x) = f(y) \longleftrightarrow E(x, y))$ .

Is this where we define PARTITION and PIECE?

Thus every surjection gives rise to an equivalence relation  $E$ , and it is a classifier for  $E$ . There are other classifiers for  $E$ , since  $\pi \cdot f$  is such a classifier whenever  $\pi$  is a permutation of  $\{d, s, t, u, v\}$ .

which i must discuss here

For example, the function that sends every set to its cardinality [notated in various ways] is a classifier for the relation of *being-in-bijection-with* aka *equipollence*.

You are not going to be asked any questions in the exam that rely on your knowing the words ‘fibre’ or ‘classifier’ but in my experience the ability to use them properly helps get things clear in your mind.

Just as we often write ‘ $\leq$ ’ rather than ‘ $R$ ’ or ‘ $S$ ’ when we want to point to a partial order (and write it as an infix to boot) so we often write ‘ $\sim$ ’ rather than ‘ $R$ ’ or ‘ $S$ ’ when we want to point to an equivalence relation (and write that as an infix too)

### Congruence relations

An equivalence relation  $\sim$  is a **congruence relation** for an  $n$ -ary function  $f$  if, whenever  $x_i \sim y_i$  for  $i \leq n$ , then  $f(x_1 \dots x_n) \sim f(y_1 \dots y_n)$ .

Congruence relations will crop up in other courses too but one particular example will be important to us here, and it’s one that may be known to you already. The equivalence relation on natural numbers: “ $n$  and  $m$  have the same remainder on division by  $p$ ” is a congruence relation for addition and for multiplication. We will deal with this in chapter 4.

Here is another real-life example of a congruence relation. Consider the relation between humans “It is safe for  $x$  to receive a transfusion of blood from  $y$ .” Ignoring for the moment the fact that there are blood-borne diseases such as HIV, CJD, Hep C and so on, we find that if  $x$  can safely receive a transfusion of blood from  $y$ , and  $y'$  belongs to the same blood group as  $y$ , then  $x$  can safely receive a transfusion of blood from  $y'$ . That is to say, the equivalence relation of having-the-same-blood-group is a congruence relation for the binary relation “ $x$  can safely receive a transfusion of blood from  $y$ ”.

That way we can think of the relation “ $x$  can safely receive a transfusion of blood from  $y$ ” as really a relation between the blood groups, and summarise it in the following matrix.

Columns are donors, rows are recipients.

	O-	O+	B-	B+	A-	A+	AB-	AB+
O-	X							
O+	X	X						
B-	X		X					
B+	X	X	X	X				
A-	X				X			
A+	X	X			X	X		
AB-	X		X		X		X	
AB+	X	X	X	X	X	X	X	X

Need some exercises on the equivalence classes under this equivalence relation.



Look at the compatibility table for blood groups in the section on congruence relations. You may be struck by the pleasing pattern made by the  $X$ s: I certainly was. It looks a bit like a thing they call a “Sierpinski sponge” (no: don’t google it!) What I want you to do is follow the same path I trod when I spotted this pattern, namely:

I) Does this pattern tell you anything significant about the properties of this compatibility relation? I’m thinking of reflexivity, transitivity, symmetry, antisymmetry etc. etc. When you’ve got that sorted out, procede to part II.

II) We have already seen other ways of representing binary relations. Try some of them on this data and see if you get any pretty pictures. I tried it and I got a three-dimensional shape. I want you to find that three-dimensional shape.

III) One moral I want to draw from this coursework is that Discrete Mathematics and mere thought can be useful in developing profitable hypotheses in the sciences. You probably know enough biology to know that characters are inherited by genes, and that we each have two copies of each gene. Each gene can come in several forms called *alleles*. Some alleles are *dominant* in that you express them even if you have only one copy (brown eyes); some are *recessive* in that you express them only if you have two copies (blue eyes, green eyes). The picture you have developed will suggest to you a hypothesis about how many genes there are that control your blood group, and how many alleles there are at each gene, and which are dominant. Formulate this hypothesis.

Do not forget that this is a discrete mathematics question, not a biology question. There is nothing to be gained—and time to be lost—in surfing the web for information about blood groups.

### 3.2.6 Partial orders

Order relations obviously have to be transitive, and they cannot be symmetrical because then they would not distinguish things, would they? Indeed transitive relations that are symmetrical are called *equivalence* relations (as long as they are reflexive). So how do we capture this failure of symmetry? We start by noticing that, although an order relation must of course be transitive and cannot be symmetrical, it is not obvious whether we want it to be reflexive or want it to be irreflexive. Since orderings represent ways of *distinguishing* things, they do not have anything natural to say about whether things are related to themselves or not. Is  $x$  less than itself? Or not? Does it matter which way we jump? Reflection on your experience with  $<$  and  $\leq$  on the various kinds of numbers you’ve dealt with (naturals, integers, reals and rationals) will make you feel that it does not much matter. After all, in some sense  $<$  and  $\leq$  contain the same information about numbers (See exercise 37.37). These two ways give rise to two definitions.

This section is a jumble of pieces all stuck together and needs to be sorted out

Get this reference right

1. A **strict partial order** is irreflexive, transitive and asymmetrical. (A relation is **asymmetrical** if it cannot simultaneously relate  $x$  to  $y$  and  $y$  to  $x$ . This of course implies irreflexivity.)

2. A **partial order** is reflexive, transitive and ... well it cannot be asymmetrical because  $x \leq x$ . We need to weaken asymmetry to a condition that says that, if  $x \neq y$ , then not both  $x \leq y$  and  $y \leq x$ . This condition, usually expressed as its contrapositive (see page ??)  $(\forall xy)(x \leq y \wedge y \leq x \rightarrow x = y)$ , is **antisymmetry** and is the third clause in the definition of partial order.

A relation that is reflexive and transitive (antisymmetry not guaranteed) is a **preorder** or **quasiorder**. For example the relation between humans “ $x$  can safely receive blood from donor  $y$ ” is a preorder. The intersection of a preorder with its converse is always an equivalence relation. In this case the equivalence relation is the relation of having-the-same-blood-group.

**You absolutely must have these definitions at your fingertips, co’s these things crop up all the time. Merely knowing where to look them up isn’t enough.**

**EXERCISE 28.** *Are either of the following true?*

1. *The identity relation is a partial order.*
2. *The empty relation is a strict partial order.*

If  $R$  is a partial ordering of a set  $X$ , then  $R \setminus \{\langle x, x \rangle : x \in X\}$  is a strict partial ordering of  $X$ , and if  $R$  is a strict partial ordering of a set  $X$ , then  $R \cup \{\langle x, x \rangle : x \in X\}$  is a partial ordering of  $X$ . Thus each concept (partial order and strict partial order) can be defined in terms of the other. There is a scrap of logical slang that comes in handy here: we say that each can be defined if we take the other as **primitive**. A primitive is a concept in terms of which you define other concepts.

Total orders are a special kind of partial order. (Do not overinterpret and assume that partial orders cannot be total!) Again, they come in two flavours:

1. A **strict total** order is a strict partial order that satisfies the extra condition  $(\forall xy)(x < y \vee y < x \vee x = y)$ . Because this condition says there are no more than three possibilities, it is called **trichotomy** (from two Greek words meaning *three* and to *cut* as in a-*tom*, lobo-*tomy*.)
2. A **total order** is a partial order with the extra condition  $(\forall xy)(x \leq y \vee y \leq x)$ . This property is called **connexity**, and relations bearing it are said to be **connected**. (“connected” also has a meaning in graph theory, so beware)

Thus trichotomy and connexity are related to each other the way antisymmetry and asymmetry are.

A **poset**  $\langle X, \leq_X \rangle$  is a set  $X$  with a partial ordering  $<_X$ .

A **monotone** function from a poset  $\langle A, \leq_A \rangle$  to a poset  $\langle B, \leq_B \rangle$  is a function  $f : A \rightarrow B$  such that  $\forall xy(x \leq_A y \rightarrow f(x) \leq_B f(y))$ .

The word ‘monotone’ in mathematics refers to functions  $f$  which satisfy conditions like

$$x \leq y \rightarrow f(x) \leq f(y).$$

We say such a function is *monotone increasing* with respect to  $\leq$ . (If instead  $f$  satisfies  $x \leq y \rightarrow f(x) \geq f(y)$  we say  $f$  is *monotone decreasing* with respect to  $\leq$ .) Of course, it may be (as it is in fact the case here) that the partial order in the antecedent of the condition is not the same partial order as in the consequent, so ideally we would need a more complex form of words along the lines of “ $f$  is monotone [increasing] with respect to  $\leq$  and  $\leq'$ ”. However this ideal notation is never used, being sacrificed by ellipses to the form of words “ $f$  is monotone [increasing]”.

We use it here because the function  $F$  that takes a set of assumptions  $A$  and returns the set  $F(A)$  of its logical consequences is monotone with respect to set-inclusion :

$$A \subseteq B \rightarrow F(A) \subseteq F(B).$$

The definition of a partial ordering as a relation that is transitive, reflexive and antisymmetrical applies equally well to relations-in-intension and relations in extension. A partial-order-in-extension is a set of ordered pairs. Generally relations-in-extension are sets of ordered tuples. But certain kinds of relations have other representations as extensional objects. We have seen that binary relations can be pictured as digraphs-with-loops as well as sets of ordered pairs. But there is more. A total ordering of a (finite) set can be represented as a list (without repetitions) of all the members of the set. Notice that this is a more economical representation of a total order than its representation as a set of ordered pairs: the representation of a total ordering of a finite set  $X$  is of length  $|X|$  whereas its representation as a set of ordered pairs has... You tell me!

**EXERCISE 29.** *How many ordered pairs are there in a total ordering of a set with  $n$  elements?*

This trick doesn’t work for an arbitrary partial order that isn’t total. We can code a partial ordering as the set of its initial or terminal segments—as a set of sets. Think of the knot of people round a airplane lavatory on a long-haul flight at dawn. Each person knows only the set of people who were there before they were. (And it is a set they know not a list, co’s they don’t know what order the people ahead of them arrived). This serves to point the useful moral that many objects of interest to us can be coded or represented in more than one way. (This point was made also in connection with the matrix representation of binary relations in section 3.2.3.)

### Chains

The **restriction** of a relation  $R$  to a carrier set  $X$  (which is  $R \cap X^n$ , where  $n$  is the arity of  $R$ ) is denoted by ‘ $R \upharpoonright X$ ’. (We saw restrictions of *functions* on page 39; restrictions of relations is a natural generalisation.) A **chain** in a poset

$\langle X, \leq_X \rangle$ , is a total ordering  $\langle X', \leq_X \upharpoonright X' \rangle$ , where  $X' \subseteq X$ . In words: a chain in a poset is a subset totally ordered by the restriction of the order relation. An **antichain** in a poset is a subset of the carrier set such that the restriction of the order relation to it is the identity relation.

Dilworth's theorem?

### Transitive closure

For any binary relation-in-extension  $R$  whatever, the relation  $R \cup 1$  (remember 1 is the identity relation) is a reflexive relation. By now you will have noticed also that for any binary relation  $R$  whatever, the relation  $R \cup R^{-1}$  is a symmetrical relation.  $R \cup 1$  is the **reflexive closure** of  $R$ , and is sometime written  $r(R)$  to commemorate this fact. Similarly  $R \cup R^{-1}$  is the **symmetric closure** of  $R$  and written ' $s(R)$ ' similarly. The work being done by the word 'closure' here is not psychobabble: you should use it to remind yourself that what you are doing in these two cases is adding to  $R$  precisely the ordered pairs needed to make it reflexive, or symmetric. (Of course you can add more still: the idea here is to add the minimum necessary). An important feature of this idea is that this process is *deterministic*: there is a unique minimal way to add ordered pairs to  $R$  to obtain a reflexive relation, or a symmetric relation. In contrast if you want to add ordered pairs to a partial order to obtain a total order there is no obvious right way to do it. If the partial order is indifferent between Tweedledum and Tweedledee there is nothing about the partial order to tell you what to do. Whereas if a relation that isn't transitive relates  $a$  to  $b$  and  $b$  to  $c$  then we know to relate  $a$  to  $c$  in the transitive closure.

To be formal about it

#### DEFINITION 2.

- The reflexive closure of a binary relation-in-extension  $R$  is the least (with respect to  $\subseteq$ ) set of ordered pairs that is both a reflexive relation and a superset of  $R$ :

$$r(R) =: \bigcap \{S : R \subseteq S \wedge 1 \subseteq S\}$$

and

- The symmetric closure of a binary relation-in-extension  $R$  is the least (with respect to  $\subseteq$ ) set of ordered pairs that is both a symmetric relation and a superset of  $R$ :

$$s(R) =: \bigcap \{S : R \subseteq S \wedge S = S^{-1}\}$$

and finally

- The transitive closure of a binary relation-in-extension  $R$  is the least (with respect to  $\subseteq$ ) set of ordered pairs that is both a transitive relation and a superset of  $R$ :

$$t(R) =: \bigcap \{S : R \subseteq S \wedge S^2 \subseteq S\}$$

Symmetric and reflexive closures of relations one can build in one hit, as above, since they are  $R \cup 1$  and  $R \cup R^{-1}$  respectively. Transitive closures are a bit more of a mouthful, which is why we left them until last.

We will show that  $t(R)$  is in fact  $\bigcup_{n \in \mathbb{N}} R^n$ ; something slightly easier to understand.

To do this it will be sufficient to show

1.  $\bigcup_{n \in \mathbb{N}} R^n$  is transitive;
2. If  $S$  is a transitive relation  $\supset R$  then  $\bigcup_{n \in \mathbb{N}} R^n \subseteq S$ .

For (1) We need to show that if  $\langle x, y \rangle$  and  $\langle y, z \rangle$  are both in  $\bigcup_{n \in \mathbb{N}} R^n$  then  $\langle x, z \rangle \in \bigcup_{n \in \mathbb{N}} R^n$ . If  $\langle x, y \rangle \in \bigcup_{n \in \mathbb{N}} R^n$  then  $\langle x, y \rangle \in R^k$  for some  $k$ , and if  $\langle y, z \rangle \in \bigcup_{n \in \mathbb{N}} R^n$  then  $\langle y, z \rangle \in R^j$  for some  $j$ . Then  $\langle x, z \rangle \in R^{j+k} \subseteq \bigcup_{n \in \mathbb{N}} R^n$ .

For (2) Let  $S \supset R$  be a transitive relation. So  $R \subseteq S$ . We prove by induction on  $\mathbb{N}$  that for all  $n \in \mathbb{N}$ ,  $R^n \subseteq S$ . Suppose  $R^n \subseteq S$ . Then

$$R^{n+1} = R^n \circ R \subseteq^{(a)} S \circ R \subseteq^{(b)} S \circ S \subseteq^{(c)} S.$$

Inclusions (a) and (b) hold because  $\circ$  is *monotone*: if  $X \subseteq Y$  then  $X \circ Z \subseteq Y \circ Z$ . Inclusion (c) holds because  $S$  is transitive. (See the first two parts of exercise 12.)

### Hasse diagrams

Need a picture here

He's German, pronounced 'Husser' (unless you are from North of the river Trent!)

The digraph picture gives rise to **Hasse diagrams**. When drawing a digraph of a transitive relation  $R$  one can safely leave out a lot of arrows and still display the same information: all one has to draw is the arrows for a relation whose transitive closure is  $R$ . One could restore all the missing arrows (should one wish to) because one knows where to put them because of transitivity. Thus the relation represented by a lot of dots joined by arrows is the relation "I can get from  $x$  to  $y$  by following the arrows".

If  $R$  is a partial order on a finite set then there is a minimal relation whose transitive closure is  $R$ . For each  $x$  in the domain of  $R$  put an edge from  $x$  to each of its immediate successors. This will even work for  $\mathbb{N} \dots$  (one can draw a Hasse diagram for  $\mathbb{N}$ ) but not for  $\mathbb{Q}$ .

In fact we can even leave out the heads on the arrows (so we draw in edges rather than arrows) by adopting the convention that the end of the edge on which the arrowhead belongs is the end that is further up the page. The result of doing this is the Hasse diagram of that transitive relation. [one effect of this is that no Hasse diagram ever has a horizontal line anywhere!] The appeal of Hasse diagrams relies on and to some extent reinforces an unspoken (and false!) assumption that every partial order can be embedded somehow in the plane. Related to this is the weaker (but nevertheless still nontrivial) assumption that all total orders can be embedded in the real line, as instance, the image of Justice, blindfolded with a pair of weighing scales.



Although this is clearly a false assumption that might perhaps push our intuitions in wrong directions, it is not such a crazy idea in computer science, where linearity of time and of machine addresses compel us to assume that all partial orders can be refined to total orders. Any representation of a set in the bowels of a computer must always be as a list!

### 3.2.7 Products of orders

There is a general notion of product of structures, and you may well need to learn it eventually. However for the moment we will restrict ourselves to the case of most immediate interest: the products of two partial orderings.

If  $\langle X, \leq_X \rangle$  and  $\langle Y, \leq_Y \rangle$  are two partial orders, then we can define partial orders on  $X \times Y$  in several ways. The product defined above is called the **pointwise** product. In the **lexicographic** order of the product we set  $\langle x, y \rangle \leq_{lex} \langle x', y' \rangle$  if  $x <_X x'$  or  $x = x'$  and  $y \leq_Y y'$ . Although straightforward examples of lexicographic products are scarce, there are a number of combinatorial devices that have the flavour of a lexicographic product. One example is the Olympic league table: one grades nations in the first instance by the number of gold medals their athletes have won, then by the number of silvers and only if these fail to discriminate between them does one count the number of bronzes. In this setting there are three preorders on the set of nations (they are preorders because antisymmetry cannot be guaranteed: two nations may have the same number of medals of any given colour), and we are combining these three preorders into one preorder on the set of nations.

Other examples include the devices used to determine which team goes forward from a qualifying group in world cup football. *Prima facie* this should be the team with the largest number of points, but if two teams have the same

ordered pair notation for  
structures

number of points, one looks at the number of goals the two teams have scored, and so on, examining the values the two teams take under a sequence of parameters of dwindling importance until we find one with respect to which they differ. In cricket the analysis of a bowler who takes  $x$  wickets while conceding  $y$  runs is preferred to that of a bowler who takes  $x'$  wickets while conceding  $y'$  runs as long as  $x > x'$  or  $x = x' \wedge y < y'$ . However, in none of these naturally occurring cases is one ordering *tuples* of things: rather, one is trying to order things by combining in various ways various preorders of the things. However, the underlying intuition is the same.

Notice that the lexicographic product is a superset of the pointwise product. If we have two partial orders with the same carrier set and (the graph of, or extension of) one is a superset of (the graph of, or extension of) the other, we say the first **extends** the second. The **colex** ordering of  $X \times Y$  orders pairs according to *last* difference. The colex ordering too is a superset of the pointwise product ordering.

**EXERCISE 30.** *Check that the pointwise product ordering is the intersection of the lexicographic ordering and the colex ordering.*

One naturally tends to think of preorders as preference orders, as the preorders in the illustrations above of course are. Although naturally not all preorders are preference orders, thinking of them as preference orders enables us to motivate the distinction between the pointwise product of  $\mathcal{P} \times \mathcal{Q}$  of two preference orderings  $\mathcal{P}$  and  $\mathcal{Q}$  (which corresponds to impartiality between parameters  $\mathcal{P}$  and  $\mathcal{Q}$ ) and the lexicographic product (according to which any increase in  $\mathcal{P}$  is more important than any increase in  $\mathcal{Q}$ ). Naturally occurring preference orderings on products of posets tend to be complicated. Lexicographic products are extremely unlikely to represent your views on baskets of apples and oranges because even if you prefer apples to oranges, you would be unlikely to prefer any increase (however small) in the number of apples you are offered to any increase (however large) in the number of oranges—unless, that is, you had no use for oranges in the first place. And in those circumstances you would hardly bother to express a preference for an-apple-and-two-oranges over an-apple-and-one-orange. (You would probably describe your tastes by giving apples more *utility*. Interesting stuff no doubt, but no concern of us in 1a Discrete Mathematics.)

On the other hand, your preference ordering is likely nevertheless to be finer than the pointwise product ordering: according to the pointwise product ordering, you would be unable to decide between a single orange-with-a-pound-of-apples and two-oranges-with-one-apple. You would have to be very blasé not to prefer the first. After all, to a certain extent apples and oranges are interchangeable: realistic product (preference) orders refine the product order but are typically not as refined as a lexicographic order. (We must not get too deeply into utility theory!) Note merely that it is a sensible motivation for the study of orderings and products of orderings.

But before leaving preference orderings altogether the reader should notice at least that preference orders have a rather odd feature not shared by partial

orders in general.  $A \not\leq B \not\leq A$  and  $B > C$  does not imply  $A > C$ , though one expects it to if the ordering is a preference ordering. This makes a nice exercise.

**EXERCISE 31.** Are the two following conditions on partial orders equivalent?

$$\begin{aligned} &(\forall xyz)(z < x \not\leq y \not\leq x \rightarrow z < y), \\ &(\forall xyz)(z > x \not\leq y \not\leq x \rightarrow z > y). \end{aligned}$$

(This exercise uses four common conventions that it takes a logician to spell out.

- (i) When ‘ $\leq$ ’ and ‘ $<$ ’ appear in the same formula they denote a partial ordering and its strict part, respectively;
- (ii) The relations  $\leq$  and  $\geq$  are converses of each other;
- (iii) that ‘ $x < y < z$ ’ is short for ‘ $(x < y) \wedge (y < z)$ ’;
- (iv) putting a slash through a symbol (as in “ $\not\leq$ ”) negates it.)

Given a subset  $X \subseteq (P \times Q)$ , the points in  $X$  that are maximal in the pointwise product  $\mathcal{P} \times_{pw} \mathcal{Q}$  are called “**Pareto-efficient** points” by economists. They are sometimes called “Pareto-optimal” because if  $X$  is the set of points that are in some sense accessible, or possible, or something, then a Pareto-efficient point in  $X$  is one that, once one has reached it, one cannot find another point in  $X$  that makes one of the coordinates better without simultaneously making another one worse. Pareto was an Italian economist. Natural illustrations are defective in the way that we have seen that natural illustrations of lexicographic products are defective, but they might still help.

(i) The critical point of a substance is that temperature and pressure at which the difference between liquid and gas disappears. When the substance is at a higher temperature and higher pressure than this it is said to be **supercritical**. Methane is the compound most easily put into a supercritical state: all other compounds require either a more extreme temperature or a more extreme pressure or both. Methane is a Pareto-efficient point.

(ii) Each of the following isotopes is a Pareto-efficient point if you plot atomic weight against half-life. For each of these isotopes it is the case that every heavier isotope has shorter half-life, and everything with a longer half-life has lower atomic weight.

Isotope	Half-life (years)
Pb <sup>208</sup>	$\infty$ ;
Bi <sup>209</sup>	$4 \times 10^{19}$ ;
Th <sup>232</sup>	$1.405 \times 10^{10}$ ;
U <sup>238</sup>	$4.468 \times 10^9$ ;
Pu <sup>244</sup>	$8.08 \times 10^7$ ;
Cm <sup>247</sup>	$1.56 \times 10^7$ .

(Just a thought ... why was i right to write down ‘ $\infty$ ’ for the half-life of Pb<sup>208</sup> rather than ‘ $\aleph_0$ ’?)

Why is U<sup>235</sup> not in this list?



**EXERCISE 32.** Go to

<http://nucleardata.nuclear.lu.se/nucleardata/toi/perchart.htm>  
to see if you can find a Pareto-optimal isotope with greater atomic weight than  $Cm^{247}$ .

(iii) No portrait survives of the mathematician Green—after whom Green Street in Cambridge is named, and who invented Green functions. There are more famous people than Green of whom no portrait survives, but they are all of them more recent. There are more recent people than Green of whom no portrait survives, but they are all of them less famous than he is.

(iv) Robert Browning is buried in Westminster Abbey. This prompted Henry James to observe that “A good many oddities and a good many great writers have been entombed in the Abbey; but none of the odd ones have been so great and none of the great ones so odd.”

(v) The airport at Christchurch in New Zealand is Pareto-efficient with respect to size and southerlyness. There are airports to the south of it, but they are all smaller. There are larger airports, but they are north of Christchurch.

However, we will not develop these ideas here, as they find their most natural expression in connection with convex optimisation rather than logic. We touch briefly on convex optimisation in chapter 6.

Once one has explained Pareto-efficiency one can make the point that if the values taken by your parameters are infinitely divisible then you can have infinitely many pareto-efficient points. If they are discrete (like  $\mathbb{N}$ ) then you can't. A sleeper for WQO theory. Don't ask. No, really.

Comment about Mendel

**EXERCISE 33.** Look at this table 3.2.5 very hard. Of the various properties (reflexivity etc. etc.) of binary relations that you know of, which does this one exhibit? Is there any significance to the fact that there are eight blood groups? There is actually quite a lot of information you can extract from this simple table. Think about it and see what you can get out of it.

**EXERCISE 34.** Match up the properties in the left column with those in the right.

- |                                    |                          |
|------------------------------------|--------------------------|
| (i) $R^2 \subseteq R$ ;            | (a) $R$ is symmetrical   |
| (ii) $R \cap R^{-1} = \emptyset$ ; | (b) $R$ is antisymmetric |
| (iii) $R \cap R^{-1} = 1$ ;        | (c) $R$ is asymmetrical  |
| (iv) $R = R^{-1}$ ;                | (d) $R$ is a permutation |
| (v) $R \circ R^{-1} = 1$ ;         | (e) $R$ is connected     |
| (vi) $R \cup R^{-1} = U$ ;         | (f) $R$ is transitive    |

### 3.2.8 Functions

The annoying feature of reflexivity we saw on page 53—that you cannot tell by looking at the graph of a relation whether it is reflexive or not, because

you need to know the intended domain—which irreflexivity does not share) is also exhibited by **surjectivity**, which is a property not of a function but a function-with-a-range. A function is surjective if every element of the range is a value. **Totality** likewise is a property of a function-and-an-intended-domain. A function  $f$  on a set  $X$  is total if it is defined for every argument in  $X$ . Normally we will assume that our functions are total unless the possibility of their being partial is explicitly flagged. (This is not so in all CS cultures. For example in the theory of computable functions it is always assumed—unless the word ‘total’ is there in black and white—that our functions need not be total.)

rewrite this para

Some mathematical cultures make this explicit, saying that a function is an ordered triple of domain, range and a set of ordered pairs. This notation has the advantage of clarity, but it has not yet won the day.

In contrast, injectivity of a function-in-extension is a property solely of the function-in-extension and not of the intended domain or range. A function is injective iff it never sends distinct arguments to the same value.

Functions of more than one variable are usually written in the style ‘ $f(x_1 \dots x_n)$ ’ but some functions (such as  $+$  and  $\times$ ) traditionally are written in the infix style that we saw earlier (page 49).

The properties of *associativity*, *commutativity* and *distributivity* that I am about to explain seem always to be stated for functions that are written in infix notation—like  $+$  and  $\times$  on numbers (of all kinds) You know the equations

$$(\forall x)(\forall y)(x + y = y + x)$$

$$(\forall x)(\forall y)(x \times y = y \times x).$$

Those said that multiplication and addition are **commutative**. These two:

$$(\forall x)(\forall y)(\forall z)(x + (y + z) = (x + y) + z)$$

$$(\forall x)(\forall y)(\forall z)(x \times (y \times z) = (x \times y) \times z)$$

say that multiplication and addition are **associative**. Finally

$$(\forall x)(\forall y)(\forall z)(x \times (y + z) = (x \times y) + (x \times z))$$

says that multiplication **distributes over** addition. Observe that  $\wedge$  distributes over  $\vee$ .

An operation  $*$  is said to be **idempotent** if

$$(\forall x)(x * x = x)$$

$\wedge$  and  $\vee$  are idempotent operations on propositions.  $+$  and  $\times$  are not idempotent on numbers (of any kind). HCF is idempotent, though we will not make much use of this fact.

We now need the concept of a **unit** for a binary operation. Notice that—for example, the following hold for natural numbers, reals etc:

$$(\forall x)(x \cdot 1 = x) \text{ and } (\forall x)(x + 0 = x).$$

We express this by saying that 1 is a unit for multiplication (a “multiplicative unit”) and 0 is a unit for addition (an “additive unit”). In general a constant  $c$  is a unit for a commutative operation  $*$  if  $(\forall x)(x * c = x)$ . For example  $\emptyset$ , the empty set, is a unit for  $\cup$ :  $(\forall x)(x \cup \emptyset = x)$ , and  $V$ , the universal set, is a unit for  $\cap$ . The propositional constants **true** and **false** are units for  $\wedge$  and  $\vee$  respectively.

Along with units come inverses—sometimes! 0 is a unit for  $+$ , and  $-x$  is the additive inverse of  $x$ , in the sense that  $x + (-x) = 0$ . Similarly  $1/x$  is the multiplicative inverse of  $x$  (unless  $x = 0$ !). In general we say that  $f(x)$  is the inverse of  $x$  from the point of view of  $*$  if  $(\forall x)(x * f(x) = c)$ . (Remember that  $c$  was the unit for  $*$ .) Sometimes but not always. Notice that  $\cup$  and  $\cap$  do not have inverse functions: there is no function  $f$  such that  $(\forall x)(x \cup f(x) = \emptyset)$ .  $\wedge$  and  $\vee$  do not have inverses either.

A binary operation on widgets that is associative can be naturally extended to a function **widget-list**  $\rightarrow$  **widget**.

If the function is also commutative then it can be naturally extended to a function from *multisets-of-widgets* to **widgets**.

If it is (associative and) commutative and also idempotent then it can be naturally extended to a function from *sets-of-widgets* to **widgets**, as in the illustrations below.

- You can add two numbers together to get a number, so you can add together all the numbers in a (multi)-set  $X$  of numbers to get a number. Similarly you can multiply together all the numbers in a multiset of numbers. (We write the sum of all numbers in  $X$  as ‘ $\Sigma X$ ’ and the product as ‘ $\Pi X$ ’.)
- You can take  $\cap$  or  $\cup$  of two sets, so you can form  $\bigcap X$  and  $\bigcup X$  if  $X$  is a set of sets. Similarly one can form the compound propositions  $p \wedge q$  and  $p \vee q$  given two propositions  $p$  and  $q$ , and so we can form the compound propositions  $\bigwedge P$  and  $\bigvee P$  when  $P$  is a set of propositions.

This raises an obvious question, or family of questions.

*What happens if we apply  $\Sigma$  or  $\Pi$  to the empty set of numbers?*

*What happens if we apply  $\bigvee$  or  $\bigwedge$  to the empty set of propositions?*

*What happens if we apply  $\bigcap$  or  $\bigcup$  to the empty set of sets?*

It’s not hard to see that, for all these questions, the answer must be *the unit for the operation in question*:  $\bigvee \emptyset = \mathbf{false}$ ,  $\bigwedge \emptyset = \mathbf{true}$ ,  $\Sigma \emptyset = 0$  and  $\Pi \emptyset = 1$ ,  $\bigcup \emptyset = \emptyset$  and  $\bigcap \emptyset = V$ . The correctness of these last two equalities can be checked by literal-mindedly unravelling the set abstracts.

$\Sigma(X \cup \{y\})$  is obviously  $\Sigma(X) + y$ . So  $\Sigma(\emptyset)$  had better be 0.

$\Pi(X \cup \{y\})$  is obviously  $\Pi(X) \cdot y$ . So  $\Pi(\emptyset)$  had better be 1.

If you are still not convinced, consider the situation where you are trying to calculate the sum of the first  $n$  elements of a list. At each stage you append an element to the list of things you have added up. Initially you have added up no items. And what is the sum? Clearly it must be 0. Now think about taking the product of a list of terms. Again, you start with the empty list. What is the product of the empty list of terms? Clearly it must be 1.

This matters, and for two reasons. The first is that by forcing yourself to think about what happens when you do these operations to the empty set you will make progress on the issues discussed in section 2.2. The second is that at least one of these facts—namely the fact that the disjunction of the empty set of propositions is the **false**—has genuine computational significance (in connection with *resolution* which you may encounter later when you do more Logic<sup>3</sup>).

What follows now is a worked example. The exercise is to show that relational composition is associative. I am writing it out in some considerable detail because altho' the result is pretty obvious it's not at all clear to 1A students what a proof must look like.

We write ' $xTy$ ' for " $x$  is related to  $y$  by  $T$ ". We define relational composition in the obvious way:

$$x(T \circ S)y \text{ iff } (\exists z)(xTz \wedge zSy)$$

We will show that  $R \circ (S \circ T) = (R \circ S) \circ T$ .

That is to say, for all  $x$  and  $y$ ,  $xR \circ (S \circ T)y$  iff  $x(R \circ S) \circ Ty$

(I am using capital Roman letters both as relation symbols and as variables in an algebra.)

Now, by definition of relational composition,

$$xR \circ (S \circ T)y$$

is

$$(\exists z)(xRz \wedge z(S \circ T)y)$$

and expand the second ' $\circ$ ' to get

$$(\exists z)(xRz \wedge (\exists w)(zSw \wedge wTy))$$

We can pull the quantifiers to the front because<sup>4</sup> ' $(\exists u)(A \wedge \phi(u))$ ' is the same as ' $A \wedge (\exists u)\phi(u)$ '. (You haven't seen a proof of this but we assume that you can see that it's true. You will see a proof in *Logic and Proof* in 1B.)

This gives us

$$(\exists z)((\exists w)(xRz \wedge (zSw \wedge wTy)))$$

<sup>3</sup>Cambridge students: you will encounter resolution in Ib Logic and Proof

<sup>4</sup>At least as long as ' $u$ ' is not free in  $A$ .

and

$$(\exists z)(\exists w)(x R z \wedge (z S w \wedge w T y))$$

and we can certainly permute the quantifiers getting

$$(\exists w)(\exists z)(x R z \wedge (z S w \wedge w T y)).$$

We can permute the brackets in the matrix of the formula because ‘ $\wedge$ ’ is associative getting

$$(\exists w)(\exists z)((x R z \wedge z S w) \wedge w T y).$$

We can import the existential quantifier again getting

$$(\exists w)((\exists z)(x R z \wedge z S w) \wedge w T y)$$

and reverse the first few steps by using the definition of  $\circ$  to get

$$(\exists w)(x(R \circ S)w \wedge w T y)$$

and

$$x(R \circ S) \circ T y$$

as desired.

### Indicator functions

Each set  $A$  has an **indicator** or **characteristic** function, written  $I_A$  or  $\chi_A$  (‘ $\chi$ ’ is the first letter of the Greek word whence we obtained our word ‘characteristic’). This is the function that, on being given an object, returns **true** if the object is in  $A$  and **false** otherwise. In lambda notation it is:

$$\lambda x. \text{ if } x \in A \text{ then true else false.}$$

Characteristic functions make it slightly easier (very slightly!) to explain why a set with  $n$  members has  $2^n$  subsets. To notate the same fact a different way, using the vertical bars and the curly  $\mathcal{P}$  we have just learned,  $|\mathcal{P}(X)| = 2^{|X|}$ . Indicator functions make it clear that  $|\mathcal{P}(X)| = |X \rightarrow \{0, 1\}|$ .

You will need to know about them for a variety of reasons, for example in section 3.5.3. They will also crop up in second year computation theory, where they are invariably called **characteristic** functions rather than indicator functions.

### Inverses of functions

If  $f : A \rightarrow B$  is a function from  $A$  to  $B$ , and  $g : B \rightarrow A$  is a function such that  $(\forall a \in A)(g \circ f(a) = a)$  we say that  $g$  is a **right inverse** of  $f$ . If  $(\forall b \in B)(f \circ g(b) = b)$  we say that  $f$  is a **left inverse** of  $g$ .

Warning: this is a completely different use of the word ‘inverse’ from the one in play when we were talking about additive and multiplicative inverse earlier.

Finally, do not forget when revising this material that the notation ‘ $f$ “ $x$ ’ was discussed earlier, in section 3.1.2 and not here; you might want to go back there too.

### 3.2.9 Some exercises

In the following questions assume the carrier set is a fixed set  $X$ , let  $1$  be the identity relation restricted to  $X$  and let  $U$  be the universal (binary) relation on  $X$ , namely,  $X \times X$ . The relations here are all relations-in-extension.

**EXERCISE 35.**

*Is  $R \setminus R^{-1}$  antisymmetric? Asymmetric?*

*Is  $R \Delta R^{-1}$  symmetrical? Antisymmetric? Asymmetric?*

*Is the composition of two symmetrical relations symmetrical?*

*Is the composition of two transitive relations transitive?*

*Is the converse of a symmetrical relation symmetrical?*

*Is the converse of a transitive relation transitive?*

**EXERCISE 36.** *Can there be a function from  $X$  to itself whose graph is*

*(i) a reflexive relation? or*

*(ii) a transitive relation? or*

*(iii) a symmetrical relation?*

(Relational algebra in this style goes back to Russell and Whitehead (1919)).

**EXERCISE 37.** *How many binary relations are there on a set of size  $n$ ? [Warning: most students get this wrong because they free-associate instead of thinking it through. They also tend to neglect the distinction between an ordered pair and a set of ordered pairs, a binary relation. So take care!]*

*(a) How many of them are reflexive?*

*(b) How many are fuzzies? (A fuzzy is a binary relation that is symmetric and reflexive.)*

*(c) How many of them are symmetrical?*

*(d) How many of them are antisymmetric?*

*(e) How many are total orders?*

*(f) How many are trichotomous?*

*(g) How many are antisymmetric and trichotomous?*

*(h) There are the same number of antisymmetric relations as trichotomous. Prove this to be true without working out the precise number.*

*(i) (For the thoughtful student). If you have done parts (g) and (c) correctly, the answers will be the same. Is there a reason why they should be the same?*

*(j) Do not answer this question. How many partial orders are there on a set of size  $n$ ?*

*(k) Do not answer this question. How many strict partial orders are there on a set of size  $n$ ?*

*(l) Should the answers to the two previous questions be the same or different? Give reasons. (Compare this with your answer to part (i).)*

### 3.3 Cardinals

If two sets have the same number of elements then there will be a bijection between them. That looks pretty obvious: just pair them off one-by one at random until they are all used up. Actually this is obvious only if the sets under consideration are *finite* and—curiously—it actually makes more sense to think of “number of elements” in terms of the converse: we will say that two sets **have the same cardinality** (= number of elements) if and only if (“iff”) there is a bijection between them. We take this as the definition of cardinality. Cardinality is what two sets have in common iff there is a bijection between them.

Why do we use the fancy word ‘cardinal’ instead of ‘number’? (I’m not doing it just to be difficult). There are different sorts of number (something that probably was never spelled out properly to you when you were little) and emphatically not all numbers are cardinals. There are all sorts of questions to which the answer is a number. For example:

- (1) How many apples have you got in that basket?
- (2) How much money have you got in your bank account?
- (3) What is your resting pulse rate?
- (4) What is your diastolic blood pressure?
- (5) How long is the hypotenuse of a right-angled isocoles triangle whose other sides are of length 1?

The answer to (1) is a cardinal number. The answer to “How many ...?” is *always* a cardinal—even if it’s infinite: that’s what cardinals are. The answer to (2) is an integer. (An integer number of pennies: it might be negative!) We write the set of integers as  $\mathbb{Z}$ . The answer to (3) and (4) are real numbers, probably given to single precision. There are purists (and I am one of them) who insist that the complex number 1, the real number 1, the cardinal number 1 and the integer 1 are all in some sense different objects. You might not be a purist, but you’d better learn how purists think, for this distinction between (for example) the real number 1 and the cardinal number 1 is made by plenty of modern programming languages.

(I’ve left complex numbers out of this discussion not because they aren’t important—they’re **extremely** important—but because they are part of continuous mathematics not discrete mathematics.)

Rationals are so called because they are *ratios*, and in fact not just any ratios but ratios of *integers*. They are answers to questions of the kind “How much bigger/nicer/higher is  $A$  than  $B$ ?” (at least if niceness, size etc is measured by an integer!). We write the set of rationals as  $\mathbb{Q}$ .

Real numbers measure lengths of line segments, or areas, volumes; that sort of thing. You buy potatoes by real numbers not by cardinal number. Avocados you buy by cardinal number. (You buy potatoes by the kilo whereas avocados are so much *each*.) We write the set of reals as  $\mathbb{R}$ .

The Greeks discovered early on that not every real number is a ratio; specifically they showed quite early on that  $\sqrt{2}$  is not rational. (You will have heard of  $e$  and  $\pi$  and they aren't rationals either. But proving that is harder than proving that  $\sqrt{2}$  is irrational!)

**THEOREM 1.**  $\sqrt{2}$  is not a rational.

We first assume that it can be expressed as a rational number (the opposite of what we believe), therefore:

$$\sqrt{2} = a/b \quad (3.1)$$

with  $a$  and  $b$  reduced to their lowest terms (no common factors)

We now square both sides of the equation to get:

$$2 = a^2/b^2 \quad (3.2)$$

We now multiply both sides by  $b^2$  to get:

$$2b^2 = a^2 \quad (3.3)$$

From this we can see that  $a^2$  must be an even number because it is equal to something multiplied by 2, and an even number multiplied by 2 is still even, as is an odd number multiplied by 2. Indeed:  $a$  is even since the square of an odd number is odd.

Even numbers are divisible by 2 so  $a = 2 \cdot c$ , for some other natural number  $c$ . Therefore  $a^2 = 4c^2$ , and we can substitute  $4c^2$  for  $a^2$  in 3.3) to get:

$$2b^2 = 4c^2 \quad (3.4)$$

The two sides of 3.4 have 2 as a common factor so we can divide through by 2:

$$b^2 = 2c^2 \quad (3.5)$$

But using the same deduction for  $b$  as we used for  $a$  in equation in 3.3, we can show that  $b$  is even, too!

And this is our contradiction: if  $a$  and  $b$  are both even then they share at least one common factor (namely 2), but we said that  $a/b$  had been simplified so that  $a$  and  $b$  had no common factors). This means that our original assumption must be wrong, and that the square root of 2 cannot be expressed as a rational number. ■

Just to check that you understand this proof, do a similar proof that  $\sqrt{3}$  is irrational.

There are infinite cardinals: that was the surprise of this section. But there are no infinite reals, rationals or complexes, I can promise you that!



Other kinds of numbers that we haven't seen yet. Ordinals and integers mod  $p$ . Quaternions. You definitely do *not* need to know about quaternions, and you definitely *do* need to know about integers mod  $p$ . You may manage to get away without knowing about ordinals for quite a long while yet.

There are now some trivial observations we can make about cardinality. The relation “ $x$  and  $y$  have the same cardinality” is an equivalence relation. Most textbooks leave this as an exercise but in my experience this is something that needs to be aired.

1. Transitivity. If  $X$  and  $Y$  have the same cardinal it is because there is a bijection between them, say  $f : X \rightarrow Y$ . Similarly if  $Y$  and  $Z$  have the same cardinal it is because there is a bijection between them, say  $g : Y \rightarrow Z$ . But then  $g \circ f : X \rightarrow Z$  is a bijection between  $X$  and  $Z$ .
2. Symmetry. If  $X$  and  $Y$  have the same cardinal it is because there is a bijection between them, say  $f : X \rightarrow Y$ . But then  $f^{-1} : Y \rightarrow X$  is a bijection in virtue of which  $Y$  has the same cardinal as  $X$ .
3. Reflexivity. The identity map  $X \rightarrow X$  certifies that  $X$  is the same size as  $X$ .

Notice that all we have defined is what it is for two sets to have-the-same-cardinality; we haven't said what cardinalities are. And what's more, we won't! And it doesn't matter! All you need to know about cardinality is that two sets have the same cardinal iff there is a bijection between them.

I think you can safely assume that the words ‘cardinal’ and ‘cardinality’ are synonymous.

So what are cardinals? You probably never worried about what the number 1 was, as all the things you wanted to do with it or to it you could without worrying about what it actually was. Perhaps you are expecting—now that you are doing rather more proper maths than hitherto—that you have to start worrying about these things. Interestingly you don't. You can think of cardinals as equivalence classes of sets under the equivalence relation of having-the-same-cardinal if you want to; but you don't have to. It's not a good idea to start worrying about what cardinals are, it can do your head in. Incredibly, there is a community of people who worry about whether or not the number 1 might be Julius Caesar. (I'm not making this up.) You don't want to end up like them.

Must establish that a composition of two injections is an injection, and of two surjections is a surjection

### Not all cardinals are finite

Remember, all sets have cardinals, and not all sets are finite, so not all cardinals are finite. The finite cardinals are the natural numbers,  $\mathbb{N}$ , but we have to remember that there are other cardinals as well. Some sets are infinite ( $\mathbb{N}$  is an infinite set) and some of these sets are of concern to you as computer scientists. You've never had to think about infinite sets before and all your reasoning about sets has relied on the tacit assumption that all sets are finite. If some of what follows in the coming sections seems too obvious to be worth stating, it may be that you are still making the tacit assumption that all sets are finite.

### The order relation on cardinals

We can define a partial order on cardinals. We write ' $|X| \leq |Y|$ ' to mean that there is an injection from a set of size  $|X|$  (as it might be,  $X$ !) into a set of size  $|Y|$  (as it might be,  $Y$ ! It won't make any difference which sets of size  $|X|$  or  $|Y|$  you choose).

Did I say 'partial order'? Obvious that it's transitive and reflexive. (Look back at the demonstration on page 73 that the relation of "having the same cardinal" is an equivalence relation). How about antisymmetrical? You are tempted to say that if there is an injection from  $A$  into  $B$  and an injection from  $B$  into  $A$  then both injections must actually be surjections, so we are done. (Beware! Merely finding an injection  $A \rightarrow B$  that is not a surjection does NOT show that  $|A| < |B|$ .) This argument certainly works if  $A$  and  $B$  are finite sets, and at this stage your intuition probably doesn't work freely with infinite sets so finite sets are likely to be the only kind you consider, so you think that it's obvious that  $\leq$  is antisymmetrical. But actually it isn't obvious at all. You appeal to the idea that if there is an injection  $f : A \rightarrow B$  and an injection  $g : B \rightarrow A$  then  $f$  (and  $g$  too for that matter) must be a surjection. This isn't true for infinite sets, as we can easily see:  $\lambda n.2n$  is an injection from  $\mathbb{N}$  to itself which is not a surjection. Strange but true... Actually we can take this strangeness as a *definition* of infinite set. *An infinite set is one that is in bijection with a proper subset of itself.* In our present case,  $\mathbb{N}$  is infinite because it is in bijection with  $\{2n : n \in \mathbb{N}\}$ —the evens.

Nevertheless it is true:  $\leq$  really is antisymmetrical. The theorem that states this is the **Cantor-Bernstein** theorem. We won't prove it!

A good illustration of why the Cantor-Bernstein theorem is useful is given by the set  $\mathbb{N}$  of natural numbers and the set  $\mathbb{Q}$  of rational numbers. There is a bijection between these two sets—*lots*, indeed—but they are all very hard to find and describe directly. However it is easy to describe *injections* from  $\mathbb{Q}$  into  $\mathbb{N}$  and from  $\mathbb{N}$  into  $\mathbb{Q}$ , as follows:

1. The function that sends the natural number  $n$  to the rational number  $n$  clearly is an injection from  $\mathbb{N}$  into  $\mathbb{Q}$ .
2. Every rational can be expressed as a ratio of two naturals with no common factor, associated with a plus or minus sign. This means we can send the rational number  $+(n/m)$  to the natural number  $2 \cdot 3^n \cdot 5^m$ , and we can send the rational number  $-(n/m)$  to the natural number  $3^n \cdot 5^m$ . (negative rationals go to even naturals and positive rationals go to odd naturals. And we can send the rational number 0 to the natural number 0) It's easy to check that this is an injection. (I know it looks fiddly: all injections from  $\mathbb{Q}$  into  $\mathbb{N}$  do!)

The Cantor-Bernstein theorem now tells us that there will be a bijection between  $\mathbb{N}$  and  $\mathbb{Q}$ . If you look hard at the proof of the theorem you can see how to give such a bijection explicitly. This is not recommended!

With a little bit of finagling (by means of an assumption called the axiom of choice which you will not need to know about) we can tidy cardinals up so that every cardinal is either infinite (in the above sense) or is a **natural number**.<sup>5</sup>

The name for the cardinal that the set of naturals and the set of rationals share is ' $\aleph_0$ '. (' $\aleph$ ' is the first letter of the Hebrew alphabet and Cantor was Jewish). It is the smallest infinite cardinal, in the sense that any set that is smaller than  $\aleph_0$  is finite.

You will need to know a bit about infinite cardinals, but not much.  $\mathcal{P}(\mathbb{N})$  is of course of size  $2^{\aleph_0}$  and there are  $2^{\aleph_0}$  real numbers. (This is because every real number can be represented as an sequence of 0s and 1s, one for each natural number. So there are  $\aleph_0$  independent choices from  $\{0, 1\}$ , making  $2^{\aleph_0}$  possible outcomes. There is a certain amount of tidying up because some reals (those rational numbers whose denominators are powers of 2) have two representations as infinite binary numbers, but we won't go into that). Cantor's theorem (which we will see in section 3.5.2) tells you that infinite sets come in infinitely many different sizes:  $\aleph_0 < 2^{\aleph_0} < 2^{2^{\aleph_0}} \dots$  after all but despite this it's a fairly safe prediction that every infinite set you meet will be of size  $\aleph_0$  or  $2^{\aleph_0}$ .

We don't yet know about  
cantor's theorem

You may be wondering: is there an  $\aleph_1$ ? There is—and an  $\aleph_2$ ,  $\aleph_3$  and so on—but you don't need to worry about them until further notice. The file [www.dpmms.cam.ac.uk/~tf/countability.pdf](http://www.dpmms.cam.ac.uk/~tf/countability.pdf) tells you a bit more about some of this material (though not about  $\aleph_1$ ). It's designed for 1a maths students and so goes slightly beyond what you are going to need immediately. However it is probably quite digestible.

## 3.4 Recursive Datatypes

We start this section with some revision of Mathematical Induction. You probably think you understand it already, but I want you to be Born Again!

### 3.4.1 Induction: revision

*Induction can only be understood backwards, but it must be lived forwards.*

Kierkegaard

Finite cardinals are called **Natural Numbers**, and the set of natural numbers is denoted with a special kind of boldface ' $\mathbb{N}$ '. Natural numbers obey a wonderful principle called *Mathematical Induction* which you have certainly heard of. Mathematical induction is not a pleasant extra but a core skill, and one you must have; do not even think about skipping this section. Unfortunately it is also a well-known problem for beginners. There are several causes of this, and life becomes easier once they are teased apart and tackled separately.

I can think of four off the top of my head:

<sup>5</sup>Q: "What about rationals and negative numbers? They're not infinite!"

A: They're numbers all right, but they're not cardinals: see the digression above.

1. One is the old problem with fault-tolerant pattern-matching, which makes the average punter so imprecise in expressing their workings that they lose track of what they are doing. Unless you are extremely precise you won't have a hope.
2. Hypothetical reasoning is the process by which we prove  $A \rightarrow B$  by assuming  $A$  and deducing  $B$ . In modern formal logic we call it " $\rightarrow$ -introduction". Lots of people find this hard. There is even a tradition in the battier parts of Western Philosophy that it cannot be done *at all* (or at least that argument by *reductio ad absurdum* is impossible). If you have done any Logic you will probably not have nightmares about this, but others may be spooked. Seek help if need be.

A lot of students are unnerved by having to think about a conditional whose antecedent is a conditional.

Need to find something more to say about this

However, for the moment I'll address the issue about notation, because it often ensnares even students who are fairly happy about hypothetical reasoning.

Summary: we are trying to prove that every natural number has a property,  $F$ , say. We will succeed if we can do two things:

1. We establish that  $F(0)$ ;
2. We establish that, for all  $n$ ,  $F(n)$  implies  $F(n + 1)$ .

Step 1 is the **base case**, and step 2 is the **induction step**. The base case doesn't always have to be 0; sometimes (and the example we are about to work through is a case in point) the zero case is exceptional and we don't worry about it. In this case we will start at 1.

### A simple illustration

Let's take a simple example. It's simple in that the proposition we are trying to prove can be easily understood and looks fairly obvious, but the proof is difficult enough to exhibit all the standard problematic features.

Let us prove by induction that—for all  $n$ —the sum of the first  $n$  odd numbers is  $n^2$ . That is to say  $F(n)$  is the assertion that the sum of the first  $n$  odd numbers is  $n^2$ .

Formula 3.2 says that the sum of the first  $n$  odd numbers is  $n^2$ . The  $n$ th odd number is of course  $2n - 1$ .

$$\sum_{r=1}^n (2r - 1) = n^2 \quad (3.1)$$

' $n$ ' is the **eigenvariable**: we are doing "induction **on**  $n$ ".

Base case,  $n = 1$  is easy.

We want to prove the induction step: if it holds for  $k$  it holds for  $k + 1$ . What we are actually doing is a proof by Universal Generalisation (AKA  $\forall$ -introduction), with ‘ $k$ ’ being the business variable. (sometimes called the *eigenvariable*, as above.)

We are going to assume it true “for  $k$ ” as we say, and hope to be able to deduce it for  $k + 1$ . Notice that in this expression ‘ $r$ ’ is bound and ‘ $k$ ’ is free. (This terminology of free and bound variables wasn’t chunked at you merely to annoy you: it’s needed to properly understand stuff like this!). Do you know what I mean by this last remark? Make sure that you do before reading further!

The assumption that we have just made, that the assertion we are trying to prove does at least hold for  $k$  (and from which we intend to deduce that it holds for  $k + 1$ ) is called the **induction hypothesis**.

So you add the  $k + 1$ th odd number to both sides, getting

$$\left(\sum_{r=1}^k (2r - 1)\right) + 2k + 1 = k^2 + 2k + 1 \quad (3.2)$$

So far so good. You now have to do quite a lot of rearranging, and it may be that it helps if this is done in excruciating detail. Let’s tackle the left-hand side first

$$\left(\sum_{r=1}^k 2r - 1\right) + 2k + 1 \quad (3.3)$$

is just

$$\sum_{r=1}^{k+1} 2r - 1 \quad (3.4)$$

This is because they are both the sum of the first  $k + 1$  odd numbers. Formula 3.3 says “the sum-of-the-first- $k$ -odd-numbers—with  $2k + 1$  added on” (and  $2k + 1$  just happens to be the  $k + 1$ th odd number). Formula 3.4 says “the sum-of-the-first- $k + 1$ -odd-numbers”.

So formula 3.2 has become

$$\sum_{r=1}^{k+1} 2r - 1 = k^2 + 2k + 1 \quad (3.5)$$

and now we can turn our attention to the RHS. Every fule kno that the RHS of this is equal to  $(k + 1)^2$ , so we get

$$\sum_{r=1}^{k+1} 2r - 1 = (k + 1)^2 \quad (3.6)$$

But now notice that this formula is **exactly** the result of taking formula 3.1 and replacing ‘ $k$ ’ by ‘ $k + 1$ ’ throughout. **Check this by hand so you understand it.**

And—just as formula 3.1 said that the sum of the first  $k$  odd numbers is  $k^2$ , formula 3.6 says that the sum of the first  $k + 1$  odd numbers is  $(k + 1)^2$ . So we have taken an assertion about  $k$ , and deduced from it the corresponding assertion about  $k + 1$ .

### This concludes the proof of the induction step

This is something you will see in all the standard cases of proof-by-induction that the sum of the first  $k$  perfect squares, or cubes, or odd numbers, or triangular numbers, or whatever it is, is some expression in ' $k$ '. In all these cases you will see a LHS that looks like  $(\sum_{r=1}^k \text{something or other})$  and an RHS that is some complex expression with ' $k$ ' free. Formula 3.1 is our example above. When proving the induction you infer from (as it were) formula 3.1 the result of substituting ' $k + 1$ ' for ' $k$ ' in (as it were) formula 3.1. You add the  $k$ th term to both sides, which makes the LHS the sum of the first  $k$  terms plus the  $k + 1$ th term—which is of course the sum of the first  $k + 1$  terms. And you add the  $k + 1$ th term to the RHS as well and hope that you will be able to rearrange it into the result of substituting ' $k + 1$ ' for ' $k$ ' in the RHS.

A stylistic detail at this point. There is something rather special about the operation of adding 1 to a number (as opposed to the operation of adding 2, or 3, for example). This is because it is this operation-of-adding-1 that generates all the natural numbers, starting from 0. A natural number is either 0 or something one can obtain from 0 by adding 1 lots of times. For this reason we have a special notation for it: ' $S$ ', so we write  $S(x)$  instead of  $x + 1$ , and (and this is the important part) express the inductive step in mathematical induction as “if it holds for  $n$ , it holds for  $S(n)$ ”. The point is that this special notation highlights the rôle of the operation of addition-of-1 in the genesis of the set of natural numbers.

**EXERCISE 38.** Suppose  $f$  and  $g$  obey the declarations:

$$f(0) := 1; (\forall n)(f(n + 1) := (n + 1) \cdot f(n))$$

$$g(0) := 1; (\forall n)(g(n + 1) := (n + 1) \cdot g(n))$$

Prove that  $(\forall n \in \mathbb{N})(f(n) = g(n))$ .

This shows we can use induction to prove the uniqueness of the function being defined.

### 3.4.2 Definition

'Recursive datatype' is the sexy, postmodern, techno-friendly way to talk about things that mathematicians used to call 'inductively defined sets'. I shall abbreviate these two words to the neologism 'rectype'.

The standard definition of the naturals is as the least (with respect to  $\subseteq$ ) set containing zero and closed under successor, or, using some notation we have just acquired:

$$\mathbb{N} = \bigcap \{Y : 0 \in Y \wedge S^*Y \subseteq Y\}.$$

Of course  $\mathbb{N}$  is merely the simplest example, but its definition exhibits the central features of a declaration of a rectype. In general, a rectype is a set defined as the smallest ( $\subseteq$ -least) set containing some **founders**<sup>6</sup> and closed under certain functions, commonly called **constructors**. (This is standard terminology.)  $\mathbb{N}$  has only one founder, namely, 0, and only one constructor, namely, successor (often written ‘ $S$ ’ or ‘**succ**’:  $S(x)$  is  $x + 1$ ). For the record, a founder is of course a nullary (0-place) constructor.

### 3.4.3 Structural induction

This definition of  $\mathbb{N}$  justifies induction over it. If  $F(0)$  and  $F(n) \rightarrow F(S(n))$  both hold, then  $\{n : F(n)\}$  is one of these  $Y$  that contains 0 and is closed under  $S$ , and therefore it is a superset of  $\mathbb{N}$ , from which it follows that every natural number is  $F$ . It is a bit like original sin: if  $F$  is a property that holds of 0, and holds of  $n + 1$  whenever it holds of  $n$ , then each natural number is innoculated with it as it is born. As you are born, you arrive with a ready-minted certificate saying that you are  $F$ . Hence induction.

### 3.4.4 Generalise from $\mathbb{N}$

$\mathbb{N}$  is of course the simplest example of a rectype: it has only one founder and only one constructor, and that constructor is unary.

My first encounter with rectypes was when I was exposed to compound past tenses in Latin, when I was about eight. I pointed out to my Latin teacher that the construction that gives rise to the future perfect tense from the perfect could be applied to the pluperfect tense as well, and what was the resulting tense called, please? Maybe the reader has had similar experiences. In UK law, if it is a crime to do  $X$ , it is also a crime to attempt to do  $X$  or to conspire to do  $X$ . So presumably it is a crime to attempt to conspire to do  $X$ ? Crimes and tenses form recursive datatypes.

The examples that will concern us here will be less bizarre. An  $X$ -list is either the empty object or the result of **consing** a member of  $X$  onto the front of an  $X$ -list. Thus a list can be thought of as a function from an initial segment of  $\mathbb{N}$  to  $X$ . Thought of as a rectype, the family of  $X$ -lists has a founder (the empty list) and a single binary constructor: **cons**. In ML the notation ‘ $h::t$ ’ denotes the list obtained by **consing** the object  $h$  onto the front of the list  $t$ .  $t$  is the **tail** of  $h::t$ , and  $h$  is its **head**.

**EXERCISE 39.** *You can also think of the transitive closure  $t(R)$  of a binary relation-in-extension as a rectype. What are the founders and the operations?*

We can develop analogues of mathematical induction for any recursive datatype, and I shall not spell out the details here, as we shall develop them in each case

<sup>6</sup>This is not standard terminology, but I like it and will use it.

as we need them. This kind of induction over a retype is nowadays called **structural induction**.<sup>7</sup>

This is an old example sheet question. You should definitely attempt it.

**EXERCISE 40.**

*“We define the length of a Boolean proposition by recursion as follows:*

$$\begin{aligned} |a| &= 1, \\ |\top| &= 1, \\ |\perp| &= 1, \\ |A \wedge B| &= |A| + |B| + 1, \\ |A \vee B| &= |A| + |B| + 1, \\ |\neg A| &= |A| + 1. \end{aligned}$$

*We define a translation which eliminates disjunction from Boolean expressions by the following recursion:*

$$\begin{aligned} tr(a) &= a, \quad tr(\top) = \top, \quad tr(\perp) = \perp, \\ tr(A \wedge B) &= tr(A) \wedge tr(B), \\ tr(A \vee B) &= \neg(\neg tr(A) \wedge \neg tr(B)), \\ tr(\neg A) &= \neg tr(A). \end{aligned}$$

*Prove by structural induction on Boolean propositions that*

$$|tr(A)| \leq 3|A| - 1,$$

*for all Boolean propositions  $A$ . ”*

### 3.4.5 An Induction Exercise Concerning Evaluation

*This section isn’t actually difficult, but it relies on truth-tables, and it might look a bit scary, so don’t feel guilty if you want to postpone it and come back to it later. Confident students should be fine.*

I’m assuming that you are happy with truth-table definitions of the operations  $\wedge$  and  $\vee$  on booleans (perhaps you prefer the notations ‘AND’ and ‘OR’). A **valuation** is a function from propositional letters to booleans. You can think of a valuation as a row of a truth-table, an assignment of boolean values to every propositional letter in sight. Given a complex formula  $A$  and a valuation  $v$ , one can *evaluate*  $A$  according to  $v$  and obtain a truth-value.

Clearly there is a function  $E$ : formulæ  $\times$  valuations  $\rightarrow$  booleans.

---

<sup>7</sup>Historical note: Russell and Whitehead called it **ancestral induction** because they called the transitive closure of a relation the **ancestral** of the relation. (This is because of the canonical example: the transitive closure of the parent-of relation is the ancestor-of relation.) I used their terminology for years—and I still think it is superior—but the battle for it has been lost; readers should not expect the word ‘ancestral’ to be widely understood any longer, though they may see it in the older literature.



**EXERCISE 41.** Write code for such a function  $E$  in your favourite functional programming language.

(In case you were wondering, your favourite functional programming language is ML!)

The recursion you have written does not contain any instruction as to the mechanics of calculating the answer. One can evaluate *lazily* or *strictly*. For example: suppose that at some point in the computation-of-the-truth-values-of- $A$ -according-to- $v$  you have determined, for some subformula  $A'$  of  $A$ , that  $A'$  is **false** according to  $v$ . Suppose  $A' \wedge B$  is the next subformula for us to tackle. If we are evaluating “lazily” we can get clever and say “Ah! Since  $A'$  has evaluated to **false** we know already that  $A' \wedge B$  must evaluate to **false**, so we don’t need to compute the truth-value of  $B$ !” In contrast, the strategy of *strict evaluation* requires us to compute the truth value of all subformulae of an input before we try to compute the truth-value of the input. Thus there are **two** functions  $E_s$  and  $E_l$  (strict evaluation and lazy evaluation ...) but these two functions have *three* arguments not two. Their three arguments are: a formula, a valuation, and a *time*; and the recursive declaration for  $E_l$  will have base clauses like

If  $A$  is atomic, then  $(\forall n \in \mathbb{N})(E_s(A, v, n) = E_l(A, v, n) =: v(A))$ .

and

$$E_s(A, v, 0) = E_l(A, v, 0) =: v(A),$$

and recursive clauses like (for example)

$$E_l(A \vee B, v, t + 1) = \text{if } E_l(A, v, t) = \text{true then true else...}$$

**EXERCISE 42.** Write code for  $E_l$  and  $E_s$  in your favourite functional programming language.

It’s probably obvious to you that  $E_s$  and  $E_l$  will give the same end result. Perhaps it even looks so obvious that you think it’s not actually worth proving. However, this fact is worth proving, and for two reasons. One is that it is a useful exercise in induction, and the other is that if our valuations are allowed to be partial functions it ceases to be true!

**EXERCISE 43.** (*Easy*)

Find  $A$  and  $v$  to illustrate how  $(\forall t > 0)(E_s(A, v, t) \neq E_l(A, v, t))$  can happen if  $v$  is not total.

However, things are better behaved if we assume that all our valuations are total functions. So, let’s make this assumption *pro tem*. Then, as we observed above,  $E_s$  and  $E_l$  will give the same end result. It’s worth thinking about how one would state this last fact properly. So shield the rest of this pdf from your eyes for the moment and give the matter some thought. The next exercise sets out my attempt at formulating this obvious fact in a way that one might prove.

Then we want to

**EXERCISE 44.** *Show that:*

*For all valuations  $v$  and all formulæ  $A$  and all but finitely many  $t$ ,*

$$E_t(A, v, t) = E(A, v) \text{ and } E_s(A, v, t) = E(A, v).$$

This is pretty obvious, but it's not totally straightforward to prove. It's certainly obvious that you are going to have to do some induction...but an induction on what? On ' $t$ '? Or a structural induction on the subformula relation? This exercise is an object lesson in getting straight quite what it is you are proving by induction, stating the induction hypothesis carefully and being clear in your own mind what kind of induction you are doing.

### 3.4.6 Well-founded induction

#### Well-founded relations and induction

Suppose we have a carrier set with a binary relation  $R$  on it, and we want to be able to infer

$$\forall x \psi(x)$$

from

$$(\forall x)[(\forall y)(R(y, x) \rightarrow \psi(y)) \rightarrow \psi(x)].$$

In words, we want to be able to infer that everything is  $\psi$  from the news that you are  $\psi$  as long as all your  $R$ -predecessors are  $\psi$ .  **$y$  is an  $R$ -predecessor of  $x$**  if  $R(y, x)$ . Notice that there is no “case  $n = 0$ ” clause in this more general form of induction: the premiss we are going to use implies immediately that a thing with no  $R$ -predecessors must have  $\psi$ . The expression “ $(\forall y)(R(y, x) \rightarrow \psi(y))$ ” is called the **induction hypothesis**. The first line says that if the induction hypothesis is satisfied, then  $x$  is  $\psi$  too. Finally, the inference we are trying to draw is this: **if**  $x$  has  $\psi$  whenever the induction hypothesis is satisfied, **then** everything has  $\psi$ . When can we do this? We must try to identify some condition on  $R$  that is equivalent to the assertion that this is a legitimate inference to draw in general (i.e., for any predicate  $\psi$ ).

Why should anyone want to draw such an inference? The antecedent says “ $x$  is  $\psi$  as long as all the immediate  $R$ -predecessors of  $x$  are  $\psi$ ”, and there are plenty of situations where we wish to be able to argue in this way. Take  $R(x, y)$  to be “ $x$  is a parent of  $y$ ”, and then the inference from “children of blue-eyed parents have blue eyes” to “everyone has blue eyes” is an instance of the rule schematised above. As it happens, this is a case where the relation  $R$  in question does *not* satisfy the necessary condition, for it is in fact the case that children of blue-eyed parents have blue eyes and yet not everyone is blue-eyed.

To find what the magic ingredient is, let us fix the relation  $R$  that we are interested in and suppose that the inference

$$\frac{(\forall y)(R(y, x) \rightarrow \psi(y)) \rightarrow \psi(x)}{(\forall x)(\psi(x))}$$

has failed for some choice  $\psi$  of predicate.<sup>8</sup> Then we will see what this tells us about  $R$ . To say that  $R$  has the magic ingredient all we have to do is stipulate that this failure (whatever it is) cannot happen for any choice of  $\psi$ .

Let  $\psi$  be some predicate for which the inference fails. Consider the set of all things that are *not*  $\psi$ . Let  $x$  be something with no  $R$ -predecessors. Then all  $R$ -predecessors of  $x$  are  $\psi$  (vacuously!) and therefore  $x$  is  $\psi$  too. This tells us that if  $y$  is something that is not  $\psi$ , then there must be some  $y'$  such that  $R(y', y)$  and  $y'$  is not  $\psi$  either. If there were not,  $y$  would be  $\psi$ . This tells us that the collection of things that are not  $\psi$  “has no  $R$ -least member” in the sense that everything in that collection has an  $R$ -predecessor in that collection.

Thus we can see that if induction fails over  $R$ , then there is a subset  $X$  of the carrier set (to wit, the extension of the predicate for which induction fails) such that every member of  $X$  has an  $R$ -predecessor in  $X$ .

One might have expected that for the inference to be good one would have had to impose conditions on both  $R$  and  $\psi$ . It is very striking that there should be a condition on  $R$  alone that is enough by itself for this inference to be good for *all*  $\psi$ . All we have to do is exclude the possibility of the domain of  $R$  having any such pathological subsets and we will have justified induction over  $R$ . Accordingly, we will attach great importance to the following condition on  $R$ :

**DEFINITION 3.**  $R$  is **well-founded** iff every nonempty subset  $X$  of the domain of  $R$  has an element  $x$  such that all the  $R$ -predecessors of  $x$  lie outside  $X$ . ( $x$  is an “ $R$ -minimal” element of  $X$ .)

This definition comes with a health warning: it is easy to misremember. The only reliable way to remember it correctly is to rerun in your mind the discussion we have gone through: well-foundedness is precisely what one needs a relation  $R$  to have if one is to be able to do induction over  $R$ . No more and no less. The definition is not memorable, but it is reconstructible.

A **well-ordering** is a well-founded strict total order. (No well-founded relation can be reflexive, so well-founded orders have to be of the strict flavour). Perhaps we should have some examples of well-orderings. Obviously any finite total order will be a well-order! What about infinite well-orderings? The only natural example of an infinite well-ordering is one we have already seen— $\langle \mathbb{N}, <_{\mathbb{N}} \rangle$ . Notice that the real line  $\langle \mathbb{R}, <_{\mathbb{R}} \rangle$  is not a well-ordering, for it is a simple matter to find sets of real numbers with no least element, for example, the set of all real numbers strictly greater than 0. This set has a lower bound all right, namely 0, but this lower bound is not a member of the set and so cannot be the least member of it.<sup>9</sup>

**EXERCISE 45.** One can define well-orderings as relations that are trichotomous and well-founded.

<sup>8</sup>This is a common way of representing arguments in logic: premisses above and conclusions below the line.

<sup>9</sup>It is important not to get confused (as many people do) by the fact that every set of reals has a *greatest lower bound*. For example,  $\{x \in \mathbb{R} : x > 0\}$  has no least member, but it does have a greatest lower bound, which is of course 0. Notice that  $0 \notin \{x \in \mathbb{R} : x > 0\}$ !!

**EXERCISE 46.**

*A pointwise product of two well-founded (strict) partial orders is a well-founded (strict) partial order.*

*A lexicographic product of two well-founded (strict) partial orders is a well-founded (strict) partial order.*

It is not hard to see that for a finite binary structure to be well-founded it is necessary and sufficient for it to have no loops.

It's clearly necessary that there should be no loops, since a loop is manifestly a subset with no least element! Sufficiency is slightly harder, but you should have no difficulty persuading yourself that if you have a subset with no least element, then you can use it to build a loop.

With infinite structures, absence of loops remains a necessary condition of course, but it is no longer sufficient: the negative integers with the relation  $\{\langle n, n-1 \rangle : n \in \mathbb{Z}^-\}$  has no loops, but it is still not well-founded. With the help of an apparently minor assumption we can show that this is the only badness that can happen in infinite ill-founded structures.

This means that one can safely think of a wellfounded relation  $R$  as a relation that **“has no infinite descending chains”**. That is to say, there is no sequence  $x_1, x_2, x_3, \dots$  where, for all  $n \in \mathbb{N}$ ,  $R(x_{n+1}, x_n)$ .

The official definition of well-foundedness is a lot more unwieldy than the definition in terms of descending sequences. In consequence, it is very easy to misremember it. A common mistake is to think that a relation is well-founded as long as its domain has a minimal element, and to forget that *every nonempty subset* must have a minimal element. The only context in which this definition makes any sense at all is induction, and the only way to understand the definition or to reconstruct it is to remember that **it is cooked up precisely to justify induction; it serves no other purpose**.

**THEOREM 2.**  *$R$  is a well-founded relation iff we can do well-founded induction over the domain of  $R$ .*

*Proof:* The left-to-right inference is immediate: the right-to-left inference is rather more interesting.

What we have to do is use  $R$ -induction to prove that every subset of the domain of  $R$  has an  $R$ -minimal element. But how can we do this by  $R$ -induction? The trick is to prove by  $R$ -induction (“on  $x$ ”) that every subset of the domain of  $R$  to which  $x$  belongs contains an  $R$ -minimal element. Let us abbreviate this to “ $x$  is  **$R$ -regular**”.

Now let  $x_0$  be such that every  $R$ -predecessor of it is  $R$ -regular, but such that it itself is not  $R$ -regular. We will derive a contradiction. Then there is some  $X \subseteq \text{dom}(R)$  such that  $x_0 \in X$  and  $X$  has no  $R$ -minimal element. In particular,  $x_0$  is not an  $R$ -minimal element of  $X$ . So there must be  $x_1$  s.t.  $R(x_1, x_0)$  and  $x_1 \in X$ . But then  $x_1$  is likewise not  $R$ -regular. But by hypothesis everything  $R$ -related to  $x_0$  was  $R$ -regular, which is a contradiction.

Therefore everything in  $\text{dom}(R)$  is  $R$ -regular. Now to show that any subset  $X$  of  $\text{dom}(R)$  is either empty or has an  $R$ -minimal element. If  $X$  is empty,

we are all right. If it is not, it has a member  $x$ . Now we have just shown by  $R$ -induction that  $x$  is  $R$ -regular, so  $X$  has an  $R$ -minimal element as desired. ■

Well-foundedness is a very important concept throughout Mathematics, but it is usually spelled out only by logicians. (That is why you read it here first.) Although the rhetoric of Mathematics usually presents Mathematics as a static edifice, mathematicians do in fact think dynamically, and this becomes apparent in mathematical slang. Mathematicians often speak of *constructions* underlying proofs, and typically for a proof to succeed it is necessary for the construction in question to terminate. This need is most obvious in computer science, where one routinely has the task of showing that a program is well-behaved in the sense that every run of it halts. Typically a program has a main loop that it goes through a number (which one hopes will be finite!) of times. The way to prove that it eventually halts is to find a parameter changed by passage through the loop. There are various sorts of parameters that can play this rôle:

- The simplest illustration is the **count** variable to be found in many programs. A **count** variable is not affected by any of the code within the loop other than the decrement command that decrements it at the start (or on the end) of each pass.
- Sometimes the rôle is played by a program variable that is not explicitly decremented at the start of each pass in the way a **count** variable, but is decremented as a side-effect of what happens on each pass.
- In general we look for a parameter that need not be a program variable at all, but merely some construct put together from program variables.

In all cases we want the parameter of interest to take values in a set  $X$  with a binary relation  $R$  on it such that

1. at each pass through the loop the value of the parameter changes from its old value  $v$  to a new value  $v'$  such that  $\langle v, v' \rangle \in R$  and
2. any sequence  $v_0, v_1 \dots$  where for all  $n$ ,  $\langle v_n, v_{n+1} \rangle \in R$ , is finite.

(If you were expecting this sentence to end “is eventually constant”, look ahead to section 3.4.6, p. 89.)

If we can do this, then we know that we can only make finitely many passes through the loop, so the program will halt. Condition (2) is of course the descending-sequence version of well-foundedness.

**EXERCISE 47.** *Go back and look at exercise 9 again. This time do the following:*

1. *Show that the colour of the ball that remains is determined by  $b$  and  $w$  alone and hence the algorithm determines a function of  $b$  and  $w$ .*
2. *\* How can you be sure that the algorithm always terminates whatever you pluck out of the bag at each stage? hint: think about the lexicographic order of  $\mathbb{N}^2$ .*

As we saw in section 3.2.3, we can think of binary relations as digraphs, where there is a vertex for each element of the domain and an edge from  $a$  to  $b$  if  $a$  is related to  $b$ . This is a very natural thing to do in the present context, since we can also think of the arrows as representing a possible step taken by the program in question. It also gives us a convenient way of thinking about composition and transitive closures.  $a$  is related to  $b$  by  $R^n$  if there is a path of length  $n$  from  $a$  to  $b$  in the digraph picture of  $R$ , and  $a$  is related to  $b$  by the transitive closure of  $R$  if there is a path from  $a$  to  $b$  at all. It also makes it very easy to see that the transitive closure of a symmetric relation is symmetric, and makes it obvious that every subset of a well-founded relation is well-founded. This makes it easy to explain why pointwise products of well-founded relations are well-founded.

### Recursion on a well-founded relation

**THEOREM 3.** *Let  $\langle X, R \rangle$  be a well-founded structure and  $g : X \times V \rightarrow V$  be an arbitrary (total) function. Then there is a unique total function  $f : X \rightarrow V$  satisfying  $(\forall x \in X)(f(x) = g(x, f\{\{y : R(y, x)\}\}))$*

Here  $V$  is the universe, so that when we say “ $g : X \times V \rightarrow V$ ” we mean only that we are not putting any constraints on what the values of  $g$  (or its second inputs) are to be.

Let us have a brief cogitate about what this says, before we start trying to prove it. It says that if  $R$  is wellfounded, then if we try to define a function  $f$  by saying “take the set of all the values of  $f$  for arguments  $R$ -related to  $x$ , and do  $g$  to that set and  $x$ ; call the result  $f(x)$ ”, then we succeed in defining  $f$  uniquely.

*Proof:* The idea is very simple. We prove by  $R$ -induction that for every  $x \in X$  there is a unique function  $f_x$  satisfying  $(\forall y)(^*R(y, x) \rightarrow f_x(y) = g(y, f_x\{\{z : R(z, y)\}\}))$ . We then argue that, if we take the union of the  $f_x$ , the result will be a function, and this function is the function we want. ■

The following commutative diagram might help.

$$\begin{array}{ccc} X \times \mathcal{P}(X) & \xrightarrow{f^\dagger} & X \times V \\ \downarrow R & & \downarrow g \\ X & \xrightarrow{f} & V \end{array}$$

$f^\dagger$  is  $\lambda a. \langle \text{fst } a, f\{\{\text{snd } a\}\} \rangle$  (“leave the first component alone and translate the second under  $f$ ”). It may be that you won’t understand until you have digested section 3.5 how  $R$  can be thought of as a map. The map  $R$  is not the map from  $X$  into  $\mathcal{P}(X)$  corresponding to  $R$  (we will see in section 3.5 how every subset of  $X \times X$  corresponds to a map  $X \rightarrow \mathcal{P}(X)$ ) but instead the map that

sends a pair  $\langle x, y \rangle$  to  $\langle x, \{z : R(z, y)\} \rangle$ . ( $V$  contains everything: not just junk but sets of junk as well, so you don't have to worry about whether values of  $g$  are sets or junk.)

The reason this crops up here is that all rectypes—since they are generated by functions—will have a sort of **engendering relation**<sup>10</sup> that is related to the functions that generate the recursive datatype rather in the way that  $<_{\mathbb{N}}$  is related to the successor function. The engendering relation is that binary relation that holds between an object  $x$  in the rectype and those objects “earlier” in the rectype out of which  $x$  was built. Thus it holds between a formula and its subformulae, between a natural number and its predecessors and so on. Put formally, the (graph of the) engendering relation is the transitive closure of the union of the (graphs of the) constructors.

The (graph of, extension of) the engendering relation is itself a rectype. For example,  $<_{\mathbb{N}}$  is the smallest set of ordered pairs containing all pairs  $\langle 0, n \rangle$  with  $n > 0$  and closed under the function that applies  $S$  to both elements of a pair (i.e.,  $\lambda p. \langle S(\text{fst } p), S(\text{snd } p) \rangle$ ).

The following triviality is important.

**THEOREM 4.** *The engendering relation of a rectype is well-founded.*

*Proof:* Let  $X$  be a subset of the rectype that has no minimal element in the sense of  $<$ , the engendering relation. We then prove by structural induction (“on  $x$ ”) that  $(\forall y)(y < x \rightarrow y \notin X)$ . ■

Theorem 4 means that we can always do well-founded induction over the engendering relation. In this simplest case,  $\mathbb{N}$ , this well-founded induction is often called *strong* induction or sometimes *course of values* induction. Quite often arguments by well-founded induction are presented in contrapositive form. We first establish that, if there is a counterexample to what we are trying to prove, then there is an earlier counterexample. So the set of counterexamples has no least element and so by well-foundedness must be empty. The standard example of this style of proof is due to Fermat, who proved that  $x^4 + y^4 = z^2$  has no nontrivial solutions in  $\mathbb{N}$ . It uses the fact that all pythagorean triples are of the form  $a^2 - b^2, 2ab, a^2 + b^2$  to show that for any solution to  $x^4 + y^4 = z^2$  there is one with smaller  $z$ . This gives us a proof by well-founded induction on  $<_{\mathbb{N}}$  that there are no solutions at all. The details are fiddly, which is why it is not an exercise. The examples which follow are more straightforward, and the example with which we start is the most natural use of this technique known to me.

define contrapositive

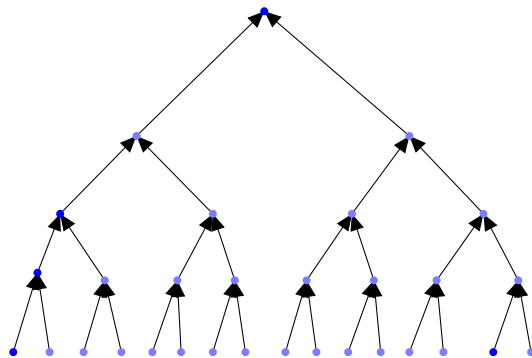
**EXERCISE 48.** *A square can be dissected into finitely many squares all of different sizes (see Gardner, [3] 1961 chapter 17). Why can a cube not be dissected into finitely many cubes all of different sizes?*

**EXERCISE 49.** *Show that the relation  $\sqsubseteq$  on  $\mathbb{N}$  defined by  $n \sqsubseteq m$  iff  $n < m \leq 100$  is well-founded.*

<sup>10</sup>This is not standard terminology.

*Prove that  $f$  and  $g$  are the same functions-in-extension.*

Let  $X$  be an arbitrary set. ( $X$  is intended to be the set of *moves*.)  $[X]^{<\omega}$  is the set of (finite) lists of members of  $X$ .  $[X]^{<\omega}$  has a natural tree structure, and indeed it is usually thought of as a tree. Let  $G$  be a subset of  $[X]^{<\omega}$  **closed under shortening** (i.e., initial segments of lists in  $G$  are also in  $G$ ). ‘ $G$ ’ naturally connotes ‘Game’.  $G$  is a subset of  $[X]^{<\omega}$  rather than the whole of it because some moves might not always be legal: P-K4 isn’t legal if there is a piece on K3! There is a map  $v$  defined on the **endpoints** of  $G$  (sequences in  $G$  with no proper end-extensions in  $G$ ) taking values in the set  $\{\mathbf{I}, \mathbf{II}\}$ .



Let  $\Pi_n$  be the proportion of these games for which player II has a winning strategy: what is the limit of  $\Pi_n$  as  $n$  gets large?



ps rearrange a bit

The connection with well-foundedness is that this condition is captured by saying that the relation “ $s \in G \wedge t \in G$  and  $s$  is an end-extension of  $t$ ” is well-founded. (If you cannot work out which way round to read this, just note: one way round it is *obviously* well-founded: what we mean is that it is well-founded the other way round too.)

Next we need the notion of **even** and **odd** positions. A sequence from  $X$  of even length is a position when it is I’s turn to move; a sequence from  $X$  of odd length is a position when it is II’s turn to move. Clearly, if  $s$  is an even position and even one of its children (positions to which I can move at his next move) is labelled ‘I’, then we can label  $s$  ‘I’ too, since I can win from there. Similarly, if  $s$  is an *odd* position and *all* its children (positions to which II can move at his next move) are labelled ‘I’, then  $s$  can be labelled ‘I’ too. This ratcheting up the upside-down tree of lists that comprise  $G$  is a recursive definition of a labelling extending  $v$  that—because of well-foundedness—is defined on the whole of  $G$ . Thus the empty sequence ends up being labelled, and the lucky owner of the label has a winning strategy.

It is very important that no assumption has been made that  $X$  is finite, nor that there is a finite bound on the length of lists in  $G$ . Notice also that these games are nothing to do with the games of chapter 6.

#### Other definitions of well-foundedness

It is clearly an immediate consequence of our definition of well-foundedness that any well-founded relation must be irreflexive. Nevertheless, one could define a relation  $R \subseteq X \times X$  to be well-founded if  $(\forall X' \subseteq X)(\exists x \in X')(\forall x' \in X')(R(x', x) \rightarrow x = x')$ . This definition of well-foundedness has a “descending chain” version too: “every  $R$ -chain is eventually constant”. This definition is more appealing to some tastes. It has the added advantage over the other definition that it distinguishes between a well-ordering of the empty set (which will be the empty relation) and a well-ordering of the singleton  $\{x\}$ , which will be the relation  $\{\langle x, x \rangle\}$ . In contrast, according to the other definition, the empty relation is not only a well-ordering of the empty set, but it is also a well-ordering of the singleton  $\{x\}$ !

It is a miniexercise to verify that each concept of well-foundedness is definable in terms of the other. The situation is rather like that with regard to strict and nonstrict partial orders.

#### Structural induction again

We know that structural induction holds for reatypes, but we could deduce it from the well-foundedness of the engendering relation if we wished. Take the example of  $\mathbb{N}$ . Suppose we know that 0 has property  $F$ , and that whenever  $n$  has property  $F$  so does  $S(n)$ . Then the set of naturals that are *not*  $F$  (if there are any) will have no least member and therefore, by well-foundedness of  $<_{\mathbb{N}}$ , will be empty.

This holds in general: we can deduce structural induction from the well-foundedness of the engendering relation. For example, if we can prove  $(\forall n)(\Phi(n))$  by a well-founded induction over  $<_{\mathbb{N}}$ , then we can prove  $(\forall n)(\forall m <_{\mathbb{N}} n)(\Phi(m))$  by structural induction.

### Other uses of well-foundedness

Intuitions of well-foundedness and failure of well-foundedness are deeply rooted in common understandings of impossibilities. For example: it is probably not unduly fanciful to claim that the song “There’s a hole in my bucket, dear Liza” captures the important triviality that a process that eventually calls itself with its original parameters will never terminate. The attraction of tricks like the ship-in-a-bottle seems to depend on the illusion that two processes, each of which (apparently) cannot run until it has successfully called the other, have nevertheless been successfully run. A similar intuition is at work in the argument sometimes used by radical feminists to argue that they can have no (nonsexist) surnames, because if they try to take their *mother’s* surname instead of their fathers, then they are merely taking their *grandfather’s* surname, and so on. Similarly one hears it argued that, since one cannot blame the person from whom one catches a cold for being the agent of infection (for if one could, they in turn would be able to pass the blame on to whoever infected them, and the process would be ill-founded<sup>11</sup>), so one cannot blame anyone at all. This argument is used by staff in STD clinics to help their patients overcome guilt feelings about their afflictions.

The reader is invited to consider and discuss the following examples from the philosophical literature.

1. “In every judgement, which we can form concerning probability, as well as concerning knowledge, we ought always to correct the first judgement, deriv’d from the nature of the object, by another judgement, deriv’d from the nature of the understanding. ’Tis certain a man of solid sense and long experience ought to have, and usually has, a greater assurance in his opinions, than one who is foolish and ignorant, and that our sentiments have different degrees of authority, even with ourselves, in proportion to the degrees of our reason and experience. In the man of the best sense and longest experience, this authority is never entire; since even such-a-one must be conscious of many errors in the past, and must still dread the like for the future. Here then arises a new species of probability to correct and regulate the first, and fix its just standard and proportion. As demonstration is subject to the control of probability, so is probability liable to a new correction by a reflex act of the mind, wherein the nature of our understanding, and our reasoning from the first probability become our subjects.

“Having thus found in every probability, beside the original uncertainty inherent in the subject, a new uncertainty deriv’d from the weakness of

---

<sup>11</sup>Unless one can blame Eve!

that faculty, which judges, and having adjusted these two together, we are oblig'd by our reason to add a new doubt deriv'd from the possibility of error in the estimation we make of the truth and fidelity of our faculties. This is a doubt, which immediately occurs to us, and of which, if we wou'd closely pursue our reason, we cannot avoid giving a decision. But this decision, though it shou'd be favourable to our preceding judgement, being founded only on probability, must weaken still further our first evidence, and must itself be weaken'd by a fourth doubt of the same kind and so *ad infinitum*; till at last there remain nothing of the original probability, however great we may suppose it to have been, and however small the diminution by every new uncertainty. No finite object can subsist under a decrease repeated *in infinitum*; and even the vastest quantity, which can enter into human imagination, must in this manner be reduc'd to nothing."

Hume (1739) Book I Part IV, Section 1, pp 5–6.

2. "Volitions we postulated to be that which makes actions voluntary, resolute [etc.]. But . . . a thinker may ratiocinate resolutely, or imagine wickedly . . . . Some mental processes then can, according to the theory, issue from volitions. So what of the volitions themselves? Are they voluntary or involuntary acts of mind? Clearly either answer leads to absurdities. If I cannot help willing to pull the trigger, it would be absurd to describe my pulling it as voluntary. But if my volition to pull the trigger is voluntary, in the sense assumed by the theory, then it must issue from a prior volition and from that another *ad infinitum*."

Ryle (1983) pp. 65–6.

**EXERCISE 51.** *Hume seems to be saying that if we multiply together infinitely many numbers all between 0 and 1 then the product must be zero, but this is incorrect. Prove Hume wrong by considering the product*

$$\prod_{1 < i < j \in \mathbb{N}} (i^2 - 1)/i^2.$$

(of  $3/4$ ,  $8/9$ ,  $15/16$  . . . ).

### 3.5 Operations on Cardinals, and Curry-Howard

There are various natural operations on cardinals, and you encountered them long ago: multiplication, addition and exponentiation. These operations on cardinals correspond to operations on sets: multiplication corresponds to cartesian product and addition to disjoint union. You know about cartesian product but perhaps not disjoint union.. Refer back to page 20. 'Disjoint union' is an important construct, and to understand it we have to recall the inclusion-exclusion principle and the idea of multisets, if only to draw contrasts. How many things in  $A \cup B$ ? Well, as we have seen,  $|A| + |B| - |A \cap B|$ , because we don't want

to count things in  $A \cap B$  twice. But what if we *do* want to count things twice? We might want a sort of union of  $A$  and  $B$  where we want to know, in this union, which elements came from  $A$  and which came from  $B$ . In this setting, if something appears in  $A \cap B$  we want it to appear *twice* in the new union. This new kind of union is called the **disjoint union** of  $A$  and  $B$  and is written  $A \sqcup B$  (sometimes also ' $A + B$ ' using overloading of '+' because  $|A \sqcup B| = |A| + |B|$ ). You can think of  $A \sqcup B$  as "Take everything in  $A$ , put a pink dot of paint on it, and take everything in  $B$  and put a blue dot of paint on it; the set of all painted things is the disjoint union  $A \sqcup B$ ."

Notice that this set isn't the same as the multiset that is the union of  $A$  and  $B$ , because in the multiset union you can't tell which of  $A$  and  $B$  was the original home of any element of the new union multiset. You have two copies of things that were in  $A \cap B$  but you can't tell them apart and you don't know which came from  $A$  and which from  $B$ . For example the union of the two multisets  $\{2, 2, 3\}$  (the factors of 12) and  $\{3, 5, 5\}$  (the factors of 75) is of course  $\{2, 2, 3, 3, 5, 5\}$ . But this is the same as the union of the two multisets  $\{2, 2, 5\}$  and  $\{3, 3, 5\}$ : you can't tell which 3 came from the 12 and which came from the 75. This is because there is no way of distinguishing the two 3s in the factorisation of 9000.<sup>12</sup>

### 3.5.1 Natural bijections and Elementary Cardinal Arithmetic

Might need to rearrange this section. Fit in somewhere Ben Millwood's observation about using a generalisation of  $\langle x, y \rangle \mapsto \langle y, x \rangle$  on a three-dimensional structure to justify associativity.

#### Commutativity of Cardinal Multiplication

Some things are important and hard, and some things are important and easy. One important and easy observation is the fact that  $A \times B$  is the same size as  $B \times A$ . You may be saying to yourself that it's obvious, because if  $|A| = n$  and  $|B| = m$  then  $|A \times B| = n \cdot m$ , but that's not the real reason. The real reason is that there is a bijection between  $A \times B$  and  $B \times A$ , and—if you think about it—it's pretty obvious what that bijection is. (When you are trying to prove that two sets are the same size, the strategy of computing their sizes and finding them to be the same is usually the wrong way round. The right thing to do is to find a bijection between them. After all, that's what it is for two things to have the same cardinality.)

A brief reality check before we go any further.

**EXERCISE 52.** Write out a formal declaration of the obvious bijection between  $A \times B$  and  $B \times A$ , using  $\lambda$  notation and **fst** and **snd**.

<sup>12</sup>Are you worried that if something is in both  $A$  and  $B$  you will have given it a pink dot and a blue dot? You needn't, because anything that belongs to both  $A$  and  $B$  can be in two places at once, and there are lots of copies of it. Remember the discussion in section 2.4.1.

The interesting thing about this bijection is that we don't need to know anything about  $A$  or  $B$  to specify it. This means that it's not merely a bijection, it's what we call a **natural** bijection.

(What would a bijection be that wasn't natural? Well, there are bijections between the two sets  $\{a, b, c\}$  and  $\{1, 2, 3\}$  (Miniexercise: how many??) One particularly obvious one is the bijection  $a \mapsto 1, b \mapsto 2, c \mapsto 3$ . This is not "natural", because in order to specify it we need access to specific information about those two sets, in particular that the first set comes equipped with an alphabetical order and that members of the second are numbers and are ordered by magnitude.)

Does your fault-tolerant pattern-matching make you think the tautology  $A \wedge B \longleftrightarrow B \wedge A$  at this point ...? If it does, then for once it is not leading you astray, though it may be a little while before the connection becomes clear.

The point that I want to hang on this natural bijection is the point that the commutativity of cardinal multiplication (which is something you learned at Primary School) relies on this natural bijection.

### Associativity of Cardinal Multiplication

Another fact you know about cardinal multiplication is that it is associative:  $(\forall n, m, k)(n \cdot (m \cdot k) = (n \cdot m) \cdot k)$ . (It's also true for multiplication of other kinds of cardinals too, but those other multiplications mean something different). This fact too, relies on the existence of a natural bijection, this time on one between  $A \times (B \times C)$  and  $(A \times B) \times C$ .

**EXERCISE 53.** Write down a Lambda term (or, if you prefer, an ML program) for this bijection.

It's a bit fiddly to write down, but you should be able to explain what it does.

Again, if you free associate from this to the fact that  $A \wedge (B \wedge C)$  is logically equivalent to  $(A \wedge B) \wedge C$  you will still be on the straight and narrow.

### Associativity and Commutativity of Addition

Clearly  $A \sqcup B$  is the same size as  $B \sqcup A$  (The lambda term says: "Swap pink and blue spots"). And  $A \sqcup (B \sqcup C)$  is the same size as  $(A \sqcup B) \sqcup C$ .

Similarly we can explain how addition distributes over multiplication.

### Distributivity

There is a distributivity law for addition and multiplication of natural numbers, which you know:

$$(\forall abc)(a(b + c) = ab + ac) \quad (3.1)$$

This assertion boils down to the fact that there is a bijection between  $A \times (B \sqcup C)$  and  $(A \times B) \sqcup (A \times C)$ . There is a lambda term and again it's a bit fiddly to give it but if you remember your pink dots and blue dots you should be able to describe its action in words.

This corresponds—as you are probably by now willing to predict—to the propositional tautology:

**EXERCISE 54.** *Well, which propositional tautology does equation 3.5.1 correspond to?*

material needed here

### Exponentiation and Currying

The time has now come to consider not only multiplication and addition, but also exponentiation. Recall that  $A \rightarrow B$  is the set of all functions from  $A$  to  $B$ . Recall also that there are  $|B|^{|A|}$  functions from  $A$  to  $B$ . (Do you remember why?)<sup>13</sup>

You will remember some equations connecting exponentiation and multiplication. We are now going to check to see if they correspond to natural bijections. A good place to start is with

$$a^0 = 1 \tag{3.2}$$

0 is the cardinality of the empty set, so what equation 3.2 is trying to tell us is that there is precisely one function from a set  $A$  to the empty set. *And* that is true whatever  $A$  is! What is this function?

That was a bit of a cheat, you may feel. (You shouldn't feel cheated if you took to heart my strictures about null objects in section 2.2). But this second one isn't. No doubt you remember:

$$(a^b)^c = a^{b \cdot c} \tag{3.3}$$

This means we should be looking for a bijection between  $(B \times C) \rightarrow A$  and  $C \rightarrow (B \rightarrow A)$ .

If this is your first encounter with this bijection you might find it hard to describe, so I'll give you a lambda term, or rather two.

- If  $f : B \times C \rightarrow A$  then  $\lambda c. \lambda b. f(\langle b, c \rangle)$  is a map from  $C$  to  $B \rightarrow A$  and so is a member of  $C \rightarrow (B \rightarrow A)$ . So  $\lambda f. \lambda c. \lambda b. f(\langle b, c \rangle)$  is a member of  $((B \times C) \rightarrow A) \rightarrow (C \rightarrow (B \rightarrow A))$ . (Remember that most people will write this last term as  $\lambda fcb. f(\langle b, c \rangle)$ ).
- If  $g : C \rightarrow (B \rightarrow A)$  then  $\lambda p. g(\text{snd}(p))(\text{fst}(p))$  is a map from  $C \times B$  to  $A$  and so is in  $(B \times C) \rightarrow A$ . So  $\lambda g. \lambda p. (g(\text{snd}(p))(\text{fst}(p)))$  is in  $(C \rightarrow (B \rightarrow A)) \rightarrow ((B \times C) \rightarrow A)$ .

<sup>13</sup>Well, for each thing in  $A$  we have a choice of  $|B|$  things to send it to, as we can send it to anything in  $B$ . These choices are independent—and we multiply independent choices (as we reminded ourselves in exercise 16 part 2)—so the answer is  $|B|^{|A|}$ .

The second one is a bit hard to read. The lambda term  $\lambda p.(g(\mathbf{snd}(p)))(\mathbf{fst}(p))$  indicates the function that, when you give it a pair  $p$  from  $B \times C$ , cracks it open to get the two components  $\mathbf{snd}(p)$  and  $\mathbf{fst}(p)$ , then applies  $g$  to  $\mathbf{snd}(p)$  to obtain a function from  $B$  to  $A$ , to which it then feeds  $\mathbf{fst}(p)$ . Some people put subscripts on the variables in contexts like this so you can tell where the arguments are coming from. So they would write

$$\lambda p_{B \times A}.(g(\mathbf{snd}(p)))(\mathbf{fst}(p))$$

for this, and

$$\lambda f_{(C \times B) \rightarrow A}.\lambda c_C.\lambda b_B.f(\langle b, c \rangle)$$

for the lambda term of the previous item.

If you find that a bit of a mouthful, try this special case. We can think of a binary relation  $R \subseteq X \times Y$  as a matrix—as we saw earlier (section 3.2.3). This makes it quite easy to see such a binary relation as a function defined on members of  $X$ . Simply send each  $x \in X$  to the set of things in  $Y$  to which it is related by  $R$ . (as it were, the set of places in its row where you find a 1 rather than a 0). A miniexercise:

**EXERCISE 55.** *Write down a lambda term for this function. (This is actually the same representation as the way the queue for the airplane loo is represented in section 3.2.6). You may wish to use the double apostrophe notation here ...*

exhumed material here

### Curry-Howard

It's not only natural bijections that concern us in the long term, but natural maps that aren't necessarily bijections. For example, there is a natural map from  $A$  to  $B \rightarrow A$ , namely  $\lambda a_A.\lambda b_B.a$ . After what you have been reading you will no doubt free-associate from this to the fact that  $A \rightarrow (B \rightarrow A)$  is a truth-table tautology. So you can see that the connection that we have been looking at above—between tautologies and the existence of lambda terms—doesn't require the lambda terms in question to denote bijections.

This connection has subtleties that we cannot go into here. If you are intrigued by this, you might try to following exercise:

**EXERCISE 56.** *Find a lambda term for a function from  $A \rightarrow (B \rightarrow C)$  to  $(A \rightarrow B) \rightarrow (A \rightarrow C)$ .*

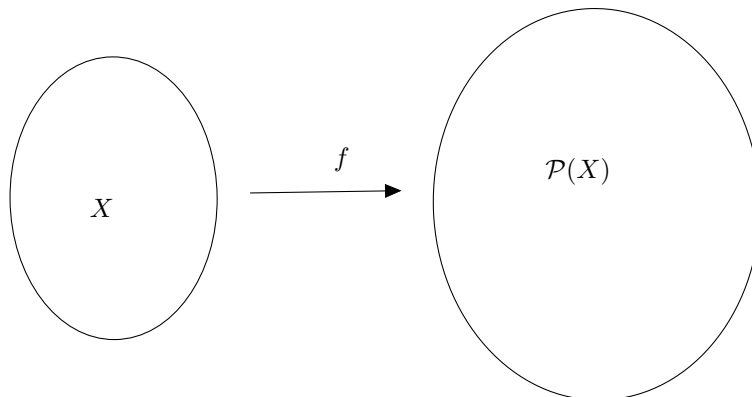
(Yes,  $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$  is a truth-table tautology!).

This dual use of ' $\rightarrow$ ' is no mere coincidence: it is a divine ambiguity, known as the *Curry-Howard correspondence*, on which a wealth of ink has been spilt. You will learn more about it when you study foundations of functional programming. Try, for example, [7] but not just yet!

**EXERCISE 57.** *You know that  $|A \rightarrow B|$  is  $|B|^{|A|}$ . How many partial functions are there from  $A$  to  $B$ ? (If you find you are heading towards a complicated answer, you are wrong: the answer is very simple, but most people find it hard to find)*

### 3.5.2 Cantor's Theorem

We've proved lots of equations, and they are all easy. There is one major theorem in the form of an *inequation*, and it is easy too. It is **Cantor's Theorem**.



Before we get stuck into the proof I want to identify a wee, wee assumption that we have to make. It is this: if there is a surjection from  $A$  onto  $B$  then there is an injection from  $B$  into  $A$ . This is another of those things (like the Cantor-Bernstein theorem) that is obvious when  $A$  and  $B$  are finite, but not obvious otherwise. (It's the axiom of choice again!)

Cantor's theorem says that that  $n < 2^n$ . Now if  $n = |X|$  then  $2^n = |\mathcal{P}(X)|$ . Clearly there is an injection  $X \rightarrow \mathcal{P}(X)$ : the singleton map  $\lambda x \in X. \{x\}$  is one. So to prove the inequality all we have to prove that there is no injection  $\mathcal{P}(X) \rightarrow X$ . In fact it's slightly easier to prove that there is no surjection  $X \twoheadrightarrow \mathcal{P}(X)$  (which by assumption is the same thing) and that is what we will do. (I could have left out the bit about injections from  $A$  to  $B$  and surjections from  $B$  to  $A$ , and given instead a slightly more complicated proof that there is no injection from  $\mathcal{P}(X)$  to  $X$ , but that proof is displeasingly messy. If you like, you can check and see how to do it for yourself. Determining which is easier is a delicate calculation)

The proof is now a doddle. Suppose  $f$  were a surjection from  $X$  onto  $\mathcal{P}(X)$ . Think about

$$\{x \in X : x \notin f(x)\}. \quad (3.1)$$

This is the set of those things in  $X$  that are not members of what  $f$  sends them to. Since  $f$  sends members of  $X$  to subsets of  $X$ , asking of a member  $x$  of  $X$  whether or not it is a member of what  $f$  sends it to is a perfectly sensible question, since  $x$  is a member of  $X$  and  $f(x)$  is a subset of  $X$ .

If  $f$  is a surjection, this subset—3.1—of  $X$  must be  $f$  of something,  $x_0$  say. Now (and I want you to work this out for yourselves) ask whether or not  $x_0$  is



a member of  $\{x \in X : x \notin f(x)\}$ . Think about this a bit before proceeding to the next paragraph.

If it is, it isn't, and if it isn't, it is. Clearly this is an impossible situation. How did we get into it? By assuming that  $f$  was a surjection. Evidently it wasn't! ■

Time invested in understanding this proof is time well spent. The same argument is used to great effect in complexity theory, and in (for example) the proof of the unsolvability of the Halting problem, which you will see in 1B. **You Absolutely Must understand This Proof.**

### 3.5.3 Inclusion-Exclusion

If  $A$  and  $B$  are multisets then the number of things in  $A \cup B$  is the number of things in  $A$  plus the number of things in  $B$ . Things are a bit more complicated with sets, since we don't want to count twice those things that appear in both  $A$  and  $B$ : we want to count everything only *once* even if it appears *twice*: once in  $A$  and once in  $B$ . We have the following equation:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Obvious, isn't it? To get the number of things in  $A \cup B$  you have to subtract from  $|A| + |B|$  the number of things in  $A \cap B$  co's the members of  $A \cap B$  are the things that get counted twice. In some sense equally obvious (but ever so slightly harder to compute) is:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

(We subtract the number of things in  $A \cap B$  because they get counted twice, and similarly  $A \cap C$  and  $B \cap C$ . But then anything in  $A \cap B \cap C$  has been counted three times and taken away three times, so it has to be put back!)

Think a bit about you might generalise this to the case where you are taking the union of several sets.

Here is a bald statement of the general principle that I found in the notes of one of my colleagues:

$$\left| \bigcup_{s \in S} A_s \right| = - \sum_{\emptyset \neq T \subseteq S} (-1)^{|T|} \cdot \left| \bigcap_{t \in T} A_t \right|. \quad (\text{inclusion-exclusion})$$

This looks **extremely** scary, but it's actually nothing more than the obvious generalisation of the equations we have just seen. Let's decode this assertion carefully and without panicking.

The thing on the left hand side of inclusion-exclusion is the number of things that belong to the union of the  $A_s$ . The family of  $A_s$  is **indexed**: each  $A$  has a pointer pointing at it from an **index set**—which in this case is called ' $S$ '. See page 45.

So in English inclusion-exclusion reads something like

“The number of things in the union of the  $A_s$  is minus the sum—over nonempty subsets  $T$  of  $S$ —of minus-one-to-the-power-of-the-number-of-things-in- $T$  times the number of things in the intersection of all those  $A_s$  whose subscripts are in  $T$ .”

Or—plainer still—

”For each nonempty  $T \subseteq S$ , take the intersection of all the  $A_s$  whose subscripts are in  $T$  (those  $A_s$  pointed to by elements of  $T$ ) take its cardinality and take it negative or positive depending on whether  $T$  has an odd or even number of elements. Add them all together, for all such  $T$ , and make the answer positive.”

The first thing to take note of is a bit of **overloading**. Primarily we write ‘ $A_s$ ’ to denote one of the  $A_s$ , and the subscript is a member of the index set  $S$ . However we are now going to write ‘ $A_T$ ’, where  $T$  is a *subset* of  $S$  not a member, and this expression will denote the intersection  $\bigcap_{t \in T} A_t$  of all the  $A_s$  whose subscripts are in  $T$ . It’s easy to detect which of these two usages are in play at any one time, because the indices themselves are *lower-case* Roman letters and the *sets* of indices are *upper-case* Roman letters. This is a common use of the difference between upper and lower case Roman letters. Notice that  $A_\emptyset$  is the whole universe of discourse— $V$ .

Now recall indicator functions from section 3.2.8. Let  $I_B$  be the indicator function for  $B$ . Normally  $I_B$  is the function which (on being given  $x \in V$ ) returns **true** or **false** depending on whether or not  $x \in B$ . However in this case we want to modify the indicator functions so that they return 0 and 1 instead of **false** and **true**. This piece of **casting** is in order that we can use *arithmetic* operations on the values of the indicator functions instead of *boolean* operations. It’s universal practice in machine code. Hacky but clever. This ensures that

- $I_{\overline{B}}(x) = 1 - I_B(x)$ ; and
- $I_{B \cap C}(x) = I_A(x) \cdot I_B(x)$ .

This second assertion generalises to

$$I_{A_1 \cap A_2 \dots \cap A_n}(x) = I_{A_1}(x) \cdot I_{A_2}(x) \cdots I_{A_n}(x)$$

so, in particular (remember that  $\overline{A_s}$  is the complement of  $A_s$ ):

$$I_{\overline{A_1 \cap A_2 \dots \cap A_n}}(x) = I_{\overline{A_1}}(x) \cdot I_{\overline{A_2}}(x) \cdots I_{\overline{A_n}}(x) \quad (\text{findalabel})$$

Now  $I_{\overline{A_1}}(x) = 1 - I_{A_1}(x)$  so findalabel becomes

$$I_{\overline{A_1 \cap A_2 \dots \cap A_n}}(x) = (1 - I_{A_1}(x)) \cdot (1 - I_{A_2}(x)) \cdots (1 - I_{A_n}(x)) \quad (3.1)$$

For the next line consider what happens when you multiply out things like  $(1 - a)(1 - b)(1 - c)(1 - d)$ : you get 1— lots of things like  $-abc$  and  $+bd$  which

are positive if the number of factors is odd and negative if the number of factors is even. “But shouldn’t it start with a ‘1–’ before the big  $\Sigma$ ?” I hear you cry. It should indeed, but that 1– is in fact included because one of the  $T$ s you sum over is the empty set! Very cunning.

$$I_{\overline{A_1 \cap A_2 \dots A_n}}(x) = \sum_{T \subseteq S} ((-1)^{|T|} \cdot (\prod_{t \in T} I_{A_t}(x))) \quad (3.2)$$

Notice now that  $I_s(x) \cdot I_t(x) = I_{\{s,t\}}(x)$ , and in general  $\prod_{t \in T} I_t(x) = I_T(x)$  giving

$$I_{\overline{A_1 \cap A_2 \dots A_n}}(x) = \sum_{T \subseteq S} ((-1)^{|T|} \cdot (I_{A_T}(x))) \quad (3.3)$$

Now  $\overline{A_1 \cap A_2 \dots A_n}$  is  $\bigcap_{s \in S} \overline{A_s}$

$$I_{\bigcap_{s \in S} \overline{A_s}}(x) = \sum_{T \subseteq S} ((-1)^{|T|} \cdot (I_{A_T}(x))) \quad (3.4)$$

Now, for any set  $X$  whatever, the number of things in  $X$  is simply the number of things  $x$  in  $V$  such that  $I_X(x) = 1$ ; this number is just the sum of all  $I_X(x)$ , so the number of things in  $\bigcap_{s \in S} \overline{A_s}$  is simply the number of  $x \in V$  such that  $I_{\bigcap_{s \in S} \overline{A_s}}(x) = 1$ . This gives us

$$|\bigcap_{s \in S} \overline{A_s}| = \sum_{T \subseteq S} ((-1)^{|T|} \cdot |A_T|) \quad (3.5)$$

Applying a minus sign to both sides gets us back to equation inclusion-exclusion.

Finish this off



## Chapter 4

# Some Elementary Number Theory

Number Theory is a relatively recent development in Discrete Mathematics courses. It became important because it's the mathematics that underlies cryptography, and cryptography became a Hot Topic for Computer Science really only with the advent of the internet and the consequent urgent need for secure secret communication between computers.

The usual ambition for a number theory slot in a level one Discrete Mathematics course is coverage of the RSA algorithm for public-key cryptography. That is what we shall aim for here!

But we'll start with something a bit more basic and familiar which will launch us in the right direction.

### 4.1 Different bases

Q: What goes "Pieces of nine! Pieces of nine!"?

A: A Parrot error.

Binary, octal, decimal and hexadecimal. They are all **positional** notations (polynomial notations). The only difference between them is the **base**. "Positional"? The meaning of a symbol depends very sensitively on where it appears in the formula. Does '1' mean *one* or *ten* or *one hundred*? It depends where it is. We take the positional nature of our decimal system for granted but we shouldn't. Roman numerals are not positional, or at least not in the same way (the 'I' in 'IX' doesn't mean the same as the 'I' in 'XI').

Familiarity with bases other than decimal and binary is not as important as it used to be, because familiarity with octal and hexadecimal is useful primarily to assembly language programmers, and the proportion of computer users who need skill in writing assembly languages is shrinking all the time. (One of my

students said to me “Assembly language programmers are the proletariat of the information age”.)

**EXERCISE 58.** *There are tests for divisibility by 3, by 9, and by 11 in base 10; tests for divisibility by 7 and by 9 in base 8, and tests for divisibility by 15 and by 17 in hexadecimal. Do you know these tests? If you do know them, can you explain why they work?*

### Euclid’s Proof that there are Infinitely many Primes

We start with an old chestnut. A prime number is a natural number with no factors other than itself and 1. Euclid proved that there are infinitely many primes. His proof is simplicity itself.

Suppose there are only finitely many primes, so that  $P$ , the set of all primes, is a finite set. Then we can multiply them all together to get  $\Pi P$ , which will be a natural number. Add 1 to obtain  $(\Pi P) + 1$ . This is a natural number too. Is it prime? It might be, but even if it isn’t we know that none of its prime factors can belong to  $P$ . (After all, no number can divide into both  $n$  and  $n + 1$ , can it!). Either way we know we have a prime that is not in  $P$ . This contradiction proves that  $P$  wasn’t finite. ■

## 4.2 Euclid’s Algorithm

The idea is to find the highest common factor of two natural numbers  $x$  and  $y$ . The key fact is that anything that divides  $x$  and  $y$  divides  $x - y$ . This tells us that the HCF of  $x$  and  $y$  is the same as the HCF of  $x$  and  $x - y$  (assuming  $x > y$ —otherwise it’s  $y$  and  $y - x$ .) So, if I want to find  $\text{HCF}(x, y)$ , I should start with two natural numbers  $x$  and  $y$  and then, at each stage, subtract the smaller of the two numbers that I have from the larger and replace the larger number with the result of that subtraction. For example, the HCF of 39 and 231 is the same as the HCF of 39 and  $231 - 39 = 192$ . So if I start with 39 and 231, at the next stage I have 39 and 192. The HCF of 39 and 192 is the same as the HCF of 39 and  $192 - 39 = 153$ . And so on.

**The HCF of the pair-of-numbers-in-hand is a loop invariant, and when the process stops with the two elements of the pair equal then we have found the HCF.**

For example if we start with the pair (12, 18) we obtain (12, 6) and then (6, 6). If we start with the pair (7, 25) we obtain (7, 18), then (7, 11), then (7, 4), (3, 4) (1, 3) and finally (1, 1).

If the bigger number is *much* bigger than the smaller one then we could end up subtracting the smaller one many times, and we would be able to save ourselves time by conflating lots of these subtractions together by dividing the bigger number by the smaller and keeping only the remainder. For example, that way—to take our (7, 25) example, we would have missed out (7, 18) and (7, 11), and gone straight to (7, 4).

If we keep track of what we are doing when we run Euclid's algorithm on two natural numbers  $a$  and  $b$  (by keeping an eye on the remainders at each division, among other things) we can not only find  $\text{HCF}(a, b)$  (hereafter  $(a, b)$  as promised on page 49) but we can even find two integers  $x$  and  $y$  such that

$$ax - by = (a, b) \quad (4.1)$$

I shall not explain how this can be done (since we don't need it for our narrow task of climbing Mount RSA) but I can give you material on this if you wish.

### 4.3 Modular Arithmetic

I mentioned earlier that there is another kind of number: integers mod  $p$ . It's easy to check that, for any natural number  $n$ , the equivalence relation " $x$  and  $y$  have the same remainder on division by  $n$ " is a congruence relation for  $+$  and  $\times$ .

That is to say since (if we care only about the remainder mod  $n$  of the answer) the  $+$  and  $\times$  operation don't notice if we replace an argument by something with the same remainder mod  $n$ , we can think of  $+$  and  $\times$  as taking for their arguments the equivalence classes under this relation, rather than the numbers themselves.

This gives us the integers mod  $n$ . How is it best to think of these numbers? Let's illustrate with integers mod 5. The equivalence classes are  $\{0, 5, 10, \dots\}$ ,  $\{1, 6, 11, \dots\}$ ,  $\{2, 7, 12, \dots\}$ ,  $\{3, 8, 13, \dots\}$  and  $\{4, 9, 14, \dots\}$ . Usually it's easier to identify these equivalence classes with their smallest members, so that—for example—the integers mod 5 is the set  $\{0, 1, 2, 3, 4\}$ , equipped with the multiplication and addition tables

$\times$	0	1	2	3	4	$+$	0	1	2	3	4
0	0	0	0	0	0	0	0	1	2	3	4
1	0	1	2	3	4	1	1	2	3	4	0
2	0	2	4	1	3	2	2	3	4	0	1
3	0	3	1	4	2	3	3	4	0	1	2
4	0	4	3	2	1	4	4	0	1	2	3

What sort of arithmetic do these numbers obey? It's easy to check that addition and multiplication are commutative as before, and that addition distributes over multiplication as usual. There is an additive unit, which is of course (the equivalence class of) 0. Of course (the equivalence class of) 1 is a multiplicative unit. What equation 4.2 tells us now is that if  $n$  is a prime, then the integers mod  $n$  have multiplicative inverses. Consider equation 4.2 again, this time where  $a$  is a prime  $p$

$$bx - py = 1 \quad (4.1)$$

(The RHS is 1, because—since  $p$  is a prime— $(p, b) = 1$ .)

But then we have

$$bx = py + 1 \quad (4.2)$$

This says that  $bx$  is one more than a multiple of  $p$ . But this says precisely that (the equivalence class of)  $x$  is a multiplicative inverse of (the equivalence class of)  $b \bmod p$ .

Actually we didn't need  $p$  to be prime: all we really needed was that the right-hand side of equation 4.3, the HCF, should be 1. So we can say:

Euclid's algorithm tells us that  $a$  has a multiplicative inverse mod  $n$  as long as  $n$  and  $a$  are coprime.

“these”...?

These are called **integers mod  $n$** . One disconcerting difference between them and all the other kinds of number you know is that they have no natural order to them: no sense of magnitude. No “greater than”. However they do have a *circular order*, like the numbers of a clock face: 1 comes after 12. (recall exercise 26)

### 4.3.1 Euler's theorem

Euler's totient function:  $\phi(n)$  is the size of the set

$$\{m < n : m \text{ and } n \text{ have no factors in common}\}.$$

Slightly more formally (remembering that we were warned on page 49 that  $(x, y)$  would sometimes mean “the highest common factor of  $m$  and  $n$ ”):

$$\phi(n) = |\{m < n : (m, n) = 1\}| \quad (4.1)$$

This set is sometimes called  $U_n$ , and its members are sometimes called *units*. The important point for us at the moment is that members of  $U_n$  have multiplicative inverses mod  $n$ .

Euler's theorem says that if  $(a, n) = 1$  (which is to say that  $a$  and  $n$  are co-prime) then  $a^{\phi(n)} = a \pmod{n}$

So what happens if I multiply  $a$  by a member  $u$  of  $U_n$ ?  $u$  and  $a$  are both prime to  $n$  so their product  $a \cdot u$  is also prime to  $n$  and will be in  $U_n$  (or at least its remainder mod  $n$  will be). So multiplying members of  $U_n$  by  $a$  simply moves them around. Indeed we can say more than that. If  $u$  and  $v$  are two distinct members of  $U_n$  then  $au$  and  $av$  are also members of  $U_n$  (we've seen this already) and are distinct. Let's prove this.

Suppose

$$au = av \quad (4.2)$$



$a$  and  $n$  are coprime so  $a$  has a multiplicative inverse mod  $n$ , which we will write  $a^{-1}$ . Multiply both sides of equation 4.3.1 by  $a^{-1}$  to obtain

Suppose

$$a^{-1}au = a^{-1}av \quad (4.3)$$

which gives  $u = v$ .

So multiplication-by- $a$  is just a permutation of  $U_n$ . So

$$\prod U_n = \prod_{i \in U_n} a \cdot i \quad (4.4)$$

because the two sets over which we are taking the products are one and the same set!

Now

$$\prod_{i \in U_n} a \cdot i = (\prod U_n) \cdot a^{\phi(n)} \quad (4.5)$$

We get this by collecting all the  $a$ 's together, and noting that there are  $\phi(n)$  of them.

But what do we get if we multiply together all the units in  $U_n$ ? They all have multiplicative inverses, and the multiplicative inverses are also in  $U_n$ , so they all cancel, giving 1.

More detail needed here?

### Modular exponentiation is easy

There is one consequence of this that we may as well mention now. Euler's theorem means that modular exponentiation is easy to calculate. What is  $3^{1,000,000,000} \bmod 257$ ? Well,  $\phi(257) = 256$  so Euler's theorem tells us that  $3^{256} = 1 \bmod 257$ . So any power of  $3^{256}$  is likewise equivalent to 1 mod 257. But 1,000,000,000 is a multiple of 256 so  $3^{1,000,000,000}$  is a power of  $3^{256}$  and therefore  $3^{1,000,000,000} \bmod 257$  must be 1!

That looks like a special case, because 256 divides into 1,000,000,000.

But, had we wanted  $3^{1,000,000,007} \bmod 257$  instead, we would only have had to calculate  $3^7 \bmod 257$ .

So, in general, how do we compute  $a^b \bmod n$  when  $(a, n) = 1$ ? Well, as the above illustration shows, all we need to worry about is the remainder of  $b$  on division by  $\phi(n)$ . So, no matter how huge  $b$  is, we never have to calculate  $a$  to the power of anything bigger than  $\phi(n)$ .

This tells us that modular exponentiation is no more difficult than division. Use inclusion-exclusion to show  $\phi$  is multiplicative.

**EXERCISE 59.** *The game of Sylver Coinage was invented by Conway, Berlekamp and Guy (1982). See [5]. It is played by two players, I and II, who move alternately, with I starting. They choose natural numbers greater than 1 and at each stage the player whose turn it is to play must play a number that is not a sum of multiples of any of the numbers chosen so far. The last player loses.*

*Notice that by 'sum of multiples' we mean 'sum of positive multiples'. The give-away is in the name: 'Sylver Coinage'. What the players are doing is trying*

at each stage to invent a new denomination of coin, one that is of a value that cannot be represented by assembling coins of the denominations invented so far. (There is a significance to the spelling of ‘silver’, but I do not think we need to concern ourselves with that.)

Prove that no play of this game can go on forever.

The way to do this is to identify a parameter which is altered somehow by each move. The set of values that this parameter can take is to have a well-founded relation defined on it, and each move changes the value of the parameter to a new value related to the old by the well-founded relation. The question for you is, what is this parameter? and what is the well-founded relation?

(You should give a much more rigorous proof of this than of your answer to exercise 48 below: it is quite easy to persuade oneself that all plays are indeed finite as claimed, but rather harder to present this intuition as reasoning about a well-founded relation.)

## 4.4 The RSA algorithm

Let  $p$  and  $q$  be two primes. Let  $m$  be  $p \cdot q$ .  $\phi(m)$  will be  $(p-1)(q-1)$ .

Alice (for some reason she is always called ‘Alice’) wishes to arrange matters so that people can send her messages that only she and the other party can read. She arms herself with  $p$ ,  $q$  and  $m$  as above, and calculates  $\phi(m)$ . Now comes the clever bit. Alice chooses a number  $e$  (the ‘e’ is intended to suggest **encryption exponent**). This encryption exponent must be prime to  $\phi(m)$ ; this is to ensure that it has a multiplicative inverse mod  $\phi(m)$ . This multiplicative inverse mod  $\phi(m)$  is the **decryption exponent** and is written ‘ $d$ ’.

Alice announces  $m$  and  $e$  to the world. (She does *not* divulge  $p$  or  $q$  or  $\phi(m)$ !). Anyone who tries to calculate  $p$  or  $q$  or  $\phi(m)$  apparently has only one way in: to factorise  $m$ . This seems to be very hard.

Now, if you wish to send Alice a message, you do the following

1. You code up your message as a natural number somehow, using ASCII perhaps. Let  $a$  be this number. You want  $a$  to be less than  $m$ , so you might have to chop up your message into blocks.
2. You then calculate  $a^e \pmod{m}$ , (this is why you want  $a < m$ !) and you send it to Alice *in clear* as the spies say: in an open way that everyone can see.

(It’s worth remembering that (2) can be done quite easily: we established in section 4.3.1 that modular exponentiation can be done quickly.)

Alice receives the message. She decrypts it as follows. Let  $t$  (for Thomas) be the number she receives. She can calculate  $t^d \pmod{m}$ , since modular exponentiation is easy.

What is  $t^d \pmod{m}$ ? Well,  $t$  is  $a^e \pmod{m}$  so

$$t^d \pmod{m} \tag{4.1}$$

is

$$(a^e)^d \pmod{m} \quad (4.2)$$

which is

$$a^{ed} \pmod{m}. \quad (4.3)$$

Now  $a^{\phi(m)}$  is  $1 \pmod{m}$ , by Euler's theorem. We know that  $d$  and  $e$  are multiplicative inverses mod  $\phi(m)$  so we can think of  $de \pmod{\phi(m)}$  as  $c \cdot \phi(m) + 1$  for some number  $c$ . This makes  $a^{ed} \pmod{m}$  the same as

$$a^{c \cdot \phi(m) + 1} \pmod{m} \quad (4.4)$$

which is

$$a^{c \cdot \phi(m)} \cdot a \pmod{m} \quad (4.5)$$

$$(a^{\phi(m)})^c \cdot a \pmod{m} \quad (4.6)$$

which simplifies, since  $a^{\phi(m)}$  is  $1 \pmod{m}$ , to

$$1^c \cdot a \pmod{m} \quad (4.7)$$

which is of course

$$a \pmod{m} \quad (4.8)$$

which is the ASCII code for my message

Do we want to use Inclusion-exclusion to show that Euler's totient function is multiplicative...?



## Chapter 5

# Graph theory

The word ‘graph’ has many uses: there is the graph of a relation or function (a relation-in-extension or function-in-extension) which is a set. There is also the graph of a function, which is a picture (the graph of  $\lambda x.x^2$  is a parabola drawn in the plane). If you stop and think about this, you will see that these are really the same thing: the second is merely a depiction of the first. However, here we are going to use the word in a different way.

A graph is a set of points (known as “vertices”) with lines joining them. Each pair of vertices in the graph either has a line joining its two members together or it doesn’t. The line between  $a$  and  $b$  (that might or might not be there) is called an *edge*. Normally we don’t think of there being an edge joining a vertex to itself. So a graph is a set of vertices with a set of edges, each edge joining *distinct* vertices. Or it can be thought of as a set of vertices with a symmetrical irreflexive relation. People in graph theory usually think of a graph as a pair  $\langle V, E \rangle$  of a set  $V$  of vertices and a set  $E$  of edges.

Draw some pictures

A digraph (short for “directed graph”) is a set of vertices joined by lines that may have directions on them. So there might be an arrow from  $a$  to  $b$  and an arrow from  $b$  to  $a$ . Normally we do not allow there to be edges from a vertex back to itself, but in settings where we do allow such edges in digraphs, we call them “digraphs with loops”.

Need some exercises here

Graphs and digraphs are very useful data structures: lots of things can be represented using them. For example, binary relations can be represented by digraphs. (Well, digraphs with loops). **Decorated graphs** are very useful not only for displaying information but also for reasoning about it. For example we can represent a network of depôts with pipelines between them by a decorated graph. Vertices represent depôts and directed edges represent the pipelines. We can decorate the vertices with numbers indicating the amount of stuff they can store, and decorate the edges with numbers indicating the rate at which they can deliver stuff. Of course if the depôts store more than one commodity (and the pipelines correspondingly transmit more than one commodity) then the vertices and edges will be decorated by more than one number. Or we might prefer to have multisets of edges between vertices (one edge for each commodity). Graphs

with multiple edges in this manner are called **multigraphs**.

A **complete** graph on a set  $V$  of vertices is the graph containing all the possible edges. The **complement**  $\bar{G}$  of a graph  $G$  is the graph containing precisely the edges missing from  $G$ . A graph is **connected** if for any two vertices in the graph there is a path between them. If it's not connected it is **disconnected**.

**EXERCISE 60.** *Prove that a graph and its complement cannot both be disconnected.*

If you have already done some Logic and are happy with resolution you may wish to try proving this using resolution. *Hint: If  $G$  and  $\bar{G}$  are both disconnected then there are vertices  $a$  and  $b$  that are disconnected in  $G$  and vertices  $c$  and  $d$  that are disconnected in  $\bar{G}$ . Invent propositional letters  $ac$ ,  $bd$  and so on, which say that there is an edge between  $a$  and  $c$ , between  $b$  and  $d$  and so on.*

A **decoration** of a graph is a function from edges (or vertices) of the graph to things.

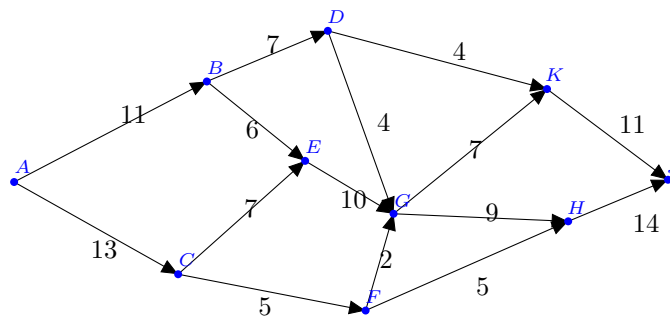
We have only one section on Graph theory, so we haven't got time or space to do anything in depth. The two results we do cover give a flavour of the kind of thing that we prove and a taste of the methods of proof.

## 5.1 Menger's theorem

We illustrate this kind of application of graph theory by exhibiting Menger's "Min cut max flow" theorem.

Menger's theorem applies to directed graphs with a **source** and a **sink**, and which have their edges decorated with whole numbers ("capacities"). These things are also called **networks**.

In the picture below  $A$  is the source and  $J$  is the sink



(Don't worry about the numbers on the edges for the moment).

A **cut** in a digraph  $G = (V, E)$  is a set of edges which disconnects the graph. (“No path from the source to the sink”) For example, the set  $\{(D, G), (F, G)\}$  containing the two edges  $F \rightarrow G$  and  $D \rightarrow G$  is a cut.

Yet ANOTHER use of round brackets! But this one isn't standard.

Alternatively a cut is a partition of the set of vertices into two pieces, one of which contains the source and the other contains the sink. These two ways of thinking about cuts are related: If  $\{A, B\}$  is a partition of the set of vertices into two pieces, then the edges of  $G$  that join things in  $A$  to things in  $B$  form a cut (in the other sense). Similarly if we have a set of edges that disconnect the graph we can define a partition of the set of vertices into two pieces. One piece contains those vertices you can reach from the source without traversing any of the edges in the cut, and the other is the set of those vertices from which you can reach the sink without traversing any of the edges in the cut.

A graph might have its edges decorated with quantities... that could in principle be anything. (That is why the datatype of graphs is so useful). The digraph above has had its edges decorated by natural numbers, and it's the kind of picture one would dream up if one were trying to represent a network of oil pipelines: each edge is a pipeline from one pumping station to the next, and the decoration of each edge (pipeline) tells you the capacity of that edge.

Now a **flow** is an allocation of numbers to edges, where the number allocated to an edge is no more than its decoration (can't pump more oil than the pipeline will carry) and the sum of the allocations to the edges going *into* a node equals the sum of the allocations to the edges *leaving* the node. (oil doesn't get lost or created at nodes). There is an obvious notion of the **value** of a flow, namely the sum of the decorations on the edges leaving the source (or, equivalently) the sum of the decorations on the edges entering the sink.

The **value** of a cut in a decorated graph is the sum of the numbers in its decorations.

Menger's “Max flow min cut” theorem says that: in any network, the largest value that a flow can have is the same as the smallest value of a cut. It's obvious that any flow must be less than the value of any cut. (Every flow must go through every cut). It's not at all obvious that the maximum flow you can propel through a network is the same as the cheapest cut.

Let's see what we can do. Suppose we are given a flow.

We are going to colour some vertices blue. (“Blue vertices are those you can increase the flow to”.) We rule that the source is blue. Thereafter if  $x$  is blue and there is an edge  $x \rightarrow y$  used to less than its capacity then  $y$  is blue. It's obvious what this condition is doing, but there is a second clause which will require a bit of thought. If  $x$  is blue and there is an edge  $y \rightarrow x$  which is used more than 0 then  $y$  is blue.

Ask: is the sink blue?

If yes, then there is a path source  $\rightarrow$  sink on which you can increase the flow. If the only way in which we made a vertex blue was by finding that it was downstream from a blue vertex along an underused edge it would be obvious that we would improve the flow: just pump more along the trail of blue vertices

joining the source to the sink. But what is the second clause doing? What is the significance of the “backward” edges?

Suppose we have—in addition to the source and the sink—two vertices  $a, b$  both blue.  $a$  is blue because there is an underused edge from the source  $\rightarrow a$ ;  $b$  is blue because there is an edge  $b \rightarrow a$  which is used (it doesn’t matter whether partially or to full capacity), and the sink is blue because there is an underused edge to it from  $b$ . How does this help? Easy! we can take some of the flow currently going from  $b$  to  $a$  and divert it so that it goes to the sink instead. That way we have increased the flow. This illustrates what we are supposed to do at each “backwards” edge. ■

If the sink is blue, we can increase the flow. So if we can’t increase the flow, the sink is not blue. Let us consider this case. Think about the two-piece partition of the set of vertices into  $\{\{v : \text{blue}(v)\}, \{v : \neg\text{blue}(v)\}\}$ . The piece containing all the blue vertices contains the source and the piece containing the non-blue vertices contains the sink, so this partition is a cut within the meaning of the act. It is now quite easy to see that the capacity of this cut is precisely the capacity of the flow we started with. Every molecule of oil starts at a blue vertex (namely, the source) and visits blue vertices until it reaches a non-blue vertex, and once having reached a non-blue vertex it never looks back: it never sees a blue vertex again. (say more about this?) So at some point it traverses an edge from a blue vertex to a non-blue vertex—which is to say, it crosses one of the edges of the cut.

## 5.2 Euler’s Theorem on graphs

An *Eulerian circuit* in a graph is a tour round the graph (a walk that takes you back to where you start) that visits every vertex (possibly several times) but traverses each edge once. This is in contrast to a *Hamiltonian circuit* which visits each vertex once. You will need to know about Hamiltonian circuits later when you do complexity theory, but we will not go into any detail about them now, as they are quite hard.

In contrast, there is a rather nice theorem about Eulerian circuits which we will prove.

We first need the concept of the *degree* of a vertex. The degree of a vertex  $v$  is the number of edges that meet at  $v$ .

**THEOREM 5.** *A (finite) graph has an Eulerian circuit if and only if every vertex has even degree.*

One direction is fairly easy. Suppose there is such a circuit. Follow it round the graph. If you are walking round the graph, and are not to get trapped at any vertex  $v$ , then there must be a way out of  $v$  as well as a way in. (So you can, unlike Omar Khayyam, always go out from a different door from that through which you came in.) Now—since you can only use each edge once—the edges at each vertex come in pairs, from the point of view of your circuit. Each time

Need some pictures



you come in on an edge, you must come out on a different edge, and this pairs up the edges that meet at  $v$ . Since you were travelling on an Eulerian circuit, you have used up all the vertices, so every vertex is of even degree.

The other direction is harder.

We are going to do a proof by wellfounded induction, and the wellfounded relation we exploit is the *subgraph* relation. We say  $G_1 \prec G_2$  if  $G_1$  is obtained from  $G_2$  by deleting edges and/or deleting disconnected vertices. We claim that  $\prec$  is wellfounded.

We will prove by induction on  $\prec$  that every graph all of whose vertices have even degree has an Eulerian circuit.

So let  $G$  be a finite graph all of whose vertices have even degree, and assume that, for all  $G' \prec G$ , if all vertices of  $G'$  have even degree, then  $G'$  has an Eulerian circuit. We will establish that  $G$  has an Eulerian circuit too.

We will try to build a circuit. Start at any vertex, and walk around it as we did in the other direction of the proof, in no particular order. (*Caminante, no hay camino. El camino se hace al andar* said Antonio Machado). The only place you can ever get stuck at is the vertex you started, and that is, indeed, where you will eventually get stuck. You might of course be lucky and have visited all the vertices, in which case we have an Eulerian circuit as desired. But suppose we don't.

You do at least have a circuit,  $C$ . It might not visit all vertices. Now we delete from  $G$  all the edges that belong to  $C$ . The graph  $G'$  that remains is a proper subgraph  $G$  all of whose vertices have even degree.  $G'$  might actually be a union of disconnected subgraphs (the **components** of  $G'$ ) rather than one single subgraph, but this doesn't make much difference. By induction hypothesis this subgraph (or these subgraphs) have Eulerian circuits.

What happens next is a bit hand-wavy, and you will have to draw some pictures. Equip  $G'$  (or each of its components) with an Eulerian circuit. Then you join up these Eulerian circuits with the circuit  $C$  that we found in the previous paragraph to obtain an Eulerian circuit for  $G$ . Hint: think about the vertices that lie both on the Eulerian circuits for  $G'$  (or its components) and on the circuit  $C$ . We start off by trying to think of  $C$  as an Eulerian circuit for  $G$ , but we find that each of these vertices is an invitation to take a *détour* round  $G$  or one of its components.



## Chapter 6

# A Bit of Game Theory

Game theory is a huge ramshackle area of mathematics. The only kind of game we are going to be concerned with here is the kind represented by a matrix. There are two players, called I (who picks rows) and II (who picks columns)—neither knowing the other’s choice at the time they make their own.

In the game corresponding to the matrix

$$\begin{array}{cc} a_{0,0} & a_{0,1} \\ a_{1,0} & a_{1,1} \end{array}$$

when I has picked the  $i$ th row and II the  $j$ th column, II must pay I the sum of  $\mathcal{L}a_{i,j}$ . ( $a_{i,j}$  is of course the entry in the  $i$ th row and the  $j$ th column).

Games represented like this are **zero-sum** games. That is to say that the sum of the payoffs to the two players is 0.

(Nonzero sum games are represented by matrices where each entry is a *pair* of numbers, being the payoffs to the two players. We will see those in section 6.1.)

We start with zero-sum games. There is a theorem due to von Neumann and Morgenstern that says that there is an optimal strategy for both players. This theorem is known as the Von Neumann and Morgenstern *minimax theorem* [ ].

What do we mean by an optimal strategy?

First let’s get the concept of dominance out of the way. (The following example is from [8])

Consider the following matrix.

$$\begin{array}{cccc} 0 & 1 & 4 & 2 \\ 2 & 0 & 1 & 4 \\ 1 & 2 & 5 & 3 \\ 4 & 1 & 3 & 2 \end{array}$$

Compare the first and third rows. Notice that whatever II does, I is always better off playing the third row than playing the first: in each column the entry in the third row is bigger than the entry in the first row. We say the third row

**dominates** the first row, so we can delete the first row, since I will never play it.

$$\begin{array}{cccc} 2 & 0 & 1 & 4 \\ 1 & 2 & 5 & 3 \\ 4 & 1 & 3 & 2 \end{array}$$

The second column—from II's point of view—dominates the fourth, so we delete the fourth, since II will never play it.

$$\begin{array}{ccc} 2 & 0 & 1 \\ 1 & 2 & 5 \\ 4 & 1 & 3 \end{array}$$

Then—from I's point of view—the third row of the result dominates the first row, so we can delete the first row, since I will never play it.

$$\begin{array}{ccc} 1 & 2 & 5 \\ 4 & 1 & 3 \end{array}$$

Finally the third column—from II's point of view—is dominated by the second, leaving us with

$$\begin{array}{cc} 1 & 2 \\ 4 & 1 \end{array}$$

### Confluence

Something to think about: should there ever be a stage at which there is both a row and a column that can be deleted, might it make any difference which one we delete first? How confident can you be that we will always end up with the same matrix once we have run out of rows and columns to delete? A reduction or simplification process that sometimes allows you a choice of ways to reduce the object-in-hand but which nevertheless guarantees that when the music stops, and you have no more reductions to perform, you will have the same thing in your hand whichever choices you made *en route* is said to be **confluent**. Clearly, when you are given a bundle of operations which you use for processing an input, it does matter greatly whether or not these operations are confluent. In general proving confluence can be hard, but in this case it's easy.

**EXERCISE 61.** *Prove that the process of deleting dominated rows and columns is confluent.*

You should be prepared to spend some time on this exercise, and really get it to come out. (It took me a while!) Confluence crops up all over the place, in evaluation, rewrite rules—in fact anywhere where there is a definitive answer to a question but various (nondeterministic) ways of reaching it. [sequent calculus, algebraic manipulations such as those used to get things into CNF and DNF, various rewrite rules etc.]

Tidy this up

By this process of weeding we end up with a matrix in which no row dominates any other row and no column dominates any other column.

What is the sensible thing to do? The *maximin* strategy is to choose that course of action which give you the best result if things go well. For player I this strategy tells him to play that row whose greatest element is the greatest among all the rows available. That is to say: he is considering, for each row  $r$ , the best case  $b_r$  that can happen if he plays  $r$ . ( $b_r$  is the biggest number in row  $r$ .) He then chooses  $r$  so as to optimize (= maximise)  $b_r$ . The trouble is, II might not oblige by picking the column in which that number appears! In contrast the **minimax** strategy is the strategy of minimising the disasters that can befall you: acting so as to ensure that the worst-case scenario in the course of action you have embarked on is less dire than the worst-case scenarios that would have awaited you down other paths.

For player I this strategy tells him to play that row whose least element is the greatest among all the rows available. That is to say: he is considering, for each row  $r$ , the worst case  $w_r$  that can happen if he plays  $r$ . ( $w_r$  is the smallest number in row  $r$ .) He then chooses  $r$  so as to optimize (= maximise)  $w_r$ . That way he can be sure of compelling II to pay him at least the largest number that is a  $w_r$  for some row  $r$ . Let us call this value  $I^*$ . II has a corresponding (“dual”) strategy which is to consider, for each column  $c$ , the largest number  $g_c$  in that column. She then chooses  $c$  so as to optimise (= minimise)  $g_c$ . That way she can be sure that she doesn’t have to pay out more than the smallest number that is a  $g_c$  for some column  $c$ . Let us call this quantity  $II^*$ .

We will minute the following fundamental fact:

$$I^* \leq II^*$$

*Proof:*

Let  $A$  be the set  $\{x : \text{for some row } r, x \text{ is the smallest thing in } r\}$  and let  $B$  be the set  $\{y : \text{for some column } c, y \text{ is the largest thing in } c\}$ . We want to show that everything in  $A$  is less than everything in  $B$ . Let  $x$  be an arbitrary member of  $A$  and  $y$  an arbitrary member of  $B$ .  $x$  belongs to row  $r$ , for some  $r$ , and  $y$  belongs to some column  $c$ . Clearly at the point where  $r$  and  $c$  meet we will find a number that is as big as the smallest thing in  $r$  (namely  $x$ ) but no bigger than the biggest thing in  $c$  (namely  $y$ ). So  $x \leq y$ . But  $x$  and  $y$  were arbitrary, so this tells us that everything in  $A$  is less than or equal to everything in  $B$ . So the biggest thing in  $A$  (which is  $I^*$ ) can be no bigger than the smallest thing in  $B$  (namely  $II^*$ ). ■

So “The sup of the infs is less than or equal to the inf of the sups.” The point is often made that this inequality is the same fact as the implication  $(\exists x)(\forall y)(F(x, y)) \rightarrow (\forall y)(\exists x)(F(x, y))$ . What is going on? If you think of the truth-values **true** and **false** as ordered **false** < **true** then you will think that the truth-value of  $(\exists x)(F(x, y))$  is the sup of the truth values of  $F(x, y)$  for all  $x$ , and the truth-value of  $(\forall x)(F(x, y))$  is the inf of the truth values of  $F(x, y)$  for all  $x$ . So the truth-value of  $(\exists x)(\forall y)(F(x, y))$  is the sup of the infs, and the

truth-value of  $(\forall y)(\exists x)(F(x, y))$  is the inf of the sups. You may recall the same ideas cropping up in connection with Menger's theorem.

Explain this imagery

The cases where  $I^* = II^*$  are games with *saddle points*. There is an element which is the largest in its column and the smallest in its row.

However there are lots of games—even  $2 \times 2$  games—without saddle points, like

$$\begin{array}{cc} 4 & 2 \\ 1 & 3 \end{array}$$

In this game I will play safe and choose the first row (the row with the largest minimum), giving  $I^* = 2$  and II will pick column 2 (with the smallest maximum) giving  $II^* = 3$ .

Games lacking saddle points merit further analysis. It's not clear what is the best thing to do. We can make progress in understanding this situation if we ask instead a different question. Instead of asking "What is the best thing to do in (a single play of) this game?", one asks: "If one is going to play a lot of plays of this game, what is the best way to maximise your aggregate payoff?" This leads us to the notion of a **mixed strategy**. A mixed strategy gives you an assignment of probabilities to rows (if you are I) or columns (if you are II) and you toss a suitably biased coin or roll a suitably biased die to decide which to choose at each play of the game.

It is in this sense of *best* that the Minimax theorem tells us that both players have a best strategy. For each player there is an optimal mixed strategy.

One way of thinking of this is to fill out the four points in the matrix above into a surface, as in the picture [that i haven't been able to draw!]. This surface is saddle-shaped, and has a saddle point. It is this saddle point that will be the solution to the game—in a sense which we must now make clear.

Get the saddle reference right

**THEOREM 6.** *In any  $n \times m$  matrix game there is a (?unique?) mixed strategy for I (and II) which is optimal in the sense that no other strategy guarantees as good an average payoff.*

For simplicity's sake let us restrict ourselves to the case where the matrix is a two-by-two matrix. We are also going to assume that neither row dominates the other and neither column dominates the other. This not only restricts our analysis to the cases we have not yet covered, but also coincidentally excludes from application of this analysis cases that would cause it to do stupid things like divide by 0. So we are looking at

$$\begin{array}{cc} a & b \\ c & d \end{array}$$

and let us assume without loss of generality that both  $a$  and  $d$  are bigger than both  $c$  and  $b$ .

I and II use mixed strategies, so that I picks row 1 with probability  $x$  and II picks column 1 with probability  $y$ . We can represent this by decorating the matrix thus:

	$y$	$1 - y$
$x$	$a$	$b$
$(1 - x)$	$c$	$d$

Let  $P$  be the expected payoff for the pair of mixed strategies. That is to say,  $P$  is the number of £ that II will be paying I per game *on average*. (Remember  $P$  may be negative!)  $P$  is the average of the matrix entries weighted in the proportion of the time that I and II choose each entry. To be precise,  $P$  is

$$axy + b(1 - y)x + cy(1 - x) + d(1 - y)(1 - x) \quad (P)$$

Thus on average, if I picks row 1 a proportion  $x$  of the time and II picks column 1 a proportion  $y$  of the time, on average II will pay I £ $P$ . We can rearrange this expression to

$$xy(a - b - c + d) + y(c - d) + x(b - d) + d. \quad (6.1)$$

Now once we have fixed on constant values of  $a$ ,  $b$ ,  $c$  and  $d$  the formula  $P$  above gives us a function of two variables  $x$  and  $y$ . What we want is to find a value of  $x$  that makes the dependence of  $P$  on  $y$  disappear. The coefficient of  $y$  in  $P$  is

$$x((a + d) - (c + b)) + (c - d) \quad (6.2)$$

For what value of  $x$  does equation 6 take the value 0? Clearly we must have

$$x((a + d) - (c + b)) = (d - c) \quad (6.3)$$

So if  $x$  takes the value

$$x = \frac{d - c}{(a + d) - (b + c)} \quad (x^*)$$

then  $P$  takes a value from which  $y$  has disappeared. This means that if I and II play repeatedly, with  $x$  playing row one with probability  $x^*$ , it makes no difference what player II does.

This probably looks horrible, but it makes good sense. We are in a situation where the two rows slope in different ways: row 1 slopes down (going from left to right) and row 2 slopes upward.  $(d - c)$  is a measure of the slope of row 2. If it's very nearly zero then—if you want a strategy that produces the same result (on average) whatever II is doing—then you want to be playing row 2 most of the time. So you want  $x$  to be very small. And it's simple to check that the top line of  $x^*$  is positive and smaller than the bottom line (which is also positive) so  $x^*$  is between 0 and 1.

Similarly we want to find a value for  $y$  that will make  $P$ 's dependency on  $x$  disappear. You might like to try this by hand, pursuing calculations analogous to equations 6 and 6. But we don't actually need to. Substituting  $x^*$  into  $P$  we get

$$d - \frac{(d-c)(d-b)}{(a+d)-(b+c)} \quad (6.4)$$

which simplifies (try it!) to

$$\frac{(ad-cb)}{(a+d)-(b+c)} \quad (v)$$

Which we call the **value** of the game.

Finally we need to check that

**EXERCISE 62.**

$$\mathbf{I}^* \leq v \leq \mathbf{II}^*$$

(Remember that  $\mathbf{I}^*$  is the larger of  $b$  and  $c$ , and that  $\mathbf{II}^*$  is the smaller of  $a$  and  $d$ ).

This resolves the unsatisfactory situation where there was a gap between the best  $\mathbf{I}$  could get for himself and the worst that  $\mathbf{II}$  had to endure. Using the mixed strategy  $\mathbf{II}$  can ensure that nothing worse than  $v$  happens, and  $\mathbf{I}$  can ensure that he does at least do as well as  $v$ .  $v$  is, in some sense, a **solution** to the game.

It is possible to find an optimal mixed strategy even if there are more than two rows or columns, but we have to use some slightly trickier mathematics to do it, and we have no space for that here. Instead we close with a brief glimpse of some very mysterious and complex generalisations, which are susceptible of wide application.

## 6.1 Bimatrix games

In these games the second components are the payoffs to the player picking the columns (player  $\mathbf{II}$ ); the first components are the payoffs to the player picking the rows (player  $\mathbf{I}$ ).

These games are deep and important objects, and there is a huge literature on them. The most famous game of this kind is:

Figure 6.1: The Prisoners' Dilemma

	cooperate	defect	
cooperate	(3, 3)	(1, 4)	cooperate
defect	(4, 1)	(2, 2)*	defect

The Prisoners' Dilemma is a game played by two players, both of them prisoners at the mercy of the Evil Gaoler. You have to choose between shopping your accomplice (the other player) and staying solid. The game is symmetrical:



the options open to the two players are the same. If you shop your accomplice you get a new identity and a case of whisky (that's 4) and your accomplice is fed to crocodiles (that's 1). If you both shop each other, your gaolers treat you with contempt and merely shoot you (that's 2). If you both stand firm and loyal you escape with your lives and your freedom (that's 3).

It is almost impossible to overestimate the importance of this discovery of the Prisoners' Dilemma. The number of real-life situations of which it is a plausible formalisation is astonishing. This makes it not merely intriguing but important. However, since the fundamental concepts of game theory are not entirely clear, our analysis of the Prisoners' Dilemma game is not as applicable as one would like. An old problem in Ethics (I think the Greeks wrote about it) is the problem of inferring individual obligation from collective obligation. Clearly all nations are under a collective obligation to disarm themselves of their nuclear weapons. But—equally clearly—one does not infer from this that each and every nation is obliged to disarm unilaterally. In contrast, in the logically very similar situation of the problem posed by global warming and the need to cut carbon emissions, there is a much stronger inclination to argue that individual countries are under individual obligations to cut their emissions. This discrepancy arises because it is not entirely clear how to draw correctly the parallel between the real-life situation and the formal version.

A subtly different game is **Chicken**:

Figure 6.2: Chicken

blink	don't blink	
(3, 3)	(2, 4)*	blink
(4, 2)*	(1, 1)	don't blink

Chicken is played by two car drivers approaching each other at high speed on a single carriageway. The one who veers off the road to avoid getting killed loses a lot of cred and probably writes off the car (that's 2). Still, it beats getting killed (that's 1). If you both veer off the road you still write off the car but you don't lose as much cred (that's 3). If you stay on the road and the other player veers off, then you gain a great deal of cred—and you keep the car (that's 4).

Can one say anything sensible about these games? Well, there are always these things called **Nash equilibria**. (The Nash equilibria are the starred entries above). What is a Nash equilibrium? It's a pair of a row  $R$  and a column  $C$  such that I cannot do better than  $R$ —given that II is going to play  $C$ —and II cannot do better than  $C$ —given that I is going to choose  $R$ .

On the face of it there may be lots of Nash equilibria. We can use a fixed point theorem to show that—if we allow mixed strategies—there must be at least one. I'm not planning to prove that all bimatrix games have Nash equilibria.

And yes, it is the Nash of the Beautiful Mind, who died in a car crash on the fourth day of the ENG v NZ Lord's Test 2015.

### 6.1.1 Symmetrical Bimatrix Games

Consider bimatrix games where the ordered pair at  $a_{i,j}$  is the flip of the ordered pair at  $a_{j,i}$  and the ordered pairs on the main diagonal have two identical components. What's this 'main diagonal'?—doesn't make sense! After all, we could have written the columns in any order and we could have written the rows in any order, and that would jumble things up terribly. Well, it does if there is a way of identifying rows with columns: that is to say, if the options available to I are the same as those available to II. This is the case in the prisoners' dilemma for example—where we can name one row (column) 'cooperate' and the other 'defect' and in chicken, where one row (column) is 'blink' and the other is 'don't blink'.

In these circumstances one can once again represent the game by a matrix (not a bimatrix, two superimposed matrices)—even though the game is not zerosum—but in this case the entry in  $a_{i,j}$  represents that payoff to strategy  $i$  played against strategy  $j$  and the payoff to strategy  $j$  played against strategy  $i$  is to be found in  $a_{j,i}$ .

It turns out that this special case has a biological motivation. (I think this is right) an **evolutionarily stable strategy** is a (possibly mixed) strategy  $\sigma$  such that  $\langle \sigma, \sigma \rangle$  is an equilibrium pair.

They write  $E(p, q)$  for the payoff to someone playing  $p$  against someone playing  $q$ .

The Bishop-Cannings theorem states that if  $I$  is a mixed strategy then  $E(p, I) = E(I, I)$  for all  $p$  in the *support* of  $I$ .

## Chapter 7

# More Exercises

Starred exercises have model answers. The following relevant tripos questions also have model answers in the answer file.

Maths tripos questions

1988:6:9E, 1988:6:10E, 1995:5:4X,

Comp Sci tripos questions

1990:1:9, 1990:1:11, 1993:11:11, 1994:10:11, 1996:1:8

### Exercises on (binary) relations

1. (Do not do more than a sample of the bits of this question: if you are making any mistakes they will always be the same mistakes, and there is no point in making the discovery more than once!)
  - (a) Given the operations of composition and union, express the following relations in terms of brother-of, sister-of, father-of, mother-of, son-of, daughter-of. (You may use your answers to earlier questions in answering later questions.)
    - i. parent-of
    - ii. uncle-of
    - iii. aunt-of
    - iv. nephew-of
    - v. niece-of
    - vi. grandmother-of
    - vii. grandfather-of
    - viii. first-cousin-of

You can also express some of the relations in the original list in terms of others by means of composition and union. Do so.

- (b) Do the same to include all the in-law and step relations, by adding spouse-of to the original list. This time you may use intersection and complement as well.

- (c) If the formalisation of “ $x$  is a parent of  $y$ ” is “ $(\text{father-of}(x, y) \vee \text{mother-of}(x, y))$ ” (i.e., use logical connectives not  $\cup$  and  $\cap$ ... you will also need to use quantifiers) what are the formalisations of the other relations in the preceding list? And for a bonus point, formalise “ $x$  is the double cousin of  $y$ ”.<sup>1</sup> Hint: might need new variables!
- (d) Using the above gadgetry, plus set inclusion (“ $\subseteq$ ”) formalise
- Every mother is a parent.
  - The enemy of [my] enemy is [my] friend
  - The enemy of my friend is my enemy.
  - The friend of my enemy is my enemy.
  - no friend is an enemy
2. \* Write out a formal proof that the intersection of two transitive relations is transitive.
3. \* Let  $R$  be a relation on  $A$ . ( $'r'$ ,  $'s'$  and  $'t'$  denote the reflexive, symmetric and transitive closure operations respectively.)
- Prove that  $rs(R) = sr(R)$ .
  - Does  $R$  transitive imply  $s(R)$  transitive?
  - Prove that  $rt(R) = tr(R)$  and  $st(R) \subseteq ts(R)$ .
  - If  $R$  is symmetrical must the transitive closure of  $R$  be symmetrical? Prove or give a counterexample.
4. Think of a binary relation  $R$ , and of its graph, which will be a directed graph  $\langle V, E \rangle$ . On any directed graph we can define a relation “I can get from vertex  $x$  to vertex  $y$  by following directed edges” which is certainly transitive, and we can pretend it is reflexive because after all we can get from a vertex to itself by just doing nothing at all. Do this to our graph  $\langle V, E \rangle$ , and call the resulting relation  $S$ . How do we describe  $S$  in terms of  $R$ ?
5. \* Show that—at least if  $(\forall x)(\exists y)(\langle x, y \rangle \in R) \rightarrow R \circ R^{-1}$  is a fuzzy. What about  $R \cap R^{-1}$ ? What about  $R \cup R^{-1}$ ?
6. \* Given any relation  $R$  there is a least  $T \supseteq R$  such that  $T$  is transitive, and a least  $S \supseteq R$  such that  $S$  is symmetrical, namely the transitive and symmetric closures of  $R$ . Must there also be a unique maximal (aka **maximum**)  $S \subseteq R$  such that  $S$  is transitive? And must there be a unique maximal (maximum)  $S \subseteq R$  such that  $S$  is symmetrical? The answer to one of these last two questions is ‘yes’: find a cute formulation.
7. What are the transitive closures of the following relations on  $\mathbb{N}$ ?
- $\{\langle 0, 1 \rangle, \langle 1, 2 \rangle, \langle 2, 3 \rangle, \dots\}$ : i.e.,  $\{\langle n, n+1 \rangle : n \in \mathbb{N}\}$ ,

---

<sup>1</sup>Fred and Bert are double cousins if they are first-cousins in two different ways.

(b)  $\{\langle n, 2n \rangle : n \in \mathbb{N}\}$ .

8. What is an antichain? Let  $D_n$  be the poset whose elements are the divisors of  $n$ , with  $x \leq y$  if  $x|y$ . Find a maximum antichain in  $D_{216}$ .
9. \* Define  $xRy$  on natural numbers by

$$xRy \text{ iff } x \leq y + 1$$

What are the following relations?<sup>2</sup>

- (a)  $R \cap R^{-1}$
- (b)  $R \setminus R^{-1}$
- (c) The transitive closure of the relation in (a)
- (d) The transitive closure of the relation in (b)
10. \* Are the two following conditions on partial orders equivalent?
- (a)  $(\forall xyz)(z < x \not\leq y \not\leq x \rightarrow z < y)$
- (b)  $(\forall xyz)(z > x \not\leq y \not\leq x \rightarrow z > y)$ .
11. Consider the set  $[1, n]$  of whole numbers from 1 up to  $n$  inclusive. How many partial orders  $\leq$  are there on this set with the property that  $(\forall xyz)(z \leq x \not\leq y \not\leq x \rightarrow z \leq y)$ ?
12. \* Show that  $R \subseteq S$  implies  $R^{-1} \subseteq S^{-1}$
13. (a) The purpose of this question was to make a point about lexicographic orders: in this case, about the order on  $\mathbb{N} \times \mathbb{N}$ . Check that you have really understood what is going on by rewriting the question for the scenario in which the balls come in three colours ...  $k$  colours.
- (b) (abstruse: not for a first pass) Extend the product order of  $\mathbb{N} \times \mathbb{N}$  by stipulating that  $\langle x, y \rangle < \langle y, S(x) \rangle$  and taking the reflexive transitive closure. Write the result  $\leq_{\mathcal{B}}$ . Is  $\leq_{\mathcal{B}}$  a total order? Define  $\leq$  between finite subsets of  $\mathbb{N} \times \mathbb{N}$  by  $X \leq Y$  iff  $(\forall x \in X)(\exists y \in Y)(x \leq_{\mathcal{B}} y)$ . Is  $\leq$  wellfounded?
14. Functions are just special kinds of relations, okay? What can you say about a function that is also a symmetrical relation? What about a function that is also a transitive relation? (That is,  $f(x) = y \wedge f(y) = z \rightarrow f(x) = z$ ). Embarrass your supervisor by demanding explanations of the words *involution* and *idempotent*.
15. Let  $K = \lambda x.(\lambda y.x)$ . Evaluate  $K8$ ,  $K(K8)$  and  $(KK)8$ .

---

<sup>2</sup>The structure  $\langle \mathbb{N}, R \rangle$  is known to students of modal logic as the *Recession Frame*.

16. What is a wellordering? What is an initial segment of an ordering? (If you don't know what a **chain** in a poset is you probably won't know what an initial segment in a total ordering is either.) If  $\langle X, \leq \rangle$  is a total order, then a *suborder* of it is a subset  $X' \subseteq X$  ordered by the obvious restriction of  $\leq$ . Prove that  $\langle X, \leq \rangle$  is a wellordering if every suborder of it is isomorphic to an initial segment of it. (The converse is also true but involves more work.)
17. \* Show that  $\bigcup_{n \in \mathbb{N}} R^n$  is the smallest transitive relation extending  $R$ .
18.  $t(R)$  is the transitive closure of  $R$ .<sup>3</sup>
- \* Give an example of a relation  $R$  on a set of size  $n$  for which  $t(R) \neq R^1 \cup R^2 \cup \dots \cup R^{n-1}$ .
  - Give an example of a set and a relation on that set for which  $t(R) \neq R^1 \cup R^2 \cup \dots \cup R^n$  for any finite  $n$ .
  - If  $R$  is reflexive then  $t(R)$  is clearly the reflexive transitive closure of  $R$  (often called just the transitive closure): if you are not happy about this, attempt to write out a proof.
  - Find an example of an *irreflexive*<sup>4</sup> relation  $R$  on a set such that  $t(R)$  is indeed the reflexive transitive closure of  $R$ .
19. Think about  $\mathbb{N}$  and  $S$  (the successor function on  $\mathbb{N}$ ). What is the transitive closure of  $S$ ? For integers  $n$  and  $m$  when do we have  $(S^n)^* \subseteq (S^m)^*$ ? When do we have  $(S^n \cup (S^n)^{-1} \cup S^m \cup (S^m)^{-1})^* = (S \cup S^{-1})^*$ ?
20. \* Show that the smallest equivalence relation containing the two equivalence relations  $R$  and  $S$  is  $t(R \cup S)$ .
21. If  $R \subseteq X \times X$  is a fuzzy on  $X$ , is there a largest equivalence relation on  $X$  that  $\subseteq R$ ? Is there a smallest equivalence relation on  $X$  that  $\supseteq R$ ?
22. (a) Suppose that for each  $n \in \mathbb{N}$ ,  $R_n$  is a transitive relation on a (presumably infinite) set  $X$ . Suppose further that for all  $n$ ,  $R_n \subseteq R_{n+1}$ . Let  $R_\infty$  be  $\bigcup_{n \in \mathbb{N}} R_n$ , the union of all the  $R_n$ . Prove that  $R_\infty$  is also transitive.
- (b) Give an example to show that the union of two transitive relations is not always transitive.
23. For all the following choices of allegations, prove the strongest of the correct options; explain why the other correct options are not best possible and find counterexample to the incorrect ones. If you find you are doing them with consummate ease, break off and do something else instead.

<sup>3</sup>Misleadingly people often use the expression "transitive closure of  $R$ " to mean the transitive reflexive closure of  $R$ .

<sup>4</sup>You don't know what 'irreflexive' means? There are only two things it can possibly be, so what are they? Answer this question for *both* versions! That'll teach you ask silly questions!

- (a) An intersection of a fuzzy and an equivalence relation is (i) an equivalence relation (ii) a fuzzy (iii) neither
  - (b) A union of a fuzzy and an equivalence relation is (i) an equivalence relation (ii) a fuzzy (iii) neither
  - (c) An intersection of two fuzzies is (i) an equivalence relation (ii) a fuzzy (iii) neither
  - (d) An intersection of the complement of a fuzzy and an equivalence relation is (i) an equivalence relation (ii) a fuzzy (iii) neither
  - (e) An intersection of a fuzzy and the complement of an equivalence relation is (i) an equivalence relation (ii) a fuzzy (iii) neither
  - (f) A union of a fuzzy and the complement of an equivalence relation is (i) an equivalence relation (ii) a fuzzy (iii) neither
  - (g) An intersection of a fuzzy and the complement of a fuzzy is (i) an equivalence relation (ii) a fuzzy (iii) neither
  - (h) An intersection of the complement of a fuzzy and the complement of an equivalence relation is (i) an equivalence relation (ii) a fuzzy (iii) neither
  - (i) A union of two fuzzies is (i) an equivalence relation (ii) a fuzzy (iii) neither.
24. A PER (*Partial Equivalence Relation*) is a binary relation that is symmetrical and transitive. Is the complement of a PER a fuzzy? Is the complement of a fuzzy a PER? In each case, if it is false, find sensible conditions to put on the antecedents that would make it true.
25. Let  $<$  be a transitive relation on a set  $X$ . Consider the two relations (i)  $\{\langle x, y \rangle : (x \in X) \wedge (y \in X) \wedge (x < y) \wedge (y < x)\}$  and (ii)  $\{\langle x, y \rangle : (x \in X) \wedge (y \in X) \wedge (x \not< y) \wedge (y \not< x)\}$ .
- (a) Are either of these fuzzies, or equivalence relations?
  - (b) If one of these isn't a fuzzy, but "ought to be", what was the correct definition?
  - (c) If the relation in (i) was an equivalence relation, what sort of relation does  $<$  induce on the equivalence classes? Why is the result a mess? What extra condition or conditions should i have put on  $<$  to start with to prevent this mess occurring?
  - (d) If (the correct definition of) relation (ii) is an equivalence relation, what can we say about the quotient?
26. Explain how to find the two greatest numbers from a set of  $n$  numbers by making at most  $n + \lfloor \log_2 n \rfloor - 2$  comparisons. Can it be done with fewer? How about the 3 biggest numbers? The  $k$  biggest numbers, for other values of  $k$ ? What happens to your answer as  $k$  gets bigger and bigger and approaches  $n$ ?

27. \* Show that the largest and smallest elements of a totally ordered set with  $n$  elements can be found with  $\lceil 3n/2 \rceil - 1$  comparisons if  $n$  is odd, and  $3n/2 - 2$  comparisons if  $n$  is even.
28. Construct *natural* bijections between the following pairs of sets. (For the purposes of this exercise a natural map is (expressed by) a closed  $\lambda$ -term; a natural bijection is (expressed by) a closed  $\lambda$  term ( $L$ , say) with an inverse  $L'$ . That is to say, both  $\text{compose}(L, L')$  and  $\text{compose}(L', L)$  simplify to  $\lambda x.x$ . Alternatively, a natural function is one you can write an ML program for. If you want to think more about what a natural bijection is, look at your earlier answers to the questions: If  $A$  is a set with  $n$  members, how many symmetrical relations are there on  $A$ , and how many antisymmetrical trichotomous relations are there on  $A$ ? The answers to these two questions are the same, but there doesn't seem to be any 'obvious' or 'natural' bijection between the set of symmetrical relations on  $A$  and the set of antisymmetrical trichotomous relations on  $A$ .) You will need to assume the existence of primitive pairing and unpairing functions which you might want to write as '**fst**', '**snd**' and  $\langle x, y \rangle$

$$\begin{aligned} &A \rightarrow (B \rightarrow C) \text{ and } B \rightarrow (A \rightarrow C); \\ &A \times B \text{ and } B \times A; \\ &A \rightarrow (B \times C) \text{ and } (A \rightarrow B) \times (A \rightarrow C); \\ &(A \times B) \rightarrow C \text{ and } A \rightarrow (B \rightarrow C); \end{aligned}$$

You may wish to try the following pairs too, but only once you have done the ML machinery for disjoint unions of types:

$$\begin{aligned} &(A \rightarrow C) \times (B \rightarrow C) \text{ and } (A + B) \rightarrow C; \\ &A + (B + C) \text{ and } (A + B) + C; \\ &A \times (B + C) \text{ and } (A \times B) + (A \times C). \end{aligned}$$

Let  $Z$  be a set with only one element. Find a natural bijection between  $(Y + Z)^X$  and the set of partial functions from  $X$  to  $Y$ .

Find natural functions<sup>5</sup>

- (i) from  $A$  into  $B \rightarrow A$ ;
- (ii) from  $A$  into  $(A \rightarrow B) \rightarrow B$ ;
- (iii) from  $A \rightarrow (B \rightarrow C)$  into  $(A \rightarrow B) \rightarrow (A \rightarrow C)$ ;
- (iv) from  $((A \rightarrow B) \rightarrow B) \rightarrow B$  into  $A \rightarrow B$ . (This one is hard: you will need your answer to (ii))
- (v) from  $(A \rightarrow B) \rightarrow A$  into  $(A \rightarrow B) \rightarrow B$ .

(it might help to think of these as invitations to write ML code of types ' $a \rightarrow b \rightarrow a$ ', ' $a \rightarrow (a \rightarrow b) \rightarrow a$ ' etc.)

<sup>5</sup>These do not have to be either injective or surjective. They only have to be functions.



29. What is a fixed point? What is a fixpoint combinator? Let  $T$  be your answer to the last bit of the preceding question. (So  $T$  is a natural function from  $(A \rightarrow B) \rightarrow A$  into  $(A \rightarrow B) \rightarrow B$ .) Show that something is a fixpoint combinator iff it is a fixed point for  $T$ .
30. Let  $P = \lambda G.(\lambda g.G(gg))(\lambda g.G(gg))$ . Show that  $P$  is a fixpoint combinator. Why is it not typed? After all,  $T$  was typed!
31. Give ML code for a higher-order function `metafact` such that any fixed point for `metafact` will turn out to be good old `fact`. Do the same for something tedious like `fib`. Delight your supervisor by finding, for other recursively defined functions, higher-order functions for which they are fixed points.
32. \* Solve

$$x^{x^{x^{x^{x^{\dots}}}}} = 2$$

and comment on the notation. Then think about

$$x^{x^{x^{x^{x^{\dots}}}}} = 4.$$

33. Prove that  $2^n - 1$  moves are sufficient to solve the Towers of Hanoi problem.
34. The fellows of Porterhouse ring each other up every sunday to catch up on the last week's gossip. Each fellow passes on (in all subsequent calls that morning) all the gossip (s)he has picked up, so there is no need for each fellow to ring every other fellow directly. How many calls are needed for every fellow to have acquired every other fellow's gossip?
35. A *triomino* is an  $L$ -shaped pattern made from three square tiles. A  $2^k \times 2^k$  chessboard, whose squares are the same size as the tiles, has one of its squares painted puce. Show that the chessboard can be covered with triominoes so that only the puce square is exposed.
36. Is it possible to tile a standard  $(8 \times 8)$  chessboard with thirty-one  $2 \times 1$  rectangles (dominoes) to leave two diagonally opposite corner squares uncovered?
37. \* Let  $k \in \mathbb{N}$  and let  $\mathcal{F}$  be a family of finite sets closed under symmetric difference, such that each set in  $\mathcal{F}$  has at most  $k$  elements. How big is  $\bigcup \mathcal{F}$ ? How big is  $\mathcal{F}$ ?
38. Fix a set  $X$ . If  $\pi_1$  and  $\pi_2$  are partitions of it, we say  $\pi_1$  *refines*  $\pi_2$  if every piece of  $\pi_1$  is a subset of a piece of  $\pi_2$ . What properties from the usual catalogue (transitivity, symmetry, etc.) does this relation between partitions of  $X$  have?

39. Let  $X$  be a set, and  $R$  the refinement relation on partitions of  $X$ . Let  $\Pi(X)$  be the set of partitions. Why is it obvious that in general the structure  $(\Pi(X), R)$  is not a boolean algebra?

### Boolean Algebra

1. Write down the truth tables for the 16 functions  $\{T, \perp\}^2 \rightarrow \{T, \perp\}$ , and give them sensible names (such as  $\wedge, \vee, \rightarrow, \text{NOR}, \text{NAND}$ ). Which of these functions **splat** that you have identified have the feature that if  $p$  **splat**  $q$  and  $p$  both hold, then so does  $q$ ? Why are we interested in only one of them?
2. (a) Show that **NAND** and **NOR** cannot be constructed by using  $\wedge$  and  $\vee$  and  $\rightarrow$  alone  
 (b) Show that none of **NAND**, **NOR**,  $\rightarrow$ ,  $\wedge$ ,  $\vee$  can be constructed by using **XOR** alone. (hard)  
 (c) Show that **XOR** and  $\longleftrightarrow$  and  $\neg$  cannot be defined from  $\vee$  and  $\wedge$  alone.  
 (d) (*for enthusiasts only*) Can  $\wedge$  and  $\vee$  be defined in terms of  $\longleftrightarrow$  and  $\rightarrow$ ?  
 (e) (*for enthusiasts only*) Show that all connectives can be defined in terms of **XOR** and  $\rightarrow$ .  
 (f) A *monotone* propositional function is one that will output 1 if all its inputs are 1. Show that no nonmonotone function can be defined in terms of any number of monotone functions. (easy)
3. What is a boolean algebra? Find a natural partial order on the set of functions from question 1 that makes them into a boolean algebra.
4. How many truth-functions of three propositional letters are there? Of four? Of  $n$ ?
5. Prove that  $\mathcal{P}([0, 2])$  and  $\{T, \perp\}^3$  are isomorphic posets.

### Generating functions etc.

1. Let  $u_n$  be the number of strings in  $\{0, 1, 2\}^n$  with no two consecutive 1's. Show  $u_n = 2u_{n-1} + 2u_{n-2}$ , and deduce  $u_n = \frac{1}{4\sqrt{3}}[(1 + \sqrt{3})^{n+2} - (1 - \sqrt{3})^{n+2}]$ .
2. Let  $m_n$  be the number of ways to obtain the product of  $n$  numbers by bracketing. (For example,  $((ab)c)d$ ,  $(ab)(cd)$ ,  $(a(bc))d$ ,  $a((bc)d)$  and  $a(b(cd))$  show  $m_4 = 5$ .) Prove  $m_n = \frac{1}{n} \binom{2n-2}{n-1}$ .
3. Prove that  $\mathbb{N} \times \mathbb{N}$ , with the lexicographical order, is well-ordered, and that  $\mathbb{N} \times \mathbb{N}$  with the product order has no infinite antichain.

4. Say  $n \in m$  (where  $n, m \in \mathbb{N}$ ) if the  $n$ th bit of  $m$  is 1.  $n \subseteq m$  is defined in terms of this in the obvious way. Prove that  $n \subseteq m$  iff  $\binom{m}{n}$  is odd. (Hint: use the fact that  $\binom{m+1}{n+1} = \binom{m}{n} + \binom{m}{n+1}$ .)
5. Let  $p_n$  be the number of ways to add  $n - 3$  non-crossing diagonals to a polygon with  $n$  sides, thus splitting it into  $n - 2$  triangles. So  $p_3 = 1$ ,  $p_4 = 2$ ,  $p_5 = 5$ , and we define  $p_2 = 1$ . Show that

$$p_n = p_2 p_{n-1} + p_3 p_{n-2} + \dots + p_{n-1} p_2 \quad \text{for } n \geq 3,$$

6. and hence evaluate  $p_n$ .
7. A question on generating functions which will keep you out of mischief for an entire afternoon!<sup>6</sup> Let  $A_n$  be the number of ways of ordering the numbers 1 to  $n$  such that each number is either bigger than (or smaller than) *both* its neighbours. (“zigzag permutations”). Find a recurrence relation for  $(A_n/2)$ . (Hint Think about how many zigzag permutations of  $[1, n]$  there are where  $n$  appears in the  $r$ th place.) Further hints: you will have to divide the  $n$ th term by  $n!$  and solve a (fairly simple) differential equation.
8. What can you say about

$$q_0 =: 1; \quad q_{n+1} =: 1 - e^{-q_n}?$$

### Truth-definitions

An ML question which will prepare you for the 1b courses entitled “Logic and Proof” and “Semantics”. You should make a serious attempt at—at the very least—the first part of this question. The fourth part is the hardest part and provides a serious work-out to prepare you for the semantics course. Parts 2 and 3 are less central, but are educational. *If you are a 1b student treating this as revision you should be able to do all these questions.*

Propositional Logic	Predicate (first-order) Logic
A recursive datatype of formulæ	A recursive datatype of formulæ
	An interpretation $\mathcal{I}$ is a domain $\mathcal{D}$ with: for each $n$ -place predicate letter $F$ a subset $\mathcal{I} \cdot F$ of $\mathcal{D}^n$ ; for each $n$ -ary function letter $f$ a function $\mathcal{I} \cdot f$ from $\mathcal{D}^n \rightarrow \mathcal{D}$ . (Also constants).
<b>states</b> : $\text{literals} \rightarrow \text{bool}$ . A (recursively defined) satisfaction relation $\text{SAT} : \text{states} \times \text{fmla} \rightarrow \text{bool}$	(Fix $\mathcal{I}$ then) <b>states</b> : $\text{vbls} \rightarrow \mathcal{D}$ ; a recursively defined satisfaction function: $\text{sat}_{\mathcal{I}} : \text{formulæ} \times \text{states} \rightarrow \text{bool}$
A formula $\phi$ is <b>valid</b> iff for all <b>states</b> $v$ , $\text{SAT}(v, \phi) = \text{true}$ .	$\phi$ is <b>true</b> in an interpretation $\mathcal{I}$ iff for all states $v$ , $\text{sat}_{\mathcal{I}}(\phi, v) = \text{true}$ . $\phi$ is <b>valid</b> iff it is true in all interpretations.

<sup>6</sup>This comes from a book called “100 great puzzles in maths” or some such title: the author’s name is Dörrie, it is published by Dover, and there is a copy in the DPMMS library. This is problem 16 on p 64.

1. Write ML code to implement the left-hand column. If you are completely happy with your answer to this you should skip the next two questions of this section.
2. (*For enthusiasts*). Expand the propositional language by adding a new unary connective, written ' $\Box$ '. The recursive definition of **SAT** for the language with this extra constructor has the following additional clause:

if  $s$  is a formula of the extended language and  $v$  is a state then  
 $\mathbf{SAT}(v, \Box s) = 1$  iff for all states  $v'$  we have  $\mathbf{SAT}(v', s) = 1$

Then redo the first question with this added complication.

3. (*For enthusiasts*). Complicate further the construction of the preceding question by altering the recursive step for  $\Box$  as follows. Accept as a new input a (binary) relation  $R$  between states (presumably presented as a list of pairs, tho' there may be prettier ways of doing it). The new clause is then:

if  $t$  is a formula of the form  $\Box s$  and  $v$  is a state then  $\mathbf{SAT}(v, t) = 1$   
 iff for all states  $v'$  such that  $v' R v$  we have  $\mathbf{SAT}(v', s) = 1$

4. Declare a recursive datatype which is the language of partial order. That is to say you have a set of variables, quantifiers, connectives etc., and two predicate letters ' $\leq$ ' and ' $=$ '. Fix an interpretation of it, possibly the ML type **int**. Implement as much as you can of the apparatus of states, truth etc.
5. Declare a recursive datatype which is the language of fields. That is to say you have a set of variables, quantifiers, connectives etc.; two constants '0' and '1'; a binary predicate letter ' $=$ ' and two function symbols, '+' and ' $\times$ '. Fix an interpretation of it, for example the natural numbers below 17. Implement as much as you can of the apparatus of states, truth etc. You should be able to write code that will accept as input a formula in the language of fields and evaluate to **true** or **false** depending on what happens in the naturals mod 17.<sup>7</sup>

In the last two questions you could make life easier for yourself (but less natural) by assuming that the language has only finitely many individual variables. This would enable you, for example (by somehow generating all the possible states, since there are now only finitely many of them) to verify that the naturals as an ordered set are a model for the theory of total order, and that the naturals mod 17 are a model for the theory of fields.

When you have done this ask the system minders or any member of the hvg group about how to run *HOL* on the machines available to you. In *HOL* is a dialect of *ML* in which all the needed datatypes are predefined.

---

<sup>7</sup>It won't run very fast!

### Other logic: for 1b revision, mainly

1.  $\pi$  and  $e$  are transcendental. By considering the equation

$$x^2 - (\pi + e)x + \pi e = 0$$

prove a trivial but amusing fact. (If you cannot see what to do, read the footnote for a HINT).<sup>8</sup> What have you proved? Is your proof constructive? If not, does this give rise to a constructive proof of something else?

2. The uniqueness quantifier  $\exists!x$  is read as “There is precisely one  $x$  such that ...”. Show how to express the uniqueness quantifier in terms of the old quantifiers  $\exists$  and  $\forall$  (and  $=$ ).
  - (a) Find an example to show that  $(\exists!x\exists!y)\phi(x, y)$  is not always the same as  $(\exists!y\exists!x)\phi(x, y)$
  - (b) Is the conjunction of  $\exists!x\phi(x)$  and  $\exists!y\psi(y)$  equivalent to something of the form  $\exists!x\exists!y \dots$ ?

### Horn clauses

1. What is a horn clause? What is an intersection-closed property of relations?<sup>9</sup> Let  $\phi(\vec{x})$  be a horn clause (in which ‘ $R$ ’ appears and the  $\vec{x}$  range over the domain of  $R$ ). Show that the property  $\forall \vec{x}(\phi(\vec{x}))$  is intersection closed. (The converse is also true but do not attempt to prove it!)
2. Let  $I$  be an index set, and for each  $i \in I$ ,  $P_i$  is a person, with an associated set of beliefs,  $B_i$ . We assume (unrealistically) that each  $B_i$  is deductively closed and consistent. Show that  $\bigcap_{i \in I} B_i$  is deductively closed and consistent. What about the set of all propositions  $p$  such that  $p$  is believed by a majority of people? (You may assume  $I$  is finite in this case, otherwise it doesn’t make sense). What about the set of things believed by all but finitely many of the  $P_i$ ? (You may assume  $I$  is infinite in this case, otherwise it doesn’t make sense).<sup>10</sup>
3. We are given a set  $\mathcal{L}$  of literals. We are also given a subset  $K_0 \subseteq \mathcal{L}$ . (‘ $K$ ’ for ‘Known’.) Also a set  $C_0$  (‘ $C$ ’ for ‘Conditionals’) of formulae of the kind

$$(p_1 \wedge p_2 \wedge \dots \wedge p_n) \rightarrow q$$

If we are given two such sets, of literals and of conditionals, we can get a new set of Known literals by adding to  $K_0$  any  $q$  that is the consequent of a conditional all of whose antecedents are in  $K_0$ . Of course we can then throw away that conditional.

<sup>8</sup>At least one of  $\pi + e$  and  $\pi e$  must be transcendental.

<sup>9</sup>A horn clause is a formula of the kind  $\bigwedge_{i \in I} \psi_i \rightarrow \phi$  where  $\phi$  and all the  $\psi_i$  are atomic.  $F()$  is an intersection-closed property of relations if an intersection of any number of relations that have property  $F$  also has property  $F$ .

<sup>10</sup>What about the set of propositions believed by an even number of people?

- (a) Turn this into a precise algorithm that will tell us, given  $K_0$ ,  $C_0$  and a candidate literal  $q$ , whether or not  $q$  can be deduced from  $K_0$  and  $C_0$ . By coding this algorithm in ML, or by otherwise concentrating the mind, determine how efficient it is.
- (b) What difference does it make to the implementation of your algorithm if the conditionals are of the form

$$p_1 \rightarrow (p_2 \rightarrow (p_3 \rightarrow \dots q) \dots)?$$

- (c) What happens to your algorithm if Conditionals are allowed to be of the (more complicated) form:

$$(p_1 \wedge p_2 \wedge \dots \wedge p_n) \rightarrow (q_1 \vee q_2)?$$

Can anything be saved?

- (d) Define a quasi-order (remember what a quasi-order is?<sup>11</sup>) on  $\mathcal{L}$  by setting  $p R q$  if there is a conditional in  $C_0$  which has  $q$  as its consequent and  $p$  as one of its antecedents, and letting  $<$  be the transitive closure of  $R$ . Is  $<$  reflexive? Irreflexive? Antisymmetrical? What happens if  $p < p$ ? What happens if  $(p < q) \wedge (q < p)$ ?

---

<sup>11</sup>And don't lose sleep over the reflexivity condition: we can add lots of silly clauses like  $p \rightarrow p$  at no cost!

## Chapter 8

# Answers to Exercises

### Exercise 11

[https://www.dpmms.cam.ac.uk/~tf/cam\\_only/keeping\\_out\\_of\\_mischief.htm](https://www.dpmms.cam.ac.uk/~tf/cam_only/keeping_out_of_mischief.htm)

See also the discussion of 1988:6:9E of the Mathematics Tripos, p. 149.

### Exercise 25

Look up ‘monophyletic’. Using only the auxiliary relation “is descended from” give a definition in first-order logic of what is for a monadic predicate of lifeforms to be monophyletic.

$F$  is monophyletic iff both  $(\forall xy)((F(x) \wedge F(y) \rightarrow (\exists z)(F(z) \wedge D(z, x) \wedge D(z, y)))$  and

$(\forall x)(\forall y)(F(x) \rightarrow (D(x, y) \rightarrow F(y)))$  hold

Should probably also accept  $(\exists x)(\forall y)(D(x, y) \longleftrightarrow F(y))$

You may many years later need the concept of a *directed subset*.  $X$  is a directed subset of a poset  $\langle P, \leq \rangle$  if  $(\forall x, y \in P)(\exists z \in P)(x \leq z \wedge y \leq z)$

### Exercise 26

The graph of the three-place order relation on the four positions on the face is

$\{\langle \text{XII, III, VI} \rangle, \langle \text{III, VI, IX} \rangle, \langle \text{VI, IX, XII} \rangle, \langle \text{IX, XII, III} \rangle,$   
 $\langle \text{XII, VI, IX} \rangle, \langle \text{III, IX, XII} \rangle, \langle \text{VI, XII, III} \rangle, \langle \text{IX, III, VI} \rangle,$   
 $\langle \text{XII, III, IX} \rangle, \langle \text{III, VI, XII} \rangle, \langle \text{VI, IX, III} \rangle, \langle \text{IX, XII, VI} \rangle\}.$

### Exercise 37

How many binary relations are there on a set of size  $n$ ?

This is not a difficult question at all, but 99% of beginners get it wrong simply because they expect to be able to wing it, and they won’t think it through.

The answer—of course—is  $2^{n^2}$ .

## Exercise 40

### Discussion

This is a beautiful question, co's it touches several important points. It tests your understanding of structural induction; it tests your ability to do the fiddly manipulation necessary to perform the inductive step; it underlines the importance of having a sufficiently strong induction hypothesis, and finally it makes a point about dereferencing.

So: we have a propositional language—a recursive datatype of formulæ—which starts off with three propositional letters (“literals”) ‘ $a$ ’, ‘ $\top$ ’ and ‘ $\perp$ ’. We then build up compound formulæ by means of the constructors ‘ $\wedge$ ’, ‘ $\vee$ ’ and ‘ $\neg$ ’. We have a *length* function defined on objects in the datatype of formulæ, written with two vertical bars as in the question, which is roughly what you think it is—so that the length of a literal is 1, and the length of a conjunction (or a disjunction) of two formulæ is one plus the sum of their lengths, and the length of the negation of a formula is one plus the length of the formula. Evidently the question-designer thought that the length of a ‘(’ or a ‘)’ is zero!

One tends naturally to write the second half of the preceding paragraph with expressions like

$$|A \wedge B| = |A| + |B| + 1.$$

This looks fair enough, and in some sense it is, but we need to be clear about the conventions we are using. The letter ‘ $A$ ’ by itself is a single symbol, so a pedant might insist that  $|A| = 1$ . This is wrong of course: the letter ‘ $A$ ’ is not a formula, but a variable ranging over formulæ. . . when looking for the length  $|A|$  of  $A$  we have to *see through* the variable all the way to the value it takes—and that value is a formula. All this is well and good, but it can cause some confusion when we start thinking about expressions like:  $|A \vee B|$ . The constructor ‘ $\vee$ ’ is something we put between two formulæ to make a new formula; we don’t put it between two *names* of formulæ or between two *pointers* to formulæ! Until we have a convention to make our practice OK, writing things like ‘ $|A \vee B|$ ’ should generate a **syntax error** warning. If you look back to page 80 where this exercise first appears you will find that i wrote

“...length of a literal is 1, and the length of a conjunction (or a disjunction) of two formulæ is one plus the sum of their lengths. . .”

. . . and this is syntactically correct. When we wrote ‘ $|A \wedge B|$ ’ we should really have written ‘| the conjunction of  $A$  and  $B$  |’.

There are two ways of dealing with this. One is to have explicit names for the constructors, as it might be ‘conjunction of . . .’ and ‘disjunction of . . .’ and ‘negation of . . .’ This makes huge demands on our supply of alphanumerics.



The other solution is to have a kind of **environment** command that creates an environment within which [deep breath]

*Constructors applied to **pointers** to objects*

construct

**pointers** to the objects thereby constructed.

Inside such a context things like ‘ $|A \vee B|$ ’ have the meaning we intend here. There is a culture within which this environment is created by the ‘ $\ulcorner$ ’ symbol (`\ulcorner`) and closed by the ‘ $\urcorner$ ’ symbol (`\urcorner`). In practice people tend to leave these things out. The fact that this is—apparently—a safe strategy tells us quite a lot about the skills of our language module: it’s very good at dereferencing (among other things)

Thus we should/should-have posed the question as:

“Define the length of a Boolean proposition by structural induction as follows:

$$\begin{aligned} |a| &= 1, \\ |\top| &= 1, \\ |\perp| &= 1, \\ |\ulcorner A \wedge B \urcorner| &= |A| + |B| + 1, \\ |\ulcorner A \vee B \urcorner| &= |A| + |B| + 1, \\ |\ulcorner \neg A \urcorner| &= |A| + 1. \end{aligned}$$

[or *something* like that, with the corners placed correctly!]

Define a translation which eliminates disjunction from Boolean expressions by the following recursion:

$$\begin{aligned} tr(a) &= a, \quad tr(\top) = \top, \quad tr(\perp) = \perp, \\ \ulcorner tr(A \wedge B) \urcorner &= tr(A) \wedge tr(B), \\ tr(A \vee B) &= \neg(\neg tr(A) \wedge \neg tr(B)), \\ tr(\neg A) &= \neg tr(A). \end{aligned}$$

Prove by structural induction on Boolean propositions that

$$|\ulcorner tr(A) \urcorner| \leq 3|A| - 1,$$

for all Boolean propositions  $A$ .

The above use of corner quotes illustrates how there is no restriction that says that the scope of the corner quotes has to live entirely inside a single formula. I use corner quotes in what follows, but (although—I *think*—I have put them in correctly) they can be inserted correctly in more than one way.

### The Proof by Structural Induction

We aspire to prove by structural induction on the recursive datatype of formulæ that

$$(\forall A)(|tr(A)| \leq 3 \cdot |A| - 1)$$

The base case we verify easily. The induction step has three cases

$\neg$  If  $|tr(A)| \leq 3 \cdot |A|$  what is  $|tr(\neg A)|$ ?  $|tr(\neg A)| = |\neg tr(A)|$  so  $|tr(\neg A)| = |tr(A)| + 1$  which is certainly  $\leq 3 \cdot |tr(\neg A)|$ .

$\wedge$  If  $|tr(A)| \leq 3 \cdot |A|$  and  $|tr(B)| \leq 3 \cdot |B|$  what is  $|tr(A \wedge B)|$ ?  $|tr(A \wedge B)|$  is  $|tr(A) \wedge tr(B)|$ . By induction hypothesis  $|tr(A)| \leq 3 \cdot |A| - 1$  and  $|tr(B)| \leq 3 \cdot |B| - 1$  so  $|tr(A) \wedge tr(B)| \leq (3 \cdot |A| - 1) + (3 \cdot |B| - 1) + 1$ . The final '+1' is for the ' $\wedge$ '. This rearranges to

$$|tr(A) \wedge tr(B)| \leq 3 \cdot (|A| + |B|) - 1$$

but  $|A| + |B| \leq |A \wedge B|$  whence

$$|tr(A) \wedge tr(B)| \leq 3 \cdot (|A \wedge B|) - 1$$
 and finally

$$|tr(A \wedge B)| \leq 3 \cdot (|A \wedge B|) - 1.$$

$\vee$  If  $|tr(A)| \leq 3 \cdot |A|$  and  $|tr(B)| \leq 3 \cdot |B|$  what is  $|tr(A \vee B)|$ ?  $|tr(A \vee B)|$  is  $|tr(\neg(\neg tr(A) \wedge \neg(tr(B))))|$ . What is the length of this last expression? Clearly it's going to be  $|tr(A)| + |tr(B)| + 1$  for the outermost ' $\neg$ ' + one for the ' $\neg$ ' attached to  $tr(A)$  + one for the ' $\neg$ ' attached to  $tr(B)$  + one for the ' $\wedge$ ' ... giving  $|tr(A)| + |tr(B)| + 4$ . By induction hypothesis  $|tr(A)| \leq 3 \cdot |A| - 1$  and  $|tr(B)| \leq 3 \cdot |B| - 1$  so we have

$$|tr(A \vee B)| \leq (3 \cdot |A| - 1) + (3 \cdot |B| - 1) + 4.$$
 We can rearrange this to

$$|tr(A \vee B)| \leq 3 \cdot (|A| + |B|) - 1 - 1 + 4$$
 and further to

$$|tr(A \vee B)| \leq 3 \cdot (|A| + |B|) + 2.$$

Now  $|A| + |B| = |A \vee B| - 1$  so we can substitute getting

$$|tr(A \vee B)| \leq 3 \cdot (|A \vee B| - 1) + 2$$
 and rearrange again to get

$$|tr(A \vee B)| \leq 3 \cdot |A \vee B| - 1$$
 as desired.

A final thought ... I wouldn't mind betting that quite a lot of thought went into this question. We've proved  $|tr(A)| \leq 3 \cdot |A| - 1$  so we've certainly also proved the weaker claim  $|tr(A)| \leq 3 \cdot |A|$ . However wouldn't stake my life on our ability to prove the weaker claim by induction. You might like to try ... i'm not going to!

## Exercises 41, 42, 43 and 44

This is just a jumbled discussion at the moment, not a suite of answers.

In the classical setting one takes a propositional valuation—a function  $\text{atoms} \rightarrow \text{bool}$ —and “extends” it (“by abuse of notation”) to a function defined on complex expressions. This is all right because one can safely conceal the evaluation process. If the functions are partial then one needs to make explicit the recursion that takes a time  $t$  and returns the estimate-at-time- $t$  of the truth-value.

Let  $v$  be a valuation, a function with values in  $\text{bool}$  defined only on atomics. We define

$E_s(A, v, 0) = E_l(A, v, 0) = v(A)$   
and thereafter

$E_s((A \wedge B), v, t + 1) = E_s((A), t) \wedge E_s(B, v, t)$   
 $E_s((A \vee B), v, t + 1) = E_s((A), v, t) \vee E_s(B, v, t)$   
 $E_s((\neg A), v, t + 1) = \neg E_s(A, t)$

where the connectives in the definiens are interpreted strictly, more explicitly:

$E_s((A \wedge B), v, t + 1) =$  if  $E_s(A, v, t) = \text{false}$  then if  $E_s(B, v, t) = \text{false}$  then false else  
if  $E_s(A, v, t) = \text{false}$  then if  $E_s(B, v, t) = \text{true}$  then false else  
if  $E_s(A, v, t) = \text{true}$  then if  $E_s(B, v, t) = \text{false}$  then false else  
if  $E_s(A, v, t) = \text{true}$  then if  $E_s(B, v, t) = \text{true}$  then true else undefined

$E_s((A \vee B), v, t + 1) =$  if  $E_s(A, v, t) = \text{true}$  then if  $E_s(B, v, t) = \text{false}$  then true else  
if  $E_s(A, v, t) = \text{true}$  then if  $E_s(B, v, t) = \text{true}$  then true else  
if  $E_s(A, v, t) = \text{false}$  then if  $E_s(B, v, t) = \text{false}$  then false else  
if  $E_s(A, v, t) = \text{false}$  then if  $E_s(B, v, t) = \text{true}$  then true else undefined

## Exercise 61

We (the match referee) start with a matrix, and delete rows or columns when dominance allows us to, and we continue until no more deletions are possible. It might be that at some stage(s) there is more than one row (or column) that can be deleted, or perhaps a stage at which both a row and a column are delete-able. Is the outcome affected by the order in which we perform these deletions?

One column dominates a second column iff at every row the entry in the first column is at least as big as the entry in the second column. (And of course the same goes for two rows *mutatis mutandis* ...). This means that if one column dominates another it will continue to do so even if some rows are deleted. This means that if a chance ever arises to delete a particular column then *that chance remains on the table whatever else we do*. So we can postpone any deletion as long as we like. (This is helpful because of course there are occasions where a chance to delete a particular column cannot arise until a particular row has been deleted.) This means that, should we ever reach a stage where no more deletions can be performed, this can only be because all deletions that ever

became possible have been performed. And that uniquely characterises our destination.

The fact that deletion-possibilities remain permanently open is what ensures confluence. Your sequence-of-deletion strategies might diverge, but the permanent-possibility feature ensure that all such strategies can rejoin.

But wait! How can we be sure that a deletion possibility that arises down one path will also arise down any other? This isn't a problem: think about the possibilities in front of your eyes at the stage where the two paths part company.

What happens if your matrix has infinitely many rows and columns? In those circumstances you have the possibility that your dependency relation between deletions ("I can't delete column  $c$  until I have deleted row  $r$ ; I can't delete row  $r$  until I have deleted column  $c'$ ; I can't delete column  $c'$  until I have deleted row  $r'$ ; I can't delete row  $r'$  until I have deleted column  $c'' \dots$ ") might not be wellfounded.

But that's for later!<sup>1</sup>

### Question 7.17

Show that  $\bigcup_{n \in \mathbb{N}} R^n$  is the smallest transitive relation extending  $R$ .

To do this it will be sufficient to show

1.  $\bigcup_{n \in \mathbb{N}} R^n$  is transitive;
2. If  $S$  is a transitive relation  $\supset R$  then  $\bigcup_{n \in \mathbb{N}} R^n \subseteq S$ .

For (1) We need to show that if  $\langle x, y \rangle$  and  $\langle y, z \rangle$  are both in  $\bigcup_{n \in \mathbb{N}} R^n$  then  $\langle x, z \rangle \in \bigcup_{n \in \mathbb{N}} R^n$ . If  $\langle x, y \rangle \in \bigcup_{n \in \mathbb{N}} R^n$  then  $\langle x, y \rangle \in R^k$  for some  $k$  and if  $\langle y, z \rangle \in \bigcup_{n \in \mathbb{N}} R^n$  then  $\langle y, z \rangle \in R^j$  for some  $j$ . Then  $\langle x, z \rangle \in R^{j+k} \subseteq \bigcup_{n \in \mathbb{N}} R^n$ .

For (2) Let  $S \supset R$  be a transitive relation. So  $R \subseteq S$ . We prove by induction on  $\mathbb{N}$  that for all  $n \in \mathbb{N}$ ,  $R^n \subseteq S$ . Suppose  $R^n \subseteq S$ . Then

$$R^{n+1} = R^n \circ R \subseteq^{(a)} S \circ R \subseteq^{(b)} S \circ S \subseteq^{(c)} S.$$

- (a) and (b) hold because  $\circ$  is *monotone*: if  $X \subseteq Y$  then  $X \circ Z \subseteq Y \circ Z$ .  
 (c) holds because  $S$  is transitive.

---

<sup>1</sup>By which I mean: *not in these notes*.

**Question 7.20**

Let  $R$  and  $S$  be equivalence relations. We seek the smallest equivalence relation that is a superset of  $R \cup S$ . We'd better note first that this really is well defined, and it is, because being-an-equivalence-relation is the conjunction of three properties all of them intersection closed, so it is itself intersection-closed.

This least equivalence relation extending  $R \cup S$  is at least transitive, so it must be a superset of  $t(R \cup S)$ , the transitive closure of  $R \cup S$ . Wouldn't it be nice if it actually were  $t(R \cup S)$ ? In fact it is, and to show this it will be sufficient to show that  $t(R \cup S)$  is an equivalence relation. Must check: transitivity, reflexivity and symmetry. Naturally  $t(R \cup S)$  is transitive by construction.  $R$  and  $S$  are reflexive so  $R \cup S$  is reflexive. In constructing the transitive closure we add new ordered pairs but we never add ordered pairs with components we haven't seen before. This means that we never have to add any ordered pairs  $\langle x, x \rangle$  because they're all already there. Therefore  $t(R \cup S)$  is reflexive as long as  $R$  and  $S$  are. Finally we need to check that  $t(R \cup S)$  is symmetrical. The transitive closure of a symmetrical relation is also symmetrical. First we show by induction on  $n$  that  $R^n$  is symmetrical as long as  $R$  is. Easy when  $n = 1$ . Suppose  $R^n$  is symmetrical: i.e.,  $R^n = (R^n)^{-1}$ .  $R^{n+1} = R \circ R^n$  anyway. The inverse of this is  $(R^{-1})^n \circ R^{-1}$ .  $(R^{-1})^n$  is of course  $R^{-n}$ , so  $(R^{-1})^n \circ R^{-1}$  is  $(R^{-n}) \circ R^{-1}$ .  $R^{-n} = R^n$  by induction hypothesis so  $(R^{-1})^n \circ R^{-1}$  is  $R^n \circ R$  which is of course  $R^{n+1}$ . Then the union of a lot of symmetrical relations is symmetrical, so the transitive closure (which is the union of all the (symmetrical) iterates of  $R$ ) is likewise symmetrical.

Actually we can give another—perhaps simpler—proof of this.  $t(R) = \bigcap \{S : R \subseteq S \wedge S^2 \subseteq S\}$ , or  $\bigcap X$  for short. Notice that  $R$  is symmetrical, then  $X$  is closed under taking inverses (the inverse of anything in  $X$  is also in  $X$ ). And clearly the intersection of a class closed under taking inverses is symmetrical.

**Question 7.2**

Show that if  $R$  and  $S$  are transitive relations, so is  $R \cap S$ .

I take it we are all agreed that if  $X \subseteq Y$  and  $X' \subseteq Y'$  then  $X \circ X' \subseteq Y \circ Y'$ . Applying this to  $R \cap S \subseteq R$  and  $R \cap S \subseteq S$  gives us the two inclusions

$$(R \cap S) \circ (R \cap S) \subseteq R \circ R \subseteq R$$

$$(R \cap S) \circ (R \cap S) \subseteq S \circ S \subseteq S$$

whence

$$(R \cap S) \circ (R \cap S) \subseteq R \cap S$$

as desired.

**Notice that the same argument shows that the intersection of any number of transitive relations is a transitive relation: i.e., transitivity is an intersection closed property of relations.**

**Question 7.3**

Let  $R$  be a relation on  $A$ . ( $'r'$ ,  $'s'$  and  $'t'$  denote the reflexive, symmetric and transitive closure operations respectively.)

1. Prove that  $rs(R) = sr(R)$ .
2. Does  $R$  transitive imply  $s(R)$  transitive?
3. Prove that  $rt(R) = tr(R)$  and  $st(R) \subseteq ts(R)$ .
4. If  $R$  is symmetrical must the transitive closure of  $R$  be symmetrical? Prove or give a counterexample.
5. Think of a binary relation  $R$ , and of its graph, which will be a directed graph  $\langle V, E \rangle$ . On any directed graph we can define a relation “I can get from vertex  $x$  to vertex  $y$  by following directed edges” which is certainly transitive, and we can pretend it is reflexive because after all we can get from a vertex to itself by just doing nothing at all. Do this to our graph  $\langle V, E \rangle$ , and call the resulting relation  $S$ . How do we describe  $S$  in terms of  $R$ ?

(a) Prove that  $rs(R) = sr(R)$ :

$$\begin{aligned}
 r(s(R)) &= s(R) \cup I \\
 &= (R \cup R^{-1}) \cup I \\
 &= (R \cup I) \cup (R^{-1} \cup I) \\
 &= (R \cup I) \cup (R^{-1} \cup I^{-1}) \\
 &= (R \cup I) \cup (R \cup I)^{-1} \\
 &= s(r(R))
 \end{aligned}$$

(b) The symmetric closure of a transitive relation is not automatically transitive: take  $R$  to be set inclusion on a power set.

(c) Prove that  $rt(R) = tr(R)$ :

$$\begin{aligned}
 r(t(R)) &= t(R) \cup I = R \cup R^2 \cup \dots R^n \dots \cup I \\
 &= (R \cup I) \cup (R^2 \cup I) \cup (R^n \cup I) \dots
 \end{aligned}$$

At this point it would be nice to be able to say  $(R^n \cup I) = (R \cup I)^n$  but this isn't true.  $(R \cup I)^n$  is actually  $R \cup R^2 \dots R^n \cup I$ . But this is enough to rewrite the last line as

$$(R \cup I) \cup (R \cup I)^2 \cup (R \cup I)^3 \dots$$

which is of course  $t(r(R))$  as desired.

The transitive closure of a symmetrical relation is also symmetrical. First we show by induction on  $n$  that  $R^n$  is symmetrical as long as  $R$  is. Easy when  $n = 1$ . Suppose  $R^n$  is symmetrical.  $R^{n+1} = R \circ R^n$ . The inverse of this is  $(R^{-1})^n \circ R^{-1}$  which by induction hypothesis is  $R^n \circ R$  which is of course  $R^{n+1}$ . Then the union of a lot of symmetrical relations is symmetrical, so the transitive closure (which is the union of all the (symmetrical) iterates of  $R$  is likewise symmetrical.

Finally  $S$  is the reflexive transitive closure of  $R$ .

**Question 7.5**

Show that—at least if  $(\forall x)(\exists y)(\langle x, y \rangle \in R) \rightarrow R \circ R^{-1}$  is a fuzzy.  
What about  $R \cap R^{-1}$ ? What about  $R \cup R^{-1}$ ?

If  $\langle x, y \rangle \in R$  then  $\langle y, x \rangle \in R^{-1}$  so  $\langle x, x \rangle \in R \circ R^{-1}$ .

That takes care of reflexivity. Suppose  $\langle x, z \rangle \in R \circ R^{-1}$ . Then there is a  $y$  such that  $\langle x, y \rangle \in R$  and  $\langle y, z \rangle \in R^{-1}$ . But then  $\langle z, y \rangle \in R$ . So  $\langle x, z \rangle \in R \circ R^{-1}$  is the same as  $(\exists y)((\langle x, y \rangle \in R) \wedge (\langle z, y \rangle \in R))$ . But this is clearly symmetric in  $x$  and  $z$ , so we can rearrange it to get  $(\exists y)((\langle y, x \rangle \in R^{-1}) \wedge (\langle z, y \rangle \in R))$  which is  $\langle z, x \rangle \in R \circ R^{-1}$  as desired.

$R \cup R^{-1}$  is the symmetric closure of  $R$  and is of course symmetric, but there is no reason to expect it to be reflexive: it'll be reflexive iff  $R$  is reflexive.

**Question 7.6**

Given any relation  $R$  there is a least  $T \supseteq R$  such that  $T$  is transitive, and a least  $S \supseteq R$  such that  $S$  is symmetrical, namely the transitive and symmetric closures of  $R$ . Must there also be a maximal  $S \subseteq R$  such that  $S$  is transitive? And must there be a maximal  $S \subseteq R$  such that  $S$  is symmetrical? The answer to one of these last two questions is 'yes': find a cute formulation.

$R \cap R^{-1}$  is the largest symmetrical relation included in  $R$ . The unwary sometimes think *this* is the symmetric closure of  $R$ . The point is that altho' being-the-complement-of-a-transitive-relation is not an intersection-closed property, nevertheless being-the-complement-of-a-symmetric-relation **is** intersection-closed, since it is the same as being symmetric.  $R \cap R^{-1}$  is the complement of the symmetric closure of the complement of  $R$ . Do not confuse complements with converses!!

**Question 7.9**

If  $x \leq S(y)$  and  $y \leq S(x)$  then  $x$  and  $y$  are neighbouring naturals. This is  $R \cap R^{-1}$ .  $x$  and  $y$  are related by the transitive closure of this relation iff there is a finite sequence  $x_0, x_1, x_2 \dots x_n = y$  such that each  $x_i$  is adjacent to  $x_{i+1}$ . But clearly any two naturals are connected by such a chain, so the transitive closure is the universal relation. For part 2, remember that  $x$  is related to  $y$  by  $R \setminus R^{-1}$  if it is related to  $y$  by  $R$  but not by  $R^{-1}$ . In this case that means  $x \leq S(y) \wedge y \not\leq S(x)$ . This is  $x \leq S(y) \wedge S(x) < y$ . The second conjunct implies the first so we can drop the first, getting  $S(x) < y$ . Getting the transitive closure of this is easy, 'cos it's transitive already!

**Question 7.10**

Are the two following conditions on partial orders equivalent?

1.  $(\forall xyz)(z > x \not\leq y \not\leq x \rightarrow z < y)$

2.  $(\forall xyz)(z > x \not\leq y \not\leq x \rightarrow z > y)$ .

Assume (i)  $(\forall xyz)(z \leq x \not\leq y \not\leq x \rightarrow z \leq y)$  and aim to deduce (ii)  $(\forall xyz)(z \geq x \not\leq y \not\leq x \rightarrow z \geq y)$ . To this end assume  $z \geq x$ ,  $x \not\leq y$  and  $y \not\leq x$  and hope to deduce  $z \geq y$ .

$x \leq z$  tells us that  $z \not\leq y$  for otherwise  $x \leq y$  by transitivity, contradicting hypothesis. Next, assume the negation of what we are trying to prove. This gives us  $y \not\leq z$ . But then we have  $y \not\leq z \not\leq y$  and  $x \leq z$  so by (i) we can infer  $x \leq y$ , contradicting assumption.

I think the proof in the other direction is similar but i haven't checked it.

For the record: to any partial order there corresponds in a obvious way a strict partial order. (like  $\leq$  and  $<$  on  $\mathbb{N}$ , for example.) Consider the strict partial order corresponding to a partial order satisfying this condition we have just been discussing. If it is wellfounded it is said to be a **prewellordering**. This is because we can think of it as a total ordering of the equivalence classes (under the relation  $x \simeq y$  iff  $x = y \vee x \not\leq y \not\leq x$ ), and if  $<$  is wellfounded this in fact a wellordering of the equivalence classes.

### Question 7.12

Show that  $R \subseteq S$  implies  $R^{-1} \subseteq S^{-1}$

The way to do this is to assume that  $R \subseteq S$  and let  $\langle x, y \rangle$  be an arbitrary ordered pair in  $R^{-1}$ . We then want to infer that  $\langle x, y \rangle$  is in  $S^{-1}$ .

If  $\langle x, y \rangle$  is in  $R^{-1}$  then  $\langle y, x \rangle$  is in  $R$ , because  $R^{-1}$  is precisely the set of ordered pairs  $\langle x, y \rangle$  such that  $\langle y, x \rangle$  is in  $R$ . (We would write this formally as:  $R^{-1} = \{\langle x, y \rangle : \langle y, x \rangle \in R\}$ .) But  $R \subseteq S$ , so  $\langle y, x \rangle$  is in  $S$ , and so (flip things round again)  $\langle x, y \rangle$  is in  $S^{-1}$ .

Notice that to tell this story successfully we have to come out of the closet and think of  $R$  and  $S$  as sets of ordered pairs, that is, as relations-in-extension.

### Question 47.2

The lexicographic order on  $\mathbb{N}^2$  is wellfounded, so we can do wellfounded induction on it. This means that if we can prove that, if every ordered pair below  $p$  has some property  $\phi$  then the pair  $p$  has property  $\phi$  as well, then every ordered pair in  $\mathbb{N}^2$  has that property.

Now let  $\phi(\langle x, y \rangle)$  say that if the bag is started with  $x$  black balls and  $y$  white balls in it the process will eventually halt with only one ball in the bag. Suppose  $\phi(\langle x', y' \rangle)$  holds for every  $\langle x', y' \rangle$  below  $\langle x, y \rangle$  in the lexicographic product  $\mathbb{N}^2$ . We want to be sure that if the bag is started with  $x$  black balls and  $y$  white balls in it the process will eventually halt with only one ball in the bag. The first thing that happens is that we pick two balls out of the bag and the result is that at the next stage we have either  $x - 2$  black balls and an unknown number of white balls, or we have  $x$  black balls and  $y - 1$  white balls. But both these situations are described by ordered pairs below  $\langle x, y \rangle$  in the lexicographic product  $\mathbb{N}^2$ , so by induction hypothesis we infer that if the bag is started with



$x$  black balls and  $y$  white balls in it the process will eventually halt with only one ball in the bag, as desired.

### Question 7.??

**Everybody loves my baby**, so in particular my baby loves my baby. **My baby loves nobody but me**. That is to say, if  $x$  is loved by my baby, then  $x = \text{me}$ . So my baby = me.

### Question ??18a

The answer is the relation that holds between  $k$  and  $k + 1$  for  $0 \leq k < n$  and between  $n$  and 0.

### Question ??28

Paula Buttery's answer to one of the fiddly ones.

```
- fun f g b a = g a b;
val f = fn : ('a -> 'b -> 'c) -> 'b -> 'a -> 'c
- fun ff g = let fun fa a = let val (b,c) = g a in b end;
= fun fe a = let val (b,c) = g a in c end;
= in (fa, fe) end;
val ff = fn : ('a -> 'b * 'c) -> ('a -> 'b) * ('a -> 'c)
-
```

### Question ??27

Show that the largest and smallest elements of a totally ordered set with  $n$  elements can be found with  $\lceil 3n/2 \rceil - 1$  comparisons if  $n$  is odd, and  $3n/2 - 2$  comparisons if  $n$  is even.

First check this for a few small values. If  $n = 2$  we need 1, for  $n = 3$  we need 3, for  $n = 4$  we need 4.

The induction step requires us to show that adding two more elements to a set requires us to perform no more than three extra comparisons.

So suppose we have a set  $X$  with  $n$  members, and we have found the top and bottom elements in  $3n/2 - 1$  comparisons. Call them  $t$  and  $b$ . Let the two new elements be  $x$  and  $y$ . With one comparison we can find out which is bigger. Without loss of generality suppose it is  $x$ . Compare  $x$  with  $t$  to find the biggest element of  $X \cup \{x, y\}$ , and compare  $y$  with  $b$  to find the smallest. This has used three extra comparisons.

### Question ??32

The exponent on the LHS is  $x^{x^{x^{x^{x^{\dots}}}}}$  which is 2, so  $x^2 = 2$  and  $x = \sqrt{2}$ . That was easy. The problem with this is that the second equation gives  $x^4 = 4$  and thence  $x = \sqrt{2}$  again. They can't both be right!

Of course the answer is that the reasoning that led us to conclude that  $x = \sqrt{2}$  in the first place doesn't prove that that is the answer. All we have done is show that **if** there is a solution it must be  $\sqrt{2}$ . We haven't shown that there **is** a solution. In fact it is a simple matter to show by induction that the approximants to the LHS, which we generate as follows

$$a_0 =: \sqrt{2}; \quad a_{n+1} =: \sqrt{2}^{a_n}$$

... are all less than 2. So the sequence has a limit which is  $\leq 2$ .

Let's see what we can do that is more general.

Let  $F(x) =_{df} x^{x^{x^{x^{x^{\dots}}}}}$ .

We have  $x^{F(x)} = F(x)$ . The inverse to this function is the function  $\lambda x. x^{1/x}$ . This is much easier to understand. For example we can differentiate it. It is the same as  $e^{(\log x)/x}$  whose differential is of course  $e^{(\log x)/x} \cdot (1/x^2 - (\log x)/x^2)$ . This is zero when  $x = e$ , and this is clearly a maximum. The fact that the differential is zero there of course means that  $F$  reaches a maximum at  $e^{1/e}$  and that  $F'(e^{1/e})$  is infinite. This gives us the amusing but (as far as I know) useless fact that

$$(e^{1/e})^{(e^{1/e})^{(e^{1/e})^{(e^{1/e})^{(e^{1/e})^{\dots}}}}}} = e$$

(Check this: if the LHS is to evaluate to  $x$  we must have  $(e^{1/e})^x = x$  and  $e$  is certainly a solution to this equation.)

We can get a power series expansion of  $F$  for values of  $x$  not much bigger than 1. Let  $\Sigma$  be the power series for  $F(1+x)$ . Then we have

$$(1+x)^\Sigma = \Sigma$$

and we can use the binomial theorem to expand the left hand side. This gives us a sequence of equations expressing later coefficients of  $\Sigma$  in terms of earlier coefficients in a wellfounded way. I haven't worked out the general formula for  $a_n$  the coefficient of  $x^n$  in  $F(1+x)$  tho' in principle it could be done. ( $a_0 = 1$  for a start!)

### Question ??37

Let  $m = |F|$  and  $p = |\bigcup F|$ . Let  $C = \{\langle x, A \rangle : x \in A \in F\}$ .

Given  $x \in \bigcup F$ , pick  $B \in F$  with  $x \in B$ . Let  $Y_x = \{A \in F : x \in A\}$  and  $N_x = \{A \in F : x \notin A\}$ . The map  $\lambda A. (A \Delta B)$  permutes  $F$  and swaps  $Y_x$  and  $N_x$ . Hence  $|Y_x| = |N_x| = m/2$ .

So  $|C| = (1/2)mp$ , as each  $x$  is in exactly  $m/2$   $A$ 's. But each  $A$  contains  $\leq k$  things, and one  $A$  contains none at all, so  $|C| \leq (m-1)k$  whence  $p \leq \frac{m-1}{m} \cdot 2k < k$ .

# Bibliography

- [1] Jorge Luis Borges “Siete Noches”
- [2] Lewis Carroll “Through the Looking-Glass and what Alice found there”
- [3] Martin Gardner
- [4] Martin Gardner “The Annotated Alice”
- [5] Conway, Berlekamp and Guy, Winning Ways, Academic Press 1982
- [6] Edgar G. Goodaire, Michael M. Parmenter “Discrete Mathematics with Graph Theory” (second edition). Prentice-Hall 2002 ISBN 0-13-092000-2
- [7] Girard, Lafont and Taylor “Proofs and Types” Cambridge University Press (1989)
- [8] Guillermo Owen: *Game theory*
- [9] Discrete Mathematical Structures. D.S. Malik and M.K. Sen. Thomson Course technology ISBN 0-619-21285-3 with software ISBN 0-619-21558-5 without software ISBN
- [10] Quine, W.v.O., Mathematical Logic
- [11] Quine, W.V. (1962) Mathematical Logic (revised edition) Harper torch-books 1962
- [12] Oliver Sacks “The man who mistook his wife for a hat” Picador 1985



## Chapter 9

# Discussion answers to old tripos questions

### 1988:6:9E (maths tripos)

The Master asked  $2n + 1$  people and got  $2n + 1$  different answers. Since the largest possible answer is  $2n$  and the smallest is 0, there are in fact precisely  $2n + 1$  possible answers and that means he has got every possible answer from 0 up to  $2n$  inclusive.

Think about the person who shook  $2n$  hands. This person shook hands with everyone that they possibly could shake hands with : that is to say everyone except their spouse. So everybody except their spouse shook at least one hand. So their spouse shook no hands at all. Thus the person who shook  $2n$  hands and the person who shook 0 hands are married. Henceforth disregard these two people and their handshakes and run the same argument to show that the person who shook  $2n - 1$  hands and the person who shook 1 hands are married. And so on.

Where does this get us? It tells us, after  $n$  iterations, that the person who shook  $n + 1$  hands and the person who shook  $n - 1$  hands are married. So what about the person who shook  $n$  hands, the odd man out? Well, it must be the odd *woman* out, because the only person of whom the Master asks this question who isn't married to another person of whom the Master asks this question is his wife.

Let's name people (other than the Master) with the number of hands they shook. (This is ok since they all shook different numbers of hands.)  $2n$  didn't shake hands with its spouse, or itself, and there are only  $2n$  people left, so it must have shaken hands with all of them, in particular with the Master. Correspondingly 0 didn't shake hands with anyone at all, so it certainly didn't shake hands with the Master. We continue reasoning in this way, about  $2n - 1$  and 1.  $2n - 1$  didn't shake hands with itself or its spouse or with 0, and that leaves only  $2n - 1$  people for it to shake hands with and since it shook  $2n - 1$  hands it must have shaken all of them, so in particular it must have shaken

hands with the Master. Did 1 shake hands with the Master? No, because 1 shook only one hand, and that must have been  $2n - 1$ 's. And so on. The people who shook the Master's hand were  $2n, 2n - 1, 2n - 2 \dots n + 1$  and the people who didn't were  $1, 2, 3, \dots n - 1$ . [or do i mean 'n'?] And of course, the Master's wife. So he shook  $n$  hands.

See also

[https://www.dpmms.cam.ac.uk/~tf/cam\\_only/keeping\\_out\\_of\\_mischief.htm](https://www.dpmms.cam.ac.uk/~tf/cam_only/keeping_out_of_mischief.htm)

### 1988:6:10E (maths tripos)

Let  $R$  be a relation on a set  $X$ . Define the reflexive, symmetric and transitive closures  $r(R)$ ,  $s(R)$  and  $t(R)$  of  $R$ . Let  $\Delta$  be the relation  $\{\langle x, x \rangle : x \in X\}$ . Prove that

1.  $R \circ \Delta = R$
2.  $(R \cup \Delta)^n = \Delta \cup (\bigcup_{i \leq n} R^i)$  for  $n \geq 1$
3.  $tr(R) = rt(R)$ .

Show also that  $st(R) \subseteq ts(R)$ .

If  $X = \mathbb{N}$  and  $R = \Delta \cup \{\langle x, y \rangle : y = px \text{ for some prime } p\}$  describe  $st(R)$  and  $ts(R)$ .

The reflexive (symmetric, transitive) closure of  $R$  is the intersection of all reflexive (symmetric, transitive) relations of which  $R$  is a subset.

1.  $R\Delta$  is  $R$  composed with the identity relation.  $x$  is related to  $y$  by  $R$ -composed-with- $S$  if there is  $z$  such that  $x$  is related to  $z$  by  $R$ , and  $z$  is related to  $y$  by  $S$ . Thus  $R\Delta = R$ . (I would normally prefer to write ' $R \circ \Delta$ ' here, using a standard notation for composition of relations: ' $\circ$ ')
2. It is probably easiest to do this by induction on  $n$ . Clearly this is true for  $n = 1$ , since the two sides are identical in that case. Suppose it is true for  $n = k$ .

$$(R \cup \Delta)^k = \Delta \cup (\bigcup_{1 \leq i \leq k} R^i)$$

$(R \cup \Delta)^{k+1} = (R \cup \Delta)^k \circ (R \cup \Delta)$ . By induction hypothesis this is

$$(\Delta \cup (\bigcup_{1 \leq i \leq k} R^i)) \circ (R \cup \Delta)$$

Now  $(A \cup B) \circ (C \cup D)$  is clearly  $(A \circ C) \cup (A \circ D) \cup (B \circ C) \cup (B \circ D)$  and applying this here we get

$$(\Delta \circ R) \cup (\Delta \circ \Delta) \cup ((\bigcup_{1 \leq i \leq k} R^i) \circ R) \cup ((\bigcup_{1 \leq i \leq k} R^i) \circ \Delta)$$

Now  $\Delta \circ R$  is  $R$ ;  $\Delta \circ \Delta$  is  $\Delta$ ;  $(\bigcup_{1 \leq i \leq k} R^i) \circ \Delta$  is  $\bigcup_{1 \leq i \leq k} R^i$  and  $(\bigcup_{1 \leq i \leq k} R^i) \circ R$  is  $(\bigcup_{1 < i \leq k+1} R^i)$  so we get

$$R \cup \Delta \cup (\bigcup_{1 < i \leq k+1} R^i) \cup (\bigcup_{i \leq k} R^i)$$

which is

$$\Delta \cup \bigcup_{1 \leq i \leq k+1} R^i$$

3. The transitive closure of the reflexive closure of  $R$  is the transitive closure of  $R \cup \Delta$  which is  $\bigcup_{n \in \mathbb{N}} (R \cup \Delta)^n$  which (as we have—more-or-less—just proved) is  $\Delta \cup (\bigcup_{i \in \mathbb{N}} R^i)$  which is the reflexive closure of the transitive closure of  $R$ .

$s$  is *increasing* so  $R \subseteq s(R)$ .  $t$  is *monotone*, so  $t(R) \subseteq t(s(R))$ . But the transitive closure of a symmetrical relation is symmetrical so  $t(R) \subseteq t(s(R))$  implies  $s(t(R)) \subseteq t(s(R))$  as desired.

Finally if  $X = \mathbb{N}$  and  $R = \Delta \cup \{(x, y) : y = px \text{ for some prime } p\}$  then  $st(R)$  is the relation that holds between two numbers when they are identical or one is a multiple of the other, and  $ts(R)$  is the universal relation  $\mathbb{N} \times \mathbb{N}$ .

### 1990:1:9

Peter Dickman's model answer

We are asked to use generating functions to prove that:

$$c_n = \frac{1}{n} \binom{2n-2}{n-1}$$

where  $c_n$  is the number of binary trees with  $n$  leaves (NB not  $n$  vertices) where no vertex has precisely one descendent. Now the formula given is remarkably similar to the one for Catalan numbers – which were introduced in the section of the course concerned with generating functions. So these may well be useful in answering this question.

Recall that for Catalan numbers:

$$C_n = \frac{1}{n+1} \binom{2n}{n}$$

so it is (hopefully) clear that  $C_n = c_{n+1}$ .

To use generating functions it is necessary to find a recurrence relation. . .

Consider trees of the form described in the question. Clearly, any such tree which has more than one leaf can be viewed as being composed of two trees joined together by a single (new) root vertex, whose descendents are the two

roots of the component smaller trees. Now the sum total of leaves in these subtrees will be the same as the number of leaves in the composite; and each tree will have at least one leaf. So, the number of trees with some given number of leaves can be determined by considering all of the ways such a tree can be split into left & right subtrees, and the parts combined together.

It follows that:

$$\forall n \geq 1 : c_{n+1} = c_1 c_n + c_2 c_{n-1} + c_3 c_{n-2} + \dots + c_n c_1$$

Note that we have  $n \geq 1$  in the above, because the equation is giving us an expression for  $n + 1$ . The recurrence only holds for the trees with two or more leaves (as we assumed that the root had two descendents).

Also we know that  $c_1 = 1$  by inspection.

Note that I've written this out for the case  $n + 1$  not, as I would normally do, the case  $n$  because it makes everything neater later. The result can be achieved from the  $n$  case but is a bit messier. The only hint I can give as to how to tell that this is helpful **in advance** is that we already knew that there was an "off by one" effect present in this question.

Now, let us consider  $d_n = c_{n+1}, \forall n \geq 0$ . Then we have that:

$$\forall n \geq 1 : d_n = d_0 d_{n-1} + d_1 d_{n-2} + \dots + d_{n-1} d_0$$

Now, if we define  $d_k = 0, \forall k < 0$  then we have that

$$\forall n \geq 1 : d_n = \sum_{i=0}^{n-1} d_i d_{n-1-i} = \sum_{i=0}^{\infty} d_i d_{n-1-i}$$

Now, the generating function for the  $d_n$ , called  $D(z)$  say, has the property that the coefficient of  $z^n$  in  $D(z)$  is  $d_n$ . So we have that:

$$[z^n]D(z) = \begin{cases} 1 & \text{if } n = 0 \\ \sum_{i=0}^{\infty} d_i d_{n-1-i} & \text{otherwise} \end{cases}$$

Whence we derive:



$$\begin{aligned}
D(z) &= \sum_{n=0}^{\infty} d_n z^n \\
&= 1 + \sum_{n=1}^{\infty} \sum_{i=0}^{\infty} d_i d_{n-1-i} z^n \\
&= 1 + \sum_{n=1}^{\infty} \sum_{i=0}^{\infty} d_i d_{n-1-i} z^i z^{n-1-i} \\
&= 1 + z \sum_{n=1}^{\infty} \sum_{i=0}^{\infty} d_i d_{n-1-i} z^i z^{n-1-i} \\
&= 1 + z \sum_{n=1}^{\infty} \sum_{i=0}^{\infty} d_i z^i \cdot d_{n-1-i} z^{n-1-i} \\
&= 1 + z(D(z))^2
\end{aligned}$$

since the penultimate line is a convolution.

This is a formula we recognise from the Catalan numbers, so we proceed by following the same argument as in the lecture notes...

Reorganising this gives us:

$$z(D(z))^2 - D(z) + 1 = 0$$

Solving this we find that:

$$D(z) = \frac{1 \pm \sqrt{1-4z}}{2z}$$

Since  $d_n$  is non-negative  $\forall n$  and since  $\sqrt{1-4z}$  has only negative signs after the first term we can eliminate the form with an addition in and find:

$$D(z) = \frac{1 - \sqrt{1-4z}}{2z}$$

Which, from a standard binomial identity leads us to:

$$D(z) = \frac{1 - \sqrt{1-4z}}{2z} = \sum_{k \geq 0} \frac{1}{k+1} \binom{2k}{k} z^k$$

So we find that:

$$d_n = [z^n]D(z) = \frac{1}{n+1} \binom{2n}{n}$$

However,  $d_n = c_{n+1}$ ,  $\forall n \geq 0$  therefore we have that:

$$\forall n \geq 1 : c_n = \frac{1}{n} \binom{2n-2}{n-1}$$

as required.

Note that the formula is obviously useless for  $n = 0$  as it would give  $c_0 = \infty$  so we clearly aren't being expected to worry about that case. However it might be worth pointing this out.

The second part of the question asks how many trees of the form considered, with  $n$  leaves, have depth  $n - 1$ . Again let's look for a recurrence relation. I'll skip through this fairly quickly... I suggest that you draw some pictures as you read through this. Be aware of the assumption that  $n > 2$  in the following.

Consider the trees of this form, that have  $n$  leaves and are of depth  $n - 1$ , for arbitrary  $n > 2$ . Given such a tree, let the number of leaves at depth  $n - 1$  (ie the maximal depth) be  $k$ .

From such a tree we can construct  $k$  distinct trees of depth  $n$  which have  $n + 1$  leaves by taking one of the leaves at the  $n - 1$  level and replacing it with a vertex with two descendents, which are themselves leaves.

Now consider a tree of depth  $n$  with  $n + 1$  leaves, satisfying the condition on numbers of descendents. Selecting any leaf at the maximal depth, its parent is at depth  $n - 1$  and, by the condition on numbers of descendents, this has another child at depth  $n$ . Replacing these two leaves and their parent vertex with a single leaf at depth  $n - 1$  we either construct a tree with  $n$  leaves of depth  $n - 1$  (if we have removed the only pair of leaves at the maximal depth) or we have a tree of  $n$  leaves of depth  $n$ .

However the depth of one of our trees must be strictly less than the number of leaves. Assume otherwise, ie that for some such tree, the number of leaves is less than or equal to the depth. Since each 'plucking' operation of the form described above reduces the number of leaves by one and the number of levels by at most one, we would be able to construct a tree with 2 leaves and depth of at least 2 – which is clearly impossible.

So, we have shown that each such tree has precisely 2 leaves at its terminal level, and that the only possible constructions are the  $k$  variants of each of the trees of one smaller size. But  $k$  is the number of leaves at the terminal level *i.e.* 2, so we have a doubling of the number of possible trees at each level. Given that there are  $1 = 2^0$  trees with 2 leaves of depth 1,  $2 = 2^1$  trees with 3 leaves of depth 2 and so forth we have that,

$$(\forall n \geq 2)(\exists 2^{n-2} \text{ trivalent trees with } n \text{ leaves and depth } n - 1)$$

### 1990:1:11

Equivalence relations correspond to partitions. A PER  $\langle X, R \rangle$  that fails to be an equivalence relation features elements  $x \in X$  such that  $\langle x, x \rangle \notin R$ . Such elements are not related to anything at all, since if  $x$  is related to  $y$ , then by symmetry  $y$  is related to  $x$  and by transitivity  $x$  is related to  $x$ .

So we put on one side all the  $x \in X$  such that  $\langle x, x \rangle \notin R$ , leaving behind a subset  $X' \subseteq X$  consisting of all those elements related to themselves by  $R$ . What is the restriction of  $R$  to this set? Clearly it is reflexive. Actually it is transitive and symmetrical as well, because  $X' \times X'$  is transitive and symmetrical, and transitivity and symmetry are intersection-closed properties so  $R \cap (X' \times X')$  will be transitive and symmetrical. So  $R \cap (X' \times X')$  is an equivalence relation on  $X'$ .

How many PER's on a set with 4 elements?

There is one way of throwing away no elements, leaving 4. These can be either

all in one piece	1
one singleton, one triple	4
two pairs	3
two singletons	6
all singletons	1

There are 4 ways of throwing away one element, leaving 3. These can be either

all in one piece	$1 \times 4 = 4$
one singleton, one pair	$3 \times 4 = 12$
three singletons,	$1 \times 4 = 4$

There are 6 ways of throwing away two elements, leaving 2. These can be either

all in one piece	$1 \times 6 = 6$
two singletons	$1 \times 6 = 6$

There are 4 ways of throwing away 3 elements leaving 1.

This can be partitioned in only one way	$1 \times 4 = 4$
	$\overline{52}$

Let us prove that  $T$  is a PER. We first show that it is transitive. Suppose

- (i)  $\langle f, g \rangle \in T$  and
- (ii)  $\langle g, h \rangle \in T$ . We want  $\langle f, h \rangle \in T$ .

By definition of  $T$  we infer

- (iii)  $(\forall x_1, x_2 \in X)(\langle x_1, x_2 \rangle \in R \rightarrow \langle f(x_1), g(x_2) \rangle \in S)$  and
- (iv)  $(\forall x_2, x_3 \in X)(\langle x_2, x_3 \rangle \in R \rightarrow \langle g(x_2), h(x_3) \rangle \in S)$ . (We have relettered variable to make life easier)

Now let  $x_1$  and  $x_3$  be two elements of  $X$  such that  $\langle x_1, x_3 \rangle \in R$ . We want to infer  $\langle f(x_1), g(x_3) \rangle \in S$ .  $R$  is symmetrical so  $\langle x_3, x_1 \rangle \in R$  too. So, by transitivity, we have  $\langle x_1, x_1 \rangle \in R$ . By (iii) we can infer  $\langle f(x_1), g(x_1) \rangle \in S$ . We now use (iv) on our assumption that  $x_1$  and  $x_3$  are two elements of  $X$  such that  $\langle x_1, x_3 \rangle \in R$  to infer that  $\langle g(x_1), h(x_3) \rangle \in S$ . Finally, by transitivity of  $S$ , we infer that  $\langle f(x_1), h(x_3) \rangle \in S$  as desired.

It is much easier to show that  $T$  is symmetric. Suppose  $\langle f, g \rangle \in T$  and let  $x_1$  and  $x_2$  be two elements of  $X$  such that  $\langle x_1, x_2 \rangle \in R$ . We want to infer  $\langle f(x_1), g(x_2) \rangle \in S$ .  $R$  is symmetric, so we infer  $\langle x_2, x_1 \rangle \in R$ , whence  $\langle f(x_1), g(x_2) \rangle \in S$  as desired.

To show that  $T$  is not in general reflexive, even if  $R$  and  $S$  both are, take  $R$  to be the universal relation on  $X$  and  $S$  to be the identity relation on  $Y$ , where both  $X$  and  $Y$  have at least two members.

### 1993:11:11

$\langle A, \leq \rangle$  is a partially ordered set if

1.  $(\forall x, y, z \in A)(x \leq y \rightarrow (y \leq z \rightarrow x \leq z))$  ( $\leq$  is transitive)
2.  $(\forall x, y \in A)(x \leq y \rightarrow (y \leq x \rightarrow x = y))$  ( $\leq$  is antisymmetrical)
3.  $(\forall x \in A)(x \leq x)$  ( $\leq$  is reflexive)

In what follows we write ' $x < y$ ' for ' $x \leq y \wedge y \neq x$ '

(a) If  $\langle A, \leq \rangle$  is to form a totally ordered set then in addition  $\leq$  must satisfy *connexity*.

$$(\forall x, y \in A)(x \leq y \vee y \leq x)$$

or equivalently  $<$  must satisfy *trichotomy*

$$(\forall x, y \in A)(x < y \vee x = y \vee y < x)$$

(b) If  $\langle A, \leq \rangle$  is to be wellfounded then in addition  $<$  (which is the strict version of  $\leq$ , namely  $\{\langle x, y \rangle : x \leq y \wedge x \neq y\}$ ) must satisfy *wellfoundedness*:

$$(\forall A' \subseteq A)(\exists x \in A')(\forall y \in A')(y \not< x)$$

(This *détour* via strict partial orders is necessary because no wellfounded relation can be reflexive.)

(c) If  $\langle A, \leq \rangle$  is to be a complete partially ordered set then one of the following conditions on  $\leq$  must be satisfied, depending on what your definition of complete poset is:

One definition is that every *subset* of  $A$  must have a least upper bound in the sense of  $\leq$ . This is

$$(\forall A' \subseteq A)(\exists x \in A)[(\forall y \in A')(y \leq x) \wedge (\forall z \in A)((\forall y \in A')(y \leq z) \rightarrow x \leq z)]$$

...or that every directed subset of  $A$  has a least upper bound.  $A'$  is a directed subset of  $A$  if  $(\forall x, y \in A')(\exists z \in A')(x \leq z \wedge y \leq z)$ . (They probably don't mean that tho'.)

To show that the restriction of a partial order of  $A$  to some subset  $B$  of  $A$  is a partial order of  $B$  we have to check that  $R \cap (B \times B)$  is reflexive transitive and antisymmetrical. Now  $B \times B$  is reflexive and transitive, as is  $R$ ; reflexivity and transitivity are intersection-closed properties, so  $R \cap (B \times B)$  is reflexive and transitive. To verify antisymmetry we have to check that if  $\langle x, y \rangle$  and  $\langle y, x \rangle$  are both in  $R \cap (B \times B)$  then  $x = y$ . But if  $\langle x, y \rangle$  and  $\langle y, x \rangle$  are both in  $R \cap (B \times B)$  then they are both in  $R$ , and we know  $R$  is antisymmetrical, whence  $x = y$  as desired.

(A deeper proof can be obtained by noting only that all the clauses in the definition of partial order are universal. Any universal sentence true in  $A$  is true in any subset of  $A$ . After all, a universal sentence is true as long as there is no counterexample to it. If  $A$  contains no counterexamples, neither can any subset of  $A$ . This shows that a substructure of a total order is a total order and this is useful later on in the question ...)

**Z** (i)  $\leq$  is a partial order of **Z**. Indeed it is a total order. (ii) It isn't wellfounded (e.g.: no bottom element) nor (iii) is it a complete poset (e.g.: no top element).

Divisibility (i) is not a partial order because for any integer  $n$ ,  $n$  and  $-n$  divide each other but are distinct, so it isn't antisymmetrical. (ii) The relation " $n$  divides  $m$  but not *vice versa*" is wellfounded on **Z** however. If  $X \subseteq \mathbf{Z}$ , then its minimal elements under " $n$  divides  $m$  but not *vice versa*" are precisely the minimal elements of  $\{|n| : n \in X\}$  under " $n$  divides  $m$  but not *vice versa*", and this relation, being a subset of a wellfounded relation (and  $\leq$  is wellfounded on **N**) is itself wellfounded. (iii) **Z** is not a complete poset under divisibility for the same reason as before.

**N**  $\leq$  is a partial order of **N**. Indeed it is a total order. It is also wellfounded but it is not a complete poset (as before)

Divisibility is a partial order on **N** but not a total order, it is wellfounded. This time we do get a complete poset, because everything divides 0.

**N**<sup>+</sup> As for **N** except that it is not a complete poset (e.g.: no top element)

**1994:10:11**

The way to do part 2 is to stop trying to be clever and do it the easy way. Let  $A_n, B_n, C_n$  be the number of valid strings in  $\{A, B, C\}^n$  ending in  $A, B$  and  $C$  respectively. Clearly

$$C_{n+1} = A_n + B_n + C_n$$

and

$$A_{n+1} = B_{n+1} = B_n + C_n$$

This is because if the last character of a legal string is an  $A$  or a  $B$  then the penultimate character cannot be an  $A$ . We are not going to try to do anything clever like *derive* the equality we have been given, but we can at least confirm it! So let's try to simplify

$$2(A_{n+1} + B_{n+1} + C_{n+1}) + A_n + B_n + C_n$$

and hope that it simplifies to  $A_{n+2} + B_{n+2} + C_{n+2}$ .

Take out  $B_{n+1} + C_{n+1}$  twice to give  $A_{n+2} + B_{n+2}$ , leaving  $2A_{n+1} + A_n + B_n + C_n$ . The last three terms add up to  $C_{n+1}$ , and  $2A_{n+1} = A_{n+1} + B_{n+1}$  so this is  $A_{n+1} + B_{n+1} + C_{n+1}$  which is  $C_{n+2}$ . Together with the  $A_{n+2} + B_{n+2}$  this adds up to  $v(n+2)$  as desired.

Part 3 is 'A'-level maths that you remember from your crèche.

**1995:5:4X (maths 1a)**

Well, adapted from it!

```
fun f n = if n = 0 then 0 else g(f(n-1) + 1, 1) - 1
and g(n,m) = f(f(n-1)) + m + 1;
```

What are the ML types of these two functions?

What are the running times of **f** and **g**?

By inspection we notice that  $(\forall n \in \mathbb{N})(f(n) = n)$ , but we had better prove it! It's true for  $n = 0$ . For the induction step the recursive declaration tells us that

$$f(n+1) = g(f(n) + 1, 1) - 1 \text{ (by substituting } n+1 \text{ for } n)$$

But  $f(n) = n$  by induction hypothesis so this becomes

$$f(n+1) = g(n+1, 1) - 1$$

Now, substituting  $(n+1)$  for  $n$  and 1 for  $m$  in the declaration for **g** we get

$$g(n+1, 1) = (n+1-1) + 1 + 1$$

which is  $n + 2$ , giving  $\mathbf{f}(n + 1) = n + 1$  as desired.

(d)

The mutual recursion gives us a pair of mutual recurrence relations:

$$\text{A: } F(n) = G(f(n - 1) + 1, 1) + F(n - 1)$$

$$\text{B: } G(n, m) = F(n - 1) + F(\mathbf{f}(n - 1)) + k$$

where  $F$  is the cost function for  $\mathbf{f}$  and  $G$  is the cost function for  $\mathbf{g}$ .

Using  $\mathbf{f}(n) = n$  we can simplify our recurrence relations as follows.

$$\text{A': } F(n) = G(n, 1) + F(n - 1)$$

$$\text{B': } G(n, m) = F(n - 1) + F(n - 1) + k \text{ whence}$$

$$\text{B'': } G(n, m) = 2 \cdot F(n - 1) + k$$

This gives

$$F(n) = F(n - 1) + F(n - 1) + F(n - 1) + k$$

so  $F(n)$  grows like  $3^n$ .

$G$  is exponential too. We have assumed that the cost of adding the second argument (' $m$ ') is constant, but altho' this simplification will cause no problems it is a simplification nevertheless. Adding two arguments takes time proportional to the logarithm of the larger of the two. Fortunately the cost functions of these algorithms are so huge that an extra log or two will make no difference to the order.

### 1996:1:7

A partial ordering is a relation that is reflexive, antisymmetrical and transitive.

'Topological sort' is CompSci jargon for refining a partial ordering, which just means adding ordered pairs to a partial ordering to get a total ordering. The two partial orders of  $\mathbb{N} \times \mathbb{N}$  that you have seen are the **pointwise product** ( $\langle x, y \rangle \leq_p \langle x', y' \rangle$  iff  $x \leq x' \wedge y \leq y'$ ) and the **lexicographic product** ( $\langle x, y \rangle \leq_{lex} \langle x', y' \rangle$  iff  $x < x' \vee (x = x' \wedge y \leq y')$ ). The second is clearly a refinement of the first. It is also clear that the lexicographic product  $\mathbb{N} \times \mathbb{N}$  is not isomorphic to  $\mathbb{N}$  in the usual ordering, since it consists of  $\omega$  copies of  $\mathbb{N}$ . ( $\omega$  is the length of  $\mathbb{N}$  in its usual ordering: the length of  $\mathbb{N} \times \mathbb{N}$  in the product ordering is therefore said to be  $\omega^2$ ).

To get a refinement of the product ordering of  $\mathbb{N} \times \mathbb{N}$  that is isomorphic to the usual ordering on  $\mathbb{N}$  we notice that for a wellordering to be isomorphic to the usual ordering on  $\mathbb{N}$  it is sufficient for each point to have only finitely many things below it (given that is also a wellordering, that is). Try  $\langle x, y \rangle \leq \langle x', y' \rangle$  iff  $(x + y) < (x' + y') \vee (x + y = x' + y' \wedge x \leq x')$ . It's a total order, each element has only finitely many things below it (so it's isomorphic to the usual order on  $\mathbb{N}$ ) and it refines the pointwise product ordering.

**1996:1:8**

The recurrence

$$R: w(n, k) = w(n - 2^k, k) + w(n, k - 1)$$

can be justified as follows. Every representation of  $n$  pfatz as a pile of coins of size no more than  $2^k$  pfatz either contains a  $2^k$  pfatz piece or it doesn't. Clearly there are  $w(n, k - 1)$  representations of  $n$  pfatz as a pile of coins of size no more than  $2^{k-1}$  pfatz so that's where the  $w(n, k - 1)$  comes from. The other figure arises from the fact that a representation of  $n$  pfatz as a pile of coins of size no more than  $2^k$  pfatz and containing a  $2^k$  pfatz piece arises from a representation of  $n - 2^k$  pfatz as a pile of coins of size no more than  $2^k$ .

Base case.  $w(n, 0) = 1$ . That should be enough.

To derive  $w(4n, 2) = (n + 1)^2$ , substitute  $4n$  for  $n$ , and 2 for  $k$  in  $R$ , getting

$$w(4n, 2) = w(4n - 2^2, 2) + w(4n, 1)$$

But this rearranges to

$$w(4n, 2) = w(4(n - 1), 2) + w(4n, 1)$$

$w(4n, 1)$  is  $2n + 1$ , since we can have between 0 and  $2n$  2-pfatz pieces in a representation of  $4n$ . This gives

$$w(4n, 2) = w(4(n - 1), 2) + 2n + 1$$

This is a bit clearer if we write this as  $f(n) = f(n - 1) + 2n + 1$ . This recurrence relation obviously gives  $f(n) = (n + 1)^2$  as desired.

We can always get an estimate of  $w(n, k)$  by applying equation  $R$  recursing on  $n$ , and this works out quite nicely if  $n$  is a multiple of  $2^k$  because then we hit 0 exactly, after  $n/(2^k)$  steps. Each time we call the recursion we add  $w(n, k - 1)$  (or rather  $w(n - y, k - 1)$  for various  $y$ ) and clearly  $w(n, k - 1)$  is the biggest of them. So  $w(n, k)$  is no more than  $n/(2^k) \cdot w(n, k - 1)$ .

Finally, using  $R$  with  $2^{k+1}$  for  $n$  again we get  $w(2^{k+1}, k) = w(2^k, k) + w(2^{k+1}, k - 1)$ . The hint reminds us that every representation of  $2^k$  pfatz using the first  $k$  coins gives rise to a representation of  $2^{k+1}$  pfatz using the first  $k + 1$  coins. Simply double the size of every coin. It's also true that every representation of  $2^k$  pfatz using the first  $k$  coins gives rise to a representation of  $2^{k+1}$  pfatz using the first  $k + 1$  coins by just adding a  $2^k$  pfatz piece. The moral is:  $w(2^{k+1}, k + 1) = 2 \cdot w(2^k, k)$ . This enables us to prove the left-hand inequality by induction on  $k$ .

To prove the right-hand inequality we note that any manifestation of  $2^k$  pfatz using smaller coins can be tho'rt of as a list of length  $k$  where the  $i$ th member of the list tells us how many  $2^i$  pfatz coins we are using. How many lists of length  $k$  each of whose entries are at most  $2^k$  are there? Answer  $(2^k)^k$ , which is  $2^{k^2}$ .



**1997:1:2**

**1997:1:7**

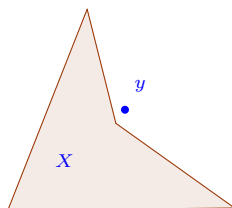
- (a) Yes: equality is a partial order, and it is tree-like because the set of strict predecessors is always empty.
- (b) Yes. The usual order is a partial (indeed *total*) order and every total order is tree-like.
- (c) No. This is a partial order but is not tree-like because (for example) 6 has two immediate strict predecessors.
- (d) This is reflexive and antisymmetrical (if  $xRy$  and  $yRx$ —so that  $x$  and  $y$  are either equal or each is the greatest prime factor of the other—then they are equal). The hard part is to show that it is transitive. Suppose  $xRy$  and  $yRz$ . If  $x = y$  or  $y = z$  we deduce  $xRz$  at once, so consider the case where  $xRy$  and  $yRz$  hold, but *not* in virtue of  $x = y$  or  $y = z$ . But this case cannot arise, because if  $yRz$  and  $y \neq z$ , then  $y$  is a prime, and the only  $x$  such that  $xRy$  is  $y$  itself. Finally, it's easy to show this relation is tree-like, because no number can have more than one greatest prime factor.

It seem to me that the number of treelike partial orderings of  $n$  elements is precisely  $n!$ . Each treelike partial ordering of  $n$  chaps gives rise to  $n$  new partial orderings because the extra chap can be stuck on top of any of the  $n$  things already there. No new partial ordering gets counted twice.

**2002:1:8**

The last part seems to have caused problems for some. Let's have a look.

We are contemplating relations that hold between elements of  $\Omega$  and subsets of  $\Omega$ . An example of the sort of thing the examiner has in mind is the relation that a point  $y$  in the plane bears to a (typically non-convex) region  $X$  when  $y$  is in the convex hull of  $X$ .



The idea is that  $y$  is one of the points you have to “add” to obtain something convex. (Check that you know what a convex set is, as i’m going to procede on the assumption that you do, and use it as a—one hopes!—illuminating illustration)

What is  $\mathcal{R}$ ?  $\mathcal{A}$  is an intersection-closed family of subsets of  $\Omega$ . (As it might be, the collection of convex subsets of the plane). We are told that it is the relation that relates  $y$  to  $X$  whenever anything in  $\mathcal{A}$  that extends  $X$  also contains  $y$ . In our illustration—where  $\mathcal{A}$  is the collection of convex subsets of the plane— $\mathcal{R}$  is the relation that hold between  $X$  and  $y$  whenever  $y$  is in the convex hull of  $X$ . (If you don’t already know the meaning of the expression “convex hull” you can probably guess it from the news that, in the picture below,  $y$  is in the convex hull of  $X$ .) Certainly in this case any set that is  $\mathcal{R}$ -closed is convex.

Assume  $C$  is  $\mathcal{R}$ -closed. That is to say

$$\forall (X, y) \in \mathcal{R}. X \subseteq C \rightarrow y \in C \quad (9.1)$$

(That’s in their notation: i’d’ve written it  $(\forall \langle X, y \rangle \in \mathcal{R})(X \subseteq C \rightarrow y \in C)$  which (i think) makes the scoping clearer.)

But  $\mathcal{R} = \{(X, y) \in \mathcal{P}(\Omega) \times \Omega : (\forall A \in \mathcal{A})(X \subseteq A \rightarrow y \in A)\}$ . Substituting this for ‘ $\mathcal{R}$ ’ in 9.1 we obtain

$$\forall (X, y) \in \{(X, y) \in \mathcal{P}(\Omega) \times \Omega : (\forall A \in \mathcal{A})(X \subseteq A \rightarrow y \in A)\}. X \subseteq C \rightarrow y \in C \quad (9.2)$$

which reduces to

$$\forall (X, y)[(\forall A \in \mathcal{A})(X \subseteq A \rightarrow y \in A) \wedge X \subseteq C. \rightarrow y \in C] \quad (9.3)$$

The examiners suggest you should consider the set  $\{A \in \mathcal{A} : C \subseteq A\}$ . I think they want you to look at  $\bigcap\{A \in \mathcal{A} : C \subseteq A\}$ .

If you’ve followed the action this far you would probably think of this anyway, since this is a set that you know must be in  $\mathcal{A}$  and it seems to stand an outside chance of being equal to  $C$ . So let’s look again at 9.3 to see if it does, in fact, tell us that  $\bigcap\{A \in \mathcal{A} : C \subseteq A\}$  is  $C$ .

And—of course—it does. First we instantiate ‘ $X$ ’ to ‘ $C$ ’ in 9.3 to obtain:

$$\forall y[(\forall A \in \mathcal{A})(C \subseteq A \rightarrow y \in A) \rightarrow y \in C] \quad (9.4)$$

Now let  $y$  be an arbitrary member of  $\bigcap\{A \in \mathcal{A} : C \subseteq A\}$ . That means that  $y$  satisfies the antecedent of 9.4. So it satisfies the consequent of 9.4 as well. So we have proved that  $\bigcap\{A \in \mathcal{A} : C \subseteq A\}$  is a subset of  $C$ . It was always a superset of  $C$ , so it is equal to  $C$ . So  $C \in \mathcal{A}$  as desired.